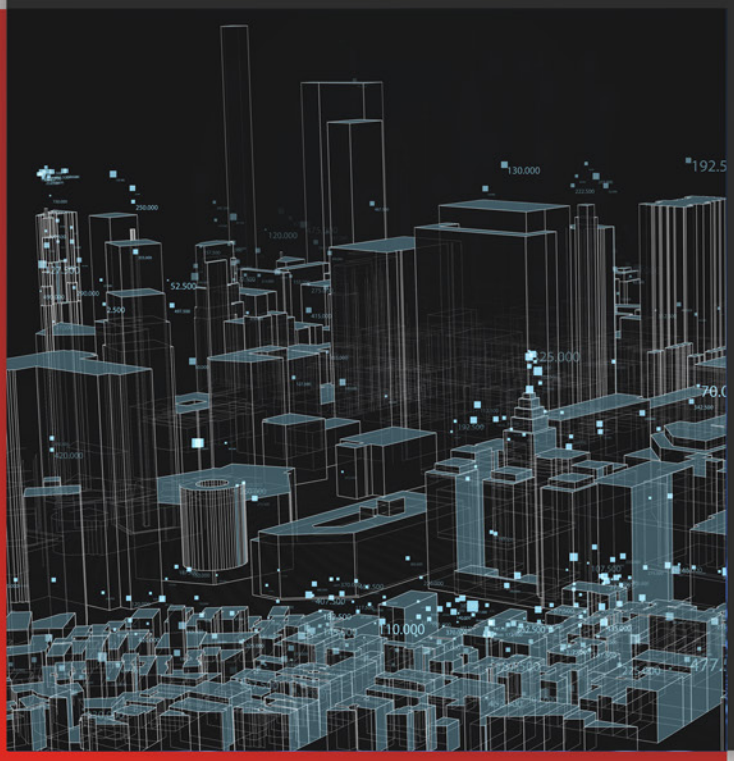
فروردین
۱۴۰۰

# ماهنامه

امنیت فناوری اطلاعات



شبکه گستر

امنیت شما | وظیفه ما

newsroom.shabakeh.net



@SGnewsroom

# فهرست مطالب

# 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 یک ماه گذشته پرداخته شده است.

همان‌طور که در این ماهنامه به تفصیل مورد بررسی قرار گرفته، مهاجمان از تصاویر در ظاهر بی‌خطر که در سایت‌های هک‌شده تزریق شده‌اند در فرایند انتشار نسخ جدید ObliqueRAT بهره می‌گیرند. ObliqueRAT بدافزاری از نوع Remote Access Trojan - به اختصار RAT - است که نخستین نسخه از آن یک سال پیش شناسایی شد. از این تکنیک با عنوان پنهان‌نگاری یا Steganography یاد می‌شود.

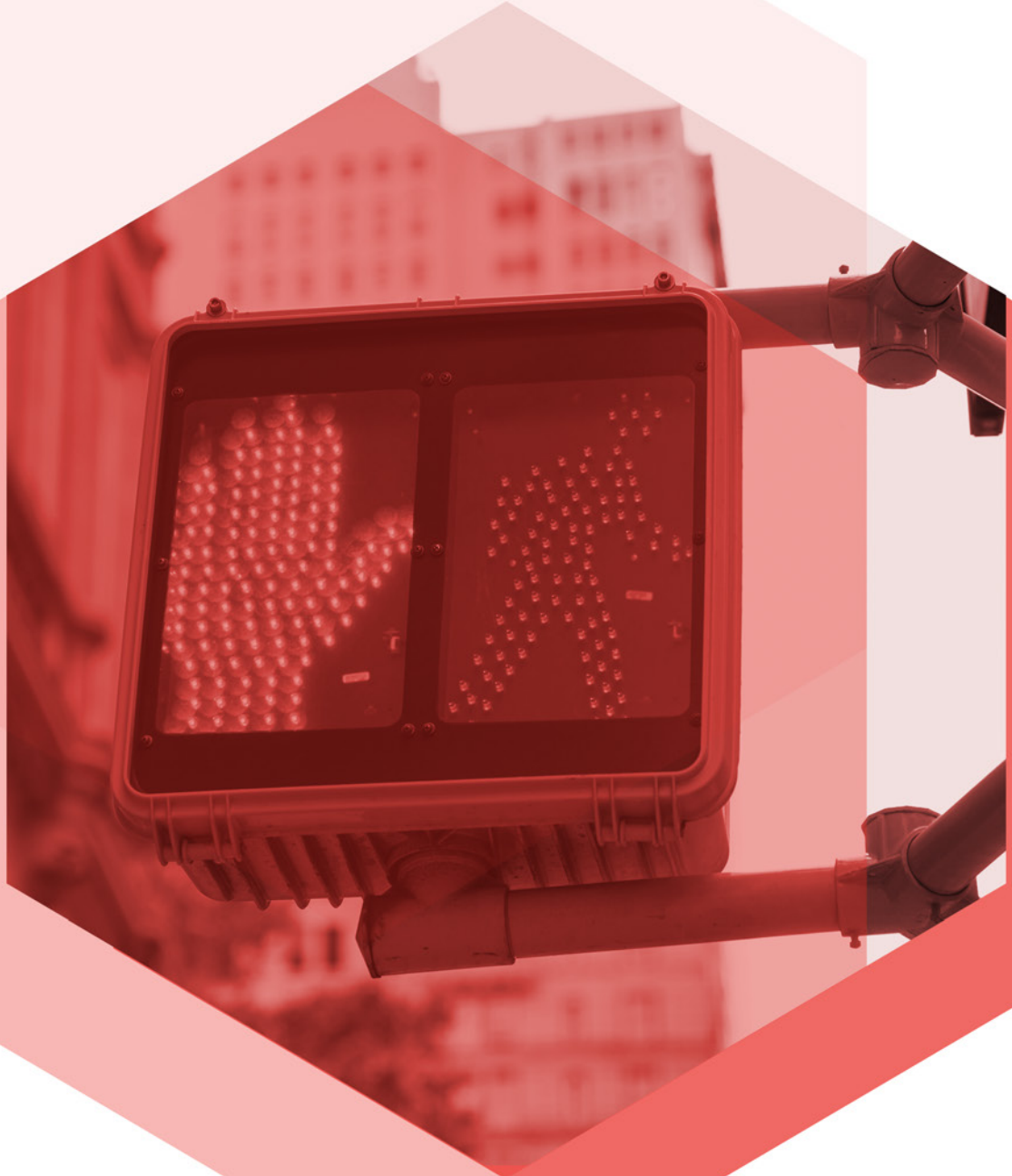
در اواخر سال ۱۳۹۹ شرکت مایکروسافت با انتشار اصلاحیه‌هایی اضطراری، چندین آسیب پذیری امنیتی، معروف به ProxyLogon را در سرویس‌دهنده ایمیل MS Exchange ترمیم کرد. از زمان انتشار اصلاحیه‌ها و افشای جزییات آن، هکرهای مستقل و گردانندگان APT متعددی، ProxyLogon را به فهرست تکنیک‌های نفوذ خود اضافه کرده‌اند. در این ماهنامه به برخی تهدیداتی که در جریان انتشار آنها از ProxyLogon بهره‌جویی شده پرداخته شده است.

