BLACKENERGY – WHAT WE REALLY KNOW ABOUT THE NOTORIOUS CYBER ATTACKS

Anton Cherepanov & Robert Lipovsky
ESET, Slovakia

Email {cherepanov, lipovsky}@eset.sk

ABSTRACT

In the past two years, BlackEnergy has become one of the top malware families of interest to system administrators with the responsibility of protecting the networks of potential targets, to security researchers who have the family in their sights, and also to the media – both technical and mainstream.

BlackEnergy recently made the headlines again after we discovered that it was used in cyber attacks against electricity distribution companies, which resulted in massive power outages in Ukraine in December 2015.

But cyber attacks using the BlackEnergy malware are nothing new. We first discussed the malware and the perpetrators behind it (later nicknamed the Sandworm Team) during our talk at the *Virus Bulletin* conference in 2014, where we discussed how it transformed from a regular piece of crimeware for DDoS attacks and online banking fraud into a complex piece of malware for espionage and industrial sabotage. Now we are publishing our most comprehensive paper on the cybercrime operations based on our three years of research.

One of the main reasons why the BlackEnergy attacks have grabbed so much attention is because they were – and still are – used in the midst of a tense geopolitical situation in Ukraine. In addition to electricity distribution companies, the targets in that country have included state institutions, news media organizations, airports, and railway companies. Ukrainian officials were quick to point an accusing finger at Russia, and many others – including security companies – followed with similar allegations. The power grid compromise has become known as the first-of-its-kind confirmed cyber warfare attack affecting civilians.

In our paper we share insights about the discoveries and our following research, including previously unpublished details. We attempt to separate facts from speculations, reality from hype, and clearly state what we know and don't know – both in regard to attribution, as well as other disputed details of the attacks.

INTRODUCTION

The BlackEnergy malware has evolved significantly from its initial version first seen in 2007, which has little in common with the samples in the wild (and in the headlines) in 2016. Over the years, the malware family has been used for (petty) cybercrime, cyber espionage, and most recently, cyber sabotage.

It is important to point out these technical aspects, since there have been many reports in recent years about 'the group' behind BlackEnergy and the origin of the malware. The initial version of BlackEnergy had Russian origins, was sold on underground forums, and its source code was leaked. Version 2 of the malware (2010) was a complete code rewrite that introduced a modular architecture. Since then, it has been used for a wide range of purposes. We know little about the perpetrators behind the current BlackEnergy attacks, but as the malware family has been used in common cybercrime attacks simultaneously with targeted attacks, it is likely that there are several groups in possession of the trojan. In this paper, we will focus on the recent targeted attacks.

We discussed the evolution of the malware, technical details, as well as some of the cyber espionage attacks conducted with it against state organizations in Ukraine, in our 2014 talk at the *Virus Bulletin* conference [1] and in a blog post [2].

The attackers continued to be active in 2015, and their activity culminated in the widely publicized attacks against the Ukrainian power grid at the end of that year.

Following our initial discovery that attackers using the BlackEnergy malware were responsible for the massive power outages [3], several reports have been released that explain the chain of events leading up to the blackout [4, 5]. It was a well-planned operation that took several months of reconnaissance to prepare.

The aim of this paper is to provide additional details about the *modus operandi* of the BlackEnergy APT group and to add previously undisclosed context.

HISTORY AND FOCUS ON UKRAINE

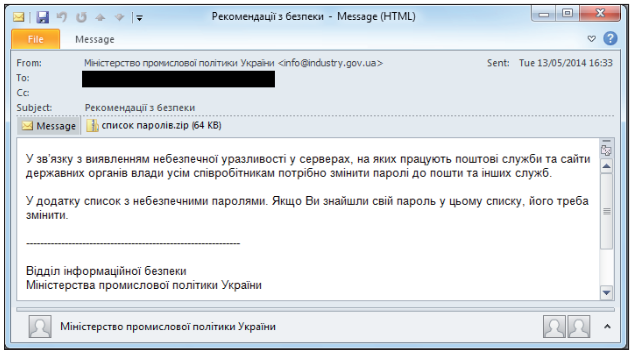
The BlackEnergy group has been focused on Ukraine ever since we first observed the trojan being used in targeted attacks. We have collected various documents containing *Microsoft Word* exploits that were used by this group.

Approximate date of use	Filename	Vulnerability
May 2012	EU chief Barroso to snub Euro 2012 in Ukraine.doc	CVE-2012-0158, Fixed in MS12-027
November 2013	Shale Gas.docx	CVE-2013-3906, Fixed in MS13-096
December 2013	Ukraine Protests.docx	CVE-2012-0158, Fixed in MS12-027

Table 1: Exploits for Microsoft Office used by the BlackEnergy group.

All of these examples use Ukraine-related topics in their filenames or in decoy-documents. Moreover, there are indications that some of these files contained exploits for security flaws that were unpatched at that time (zero-days).

In May 2014, this group used spear-phishing emails against various targets, including elements of critical infrastructure such as energy companies. In these emails attackers impersonated government entities. Figure 1 shows an example of a spear-phishing email with a forged sender address. The attackers were impersonating the Ministry of Industrial Policy of Ukraine and the text of these emails explained that recipients should change their passwords if they were contained in a list of passwords attached to the email. The attached zip archive actually contained the BlackEnergy executable.



