Spyware

202213007 조서윤

Malware Trends Report Q4, 2023

Q4, 2023 REVIEW

ANY RUN

Overall tasks 748,298:

- Malicious 170,202
- Suspicious 48,180

IOCs 210,469,912

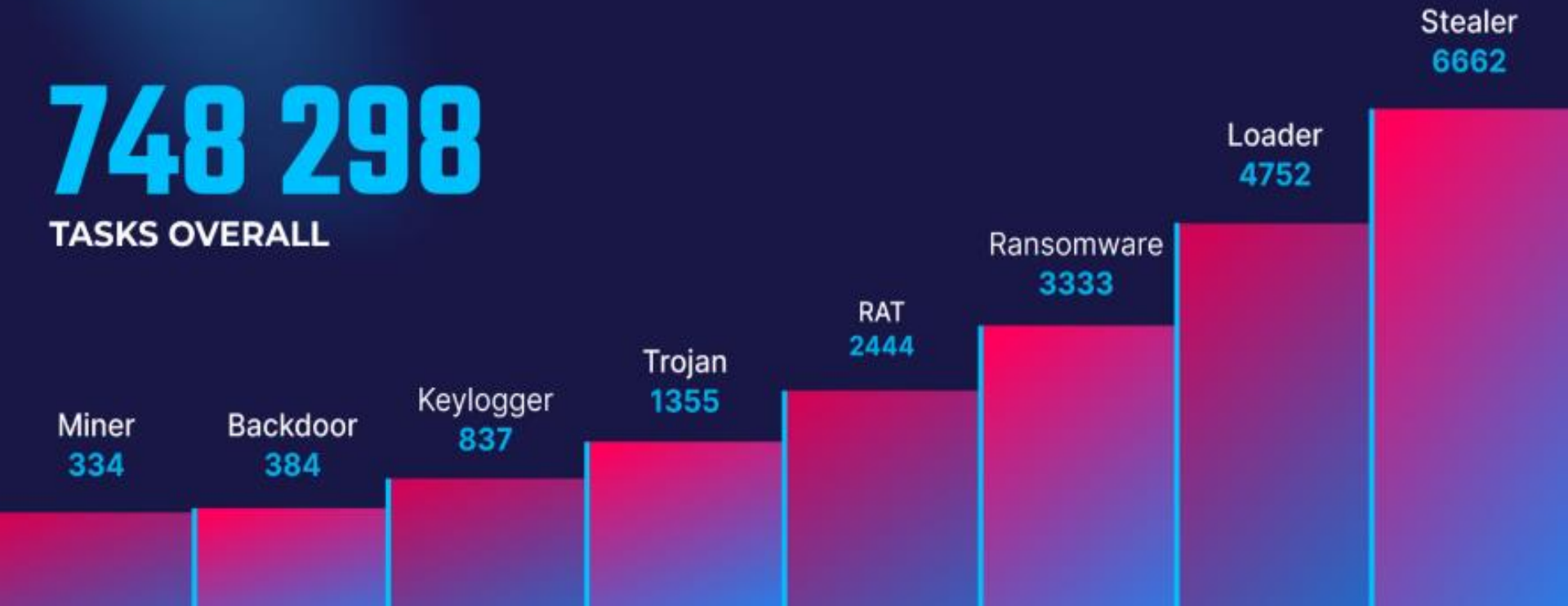
TOP MALWARE TYPES FROM Q4 2023

BY UPLOADS

ANY RUN

748 298

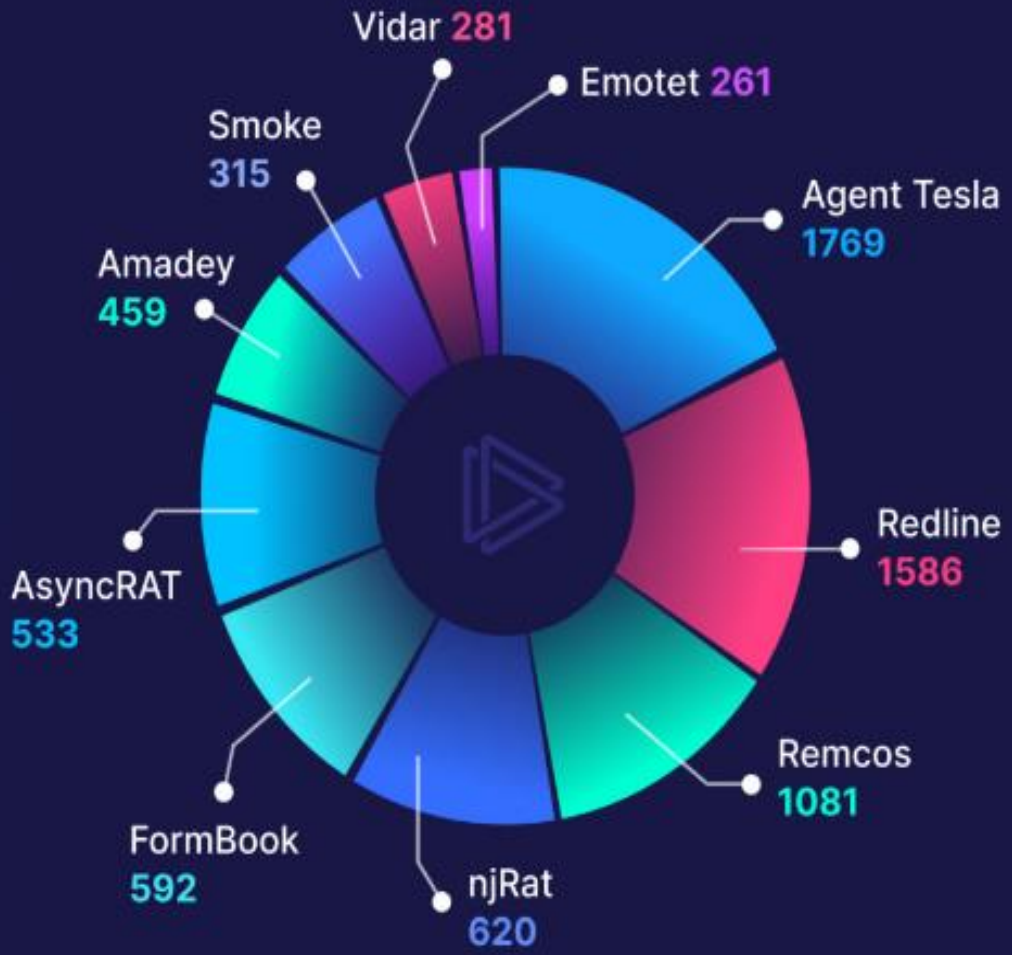
TASKS OVERALL



ANY RUN

TOP MALWARE FAMILIES FROM Q4 2023

BY UPLOADS



TASKS OVERALL

748 298

TOP MITRE ATT&CK TECHNIQUES FROM Q4 2023

ANY RUN

BY UPLOADS

TASKS OVERALL

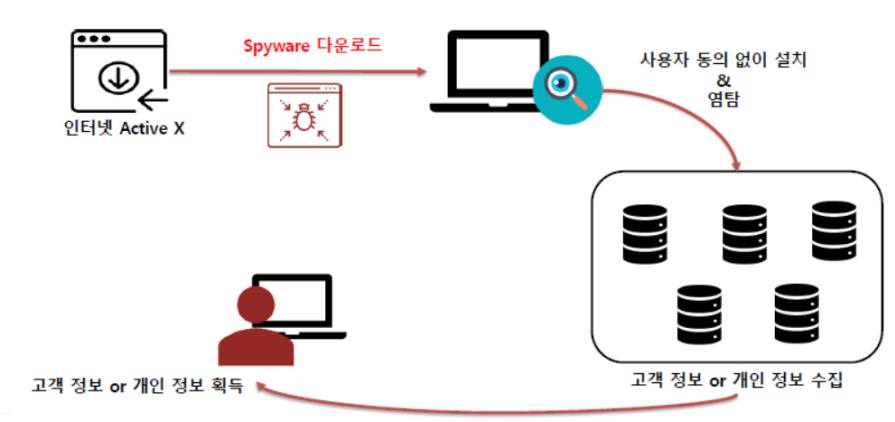
