HYBRID ANALYSIS

5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1...

malicious

This report is generated from a file or URL submitted to this webservice on June 16th 2017 22:44:37 (UTC) Threat Score: 100/100
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1 AV Detection: 81%
Report generated by Falcon Sandbox © Hybrid Analysis Labeled as: Fragtor.Generic

Overview | Sample unavailable | Downloads | External Reports | Re-analyze | Post | Link | E-Mail
Looking for file context ... | Looking for similar samples ... | Report False-Positive | Request Report Deletion

Incident Response

Risk Assessment

Remote Access	Contains a remote desktop related string
Fingerprint	Reads the active computer name
Evasive	Possibly checks for the presence of a forensics/monitoring tool Possibly checks for the presence of an Antivirus engine References security related windows services
Network Behavior	Contacts 5 domains and 6 hosts. View all details

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Malicious Indicators 12

External Systems

Detected Emerging Threats Alert

HYBRID ANALYSIS

Sample was identified as malicious by at least one Antivirus engine

Installation/Persistance

Changes memory access rights in a remote process to write/execute

Network Related

Malicious artifacts seen in the context of a contacted host

Multiple malicious artifacts seen in the context of different hosts

Sends network traffic on a typical mail related ports

Sends network traffic on the official file transfer ports

Pattern Matching

YARA signature match

System Security

References security related windows services

Unusual Characteristics

References suspicious system modules

Hiding 1 Malicious Indicators

Suspicious Indicators 16

Anti-Detection/Stealthyness

Possibly checks for the presence of an Antivirus engine

HYBRID ANALYSIS

PE file has unusual entropy sections

Environment Awareness

Reads the active computer name

External Systems

Found an IP/URL artifact that was identified as malicious by at least one reputation engine

General

Opened the service control manager

Requested access to a system service

Sends UDP traffic

Installation/Persistance

Creates new processes

Network Related

Detected increased number of ARP broadcast requests (network device lookup)

Found potential IP address in binary/memory

Remote Access Related

Contains a remote desktop related string

Unusual Characteristics

Entrypoint in PE header is within an uncommon section

Imports suspicious APIs

HYBRID ANALYSIS

Hiding 2 Suspicious Indicators

All indicators are available only in the private webservice or standalone version

Informative 9

Environment Awareness

- Contains ability to query the machine version

General

- Contacts domains
- Contacts server
- Contains PDB pathways
- Creates mutants
- Spawns new processes

Installation/Persistance

- Dropped files

Network Related

- Found potential URL in binary/memory

Spyware/Information Retrieval

- Found a reference to a known community page

File Details

All Details: Off

HYBRID ANALYSIS

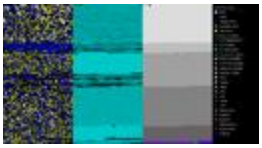
Filename	5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16
Size	928KiB (950368 bytes)
Type	pedll executable
Description	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Architecture	WINDOWS
SHA256	5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16

Resources

Language	ENGLISH
Icon	

Visualization

Input File (PortEx)



File Sections

Details

Name	.text
Entropy	6.61709581894
Virtual Address	0x1000
Virtual Size	0x3fb5b
Raw Size	0x3fc00
MD5	163c64599d79322c596724b07b8b1c3e

Name	.rdata
Entropy	6.04819112895
Virtual Address	0x41000
Virtual Size	0x1044e
Raw Size	0x10600
MD5	882510633f1de7ca620f954d9d938b2b

Name	.data
Entropy	7.31579510315
Virtual Address	0x52000
Virtual Size	0x5bd24

HYBRID ANALYSIS

Name	.zh0
Entropy	6.65262224797
Virtual Address	0xae000
Virtual Size	0x418d4
Raw Size	0x41a00
MD5	18c2f27a8641da65a8936242bbce2ac7

Name	.zh1
Entropy	7.81647523364
Virtual Address	0xf0000
Virtual Size	0x19795
Raw Size	0x19800
MD5	c7fd2160012526aa7708d5a3784cd929

Name	.reloc
Entropy	6.72713895203
Virtual Address	0x10a000
Virtual Size	0x3bb4
Raw Size	0x3c00
MD5	cebfde9dc81a4587832ef23054c66282

Name	.rsrc
Entropy	4.0970208424
Virtual Address	0x10e000
Virtual Size	0x2b7
Raw Size	0x400
MD5	174d54af2191173b9759cd8a003f9194

File Imports

ADVAPI32.dll | AVICAP32.dll | DNSAPI.dll | GDI32.dll | IPHLPAPI.DLL | KERNEL32.dll | MPR.dll | NETAPI32.dll | ole32.dll | PSAPI.DLL | SHELL32.dll | SHLWAPI.dll | USER32.dll | USERENV.dll | WININET.dll | WS2_32.dll | WTSAPI32.dll

GetServiceDisplayNameA

HYBRID ANALYSIS

Screenshots

Loading content, please wait...

Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 12 processes in total (System Resource Monitor).

- *<Ignored Process>*
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",zxFunction001" (PID: 3988)
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",DebugHelp" (PID: 3996)
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",ShellMainThread" (PID: 3928)
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",DllMain" (PID: 4068)
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",Install" (PID: 2220)
    - sc.exe sc failure Ntmssvc reset= 0 actions= restart/0 (PID: 324)
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",RemoteDiskXXXXX" (PID: 1016)
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",HideLibrary" (PID: 2508)
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",ShellMain" (PID: 3008)
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",doAction_CreateThread" (PID: 3160)
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",UnInstall" (PID: 3044)
  - rundll32.exe C:\5d2a4cde9fa7c2fdbf39b2e2ffd23378d0c50701a3095d1e91e3cf922d7b0b16.dll",zxFunction002" (PID: 3800)

HYBRID ANALYSIS

Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
<Unknown extended label>,<Unknown extended label>,<Unknown extended label>,< Unknown extended label>,<Unknown extended label>,<Unknown extended label>,h5 e355ckJkcmUtRE5EQ1JaV0VyenZlfGQtWUJbW1c3WEQtN19.enI3REcmOSc-ICEnJj43 VEdCLSYnIyE3WI9tO0VWWi0lJyMgWlU=,<Root>,<Root>,<Root>,<Root>,<Root>,<R oot>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,< Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>, <Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root >,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Ro ot>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<R oot>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,< Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>, <Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root >,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Ro ot>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<R oot>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,< Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>, <Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root >,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Root>,<Ro	-	-	-

Contacted Hosts

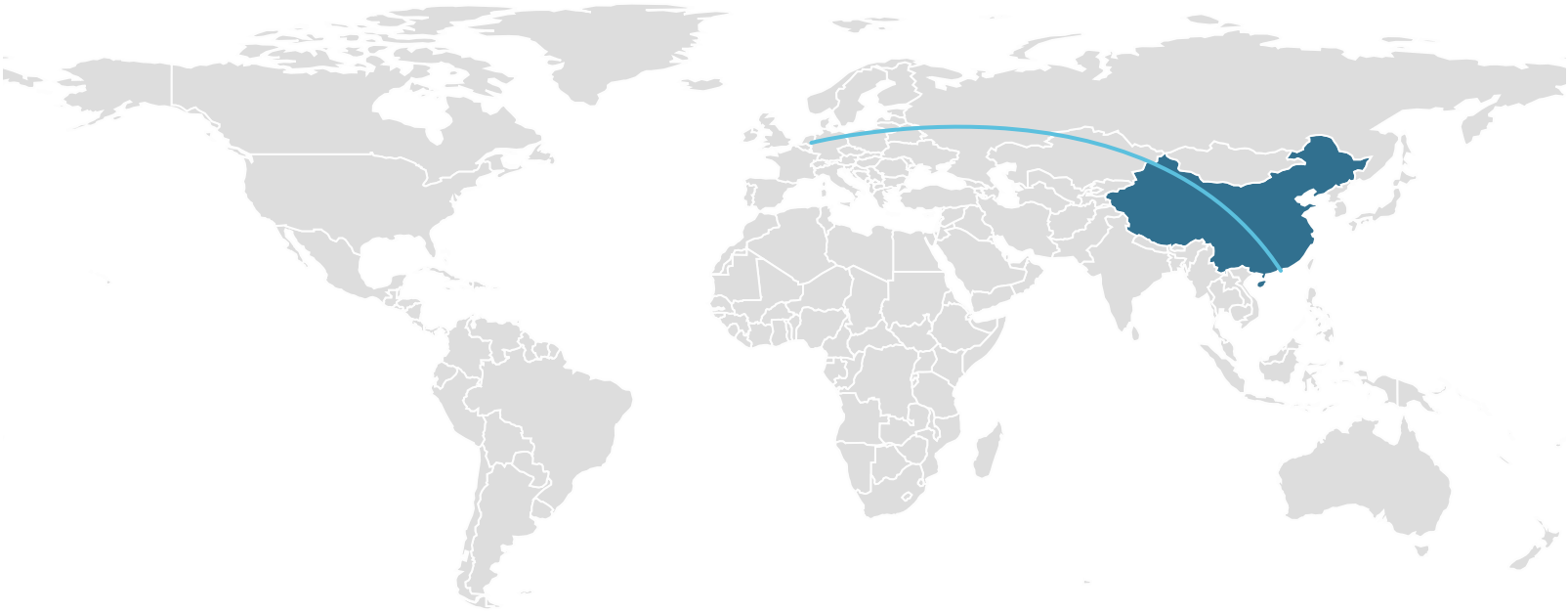
Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
103.224.81.159 OSINT	21 TCP	rundll32.exe PID: 3928 svchost.exe PID: 2096	China ASN: 24544 (Pang International Limited-AS number)
103.224.81.159 OSINT	53 UDP	rundll32.exe PID: 3928 svchost.exe PID: 2096	China ASN: 24544 (Pang International Limited-AS number)