Рекомендації з безпеки - Message (HTML)

From: Міністерство промислової політики України <info@industry.gov.ua>
Sent: Tue 13/05/2014 16:33
To: [redacted]
Cc:
Subject: Рекомендації з безпеки

Message | список паролів.zip (64 KB)

У зв'язку з виявленням небезпечної уразливості у серверах, на яких працюють поштові служби та сайти державних органів влади усім співробітникам потрібно змінити паролі до пошти та інших служб.

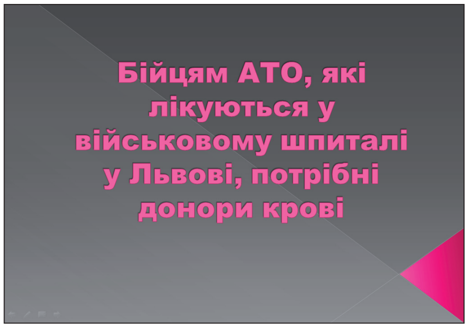
У додатку список з небезпечними паролями. Якщо Ви знайшли свій пароль у цьому списку, його треба змінити.

Відділ інформаційної безпеки
Міністерства промислової політики України

Міністерство промислової політики України

Figure 1: An email impersonating the Ministry of Industrial Policy of Ukraine.

In the beginning of August 2014 the group started to send spear-phishing emails with a *PowerPoint* presentation attached. The *PowerPoint* file was named ‘zdacha_krovi.ppsx’ (Ukrainian for ‘blood donation’). The *PowerPoint* presentation included one of the first exploits of the CVE-2014-4114 vulnerability. At that time, the vulnerability had not been patched.



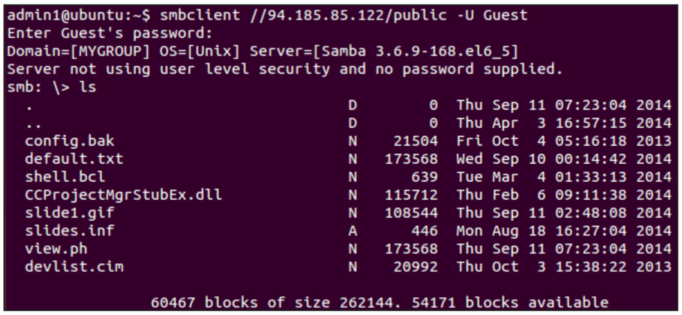
Бійцям АТО, які лікуються у військовому шпиталі у Львові, потрібні донори крові

Figure 2: Decoy text displayed by zero-day exploit sample used by the BlackEnergy group in August 2014.

Ten days later the attackers started using a new *PowerPoint* file, named ‘spiski_deputatov_done.ppsx’, in a much larger spear-phishing campaign [1]. That’s when it was spotted by *ESET* and *iSIGHT Partners* and reported to *Microsoft* by both companies.

The vulnerability, in the *Windows* Object Linking and Embedding (OLE) package, allowed attackers to perform remote code execution on the target system. The *PowerPoint* package contained two embedded OLE objects, each with a remote path where the resource was located. The final payload was located on a remote SMB share. Other files were also located on the SMB share, including files which were possibly used against users of a SCADA platform called the *CIMPLICITY HMI* solution suite [6].

In late October 2014, the Department of Homeland Security’s (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an alert warning stating that the BlackEnergy group was targeting the human-machine interfaces (HMIs) of industrial control systems [7]. The alert warned that users of *GE CIMPLICITY*, *Advantech/Broadwin WebAccess*, and *Siemens WinCC* had been targeted by this cyber threat actor.



```
admin1@ubuntu:~$ smbclient //94.185.85.122/public -U Guest
Enter Guest's password:
Domain=[MYGROUP] OS=[Unix] Server=[Samba 3.6.9-168.el6_5]
Server not using user level security and no password supplied.
smb: \> ls
  .                                   D        0  Thu Sep 11 07:23:04 2014
  ..                                  D        0  Thu Apr  3 16:57:15 2014
  config.bak                          N    21504  Fri Oct  4 05:16:18 2013
  default.txt                         N   173568  Wed Sep 10 00:14:42 2014
  shell.bcl                           N      639  Tue Mar  4 01:33:13 2014
  CCProjectMgrStubEx.dll              N   115712  Thu Feb  6 09:11:38 2014
  slide1.gif                          N   108544  Thu Sep 11 02:48:08 2014
  slides.inf                          A      446  Mon Aug 18 16:27:04 2014
  view.ph                             N   173568  Thu Sep 11 07:23:04 2014
  devlist.cim                         N    20992  Thu Oct  3 15:38:22 2013

                60467 blocks of size 262144. 54171 blocks available
```

Figure 3: Content of remote SMB share used by the BlackEnergy group.