748 298

Spyware

Spyware

다른 국가 또는 기업의 비밀 정보를 파헤치는 일을 하는 행위 또는 행위자라는 뜻을 가진 ‘스파이(Spy)’와 컴퓨터 ‘소프트웨어(Software)’를 합성한 단어로, ‘악의적인 행위를 하는 컴퓨터 소프트웨어를 뜻한다.

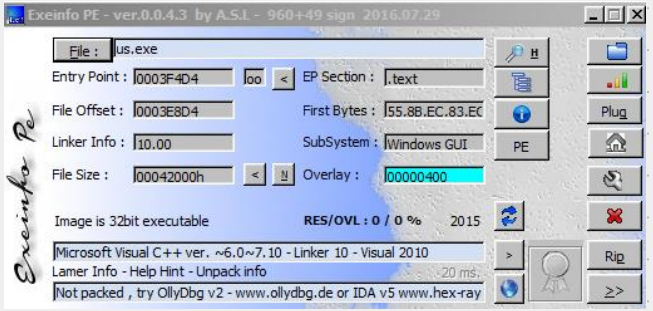
- 사용자 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어
- 금융 정보 및 신상 정보 등의 각종 정보 수집
- 애드웨어, 키로거, 랜섬웨어, 백도어



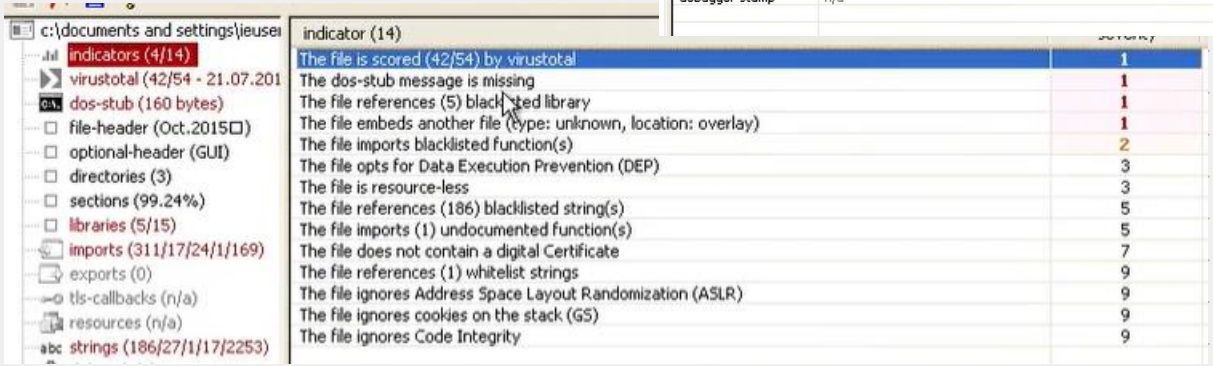
미국의 인터넷 광고전문회사인 라디에이트(Radiate)가 개인 사용자의 취향을 파악하기 위해 처음 도입하였다. 사용자의 컴퓨터에 번호를 매겨 몇 명의 사용자가 광고를 보고 있는지를 알기 위해 이 기술을 사용했다. 시간이 흐르면서 스파이웨어는 다른 사람의 컴퓨터에 몰래 숨어들어가 있다가 중요한 개인정보를 빼가는 프로그램으로 변질됐다.

