BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry

BY ROBERT LIPOVSKY IN COOPERATION WITH ANTON CHEREPANOV POSTED 4 JAN 2016 - 12:49PM

CYBERCRIME TAGS

On December 23rd, 2015, around half of the homes in the Ivano-Frankivsk region in Ukraine (population around 1.4 million) were left without electricity for a few hours. According to the Ukrainian news media outlet TSN, the cause of the power outage was a “hacker attack” utilizing a “virus”.

Looking at ESET’s own telemetry, we have discovered that the reported case was not an isolated incident

and that other energy companies in Ukraine were targeted by cybercriminals at the same time.

Furthermore, we found out that the attackers have been using a malware family on which we have had our eye for quite some time now: BlackEnergy. Specifically, the BlackEnergy backdoor has been used to plant a KillDisk component onto the targeted computers that would render them unbootable.

(Un)related events?

The BlackEnergy trojan has been used for various purposes in the past few years. At the Virus Bulletin conference in 2014, we discussed a series of cyber-espionage attacks against high-value, government-related targets in Ukraine. The malware operators have used numerous spreading mechanisms to infect their victims, including the infamous PowerPoint 0-day CVE-2014-4114. While the primary objectives of the 2014 attacks appeared to be espionage, the discovery of BlackEnergy trojan-droppers capable of infecting SCADA Industrial Control Systems hinted that the gang might be up to something more dramatic.

In the recent attacks against electricity distribution companies in Ukraine, a destructive KillDisk trojan was downloaded and executed on systems previously infected with the BlackEnergy trojan.

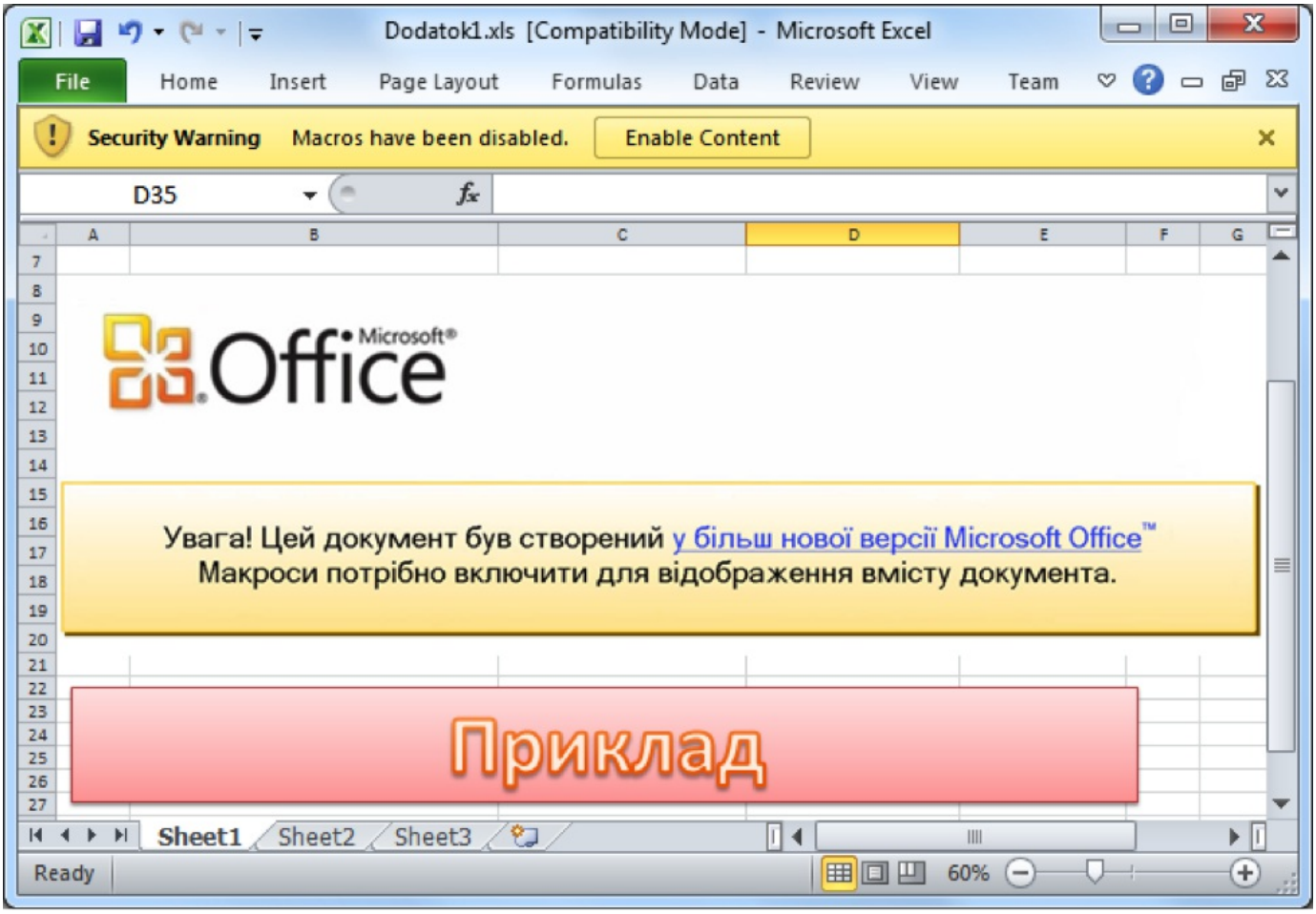
The link between BlackEnergy and KillDisk was first reported by CERT-UA in November. In that instance, a number of news media companies were attacked at the time of the 2015 Ukrainian local elections. The report claims that a large number of video materials and various documents have been destroyed as a result of the attack.