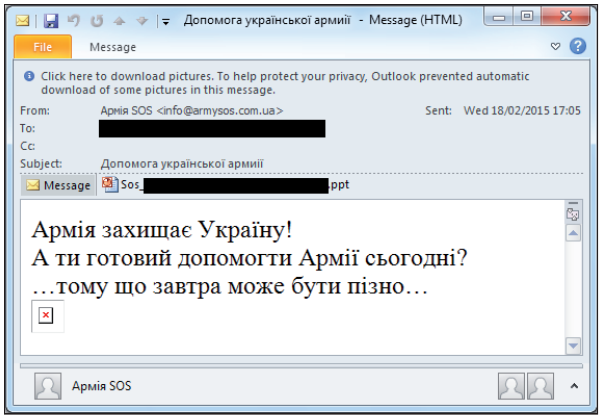
These findings demonstrated the interest of the BlackEnergy group in Ukraine and industrial control systems.

ATTACKS IN 2015

For some of the victims, attacks in 2015 started in February. At that time the attackers sent out spear-phishing messages, but surprisingly these messages didn’t contain any malicious objects. Instead, the emails contained HTML content with a link to a .PNG file located on a remote server, so that the attackers would receive a notification that the email had been delivered and opened by the target. The name of the .PNG file was unique to each recipient and represented the victim’s base64 encoded email address. (It should be noted that not all email clients load remote content by default.)

The attached *PowerPoint* presentation was not malicious, but it also contained external pictures. Once opened, *PowerPoint* displays a warning and does not load such pictures by default.

We have a conjecture that by sending these spear-phishing emails, the attackers intended to find out how many people read the emails, and how many of them actually open attachments.



Допомога української армиії - Message (HTML)

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

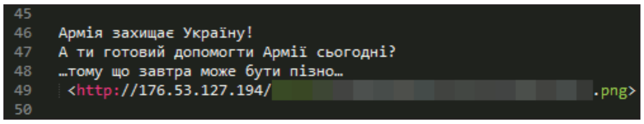
From: Армія SOS <info@armysos.com.ua>
Sent: Wed 18/02/2015 17:05
To: [redacted]
Cc:
Subject: Допомога української армиії

Message | Sos_[redacted].ppt

Армія захищає Україну!
А ти готовий допомогти Армії сьогодні?
…тому що завтра може бути пізно…

Армія SOS

Figure 4: The spear-phishing email with forged sender used by the BlackEnergy group in February 2015.



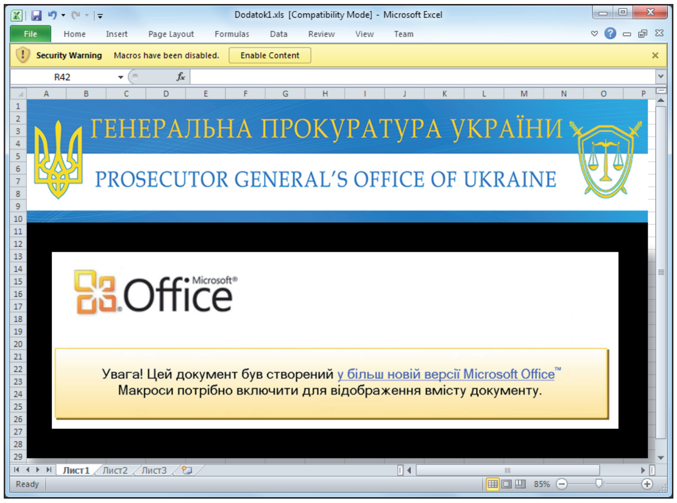
```

Армія захищає Україну!
А ти готовий допомогти Армії сьогодні?
…тому що завтра може бути пізно…
 <http://176.53.127.194/[redacted].png>

```

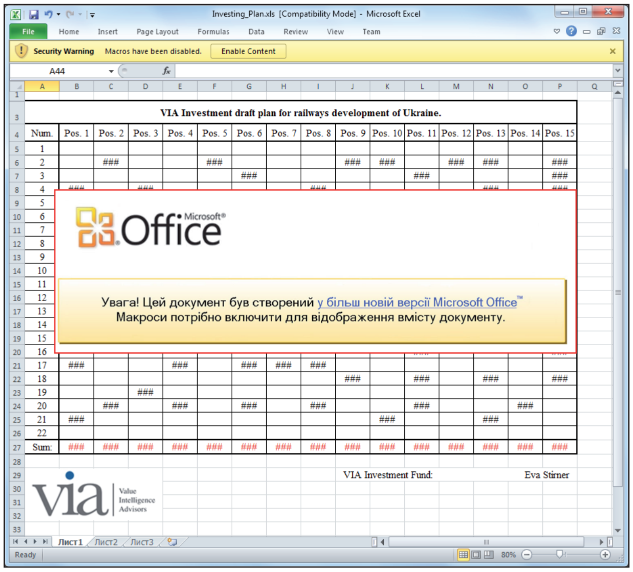
Figure 5: HTML content of email with PNG file on remote server.

During the next few months, the attackers were sending spear-phishing emails that actually contained malicious attachments – specifically *Microsoft Office* files with malicious macros, and *PowerPoint* files. Once such a *PowerPoint* file was opened, it displayed a security warning to the victim about potentially malicious content. If the user allowed this content, then *PowerPoint* made an attempt to create and execute a malicious .JAR file, which tried to launch the BlackEnergy dropper. This approach relied on the assumption that the victim had Java Runtime Installed.