사고 사례

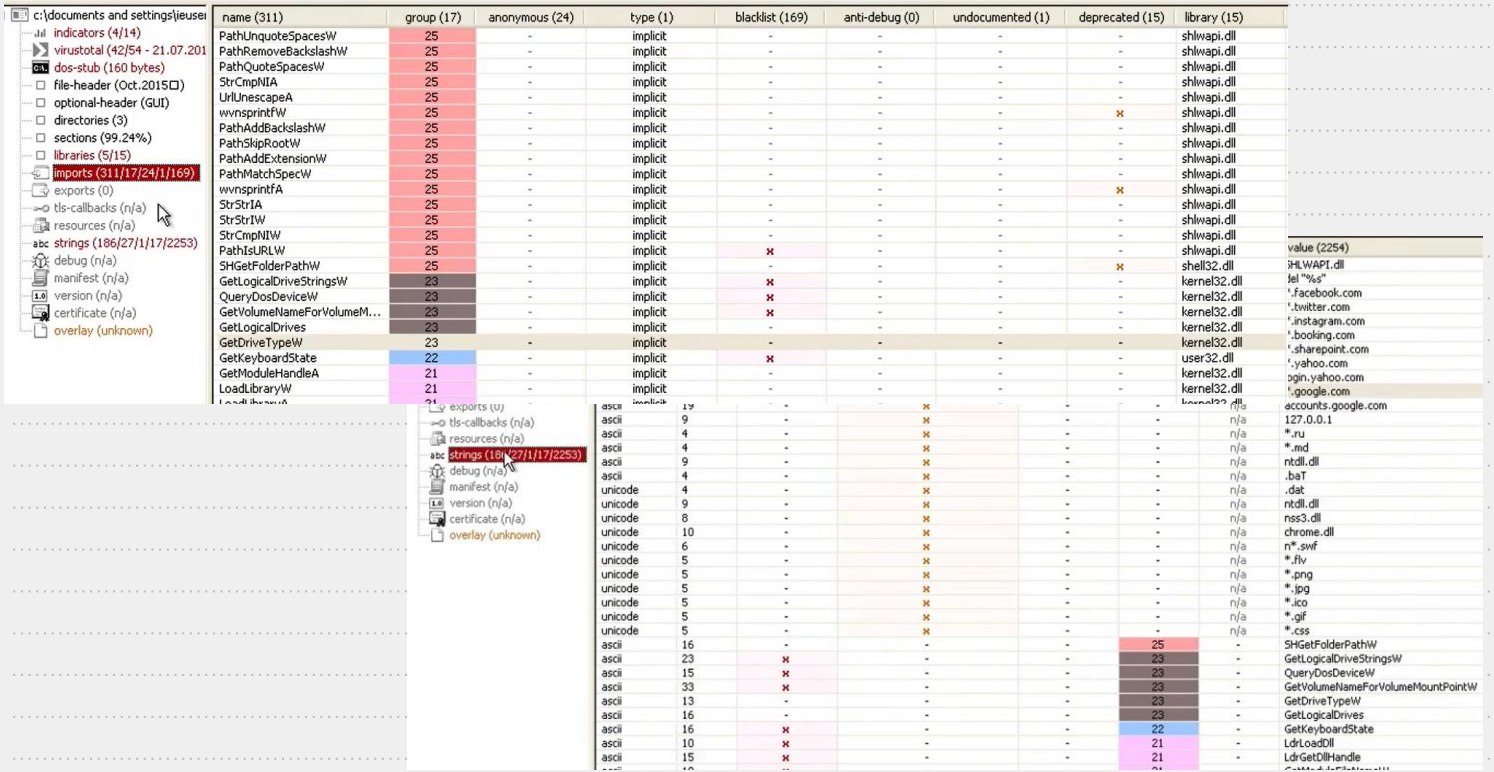
제우스 봇	2007년부터 미국, 유럽 등에서 수많은 유포 사례 및 금융 피해 사례가 발생. 금융 계좌 비밀번호 획득, 위조 여권을 통한 가짜 계좌 개설하는데 제우스 봇이 사용
코어플러드	해외 금융 사고 사례로 2011년 경 사용자의 금융 정보를 획득하여 수억 원을 챙김 사용자의 키보드 입력 내용을 암호화하여 특정 파일에 저장하고 유출
시타델	시타델은 '시타델 빌더'라 불리는 악성코드 생성기로 만들어진 악성코드로, 과거 제우스 악성코드와 작동 방식이 유사. 악성코드에 감염된 PC의 네트워크인 봇 넷을 구성하기 위한 기능을 기본으로, 사용자의 인터넷 뱅킹 정보, 웹 브라우저 내 저장 정보, SNS 개인정보 등 다양한 데이터를 탈취하는 기능을 가지고 있다. 또한 공격자용 서버인 C&C 서버를 이용해 허위 백신등을 추가적으로 내려 받아 감염된 PC 사용자에게 직접적으로 금전을 요구하기도 한다.
오징어 게임	지난해 웹하드와 사회관계망서비스(SNS) 등 일부 온라인 공간에는 가짜 '오징어 게임' 파일이 퍼짐. 'Squid_Game_2_full_HD' 등 동영상을 가장한 제목이지만, 이 파일을 설치하면 컴퓨터를 원격 제어하거나 자료 유출 기능을 가진 악성코드가 깔리게 됨.

