Trojan:Win32/CrashOverride.A

Article URL
malware.php?mal_id=1904826537594dc9bfd0a814.22418869

Author
SecurityHome.eu

Published: 24 June 2017

Aliases :

There are no other names known for **Trojan:Win32/CrashOverride.A**

.

Explanation :

Payload

Connects to a remote host

We have seen this threat connect to any of the following remote hosts (C2 server/ToR nodes):

* 195.16.88.6
* 46.28.200.132
* 188.42.253.43
* 5.39.218.152
* 93.115.27.57

It connects to a remote host to:
* Send information about the hardware profile, malware version
* Execute arbitrary commands and files
* Download files
* Copy files
* Start or stop a service

Creates the following mutex

We have seen this threat create the following mutex: â€œSessions1WindowsApiPortectionâ€•

Manipulates power control system without your consent

It also uses four different types of payloads that are used to control switches and circuit breakers at an electric power control system. To achieve this goal, it implements the following protocols:
* IEC101
* IEC104
* IEC61850

Wipes data

It also has a data wiper component named haslo.dat which can:
* Delete registry keys and files (this can render the system unusable)
* Overwrite files

Analysis by: Andrei Saygo

Last update 24 June 2017