Dodatok1.xls [Compatibility Mode] - Microsoft Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Team
Security Warning
Macros have been disabled.
Enable Content
R42
ГЕНЕРАЛЬНА ПРОКУРАТУРА УКРАЇНИ
PROSECUTOR GENERAL'S OFFICE OF UKRAINE
Microsoft® Office
Лист1
Лист2
Лист3
Ready
85%

Увага! Цей документ був створений у більш новій версії Microsoft Office™
Макроси потрібно включити для відображення вмісту документу.

Figure 6: The Microsoft Excel document with a malicious macro that was used against Ukrainian media companies.



VIA Investment draft plan for railways development of Ukraine.

Num.	Pos. 1	Pos. 2	Pos. 3	Pos. 4	Pos. 5	Pos. 6	Pos. 7	Pos. 8	Pos. 9	Pos. 10	Pos. 11	Pos. 12	Pos. 13	Pos. 14	Pos. 15
1															
2		###			###				###	###		###	###		###
3						###					###				###
4	###		###					###					###		###
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17	###			###		###	###	###							
18									###		###		###		###
19			###												
20		###		###		###		###			###			###	
21	###									###			###		
22															
Sum:	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###

Увага! Цей документ був створений у більш новій версії Microsoft Office™
Макроси потрібно включити для відображення вмісту документу.

VIA Investment Fund: Eva Stirner

Figure 7: The Microsoft Excel document with a malicious macro that may have been used against the Ukrainian railway company.

The *Microsoft Office* files used in the 2015 attacks had different content and layout; in some cases, attackers used a template that was customized for a particular victim. Previously unpublished examples of such malicious *Excel* files are shown in Figures 6 and 7.

BLACKENERGY ATTACKS ON THE ENERGY SECTOR

On 23 December 2015, attackers behind the BlackEnergy malware successfully caused power outages for several hours in different regions of Ukraine. This cyber attack against three energy companies has been confirmed by the Ukrainian government [8] and by the DHS [9].

While some security experts are skeptical about any involvement of the BlackEnergy malware in the power outage incident, we should say that this malware was indeed detected in Ukrainian energy companies. It is likely that attackers didn't use the BlackEnergy malware to cause the outage itself, but the malware was definitely used for the preparation of power outage attacks.

We are aware of a case in which attackers used existing tools within the environment, specifically the *Radmin* application. *Radmin* is client-server software that allows computers to be controlled remotely; it's often used by network administrators to fix various issues. The attackers gained access to an operator's computer using this tool and, 'on behalf of operator', performed operations that caused a power outage. Since this software has a verbose log file, the coherence between the time of incoming *Radmin* connections to the operator's machine and the time of outage strengthens the assumption that *Radmin* software was used.

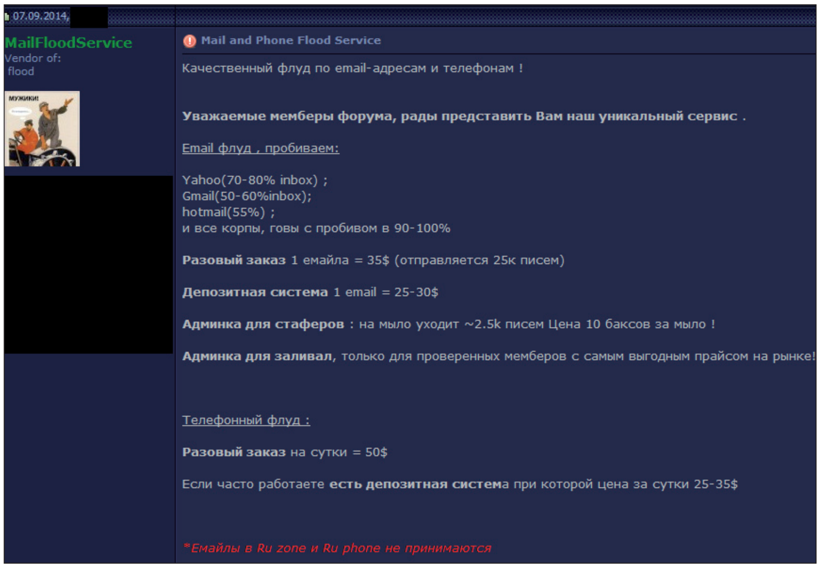
In some reports there was information about a telephone DDoS attack (also sometimes referred to as a 'telephone flood' by cybercriminals) against one energy company [10]. This tactic has been used in the past by cybercriminals to hide a cyber heist or major hack [11]. In fact, there are individuals on underground forums who are offering such services to anyone for US$50 per day, which means that the victim of such an attack would receive a huge number of incoming calls for a whole day and it would cost the attacker only US$50 (see Figure 8).

TACTICS, TOOLS AND PROCEDURES

In this section, we will examine the different tactics, tools and procedures used by the BlackEnergy group at each stage of the attack.