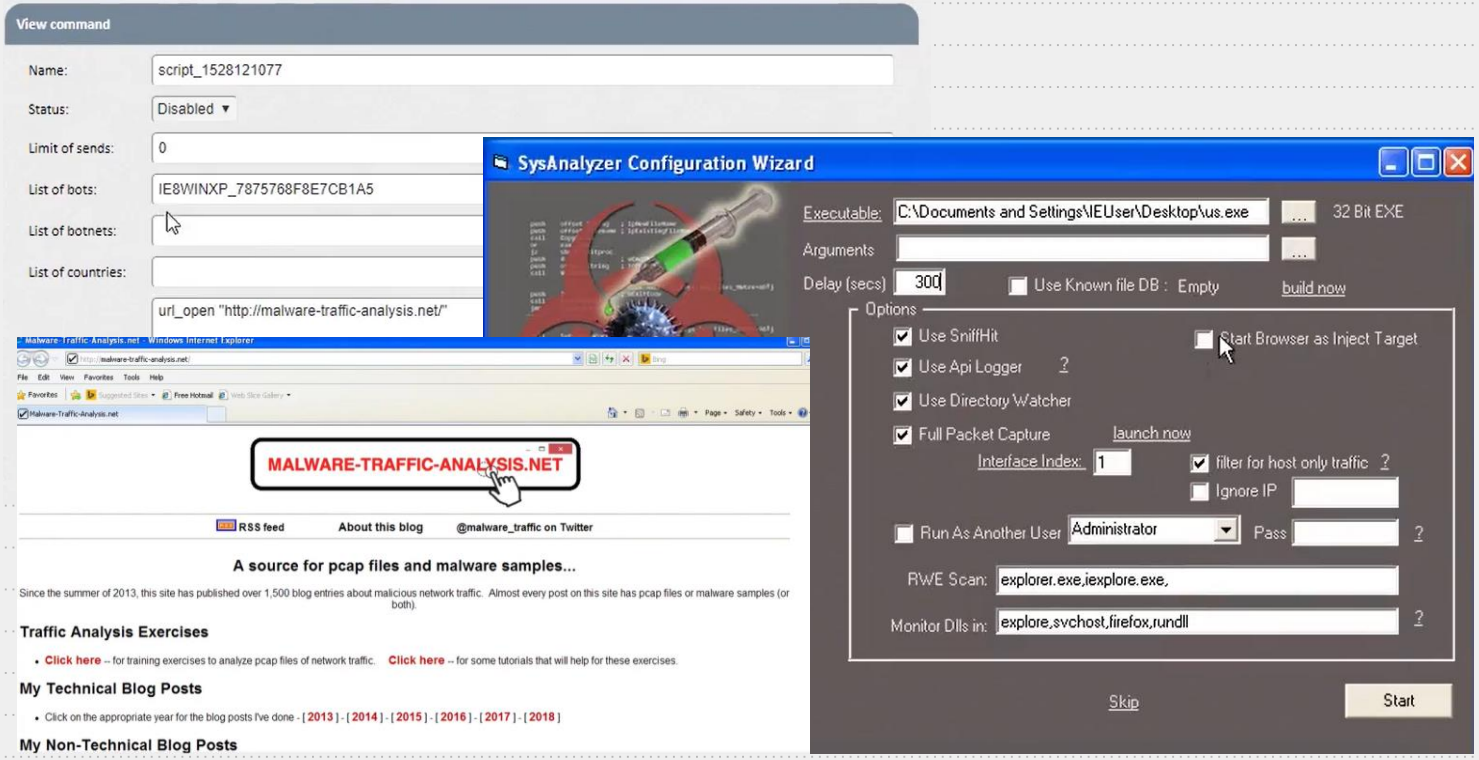


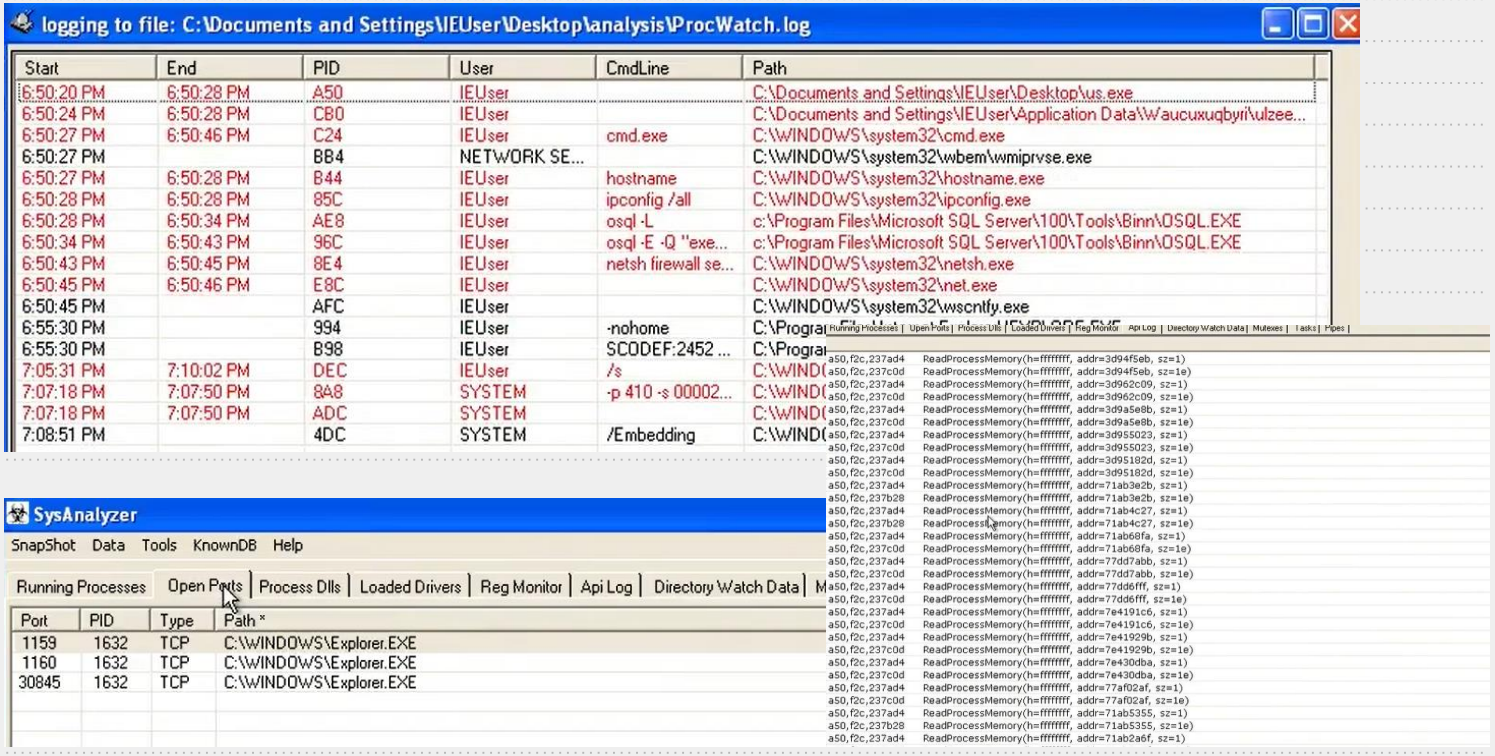
property	value
md5	CA3C0226EE105C6B5FC53867C7DDF2B8
sha1	203EC815D9885DBB7BF0C76B84D2343C2CF5F229
sha256	FCEB22442C73F14123CB831F0222DD4A3DEE168492D8A15416EDEAB5474B9575
first-bytes (hex)	4D 5A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
first-bytes (text)	M Z . . . . .
size	270336 bytes
entropy	7.140
imphash	n/a
cpu	32-bit
signature	n/a
entry-point (hex)	55 8B EC 83 EC 0C 53 56 8B 35 48 11 40 00 57 33 DB
file-version	n/a
file-description	n/a
file-type	executable
subsystem	GUI
compiler-stamp	Mon Oct 12 08:42:38 2015
debugger-stamp	n/a

