malware-ioc/evilnum at master · eset/malware-ioc

github.com/eset/malware-ioc/tree/master/evilnum

eset

Evilnum — Indicators of Compromise

An analysis of Evilnum is available as a blogpost on WeLiveSecurity.

JS component

LNK files

```
3F71525D531690A6B75CABE113B7221504108B44
212FA26C100BF56120C7F2F2D569819E3DABE556
46AA42970418010DBD5EFD571BC7056BECBCB2DC
7379FD28E0816555D081196F0CA3EB44C8E62911
27A75DE6BC73106BF192A38A45740DEE47A1D9D3
EF2B07B2C6B5B1F25C18FA7546EDC1EEDB3CC055
EDD1CA115D600E982623A3A2342810855B0DE543
F113CA2DA0F1E4ECC92000E419DAD2B259A9F839
DB50FC4EA4F6C13FDBCD28EBE2F1CC44A74A83BF
EE050A767EAA5227ED40D7A77B7746AEA0554AE5
97820A79FD43F664F553C46DCA682BCE135B2CC3
C7575DCCC6D1A228393E9AC0840A4C10BB4C1FB2
AA7585DF29E8F1D058FF267B94E8E7084DE4C7C1
F35961EB47EC4FF1B79300B8115FECD2313C6DFC
A2DBD75DD079594D36509F5EF84A22F869DF68CF
EB046DEB4BDF36461BB828967CE15D5123637CEE
228FE78F80565BC7C02DA137505196E9EDBA767C
45BB89DF5A612F53B119A6111E6AC6DE60E071D5
AF0A98F04697F836878D76DC402668C42FF1E2CA
A5F300C880842328B4D0D9C83F8314180520BD5A
29EF1FE11A063FBE218DE9BF91A4C2F871592F26
513B161299D99F4BE1DFFBB171B7C4040FF83DE7
BD8D4C93234B01A155128E3FABB61AE1CC81B5F1
F15C8F755B32A70471639B050B93FDBFB5A4D403
438B0C180A7CFF5AEDBFC9FF83668A0DEC0174A4
910382E02738661583813D212904742390C5008A
B6767E63CC8483444540D701F00705B65055C69B
A5C91E06881E19079B7E8496C6F229A790E8C1EE
3AAED43B2B8E36DA80046AF51C33A3ADFB49BD1F
854A17550FF473FB4C5AB03FD39ABFD1B3953E9C
E29011596AFE794BA673906F8F8F35AB71F397ED
C2739DDC99027AB515C75C352FB532524A082066
23DA05A5FAD175F2C035A8C4601E09E30C98B202
DBB54C9B29AEA16EFA8E3AE663428E6F2BDE4919
55D1AEA9BBB49A96A383AA5B604870DF06E7DE09
34A72738DC025353EBDC3D5C99B19DAE4D9DE2E6
A21522A20DB85C24CDC0CF46818E576F19CB0927
5A2227A37676564969F4392790FE9E3B995D7782
36345044D5E88CC8C002863E3F1F48FDEC8FF4D9
DE0FF4B04F05482ADE4CF3BA765A453818F6858E
EE59BC476BB3A7DB1190BEB791A5AA8550FC9541
4CDD87F5B9AB8C2AFCD76E4B8127B0CB6E880CF1
FBCB367EC7DD64B253482B4475CCDE6FF6B10AB0
F0DB18E0FD8C376A7EF7316C413240857F37CCAA
B4A63BD81C5388390DBDA8B92770DA88581610D1
650DEB9BAFF4B7564146222DEB555E77D5CBBE36
```

ESET detection names

```
JS/GitBot.B
JS/GitBot.J
JS/GitBot.M
JS/GitBot.Q
JS/GitBot.R
JS/GitBot.T
JS/GitBot.U
JS/GitBot.V
```

Filenames

```
%APPDATA%\Microsoft\Credentials\MediaPlayer\MediaManager\media.js
```

C&C servers

```
139.28.39[.]165
139.28.37[.]63
185.62.190[.]89
```

URLs parsed for C&C

```
https://gitlab[.]com/jhondeer123/test/raw/master/README.md
https://gitlab[.]com/bliblobla123/testingtesting/-/raw/master/README.md
https://www.digitalpoint[.]com/members/johndeer123.923670
https://www.digitalpoint[.]com/members/bliblobla.943007/
https://www.reddit[.]com/user/deltadelta2222/comments/gepb1w/hey/
```

C# component

MSI installer

```
A6ECD3A818D463155C31977000E6FDE3EB8A2352 - SecuUpdate2021.msi
```

File copier

```
D6341CD464847C9C2716030111261D5B84A43B2A - ypoc.exe
AB0C6268C61D9F36996BA7653B3A3E1EDE2AEE51 - ypoc.exe
```

Loader

```
4187F714076853B1FFA38A84835DB2623460F537 - Policy.exe
04F7FEDF8FDDF8EB5B592A57F67F72B1075C7CC1 - ServiceHud.exe
B6B9C5EFFDD14E2920183B313C56E5068C57A709 - ServiceHud.exe
```

Agent

```
B3C8C1C80824278661FBB26B17040B87180D1D34 - system.memmory.dll
C23F0551C2F7937EA4AD4B970B01CBD4D104EFFE - Policy.exe
6E7493BD1EF727FBC6EECD3AE5EC31BB8C1E897D - Policy.exe
```

Other files

```
%LOCALAPPDATA%\microsoft\windows\explorer\iconcache_2048.db (stores C&C address)
```

ESET detection names

```
MSIL/Evilnum.A
MSIL/Evilnum.B
MSIL/Evilnum.C
MSIL/Evilnum.D
```