Entry point and initial phase

As explained before, the BlackEnergy group makes heavy use of spear-phishing emails. The attached file that leads to compromise takes a variety of forms; we have seen the use of *Microsoft Word* or *Excel* documents with a malicious VBA macro, Rich Text Format (RTF) documents embedding exploits



07.09.2014, [redacted]

MailFloodService
Vendor of:
flood

[redacted]

Mail and Phone Flood Service

Качественный флуд по email-адресам и телефонам !

Уважаемые мемберы форума, рады представить Вам наш уникальный сервис .

Email флуд , пробиваем:

Yahoo(70-80% inbox) ;
Gmail(50-60%inbox);
hotmail(55%) ;
и все корпы, говы с пробивом в 90-100%

Разовый заказ 1 емайла = 35$ (отправляется 25к писем)

Депозитная система 1 email = 25-30$

Админка для стаферов : на мыло уходит ~2.5k писем Цена 10 баксов за мыло !

Админка для заливал, только для проверенных мемберов с самым выгодным прайсом на рынке!

Телефонный флуд :

Разовый заказ на сутки = 50$

Если часто работаете **есть депозитная систем**а при которой цена за сутки 25-35$

**Емайлы в Ru zone и Ru phone не принимаются*

Figure 8: Russian-speaking individual offering telephone DDoS services on an underground forum.

for *Microsoft Word*, *PowerPoint* files, including zero-day exploits, and straightforward executable binaries.

In addition, there is a report by the Ukrainian security company *CyS Centrum* that states that the BlackEnergy group compromised a web server that was connected to the company's local network. Afterwards, attackers were able to move onto the local network via the compromised web server [12].

The BlackEnergy group may use different approaches for spear-phishing attacks. In some cases, we observed the attackers mass-mailing spear-phishing messages to a number of employees in targeted organizations. Alternatively, attackers may select just a few email addresses and target those addresses only.

Since many victims in corporate environments don't have administrator privileges, the attackers introduced the BlackEnergy3 (mini or light) version in 2013. The major difference between BlackEnergy2 and BlackEnergy3 is that the latter was designed to work without administrator privileges. Other differences between these versions are less significant. We are aware of an analysis of BlackEnergy3 malware that inaccurately claims that the malware is able to start system services or works as a network sniffer. However, BlackEnergy3 does not have these features simply because it was not designed to have them. The researchers confused BlackEnergy itself with its wrapper, which was used to disguise one of BlackEnergy's components.

While monitoring this threat, we observed another interesting detail. When the attackers are not familiar with the security measures implemented in the victim's network, or when they are attempting to attack the victim for the first time, they prefer to use HTTP rather than HTTPS, for communication with C&C servers. However, the HTTP communication is still encrypted with the RC4 algorithm. Such behaviour could be explained by the fact that some security solutions are able to notify a system administrator about suspicious HTTPS traffic in the network. If there were no such issue, then the attacker would switch to HTTPS communication later.

Reconnaissance and lateral movement

As with a number of modern, sophisticated threats, the BlackEnergy malware has a modular architecture. The core component of BlackEnergy does not provide the attackers with much functionality: it is able merely to download and execute a binary or shell command, uninstall itself, modify internal settings, or load additional modules.

The functionality of BlackEnergy can dramatically be extended with additional modules. These modules are stored in encrypted form in a separate file, which can be referred to as a plug-in-container. Thus, analysing such containers can reveal interesting details about new functionality or other changes.

During our research in 2014 we discovered and analysed 14 different BlackEnergy plug-ins [1], while in other publications on BlackEnergy activity, researchers revealed 17 plug-ins [13]. The difference could be explained by a focus on different botnets. BlackEnergy operators don't push all the possible plug-ins at once; they use only those plug-ins that they need at that time.

In 2015, we collected and analysed 20 containers from various victims, including energy companies. Five of those containers were empty. The malware has a command which allows an operator to modify or delete entries in a container.

Table 2 lists the BlackEnergy plug-ins used in attacks in 2015.

Since some of the plug-in containers were recovered from computers in energy companies in Ukraine, we expected to discover new plug-ins that potentially could be used in attacks against SCADA systems. However, nothing like that was found. Moreover, if the PE timestamps are genuine, it means that the attackers hadn't even updated plug-ins since 2013 and 2014.

Module name	PE time stamp	Purpose
ps.dll	Nov 10 05:25:51 2013	Password stealer
vs.dll	Nov 10 05:27:45 2013	Network discovery & remote execution
ss.dll	Nov 10 05:27:02 2013	Screenshots
scan.dll	Nov 10 05:28:06 2013	Network scanner
kl.dll	Aug 04 07:17:07 2014	Key logger
fs.dll	Apr 10 16:15:37 2015 Jul 17 09:02:39 2015	File system operations, gathering information about the victim's system

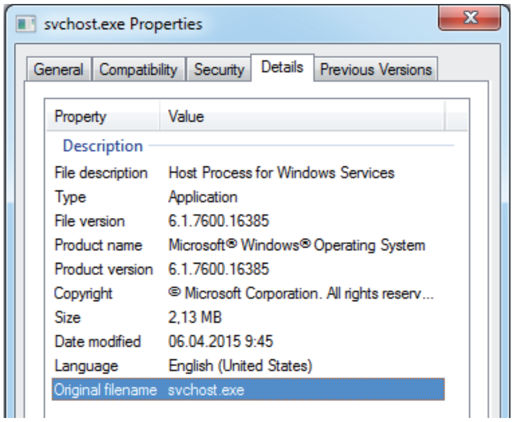
Table 2: BlackEnergy modules used in 2015.