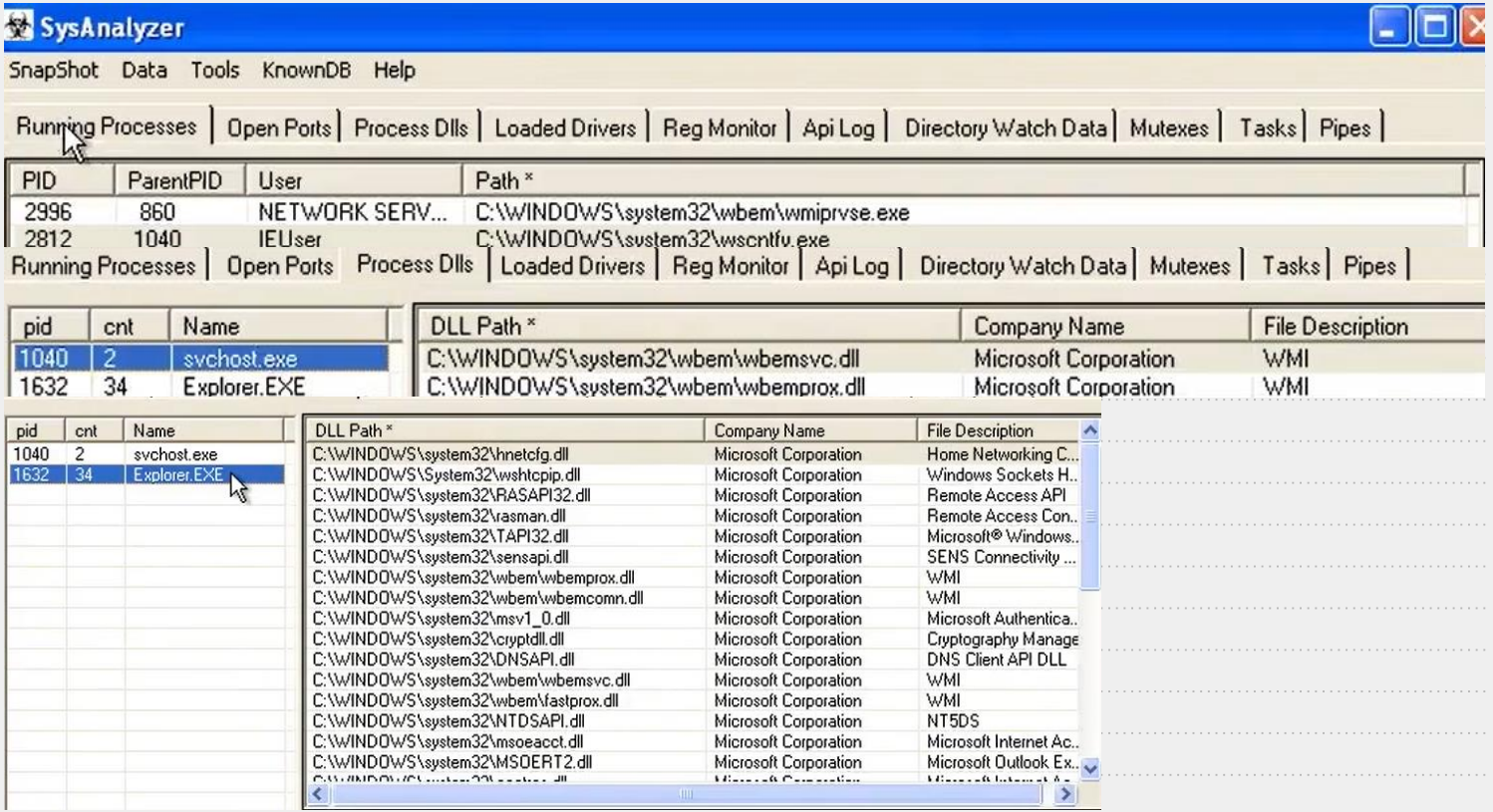


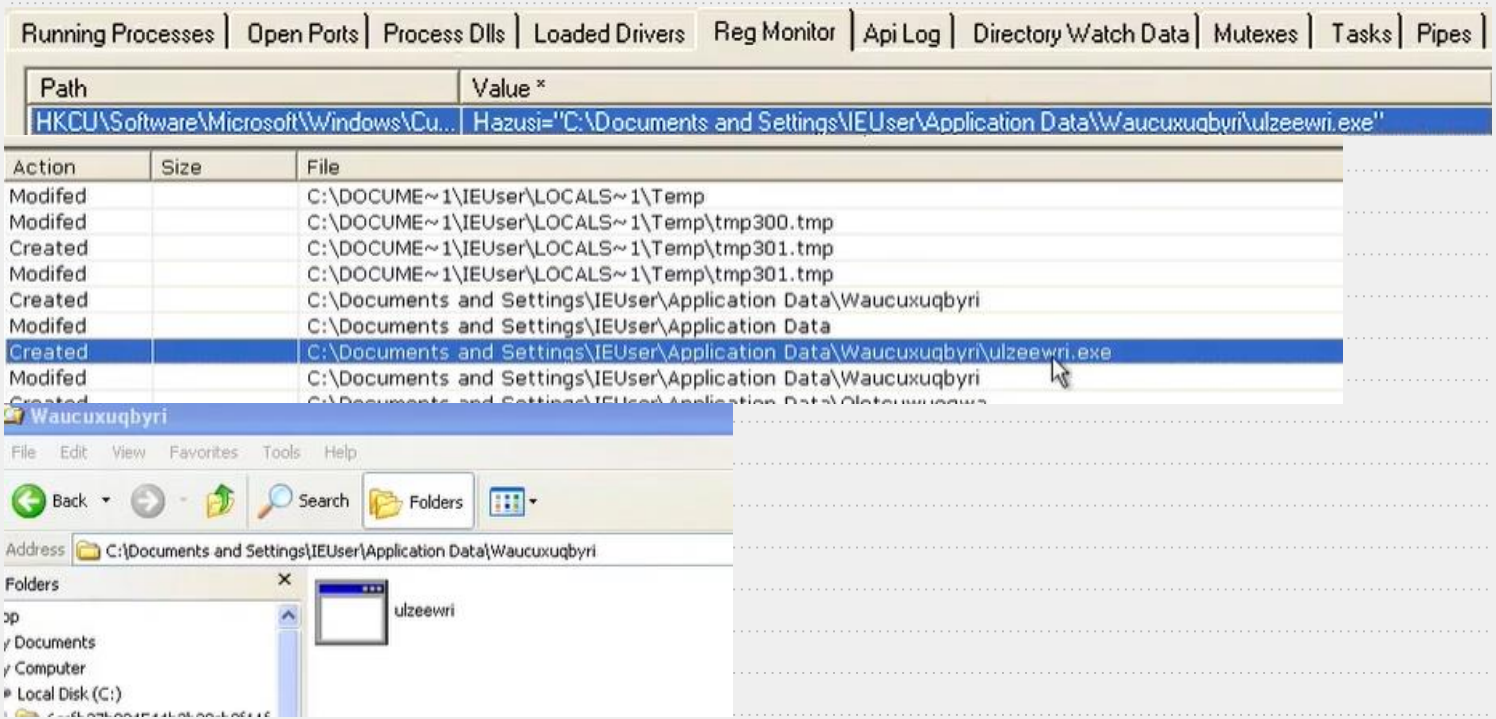

documents and settings\ieuser
indicators (4/14)
virustotal (42/54 - 21.07.2016)
dos-stub (160 bytes)
file-header (Oct.2015)
optional-header (GUI)
directories (3)
sections (99.24%)
libraries (5/15)
imports (311/17/24/1/169)
exports (0)
tls-callbacks (n/a)
resources (n/a)
strings (186/27/1/17/2253)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (unknown)
engine (54) detection (42) date (dd.mm.yyyy) age (da
Bkav W32.Clod087.Trojan.c456 20.07.2016 688
MicroWorld-eScan Gen:Variant.Kazy.710106 21.07.2016 687
CAT-QuickHeal Trojan.Generic.21003 21.07.2016 687
McAfee PWS-Zbot.gen.uo 21.07.2016 687
VIPRE Trojan.Win32.Zbot.n (v) 21.07.2016 687
SUPERAntiSpyware Trojan.Agent/Gen-MalPE 21.07.2016 687
BitDefender Gen:Variant.Kazy.710106 21.07.2016 687
K7GW Spyware (0029a43a1) 21.07.2016 687
K7AntiVirus Spyware (0029a43a1) 20.07.2016 688
Baidu Win32.Trojan.WisdomEyes.151026.9950.9999 20.07.2016 688
F-Prot W32/Zbot.BR.gen!Eldorado 21.07.2016 687
ESET-NOD32 a variant of Win32/Spy.Zbot.AAO 20.07.2016 688
TrendMicro-HouseCall TROJ_FORUCON.BMC 21.07.2016 687
Avast Sf:Crypt-BR [Trj] 21.07.2016 687
Kaspersky Trojan-Spy.Win32.Zbot.wuuc 21.07.2016 687
NANO-Antivirus Trojan.Win32.Panda.dykrlv 21.07.2016 687
Ad-Aware Gen:Variant.Kazy.710106 21.07.2016 687
Sophos Mal/Behav-010 21.07.2016 687
Comodo TrojWare.Win32.Zbot.NEWA 21.07.2016 687
F-Secure Gen:Variant.Kazy.710106 21.07.2016 687
