BlackEnergy (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:40:17 UTC

BlackEnergy

Actor(s): Sandworm

VTCollection

BlackEnergy, its first version shortened as BE1, started as a crimeware being sold in the Russian cyber underground as early as 2007. Initially, it was designed as a toolkit for creating botnets for conducting DDoS attacks. It supported a variety of flooding commands including protocols like ICMP, TCP SYN, UDP, HTTP and DNS. Among the high profile targets of cyber attacks utilising BE1 were a Norwegian bank and government websites in Georgia three weeks before Russo-Georgian War.

Version 2 of BlackEnergy, BE2, came in 2008 with a complete code rewrite that introduced a protective layer, a kernel-mode rootkit and a modular architecture. Plugins included mostly DDoS attacks, a spam plugin and two banking authentication plugins to steal from Russian nad Ukrainian banks. The banking plugin was paired with a module designed to destroy the filesystem. Moreover, BE2 was able to
- download and execute a remote file;
- execute a local file on the infected computer;
- update the bot and its plugins;

The Industrial Control Systems Cyber Emergency Response Team issued an alert warning that BE2 was leveraging the human-machine interfaces of industrial control systems like GE CIMPLICITY, Advantech/Broadwin WebAccess, and Siemens WinCC to gain access to critical infrastructure networks.

In 2014, the BlackEnergy toolkit, BE3, switched to a lighter footprint with no kernel-mode driver component. Its plugins included:
- operations with victim's filesystem
- spreading with a parasitic infector
- spying features like keylogging, screenshoots or a robust password stealer
- Team viewer and a simple pseudo “remote desktop”
- listing Windows accounts and scanning network
- destroying the system

Typical for distribution of BE3 was heavy use of spear-phishing emails containing Microsoft Word or Excel documents with a malicious VBA macro, Rich Text Format (RTF) documents embedding exploits or a PowerPoint presentation with zero-day exploit CVE-2014-4114.

On 23 December 2015, attackers behind the BlackEnergy malware successfully caused power outages for several hours in different regions of Ukraine. This cyber sabotage against three energy companies has been confirmed by the Ukrainian government. The power grid compromise has become known as the first-of-its-kind cyber warfare attack affecting civilians.

References

2024-04-16 · Mandiant · Alden Wahlstrom, Anton Prokopenkov, Dan Black, Dan Perez, Gabby Roncone, John Wolfram, Lexie Aytes, Nick Simonian, Ryan Hall, Tyler McLellan
APT44: Unearthing Sandworm
VPNFilter BlackEnergy CaddyWiper EternalPetya HermeticWiper Industroyer INDUSTROYER2 Olympic Destroyer PartyTicket RoarBAT Sandworm

2022-05-09 · cocomelonc · cocomelonc
Malware development: persistence - part 4. Windows services. Simple C++ example.
Anchor AppleJeus Attor BBSRAT BlackEnergy Carbanak Cobalt Strike DuQu

2022-04-20 · cocomelonc · cocomelonc
Malware development: persistence - part 1. Registry run keys. C++ example.
Agent Tesla Amadey BlackEnergy Cobian RAT COZYDUKE Emotet Empire Downloader Kimsuky

2022-04-20 · CISA · CISA
Alert (AA22-110A): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
VPNFilter BlackEnergy DanaBot DoppelDridex Emotet EternalPetya GoldMax Industroyer Sality SmokeLoader TrickBot Triton Zloader Killnet

2022-04-20 · CISA · Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), CISA, FBI, Government Communications Security Bureau, National Crime Agency (NCA), NCSC UK, NSA
AA22-110A Joint CSA: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
VPNFilter BlackEnergy DanaBot DoppelDridex Emotet EternalPetya GoldMax Industroyer Sality SmokeLoader TrickBot Triton Zloader

2022-02-24 · Tesorion · TESORION
Report OSINT: Russia/ Ukraine Conflict Cyberaspect
Mirai VPNFilter BlackEnergy EternalPetya HermeticWiper Industroyer WhisperGate

2021-09-09 · Recorded Future · Insikt Group
Dark Covenant: Connections Between the Russian State and Criminal Actors
BlackEnergy EternalPetya Gameover P2P Zeus

2021-08-05 · Symantec · Threat Hunter Team
Attacks Against Critical Infrastructure: A Global Concern

BlackEnergy DarkSide DistTrack Stuxnet

2020-12-21 · IronNet · Adam Hlavek, Kimberly Ortiz

Russian cyber attack campaigns and actors

WellMail elf.wellmess Agent.BTZ BlackEnergy EternalPetya Havex RAT Industroyer Ryuk Triton WellMess

2020-10-19 · Riskint Blog · Curtis

Revisited: Fancy Bear's New Faces...and Sandworms' too

BlackEnergy EternalPetya Industroyer Olympic Destroyer

2020-10-19 · UK Government · Dominic Raab, ForeignCommonwealth & Development Office

UK exposes series of Russian cyber attacks against Olympic and Paralympic Games

VPNFilter BlackEnergy EternalPetya Industroyer

2020-05-21 · PICUS Security · Süleyman Özarslan

T1055 Process Injection

BlackEnergy Cardinal RAT Downdelph Emotet Kazuar RokRAT SOUNDBITE

2020-01-01 · Secureworks · SecureWorks

IRON VIKING

BlackEnergy EternalPetya GreyEnergy Industroyer KillDisk TeleBot TeleDoor

2019-05-08 · Verizon Communications Inc. · Verizon Communications Inc.

2019 Data Breach Investigations Report

BlackEnergy Cobalt Strike DanaBot Gandcrab GreyEnergy Mirai Olympic Destroyer SamSam

2019-01-18 · Mark Edmondson

BLACK ENERGY – Analysis

BlackEnergy

2017-09-18 · ThreatConnect · Paul Vann

Casting a Light on BlackEnergy

BlackEnergy

2017-07-03 · ESET Research · Anton Cherepanov, Robert Lipovsky

BlackEnergy – what we really know about the notorious cyber attacks

BlackEnergy

2017-05-31 · MITRE · MITRE ATT&CK

Sandworm Team

CyclopsBlink Exaramel BlackEnergy EternalPetya Exaramel GreyEnergy KillDisk MimiKatz Olympic Destroyer Sandworm

2016-01-28 · Kaspersky Labs · GReAT

BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents

BlackEnergy

2015-02-17 · Kaspersky Labs · Kurt Baumgartner, Maria Garnaeva
BE2 extraordinary plugins, Siemens targeting, dev fails
BlackEnergy

2014-11-03 · Kaspersky Labs · Kurt Baumgartner, Maria Garnaeva
BE2 custom plugins, router abuse, and target profiles
BlackEnergy

2014-10-14 · ESET Research · Robert Lipovsky
CVE-2014-4114: Details on August BlackEnergy PowerPoint Campaigns
BlackEnergy

2010-07-15 · Kaspersky Labs · Dmitry Tarakanov
Black DDoS
BlackEnergy

2010-03-03 · FireEye · Julia Wolf
Black Energy Crypto
BlackEnergy

2010-03-03 · Secureworks · Joe Stewart
BlackEnergy Version 2 Threat Analysis
BlackEnergy

2007-10-01 · Arbor Networks · Jose Nazario
BlackEnergy DDoS Bot Analysis
BlackEnergy

Yara Rules

▶ [TLP:WHITE] win_blackenergy_auto (20251219 | Detects win.blackenergy.)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.blackenergy