Perhaps the existing functionality was enough for their purposes.

When attackers get into the local network, they start to gather information about the system and network perimeter. Initial reconnaissance is made by the FS plug-in. This module collects a great deal of valuable information for attackers: *Windows* version, current privileges, installed applications, running processes, proxy settings, and the output of system utilities such as systeminfo, ipconfig, netstat, route, and tracert. In addition, this module may parse and collect information from the *Windows* System Event Log. Specifically, it collects the dates and times of system starts, reboots and shutdowns. This information reveals to attackers the victim's work habits, for example whether the employee turns his computer off over the weekend, or at what time he or she comes to work and turns the computer on.

With help from the password stealer and key logger plug-ins, attackers are able to collect login credentials to various applications such as browsers, email clients and passwords stored in the *Windows* Credentials Store. Once the BlackEnergy operators have obtained valid credentials, they are able to move to the other computers in the network. This is done by use of the VS module. This module has embedded PsExec within it – a legitimate *Microsoft* tool that allows the execution of programs on remote systems.

The attackers may explore the network perimeter using their SCAN module, which allows them to map the network and scan hosts for open ports. Interestingly, it seems that this module was not efficient enough for the attackers. We have seen them making use of the *Nmap* network scanner version 6.47. The scanner tool's executable was located in the C:\Windows\Temp\Syslog\ directory and disguised as the *Microsoft* svchost.exe executable (see Figure 9).



Property	Value
Description	
File description	Host Process for Windows Services
Type	Application
File version	6.1.7600.16385
Product name	Microsoft® Windows® Operating System
Product version	6.1.7600.16385
Copyright	© Microsoft Corporation. All rights reserv...
Size	2,13 MB
Date modified	06.04.2015 9:45
Language	English (United States)
Original filename	svchost.exe

Figure 9: The binary of the Nmap scanner used by the BlackEnergy group and made to look like a normal Windows component.

The ultimate goal for any APT is to gain access to the Active Directory server and obtain domain administrator privileges. The BlackEnergy group is no exception, and to do that they used Mimikatz. This is a tool that can retrieve *Windows* account passwords and hashes from memory. We have seen that attackers were trying to download the Mimikatz tool right away from the *GitHub* site. Since Mimikatz requires local administrator or system privileges in order to perform certain actions, attackers need to obtain such privileges beforehand. We didn't observe any use of local privilege escalation (LPE) exploits by this group, but we don't exclude that possibility.

Once the attackers have gained the required credentials, they can infect key network nodes using BlackEnergy2: specifically, this group is interested in infecting *Windows* servers. BlackEnergy2 exists in the form of a kernel-mode driver, which makes it harder for network administrators to discover the compromise. Current versions of the *Windows Server* operating system don't exist for 32-bit platforms, and for 64-bit platforms *Microsoft* driver signing policy requires kernel-mode drivers to have a valid digital signature [14]. Previously, the BlackEnergy2 dropper bypassed this security measure by enabling the TESTSIGNING boot configuration option [15]. However, the infected system still needed to be rebooted in order to start the BlackEnergy driver. This unplanned reboot of the *Windows* server could raise suspicion. To solve the reboot issue, in 2015 the attackers started to use a tool called DSEFix [16]. This is an open-source tool that exploits CVE-2008-3431, a vulnerability in the legitimate VirtualBox driver, in order to disable the driver signature check. Since DSEFix disables this check only until the next reboot, the attackers made a custom version of DSEFix that also modifies boot configuration data (BCD) in order to enable TESTSIGNING mode.

Another tool that we discovered in BlackEnergy's 2015 arsenal is detected by *ESET* products as the Win32/SSHBearDoor.A trojan [17]. This is a backdoored version of a legitimate SSH server called Dropbear SSH. The attackers used this tool to regain access to the server, in the event that the BlackEnergy malware was discovered and deleted.

Sometimes the BlackEnergy group may insert their implant on computers that are used as part of critical infrastructure and wait until they need it, 'just in case'. In such cases the attackers are trying to stay under the radar: they don't exfiltrate large amounts of data to C&C servers or even attempt to perform lateral movement.

We observed that attackers may use a unique C&C server for each infected computer in the same network. This tactic has the potential to allow attackers to stay longer on the network, since even if infection is discovered on a particular computer, other infections may remain unnoticed.

Final phase

In 2015, attackers used the KillDisk component as the final phase of attacks. This destructive component deletes important files on the disk drive, empties *Windows* event logs and, to make the system unbootable, rewrites the first sectors on physical drives. The first use of this component was documented by CERT-UA against media companies [18]. In the case described by CERT-UA, it is unclear whether this component was used to cover tracks or whether it was the original intent of the attackers.