Electricity distribution companies under attack

Currently we know of several electricity distribution companies in Ukraine (other than the medialized case of Prykarpattya Oblenergo, already picked up by the media) that have been targeted by cybercriminals. We can confirm that the BlackEnergy backdoor was used against some of them and that the destructive KillDisk component was also used in more recent cases observed during the week of Christmas Eve, 2015. Additionally, BlackEnergy was also detected at electricity companies earlier in 2015; while we have no indication of KillDisk being used at that time, it is possible that the cybercriminals were then at the preparatory stage of the attack.

The infection vector used in these attacks is Microsoft Office files containing malicious macros. We have observed the BlackEnergy gang using this common technique, also employed by Dridex and other gangs, throughout 2015.

The attack scenario is simple: the target gets a spear-phishing email that contains an attachment with a malicious document. The Ukrainian security company CyS Centrum published two screenshots of emails used in BlackEnergy campaigns, where the attackers spoofed the sender address to appear to be one belonging to Rada (the Ukrainian parliament). The document itself contains text trying to convince the victim to run the macro in the document. This is an example where social engineering is used instead of exploiting software vulnerabilities. If victims are successfully tricked, they end up infected with BlackEnergy Lite.



As explained in our Virus Bulletin talk, the BlackEnergy trojan is modular and employs various downloadable components to carry out specific tasks. In the case of the most recent attack in Ukraine, the Win32/KillDisk malware was found on the infected system.

As well as being able to delete system files to make the system unbootable – functionality typical for such destructive trojans – the KillDisk variant detected in the electricity distribution companies also appears to contain some additional functionality specifically intended to sabotage industrial systems.

Firstly, it was possible to set a specific time delay after which the destructive payload was activated. Then, apart from the regular KillDisk functionality, it would try to terminate two non-standard processes: komut.exe and sec_service.exe. The second process, sec_service.exe, may belong to software called ELTIMA Serial to Ethernet Connector or to ASEM Ubiquity, a platform commonly used in Industrial Control Systems (ICS). If this process is found on the target system, the trojan will not only terminate it but will also overwrite its corresponding executable file on the hard drive with random data in order to make restoration of the system more difficult.

