McAfee Labs

Updated BlackEnergy Trojan Grows More Powerful

By Raj Samani on Jan 14, 2016

AddThis

This post was written by Raj Samani and Christiaan Beek of Intel Security.

In late December, a cyberattack caused a power outage in the Ukraine, plunging hundreds of thousands of citizens into darkness for hours. Threat researchers soon confirmed that the BlackEnergy malware package, first developed in 2007, was the culprit. They also discovered that the malware has been significantly upgraded since its first release.

The initial BlackEnergy was a simple Trojan with distributed denial of service capabilities. Since then, there have been two upgrades.

BlackEnergy 2

In 2010, BlackEnergy 2 appeared. In that development cycle, the authors completely rewrote the code and began to incorporate a more professional approach. For example, they implemented a rudimentary installer that made it simpler to use BlackEnergy.

With the growth in BlackEnergy 2's popularity, the authors decided that they needed to add additional features and provide BlackEnergy with a more modular framework. In 2011, they added UAC bypass installers. This method allowed BlackEnergy 2 to gain elevated code execution privileges using the framework Microsoft provides to help legacy applications work with newer versions of Windows. One of BlackEnergy 2's most impressive features was released in 2013 with the support of 64-bit drivers.

BlackEnergy 3

In the second quarter of 2014, F-Secure was the first to report a new variant of BlackEnergy. This variant no longer uses many of the features of BlackEnergy 2.

Each major release has seen an almost complete rewrite of the code. BlackEnergy 3 has more advanced features than its predecessors and is more cleanly developed. The new release does not have a driver, the build ID format is a timestamp, and it has many advanced protection mechanisms. These internal protections include defenses against virtual environments, antidebugging methods, and continued checks throughout the code that will kill the program if it detects other security functions or countermeasures. What stands out about Black Energy 3 are the variety of plug-ins it incorporates:

BlackEnergy 3 plug-ins*:

- fs.dll — File system operations
- si.dll — System information, "BlackEnergy Lite"
- jn.dll — Parasitic infector
- ki.dll — Keylogger
- ps.dll — Password stealer
- ss.dll — Screenshots
- vs.dll — Network discovery, remote execution
- tv.dll — Team viewer
- rd.dll — Simple pseudo "remote desktop"
- up.dll — Update malware
- dc.dll — List Windows accounts
- bs.dll — Query system hardware, BIOS, and Windows info
- dstr.dll — Destroy system
- scan.dll — Network scan

These plug-ins are critical and powerful features in BlackEnergy 3 that make it a "go-to" tool for both crimeware and state-sponsored actors.

The Ukrainian critical infrastructure attack was initially seen as politically driven. Indeed, the use of BlackEnergy 3 could well be a cover for a targeted manual attack in an effort to disrupt availability. However, at this point in the analysis, attributing the attack to a group or actor is premature.

Based on its functionality, BlackEnergy 3 could certainly be used by state-sponsored groups as it allows these actors to hide among other crimeware groups known to use BlackEnergy variants. Tradecraft is often shared and many actors like to impersonate other actors in efforts to hide their true affiliations and sponsorships.

This is in stark contrast to Stuxnet, which first captured headlines in 2010. Examination of the Stuxnet code by threat researchers revealed that the authors needed unique domain knowledge to execute it in a specific environment and that only state-sponsored groups likely had the insight and capability to create this malicious piece of code.

At the end of this post you will find all of the MD5 hashes associated with BlackEnergy in 2015. Intel Security products provide full coverage for all hashes listed.

Several of the malicious binaries used in these attacks contain fake Microsoft digital certificates. The process of code signing is used to authenticate the software's author and guarantee that the code has not been altered or corrupted since it was signed. Faking the code signing process reduces trust in this system and is indicative of a higher level of adversary involvement. Such techniques have been used by many actors and advanced-threat groups, but it is still too early to attribute this attack to any group or actor.

We would like to thank Intel Security's Advanced Programs Group for their support in the development of this analysis.

MD5 hashes associated with BlackEnergy 3 in 2015:

Binaries allegedly associated with Ukraine attack:

```
c2fb8a309aef65e46323d6710ccdd6ca
2cae5e949f1208d13150a9d492a706c1
ed55997aada076dc61e20e1d1218925a
60d3185aff17084297a2c4c2efdabdc9
7361b64ddca90a1a1de43185bd509b64
97d6d1b36171bc3eafdd0dc07e7a4d2d
72bd40cd60769baffd412b84acc03372
97b41d4b8d05a1e165ac4cc2a8ac6f39
979413f9916e8462e960a4eb794824fc
956246139f93a83f134a39cd55512f6d
d98f4fc6d8bb506b27d37b89f7ce89d0
```

66676deaa9dfe98f8497392064aefbab
8a40172ed289486c64cc684c3652e031
cd1aa880f30f9b8bb6cf4d4f9e41ddf4
0af5b1e8eaf5ee4bd05227bf53050770
1d6d926f9287b4e4cb5bfc271a164f51
e60854c96fab23f2c857dd6eb745961c

Other BlackEnergy binaries:

97b7577d13cf5e3bf39cbe6d3f0a7732
18e7885eab07ebfb6d1c9303b992ca21
66b96dcef158833027fcf222004b64d8
03e9477f8da8f6f61b03a01d5a38918f
0d2022d6148f521c43b9573cd79ead54
1e439a13df4b7603f5eb7a975235065e
a0b7b80c3c1d9c1c432a740fa17c6126
dcf6906a9a0c970bcd93f451b9b7932a
973e0c922eb07aad530d8a1de19c7755
557f8d4c6f8b386c32001def807dc715
fffeaba10fd83c59c28f025c99d063f8
0037b485aa6938ba2ead234e211425bb
abeab18ebae2c3e445699d256d5f5fb1

BlackEnergy 3 IP addresses:

109.236.88.12
124.217.253.10
146.0.74.7
184.22.205.194
188.128.123.52
188.227.176.74
188.40.8.72
194.28.172.58
212.124.110.62
212.175.109.10
31.210.111.154
37.220.34.56
46.165.222.101
46.165.222.28
46.165.222.6
46.4.28.218
5.149.254.114
5.255.87.39
5.61.38.31
5.79.80.166
5.9.32.230
78.46.40.239
84.19.161.123
85.17.94.134
88.198.25.92
89.149.223.205
93.170.127.100
94.185.85.122
95.143.193.182
95.211.122.36

* 24th Virus Bulletin International Conference presentation by Robert Lipovsky and Anton Cherepanov. "Back in BlackEnergy," September 2014.

Tags: computer security, malware, network security

AddThis

No Comments

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

reCAPTCHA

Type the text

Privacy & Terms

Post Comment

Intel Security on Twitter

elSecurity Open nmunication is key to keeping your kids safe online. https://t.co/L1UGkA42Ce

9 hours ago·Reply·Retweet·Favorite

elSecurity Your obile device is a data gold mine, and a digital pickpocket's paradise. More from @garyjdavis: https://t.co/knNxGH2LAy

13 hours ago·Reply·Retweet·Favorite

Follow @IntelSecurity

Also Find Us On

© 2016 McAfee, Inc.