Recorded Future®
Triage

Submit   Reports

Overview overview 10 | Static static | VEulqIlSMa.vbs windows7_x64 10 | VEulqIlSMa.vbs windows10-2004_x64

Download Sample

Feedback

Print to PDF

Resubmissions

22-04-2022 21:47
220422-1nnmyagdf2 10

Sharing

Copy URL

Twitter

E-mail

General

Target
VEulqIlSMa.vbs

Size
2KB

Sample
220422-1nnmyagdf2

MD5
e759c57fef989e9230cf121b31e077ec

SHA1
434f3d7d49a06606c0fb73e1a2378836f2018338

SHA256
bc84d7201f37b0c02ff742f4b8c5d78412796676724fc0af530975dac2fff063

SHA512
552b94d3950641f62bcd5be46308fb3e2ab1014b3235c2b4a74d6c4f222fbe71d6991c4cb7325aa5b57f20edbd112c6b89320362ca87ee8c3a24c7f8a605e736

Score
10/10

EMOTET
EPOCH4
BANKER
TROJAN

Malware Config

Extracted

Family	emotet
Botnet	Epoch4
C2	138.201.142.73:8080
	138.197.147.101:443
	134.195.212.50:7080
	104.168.154.79:8080
	149.56.131.28:8080
	129.232.188.93:443
	212.24.98.99:8080
	119.193.124.41:7080
	45.118.115.99:8080
	188.44.20.25:443
	103.132.242.26:8080
	201.94.166.162:443
	1.234.21.73:7080
	206.189.28.199:8080
	185.8.212.130:7080

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy.

Accept

Show all Copy all

eck1.plain

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE86M1tQ4uK/Q1Vs0KTCk+fPEQ3cuw
TyCz+gIgzky2DB5Elr60DubJW5q9Tr2dj8/gEFs0TIIEJgLTuqzx+58sdg==
-----END PUBLIC KEY-----
```

ecs1.plain

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEQF90tsTY3Aw9HwZ6N9y5+be9Xoov
pqHyD6F5DRTl9THosAoePIs/e5AdJiYxhmV8Gq3Zw1ysSPBghxjZdDxY+Q==
-----END PUBLIC KEY-----
```

Targets

Target	VEulqlISMa.vbs
Size	2KB
MD5	e759c57fef989e9230cf121b31e077ec
SHA1	434f3d7d49a06606c0fb73e1a2378836f2018338
SHA256	bc84d7201f37b0c02ff742f4b8c5d78412796676724fc0af530975dac2fff063
SHA512	552b94d3950641f62bcd5be46308fb3e2ab1014b3235c2b4a74d6c4f222fbe71d6991c4cb7325aa5b57f20edbd112c6b89320362ca87ee8c3a24c7f8a605e736

Score

10/10

EMOTET
EPOCH4
BANKER
TROJAN

Emotet
Emotet is a trojan that is primarily spread through spam emails.
EMOTET TROJAN BANKER

Blocklisted process makes network request

Downloads MZ/PE file

Deletes itself

Loads dropped DLL

Drops file in System32 directory

behavioral1 behavioral2

MITRE ATT&CK Matrix

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy.

static1					Score N/A
behavioral1	EMOTET	EPOCH4	BANKER	TROJAN	Score 10/10
behavioral2	EMOTET	EPOCH4	BANKER	TROJAN	Score 10/10

Recorded Future®

Terms | Privacy