HYBRID ANALYSIS

		svchost.exe PID: 2096	
103.224.81.159 OSINT	53 TCP	rundll32.exe PID: 3928 svchost.exe	China ASN: 24544 (Pang International Limited-AS number)

Contacted Countries



HTTP Traffic

No relevant HTTP requests were made.

Memory Forensics

String	Context	Stream UID
www.222.com	Domain/IP reference	20785-5059-3200FD1D
time.microsoft.com	Domain/IP reference	20785-7683-3201D6B3
1.1.1.1	Domain/IP reference	20785-4431-32018E89
61.8.8.13	Domain/IP reference	20785-6650-3200A2B7

HYBRID ANALYSIS

61.8.9.28	Domain/IP reference	20785-6650-3200A2B7
www.333.com	Domain/IP reference	20785-5059-3200FD1D
www.google.com	Domain/IP reference	20785-4432-32017E1E
www.555.com	Domain/IP reference	20785-5059-3200FD1D
http://www.facebook.com/comment/update.exe	Domain/IP reference	20785-4599-3200FF68

Suricata Alerts

Event	Category	Description	SID
local -> 103.224.81.159:53 (UDP)	Potential Corporate Privacy Violation	ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set	2014702
local -> 103.224.81.159:53 (UDP)	Potential Corporate Privacy Violation	ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set	2014702
local -> 103.224.81.159:53 (UDP)	Potential Corporate Privacy Violation	ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set	2014702

ET rules applied using Suricata. Find out more about proofpoint ET Intelligence here.

Extracted Strings

Search

All Details: Off

Download All Memory Strings (7.9KiB)

All Strings (2094) | Interesting (860) | 5d2a4cde9fa7c2fdbf39b2... | PCAP (5) | rundll32.exe (11)

rundll32.exe:1016 (2) | rundll32.exe:2220 (5) | rundll32.exe:3008 (26) | rundll32.exe:3928 (16)

rundll32.exe:3988 (49) | rundll32.exe:3996 (1) | sc.exe (1) | sc.exe:324 (2)

```
!"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~
```

HYBRID ANALYSIS

"%SystemRoot%\System32\svchost.exe -k netsvcs"

"==>" Parameter Description.List of commands:Help | ? -->Show helpPs ==>Processgetcmmd ==>get a cmd ==> example:getcmmd or getcmmd cmdpathSC ==>ServicesShareS

"==>" Parameter Description.List of commands:Help | ? -->Show helpPs ==>Processgetcmmd ==>get a cmd ==> example:getcmmd or getcmmd cmdpathSC ==>ServicesShareShell ==>Show a ShellSysinfo -->SystemInfoUser ==>Account Management SystemZXNC ==>NCZXFtpServer ==>FTP serverTFtp ==>TFTP clientZXHttpProxy ==>HTTP proxy serverZXHttpServer ==>HTTP serverZXSockProxy ==>Socks 4 & 5 proxyFileTime ==>Cloning of a file time informationSpecifiedPort ==>Config PortRemarks ==>RemarksZXPlug ==>PlugUserOnline ==>change the power(access a logged user of remote disks)AddHosts ==>add hostsDownFile ==>down a file from internet

Extracted Files

Informative 1

Netsetup.log

Download Disabled | Looking for file context ...

Size	13B (13 bytes)
Type	text
Description	ASCII text, with no line terminators
Runtime Process	rundll32.exe (PID: 3928)
MD5	69504a4cf4917047dd147a85801b2bcf
SHA1	3daeef524043ba72f80b454a00b541c4b6b292c4
SHA256	6503da3e1da89340551ed1da219053121c081ab42f2840dfb1752f40690f44d5

Notifications

Runtime

HYBRID ANALYSIS

Community

There are no community comments.

You must be logged in to submit a comment.