Use of other malware

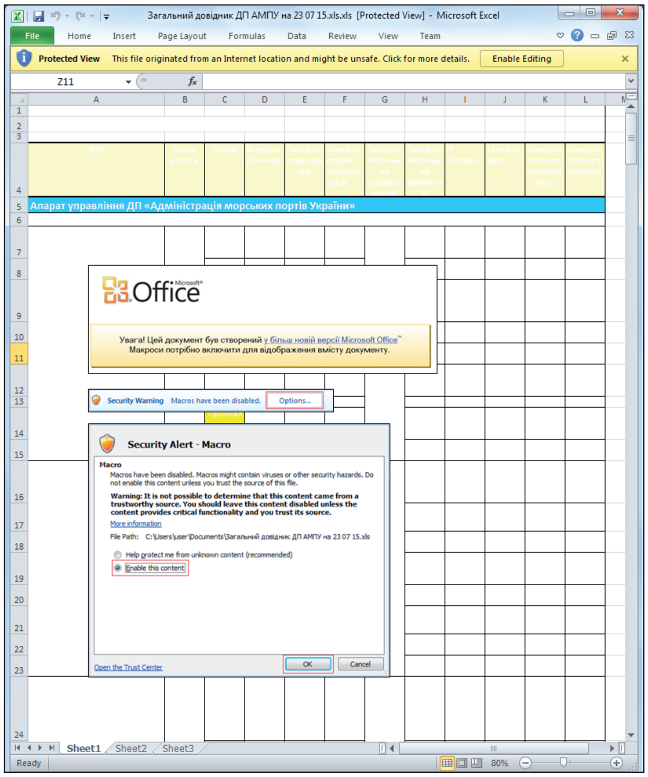
On 20 January 2016, *ESET* identified a new attempted attack on energy companies in Ukraine [19]. The attackers used exactly the same infection vector as in previous attacks: a spear-phishing email with an attached *Excel* document containing a malicious VBA macro. This time, however, instead of using BlackEnergy, the attackers used different malware. The first-stage payload was a simple trojan downloader, which connected to and downloaded a second-stage payload from a compromised Ukrainian server. The second-stage payload was a backdoor, written in Python, called Gcat. This backdoor is open source and freely available to everyone on *GitHub*.

Why do we conclude that the same group was behind this attack? We know because the spear-phishing emails were sent from the same server as was used by the BlackEnergy group [20]. In addition, the attackers' email used the same notification technique, with a PNG image, as described above.

The fact that this group is able to use different types of malware inspired us to look for similar cases in the past. We found one such case, but there is no proven link to the BlackEnergy group as seen in the 20 January 2016 case. However, we still believe that it was used by the same group.

As before, the initial infection vector was an *Excel* document containing a malicious VBA macro. The document was named `Загальний довідник ДП АМПУ на` 23 07 15.xls, which translates from Ukrainian as the General Directory of State Enterprise «Ukrainian Sea Ports Authority» on 23 07 15. Since this document uses the topic of sea ports, and we are aware that the BlackEnergy group is known to attack such critical infrastructure components, it is fair to assume that this document was used against sea port companies or companies in some way associated with them (see Figure 10).

The VBA macro code in this document is very similar to a macro used by BlackEnergy in delivering documents. Once the macro is activated, this document creates the file vba_macro.exe in %TEMP% and executes it afterwards. The executable is an obfuscated .NET binary, which simply downloads a second-stage payload. Unfortunately, it is not possible to say now what was downloaded when the server was active.



Загальний довідник ДП АМПУ на 23 07 15.xls.xls [Protected View] - Microsoft Excel

Protected View This file originated from an Internet location and might be unsafe. Click for more details. Enable Editing

Z11

Апарат управління ДП «Адміністрація морських портів України»

Увага! Цей документ був створений у більш новій версії Microsoft Office™
Макроси потрібно включити для відображення вмісту документу.

Security Warning Macros have been disabled. Options...

Security Alert - Macro

Macro

Macros have been disabled. Macros might contain viruses or other security hazards. Do not enable this content unless you trust the source of this file.

Warning: It is not possible to determine that this content came from a trustworthy source. You should leave this content disabled unless the content provides critical functionality and you trust its source.

More information

File Path: C:\Users\user\Documents\Загальний довідник ДП АМПУ на 23 07 15.xls

○ Help protect me from unknown content (recommended)
● Enable this content

Open the Trust Center OK Cancel

Figure 10: The Excel document with a malicious macro, which is possibly intended for use against Ukrainian sea ports.

The document was saved on 23 July 2015 and the payload dropped was detected by our products in the fourth quarter of 2015. We don't know how successful this attempted attack was.

CONCLUSION

The perpetrators behind BlackEnergy have caused the first documented act of cyber sabotage against a mass civilian population. That fact by itself makes the threat and threat actors interesting but, as our research has showed, there are also many other noteworthy details that have come to light over the years, for example, the use of the *PowerPoint* zero-day exploit CVE-2014-4114.

