Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:28:34 UTC

DescriptionBlackEnergy, 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.