هک شبکه‌ها و فروش دسترسی به آنها، توسط افرادی که از آنها با عنوان "دلال‌های دسترسی اولیه" (Initial Access Broker) یاد می‌شود صورت می‌گیرد. این افراد با هک سرور یا سامانه سازمان، پس از دستیابی به اطلاعات لازم جهت رخنه به آنها، اقدام به فروش دسترسی فراهم شده به سایر تبهکاران سایبری می‌کنند. اما بر اساس گزارشی که خلاصه‌ای از آن در این ماهنامه ارائه شده سرقت و فروش دسترسی به شبکه سازمان‌ها در سال ۲۰۲۰ و در پی فراگیری دورکاری کارکنان افزایشی چشم‌گیر داشته است.

در دوازدهمین ماه ۱۳۹۹، شرکت‌های مایکروسافت، سیسکو، وی‌ام‌وِر، اف‌فایو، سونیک‌وال، بیت‌دیفندر، گوگل، موزیلا، ادوبی، اس‌آپ و اپل اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند. جزییات این به‌روزرسانی‌ها و گزارش‌های متنوع دیگر 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



# پنهان‌نگاری؛
## تکنیک جدید ObliqueRAT

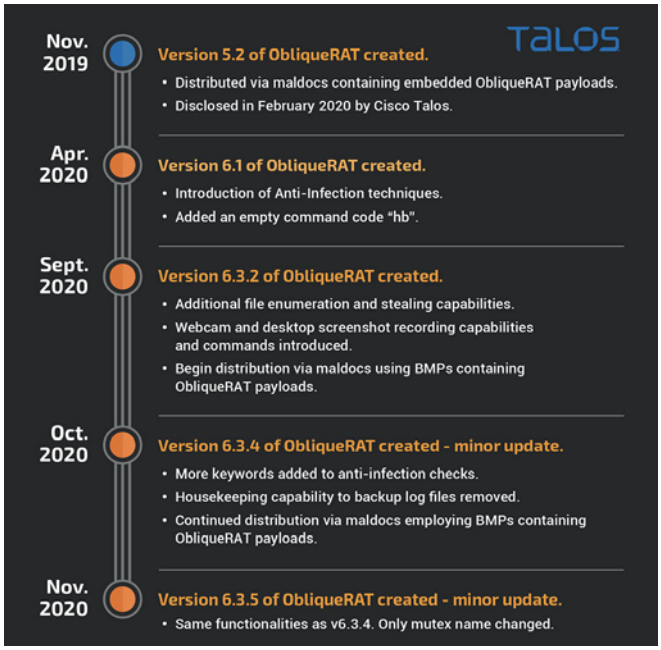
بررسی محققان سیسکو نشان می‌دهد مهاجمان از تصاویر در ظاهر بی‌خطری که در سایت‌های هک‌شده تزریق شده‌اند در فرایند انتشار نسخ جدید ObliqueRAT بهره می‌گیرند.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده چکیده‌ای از یافته‌های این محققان ارائه است.