DrWeb Trojan.PWS.Panda.2401 21.07.2016 687
Zillya Trojan.Zbot.Win32.195413 20.07.2016 688
TrendMicro TROJ_FORUCON.BMC 21.07.2016 687
McAfee-GW-Edition BehavesLike.Win32.PWSZbot.dc 21.07.2016 687
Emsisoft Gen:Variant.Kazy.710106 (B) 21.07.2016 687
c:\documents and settings\ieuser
indicators (4/14)
virustotal (42/54 - 21.07.201
dos-stub (160 bytes)
file-header (Oct.2015)
optional-header (GUI)
directories (3)
sections (99.24%)
libraries (5/15)
imports (311/17/24/1/169)
exports (0)
tls-callbacks (n/a)
resources (n/a)
strings (186/27/1/17/2253)
debug (n/a)
library (15) blacklist (5) missing (0) type (1) imports (311) file-description
secur32.dll × - implicit 1 Security Support Provider Interface
ws2_32.dll × - implicit 35 Windows Socket 2.0 32-Bit DLL
crypt32.dll × - implicit 8 Crypto API32
wininet.dll × - implicit 27 Internet Extensions for Win32
netapi32.dll × - implicit 3 Net Win32 API DLL
kernel32.dll - - implicit 129 Windows NT BASE API Client DLL
user32.dll - - implicit 21 Windows XP USER API Client DLL
advapi32.dll - - implicit 43 Advanced Windows 32 Base API
shlwapi.dll - - implicit 22 Shell Light-weight Utility Library
shell32.dll - - implicit 4 Windows Shell Common Dll
ole32.dll - - implicit 9 Microsoft OLE for Windows
gdi32.dll - - implicit 1 GDI Client DLL
oleaut32.dll - - implicit 4 Copyright © Microsoft Corp. 1993-2001.
version.dll - - implicit 3 Version Checking and File Installation Libraries
ntdll.dll - - implicit 1 NT Layer DLL

