# Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland

*Thursday 25 September 12:00 - 12:30, Green room.*

**Robert Lipovsky** *ESET*
**Anton Cherepanov** *ESET*

A large number of state organizations and businesses from various industry fields in the Ukraine and Poland have been targeted in recent attacks. What would otherwise be a mundane scenario in today's world of cybercrime is spiced up by the fact that the malware-spreading campaigns have leveraged the tense current geopolitical situation in Eastern Ukraine and the use of a malware family with a rich history. The most recent campaigns are dated August 2014.

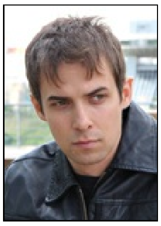
BlackEnergy is a trojan which has undergone significant functional changes since it was first publicly analysed by Arbor Networks in 2007. It has evolved from a relatively simple DDoS trojan into a relatively sophisticated piece of modern malware with a modular architecture, making it a suitable tool for sending spam and for online bank fraud, as well as for targeted attacks. BlackEnergy version 2, which featured rootkit techniques, was documented by SecureWorks in 2010. The targeted attacks recently discovered are proof that the trojan is still alive and kicking in 2014.

We provide a technical analysis of the BlackEnergy family, focusing on novel functionality and the differences introduced by new 'lite' variants. We describe the most notable aspects of the malware, including its techniques for bypassing UAC, defeating the signed driver requirement in Windows and a selection of BlackEnergy2 plug-ins used for parasitic file infections, network discovery and remote code execution and data collection.

The many targets in the Ukraine and Poland have been infected through several known and unknown infection vectors. The most effective ones appear to be spear-phishing emails with subjects related to the current Ukrainian crisis combined with the exploitation of MS Office documents. CVE-2014-1761, which made the headlines earlier this year, was also used to spread BlackEnergy.

Apart from sharing our most noteworthy findings, we aim to pose some questions that warrant further research.

*Click here for more details about the conference or register online.*



### Robert Lipovsky

Robert Lipovsky is a malware researcher in ESET's security research laboratory in Bratislava, having been working for ESET since 2007. He is responsible for malware intelligence and research, in which he focuses on rootkit techniques, Android malware and other areas. He has given presentations at several security conferences, including EICAR, CARO and Virus Bulletin. He holds a Master's degree in computer science from the Slovak University of Technology in Bratislava. When not bound to a keyboard, he enjoys travelling, sports, and playing the guitar.

@Robert_Lipovsky

### Anton Cherepanov

Anton Cherepanov graduated from the South Ural State University in 2009. Currently working at ESET as a malware researcher, his responsibilities include the analysis of complex threats. Anton has analysed such complex malware families as Rovnix, Gapz and Avatar. His interests focus on IT security, reverse engineering and malware analysis automation.

@cherepanov74

Like +1 Share Tweet

**VB2005 (Dublin)**
**VB2004 (Chicago)**
**VB2003 (Toronto)**
**VB2002 (New Orleans)**
**VB2001 (Prague)**
**VB2000 (Orlando)**
**VB99 (Vancouver)**
**VB98 (Munich)**
**VB97 (San Francisco)**
**VB96 (Brighton)**
**VB95 (Boston)**
**VB94 (Jersey)**
**VB93 (Amsterdam)**
**VB92 (Edinburgh)**
**VB91 (Jersey)**

*'VB is one of the best run conferences I attend each year.'*