Conclusion

Destructive malware is not a new phenomenon. While even some of the earliest viruses used to have destructive functionality intended mostly as a prank, today's cybercriminals use such components for a number of reasons, ranging from sabotage, or hacktivism, to covering their tracks after a successful cyber-espionage attack. The Flamer (a.k.a. Flame or sKyWIper) malware is one of the most notorious examples. A data-wiping component has, reportedly, also been used in the attack against Sony Pictures. It should be clear, though, that a trojan capable of 'wiping' files or a few sectors of a hard-drive is not exactly unique and if we take into account the imprecise nature of malware naming (many such trojans have been called

'Wiper', or a similar derivative of the word), then speculations, unsubstantiated correlations and linking of unrelated incidents are bound to happen.

Even the BlackEnergy malware family has used a dstr destructive plugin in 2014. However, unlike the recent KillDisk variants used in attacks against media companies and the electricity distribution industry, it appeared as a generic 'self-destruct' component and we are not sure of its intended purpose.

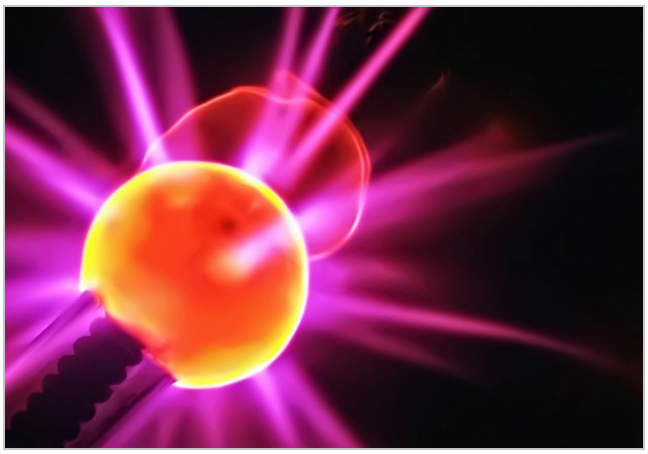
Our analysis of the destructive KillDisk malware detected in several electricity distribution companies in Ukraine indicates that it is theoretically capable of shutting down critical systems. However, there is also another possible explanation. The BlackEnergy backdoor, as well as a recently discovered SSH backdoor, themselves provide attackers with remote access to infected systems. After having successfully infiltrated a critical system with either of these trojans, an attacker would, again theoretically, be perfectly capable of shutting it down. In such case, the planted KillDisk destructive trojan would act as a means of making recovery more difficult.

We can assume with a fairly high amount of certainty that the described toolset was used to cause the power outage in the Ivano-Frankivsk region.

Although in Ukraine, Christmas is traditionally not celebrated on December 24th and 25th, a group of cybercriminals has chosen this time of year to deliver a dark 'present' to a few hundred thousand people and many more might have also been this 'lucky', had the malware not been detected.

For further information on the situation, thoughts and takeaways, read this post on the SANS Industrial Control Systems Security Blog. Additional details on the malware used in the attacks and Indicators of Compromise can be found in our technical blog post.

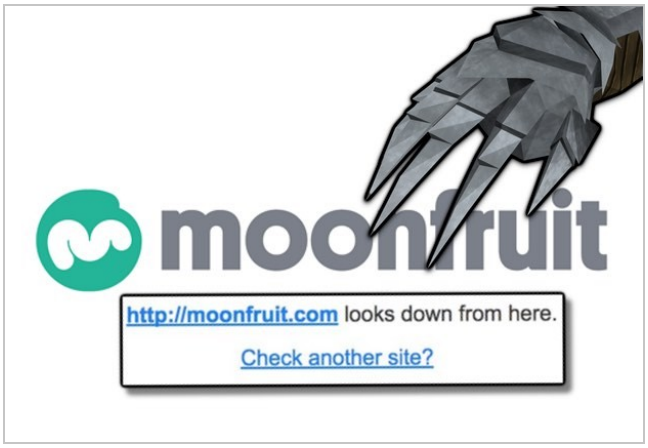
You might also be interested in:



BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry

5 things you need to know about social engineering

Europol makes 12 arrests in Remote Access Trojan crackdown



Moonfruit takes customers' sites offline, as it prepares for DDoS attack

Follow us

Sign up to our newsletter

The latest security news direct to your inbox

Email...

Submit

welivesecurity
news, views and insight from the ESET security community

VIRUS RADAR

eset ENJOY SAFER TECHNOLOGY™