BlackEnergy

By Contributors to Wikimedia projects

Published: 2018-04-08 · Archived: 2026-04-05 14:52:25 UTC

From Wikipedia, the free encyclopedia

BlackEnergy Malware was first reported in 2007 as an HTTP-based toolkit that generated bots to execute distributed denial of service attacks.[1] It was created by Russian hacker Dmyrtro Oleksiuk around 2007. Oleksiuk also utilized the alias **Cr4sh**.[2] In 2010, **BlackEnergy 2** emerged with capabilities beyond DDoS. In 2014, **BlackEnergy 3** came equipped with a variety of plug-ins.[3] A Russian-based group known as Sandworm (aka Voodoo Bear) is attributed with using BlackEnergy targeted attacks. The attack is distributed via a Word document or PowerPoint attachment in an email, luring victims into clicking the seemingly legitimate file.[4]

BlackEnergy 1 (BE1)

[edit]

BlackEnergy's code facilitates different attack types to infect target machines. It is also equipped with server-side scripts which the perpetrators can develop in the command and control (C&C) server. Cybercriminals use the BlackEnergy bot builder toolkit to generate customized bot client executable files that are then distributed to targets via email spam and phishing e-mail campaigns.[5] BE1 lacks the exploit functionalities and relies on external tools to load the bot.[6] BlackEnergy can be detected using the YARA signatures provided by the United States Department of Homeland Security (DHS).

[6]

- Can target more than one IP address per hostname
- Has a runtime encrypter to evade detection by antivirus software
- Hides its processes in a system driver (syssrv.sys)

- DDoS attack commands (e.g. ICMP flood, TCP SYN flood, UDP flood, HTTP get flood, DNS flood, etc.) [1][*clarification needed*]
- Download commands to retrieve and launch new or updated executables from its server
- Control commands (e.g. stop, wait, or die)

BlackEnergy 2 (BE2)

[edit]

BlackEnergy 2 uses sophisticated rootkit/process-injection techniques, robust encryption, and a modular architecture known as a "dropper".[7] This decrypts and decompresses the rootkit driver binary and installs it on

the victim machine as a server with a randomly generated name. As an update on BlackEnergy 1, it combines older rootkit source code with new functions for unpacking and injecting modules into user processes.[7] Packed content is compressed using the LZ77 algorithm and encrypted using a modified version of the RC4 cipher. A hard-coded 128-bit key decrypts embedded content. For decrypting network traffic, the cipher uses the bot's unique identification string as the key. A second variation of the encryption/compression scheme adds an initialization vector to the modified RC4 cipher for additional protection in the dropper and rootkit unpacking stub, but is not used in the inner rootkit nor in the userspace modules. The primary modification in the RC4 implementation in BlackEnergy 2 lies in the key-scheduling algorithm.[7]

- Can execute local files
- Can download and execute remote files
- Updates itself and its plugins with command and control servers
- Can execute die or destroy commands

BlackEnergy 3 (BE3)

[edit]

The latest full version of BlackEnergy emerged in 2014. The changes simplified the malware code: this version installer drops the main dynamically linked library (DLL) component directly to the local application data folder.[8] This variant of the malware was involved in the December 2015 Ukraine power grid cyberattack.[9]

[3]

- **fs.dll** — File system operations
- **si.dll** — System information, “BlackEnergy Lite”
- **jn.dll** — Parasitic infector
- **ki.dll** — Keystroke Logging
- **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

1. ^ Jump up to: *a b* *Nazario, Jose (October 2007). "BlackEnergy DDoS Bot Analysis" (PDF). Arbor Networks. Archived from the original (PDF) on 21 February 2020. Retrieved 17 April 2019.*
2. ^ *Greenberg, Andy (2019). Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. New York: Doubleday. ISBN 978-0-385-54440-5.*
3. ^ Jump up to: *a b* *"Updated BlackEnergy Trojan Grows More Powerful - McAfee Blogs". 14 January 2016.*

4. ^ *"Details on August BlackEnergy PowerPoint Campaigns". 4 October 2014.*
5. ^ *"BlackEnergy APT Malware - RSA Link". community.rsa.com. 23 March 2016. Archived from the original on 18 April 2018. Retrieved 15 April 2018.*
6. ^ Jump up to: ***a*** ***b*** *Khan, Rafiullah; Maynard, Peter; McLaughlin, Kieran; Laverty, David M.; Sezer, Sakir (1 October 2016). Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid (PDF). Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016. doi:10.14236/ewic/ICS2016.7. Archived from the original (PDF) on 20 October 2016. Retrieved 5 November 2022.*
7. ^ Jump up to: ***a*** ***b*** ***c*** *Joe Stewart (3 March 2010). "BlackEnergy Version 2 Threat Analysis". www.secureworks.com.*
8. ^ *"ThreatSTOP Report: BlackEnergy" (PDF). threatstop.com. 7 March 2016. Archived (PDF) from the original on 28 May 2022. Retrieved 5 November 2022.*
9. ^ *Cherepanov A., Lipovsky R. (7 October 2016). "BlackEnergy – what we really know about the notorious cyber attacks" (PDF).*