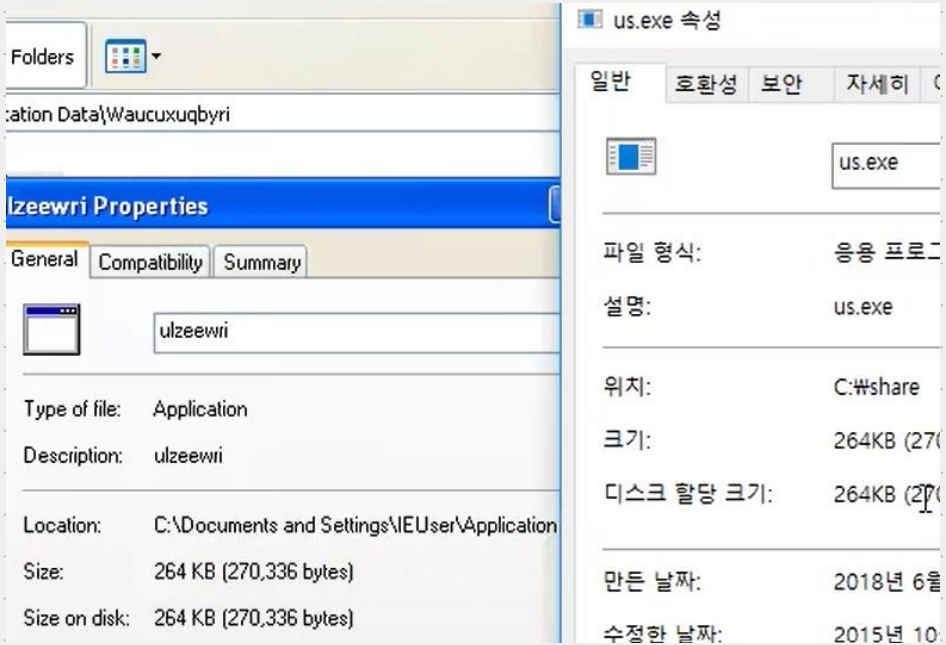

c:\documents and settings\ieuser
indicators (4/14)
virustotal (42/54 - 21.07.201
dos-stub (160 bytes)
file-header (Oct.2015)
optional-header (GUI)
directories (3)
sections (99.24%)
libraries (5/15)
imports (311/17/24/1/169)
exports (0)
tls-callbacks (n/a)
resources (n/a)
strings (186/27/1/17/2253)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (unknown)
name (311) group (17) anonymous (24) type (1) blacklist (169) anti-debug (0) undocumented (1) deprecated (15) library (15)
PathUnquoteSpacesW 25 - implicit - - - - shlwapi.dll
PathRemoveBackslashW 25 - implicit - - - - shlwapi.dll
PathQuoteSpacesW 25 - implicit - - - - shlwapi.dll
StrCmpNIA 25 - implicit - - - - shlwapi.dll
UrlUnescapeA 25 - implicit - - - - shlwapi.dll
wvnsprintfW 25 - implicit - - - x shlwapi.dll
PathAddBackslashW 25 - implicit - - - - shlwapi.dll
PathSkipRootW 25 - implicit - - - - shlwapi.dll
PathAddExtensionW 25 - implicit - - - - shlwapi.dll
PathMatchSpecW 25 - implicit - - - - shlwapi.dll
wvnsprintfA 25 - implicit - - - x shlwapi.dll
StrStrIA 25 - implicit - - - - shlwapi.dll
StrStrIW 25 - implicit - - - - shlwapi.dll
StrCmpNIW 25 - implicit - - - - shlwapi.dll
PathIsURLW 25 - implicit x - - - shlwapi.dll
SHGetFolderPathW 25 - implicit - - - x shell32.dll
GetLogicalDriveStringsW 23 - implicit x - - - kernel32.dll
QueryDosDeviceW 23 - implicit x - - - kernel32.dll
GetVolumeNameForVolumeM... 23 - implicit x - - - kernel32.dll
GetLogicalDrives 23 - implicit - - - - kernel32.dll
GetDriveTypeW 23 - implicit - - - - kernel32.dll
GetKeyboardState 22 - implicit x - - - user32.dll
GetModuleHandleA 21 - implicit - - - - kernel32.dll
LoadLibraryW 21 - implicit - - - - kernel32.dll
value (2254)
SHLWAPI.dll
del "%s"
*.facebook.com
*.twitter.com
*.instagram.com
*.booking.com
*.sharepoint.com
*.yahoo.com
login.yahoo.com
*.google.com
accounts.google.com
127.0.0.1
*.ru
*.md
ntdll.dll
.baT
.dat
ntdll.dll
nss3.dll
chrome.dll
n*.swf
*.flv
*.png
*.jpg
*.ico
*.gif
*.css
SHGetFolderPathW
GetLogicalDriveStringsW
QueryDosDeviceW
GetVolumeNameForVolumeMountPointW
GetDriveTypeW
GetLogicalDrives
GetKeyboardState
LdrLoadDll
LdrGetDllHandle


View command
Name:
script_1528121077
Status:
Disabled
Limit of sends:
0
List of bots:
IE8WINXP_7875768F8E7CB1A5
List of botnets:
List of countries:
url_open "http://malware-traffic-analysis.net/"
SysAnalyzer Configuration Wizard
Executable:
C:\Documents and Settings\IEUser\Desktop\us.exe
32 Bit EXE
Arguments
Delay (secs)
300
Use Known file DB : Empty
build now
Options
Use SniffHit
Start Browser as Inject Target
Use Api Logger
Use Directory Watcher
Full Packet Capture
launch now
Interface Index:
1
filter for host only traffic
Ignore IP
Run As Another User
Administrator
Pass
RWE Scan:
explorer.exe,iexplore.exe,
Monitor Dlls in:
explore,svchost,firefox,rundll
Skip
Start
MALWARE-TRAFFIC-ANALYSIS.NET
RSS feed
About this blog
@malware_traffic on Twitter
A source for pcap files and malware samples...
Since the summer of 2013, this site has published over 1,500 blog entries about malicious network traffic. Almost every post on this site has pcap files or malware samples (or both).
Traffic Analysis Exercises
Click here -- for training exercises to analyze pcap files of network traffic.
Click here -- for some tutorials that will help for these exercises.
My Technical Blog Posts
Click on the appropriate year for the blog posts I've done - [2013] - [2014] - [2015] - [2016] - [2017] - [2018]
My Non-Technical Blog Posts