The BlackEnergy attacks in Ukraine have been taking place at the time of an armed conflict, which makes it an exceptionally sensitive issue. Given the geopolitical situation in the region and the types of victims targeted in the attacks (high-value state and government organizations but also critical infrastructure – power grid, railway, airport, news media, and others) political motives are very likely. Ukrainian officials were quick to point an accusing finger at Russia, and many others – including security companies – followed with similar allegations. Since attribution in the cyber world is always tricky, we can neither confirm nor deny this. In fact, it is somewhat disturbing when speculations are presented as facts without hard evidence.

Whoever stands behind the BlackEnergy attacks, we can expect to see more in the future. We will continue monitoring the situation for new developments.

INDICATORS OF COMPROMISE

Exploits:

4AE76B5ABF77B3589031E435EBE034A33E0888F369513D4A84592196C3C13D9C

38531CAEB2C314487714E4CE7A5B9791B67E7AA8693FE12E33A585AFD5313FC5

EB4E5923DCE5E2906BB51A4AE0B536F42C5659CAED2CD991F23F6C91FA38A188

15F42698829D169AB783F799615E7E14EEF7658F354534EOFB79814A9AB7CF4D

Malicious documents:

554D284C533231466A79D798334AE3212F4EFA30637B055E26842209CB5B24C1

2CD03D202E02D6B3E6715924BA5E6E1B5C29B87840C78354764C659DC46173AC

969E9156C3ED97F56E3F2C9A7B372ED193A4ED7ADD74AF533955B1482A3BB519

3E843F2973E6A1486A04CC980A14B9E3EBD19B5D3AD5E2D45828239E543C784E

Tools:

5CB4147C6FE72BA3782CC6C2BC0B1DA69D5576B2E993C6C3649B0488E2364472 (Nmap scanner)

BC190E0533C4F75F3E303979BE21C06C40B3F6CEEC86071A46692C3D85370772 (Custom DSEFix)

0969DAAC4ADC84AB7B50D4F9FFB16C4E1A07C6DBFC968BD6649497C794A161CD (Win32/SSHBearDoor.A)

REFERENCES

[1] Lipovsky R.; Cherepanov A. Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland. September 2014. https://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland. http://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/.

[2] Lipovsky R. CVE-2014-4114: Details on August BlackEnergy PowerPoint Campaigns. October 2014. http://www.welivesecurity.com/2014/10/14/cve-2014-4114-details-august-blackenergy-powerpoint-campaigns.

[3] Lipovsky R.; Cherepanov A. BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry. January 2016. http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/.

[4] Zetter K. Everything We Know About Ukraine’s Power Plant Hack. Jauary 2016. https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.

[5] Zetter K. Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid. March 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[6] Wilhoit K.; Gogolinski J. Sandworm to Blacken: The SCADA Connection. October 2014. http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection.

[7] ICS-CERT. Alert (ICS-ALERT-14-281-01E) Ongoing Sophisticated Malware Campaign Compromising ICS. October 2014. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[8] The Ministry of Energy and Coal Mining of Ukraine. Міненерговугілля має намір утворити групу за участю представників усіх енергетичних компаній, що входять до сфери управління Міністерства, для вивчення можливостей щодо запобігання несанкціонованому втручанню в роботу енергомереж. February 2016. http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109.

[9] US Department of Homeland Security. DHS Works with Critical Infrastructure Owners and Operators to Raise Awareness of Cyber Threats. March 2016. https://www.dhs.gov/blog/2016/03/07/dhs-works-critical-infrastructure-owners-and-operators-raise-awareness-cyber-threats.

[10] SANS ICS; E-ISAC. Analysis of the Cyber Attack on the Ukrainian Power Grid. http://ics.sans.org/duc5.

[11] Federal Bureau of Investigation. The Latest Phone Scam. June 2010. https://www.fbi.gov/news/stories/2010/june/phone-scam.

[12] CyS Centrum. Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины. January 2016. https://cys-centrum.com/ru/news/black_energy_2_3

[13] Baumgartner K.; Garnaeva M. BE2 custom plugins, router abuse, and target profiles. November 2014. https://securelist.com/blog/research/67353/be2-custom-plugins-router-abuse-and-target-profiles.

[14] Microsoft. Driver Signing Policy. https://msdn.microsoft.com/en-us/library/windows/hardware/ff548231(v=vs.85).aspx.

[15] Microsoft. The TESTSIGNING Boot Configuration Option. https://msdn.microsoft.com/en-us/library/windows/hardware/ff553484(v=vs.85).aspx.

[16] hfiref0x. Windows x64 Driver Signature Enforcement Overrider. https://github.com/hfiref0x/DSEFix.

[17] Cherepanov A. BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry. January 2016. http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry.

[18] CERT UA. Українські ЗМІ атакують за допомогою Black Energy. November 2015. http://cert.gov.ua/?p=2370.

[19] Lipovsky R. New wave of cyberattacks against Ukrainian power industry. January 2016. http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry.

[20] CyS Centrum. Атака на энергетические объекты 19-20 января 2016 года. Постфактум. January 2016. https://cys-centrum.com/ru/news/attack_on_energy_facilities_jan_ps.

[21] F-Secure. BlackEnergy & Quedagh: The convergence of crimeware and APT attacks. September 2014. https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.