Paths

```
%LOCALAPPDATA%\Microsoft\Mediia
%LOCALAPPDATA%\Microsoft\policy
%LOCALAPPDATA%\Microsoft\Windows\Explorer
%LOCALAPPDATA%\Microsoft\Windows\Explore
C:\Users\<user>\AppData\Localpolicy
```

Windows registry

```
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
HKCU\Control Panel\Cursors\AppStarting = “%SystemRoot%\cursors\aero_arrow.cur”
```

C&C servers

```
176.107.176[.]237
185.20.186[.]75
http://176.107.176[.]237/secupdate202222.msi
http://176.107.176[.]237/67364732647836478231.msi
http://45.9.239[.]50/secupdate2021.msi
```

HTTP requests

```
/Validate/getid?action=getSerial&computer_name=<name>&username=
<user>&version=4.0&cli=***
/Validate/getid?action=up&uid=<id>&antivirus=<av_name>
/Validate/zaqxswcde123456789?action=sendScreenshot&uid=<id>&data=<b64imgdata>
/Validate/getcommand?action=getCommand&uid=<id>
/Validate/zaqxswcde1224567891?action=error&uid=<id>&data=<errormsg>
```

URLs parsed for C&C

```
https://gitlab[.]com/amigo_159753/gold/-/raw/master/README.md
https://gitlab[.]com/galagroba/myoneandonly-haled/raw/master/README.md
https://gitlab[.]com/deadpooool/awesome-news/raw/master/README.md
```

PDB paths

```
C:\work\Marvel\vs\Marvel.LLDTenga\obj\Release\System.Memmory.pdb
C:\work\Marvel\vs\Marvel.Agent\obj\Release\Policy.pdb
C:\work\Marvel\vs\MarvelCopyForMSI\obj\Release\ypoc.pdb
C:\work\Marvel\vs\MarvelCopyForMSI\obj\Release\znn.pdb
C:\git\VS\out\binaries\x86ret\bin\i386\DPCA.pdb
```

More_eggs

Files

```
976DA2E8BDD698D974D38D01593897CA64946D92 — load.ocx
1303EB76FE1F978C6BFB6EA28329E7CDA61126AF — loadsigned.ocx
3200E9832CD61828DDF4E82155D66B63D2E6A54E — 32753.ocx
AF68B3E310BF8446E4CD10EFCF4776196131E785 — 13681.ocx
D675D3AC1C05DC7AC73674C47FA141D75F537DD3 — 13435.ocx
```

ESET detection names

```
Win32/Agent.ABRV.gen
Win32/Agent.ABOZ
Win32/Agent.ABWP
```

Paths

```
%APPDATA%\Microsoft
```

C&C servers

```
https://api.win640[.]com/json
https://api.adobe.com[.]kz/v1
https://api.adobe.com[.]kz/update/check
https://api.adobe.com[.]kz/release/init
```

Code-signing certificate SHA-1 thumbprint

```
90C22DB300F44EC79BEAB4662BB77ED1E81843BC
```

TerraPreter

Files

```
1C1D8D0AF6AA728589C5D0D0F46C01B129C75BA0 — msf_64.ocx
A7F1C2BE87B5EE4392757948FB7C895CAD95520B — msfsigned.ocx
7D9037377DC2A2E3FC1985983942D1E9F986AA42 — msfsignednofront.ocx
```

ESET detection names

```
Win64/Agent.ZQ
```

C&C Servers

```
https://cdn.lvsys[.]com/
https://d2nz6secq3489l.cloudfront[.]net/
https://faxing-mon[.]best/
```

Code-signing certificate SHA-1 thumbprint

```
90C22DB300F44EC79BEAB4662BB77ED1E81843BC
```

Other files

```
9677FCBF6F59BE2A5AB61BE5E6DF91599FB67602 – abc.bat (executes Golden Chickens
components)
476BB78BCF194523C385E2CEE364D6D097464ECA – hi.txt (remote scriptlet)
```

TerraStealer

Files

```
7C98E37CBA9B9C757E77892F02E1783A80AC450F
73C5792AA05C122903C1AEA1E1F965D223C073D8
C341D18A79057B032DC0A03F4524606205057F62
E8A95EC590E5786B780D3D6986282273895B4C8A
```

ESET detection names

```
Win32/Agent.ABNX
Win32/Agent.ABUP
```

C&C servers

```
http://json.ama-prime-client[.]com/
```

TerraTV

Files

```
E0957B2421A6EF3237A33A37DA8B52A9F29863D6 – 15159.ocx
1F287AA922911F72F68B4B0C8645B4C909EB07B9 – ACTIVEDS.dll
```

ESET detection names

```
Win32/Agent.ZZF
Win32/PSW.Agent.OJX
```

Path

```
C:\Users\Public\Public Documents\57494E2D3850535046373333503532\
```

Other tools and scripts

Files

```
401BC3740385A73EF0D3AD93DFCE03C82770072A – rev.py
27054C073C10F61452101646DA5AC9AA21DC90DB – runner.py
C4817D8C8E0B147ED5220229987FC84A43DA16A5 – PythonProxy.py
480C6F0C3998009C017051A8D6FFE199BC2A18DF – socks.py
C17CF1E8B4806A931F5FA0D73AD4BB521C43849A – log.py
47A7CD789C90735325EBD2C495A983A9C7E56E6F – l.py
2B8522ED748178037BD13FC4D3F564CE8B7BA6D6 – Win.ps1
```

ESET detection names

```
Python/Agent.JM
Python/TrojanProxy.Agent.B
Python/Spy.KeyLogger.HF
Python/RiskWare.LaZagne.D
```

Servers

```
185.61.137[.]141
185.62.189[.]210
```