logging to file: C:\Documents and Settings\IEUser\Desktop\analysis\ProcWatch.log
Start End PID User CmdLine Path
6:50:20 PM 6:50:28 PM A50 IEUser C:\Documents and Settings\IEUser\Desktop\us.exe
6:50:24 PM 6:50:28 PM CB0 IEUser C:\Documents and Settings\IEUser\Application Data\Waucuxuqbyri\ulzee...
6:50:27 PM 6:50:46 PM C24 IEUser cmd.exe C:\WINDOWS\system32\cmd.exe
6:50:27 PM BB4 NETWORK SE... C:\WINDOWS\system32\wbem\wmiprvse.exe
6:50:27 PM 6:50:28 PM B44 IEUser hostname C:\WINDOWS\system32\hostname.exe
6:50:28 PM 6:50:28 PM 85C IEUser ipconfig /all C:\WINDOWS\system32\ipconfig.exe
6:50:28 PM 6:50:34 PM AE8 IEUser osql -L c:\Program Files\Microsoft SQL Server\100\Tools\Binn\OSQL.EXE
6:50:34 PM 6:50:43 PM 96C IEUser osql -E -Q "exe... c:\Program Files\Microsoft SQL Server\100\Tools\Binn\OSQL.EXE
6:50:43 PM 6:50:45 PM 8E4 IEUser netsh firewall se... C:\WINDOWS\system32\netsh.exe
6:50:45 PM 6:50:46 PM E8C IEUser C:\WINDOWS\system32\net.exe
6:50:45 PM AFC IEUser C:\WINDOWS\system32\wscntfy.exe
6:55:30 PM 994 IEUser -nohome C:\Progra
6:55:30 PM B98 IEUser SCODEF:2452 ... C:\Progra
7:05:31 PM 7:10:02 PM DEC IEUser /s C:\WIND
7:07:18 PM 7:07:50 PM 8A8 SYSTEM -p 410 -s 00002... C:\WIND
7:07:18 PM 7:07:50 PM ADC SYSTEM C:\WIND
7:08:51 PM 4DC SYSTEM /Embedding C:\WIND
SysAnalyzer
SnapShot Data Tools KnownDB Help
Running Processes Open Ports Process Dlls Loaded Drivers Reg Monitor Api Log Directory Watch Data
Port PID Type Path *
1159 1632 TCP C:\WINDOWS\Explorer.EXE
1160 1632 TCP C:\WINDOWS\Explorer.EXE
30845 1632 TCP C:\WINDOWS\Explorer.EXE
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=3d94f5eb, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=3d94f5eb, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=3d962c09, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=3d962c09, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=3d9a5e8b, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=3d9a5e8b, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=3d955023, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=3d955023, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=3d95182d, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=3d95182d, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=71ab3e2b, sz=1)
a50,f2c,237b28 ReadProcessMemory(h=ffffffff, addr=71ab3e2b, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=71ab4c27, sz=1)
a50,f2c,237b28 ReadProcessMemory(h=ffffffff, addr=71ab4c27, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=71ab68fa, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=71ab68fa, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=77dd7abb, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=77dd7abb, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=77dd6fff, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=77dd6fff, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=7e4191c6, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=7e4191c6, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=7e41929b, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=7e41929b, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=7e430dba, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=7e430dba, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=77af02af, sz=1)
a50,f2c,237c0d ReadProcessMemory(h=ffffffff, addr=77af02af, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=71ab5355, sz=1)
a50,f2c,237b28 ReadProcessMemory(h=ffffffff, addr=71ab5355, sz=1e)
a50,f2c,237ad4 ReadProcessMemory(h=ffffffff, addr=71ab2a6f, sz=1)


SysAnalyzer
SnapShot Data Tools KnownDB Help
Running Processes | Open Ports | Process Dlls | Loaded Drivers | Reg Monitor | Api Log | Directory Watch Data | Mutexes | Tasks | Pipes
PID ParentPID User Path *
2996 860 NETWORK SERV... C:\WINDOWS\system32\wbem\wmiprvse.exe
2812 1040 IEUser C:\WINDOWS\system32\wscntfy.exe
Running Processes | Open Ports | Process Dlls | Loaded Drivers | Reg Monitor | Api Log | Directory Watch Data | Mutexes | Tasks | Pipes
pid cnt Name
1040 2 svchost.exe
1632 34 Explorer.EXE
DLL Path * Company Name File Description
C:\WINDOWS\system32\wbem\wbemsvc.dll Microsoft Corporation WMI
C:\WINDOWS\system32\wbem\wbemprox.dll Microsoft Corporation WMI
pid cnt Name
1040 2 svchost.exe
1632 34 Explorer.EXE
DLL Path * Company Name File Description
C:\WINDOWS\system32\hnetcfg.dll Microsoft Corporation Home Networking C...
C:\WINDOWS\System32\wshtcpip.dll Microsoft Corporation Windows Sockets H..
C:\WINDOWS\system32\RASAPI32.dll Microsoft Corporation Remote Access API
C:\WINDOWS\system32\rasman.dll Microsoft Corporation Remote Access Con..
C:\WINDOWS\system32\TAPI32.dll Microsoft Corporation Microsoft® Windows..
C:\WINDOWS\system32\sensapi.dll Microsoft Corporation SENS Connectivity ...
C:\WINDOWS\system32\wbem\wbemprox.dll Microsoft Corporation WMI
C:\WINDOWS\system32\wbem\wbemcomn.dll Microsoft Corporation WMI
C:\WINDOWS\system32\msv1_0.dll Microsoft Corporation Microsoft Authentica..
C:\WINDOWS\system32\cryptdll.dll Microsoft Corporation Cryptography Manage
C:\WINDOWS\system32\DNSAPI.dll Microsoft Corporation DNS Client API DLL
C:\WINDOWS\system32\wbem\wbemsvc.dll Microsoft Corporation WMI
C:\WINDOWS\system32\wbem\fastprox.dll Microsoft Corporation WMI
C:\WINDOWS\system32\NTDSAPI.dll Microsoft Corporation NT5DS
C:\WINDOWS\system32\msoeacct.dll Microsoft Corporation Microsoft Internet Ac..
C:\WINDOWS\system32\MSOERT2.dll Microsoft Corporation Microsoft Outlook Ex..


Running Processes
Open Ports
Process Dlls
Loaded Drivers
Reg Monitor
Api Log
Directory Watch Data
Mutexes
Tasks
Pipes
Path
Value *
HKCU\Software\Microsoft\Windows\Cu...
Hazusi="C:\Documents and Settings\IEUser\Application Data\Waucuxuqbyri\ulzeewri.exe"
Action
Size
File
Modifed C:\DOCUME~1\IEUser\LOCALS~1\Temp
Modifed C:\DOCUME~1\IEUser\LOCALS~1\Temp\tmp300.tmp
Created C:\DOCUME~1\IEUser\LOCALS~1\Temp\tmp301.tmp
Modifed C:\DOCUME~1\IEUser\LOCALS~1\Temp\tmp301.tmp
Created C:\Documents and Settings\IEUser\Application Data\Waucuxuqbyri
Modifed C:\Documents and Settings\IEUser\Application Data
Created C:\Documents and Settings\IEUser\Application Data\Waucuxuqbyri\ulzeewri.exe
Modifed C:\Documents and Settings\IEUser\Application Data\Waucuxuqbyri
Waucuxuqbyri
File Edit View Favorites Tools Help
Back
Search
Folders
Address C:\Documents and Settings\IEUser\Application Data\Waucuxuqbyri
Folders
Documents
Computer
Local Disk (C:)
ulzeewri


Folders
ation Data\Waucuxuqbyri
lzeewri Properties
General
Compatibility
Summary
ulzeewri
Type of file: Application
Description: ulzeewri
Location: C:\Documents and Settings\IEUser\Application
Size: 264 KB (270,336 bytes)
Size on disk: 264 KB (270,336 bytes)
us.exe 속성
일반
호환성
보안
자세히
us.exe
파일 형식:
설명: us.exe
위치: C:₩share
크기: 264KB
디스크 할당 크기: 264KB
만든 날짜: 2018년 6
수정한 날짜: 2015년 10