ObliqueRAT بدافزاری از نوع Remote Access Trojan - به اختصار RAT - است که نخستین نسخه از آن یک سال قبل شناسایی شد.

نسخ ابتدایی آن دارای عملکرد معمول بدافزارهای RAT نظیر سرقت داده‌ها و متوقف‌سازی برخی پروسه‌ها بودند.

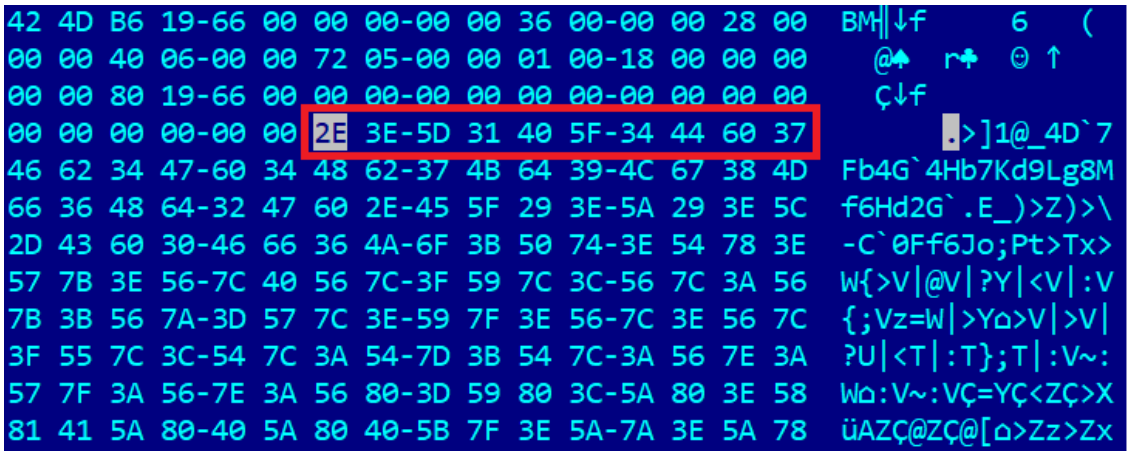
با گذشت زمان و استمرار در ظهور نسخ جدید، این بدافزار مجهز به قابلیت‌های فنی پیشرفته و توانایی انتشار با روش‌های مختلف شد.



یکی از روش‌های انتشار ObliqueRAT ایمیل‌های فیشینگ ناقل اسناد Office است. در اسناد مذکور ماکرویی (Macros) مخرب تزریق شده که اجرای آن موجب آلوده شدن دستگاه به ObliqueRAT می‌شود.

در حالی که تا مدتی پیش ObliqueRAT مستقیماً توسط ماکرو توزیع می‌شد در نسخ اخیر این بدافزار از سایت‌های هک‌شده به‌عنوان واسط (احتمالاً برای عبور از سد کنترل‌ها و پویشگرهای امنیتی ایمیل) استفاده می‌شود.

همچنین در نسخ جدید از تکنیک پنهان‌نگاری (Steganography) بهره گرفته شده است. بدین‌صورت که کد مخرب ObliqueRAT در فایل‌های تصویری BMP و در میان داده‌های معتبر آنها درج شده است.




مهاجمان فایل BMP آلوده را در سایت‌های هک شده تزریق می‌کنند تا ماکرو در زمان اجرا، آن را دریافت و پس از استخراج کد مخرب، ObliqueRAT را بر روی دستگاه قربانی فراخوانی کند.

ObliqueRAT قادر به شناسایی بسترهای موسوم به Sandbox است؛ بسترهایی که عمدتاً توسط محققان بدافزار به‌منظور مهندسی معکوس و تحلیل کد مورد استفاده قرار می‌گیرند. از جمله آن‌که در صورت فعال بودن هر یک از پروسه‌های زیر، اجرای خود را متوقف می‌کند:

| | | |
|---|---|---|
| python | ProcessHacker | ida64 |
| vmacthlp | procexp | Procmon |
| VGAuthService | Autoruns | ollydbg |
| vmtoolsd | pestudio | LordPE |
| TPAutoConnSvc | Wireshark | Fiddler |
| ftnlsv | dumpcap | CFF Explorer |
| ftscanmgrhv | TSVNCache | sample |
| vmwsprrdpwks | dnSpy | vboxservice |
| usbarbitrator | ConEmu | vboxtray |
| horizon_client_service | 010Editor | ida64 |

در نسخ اخیر ObliqueRAT بدافزار از اجرای بر روی سیستم‌هایی که نام دستگاه یا نام کاربری آنها یکی از موارد زیر است نیز خودداری می‌کند:

| | | |
|---|---|---|
| 15pb | roslyn | virlab |
| 7man2 | vince | beginer |
| stella | test | beginner |
| f4kh9od | sample | markos |
| willcarter | mcafee | semims |
| biluta | vmscan | gregory |
| ehwalker | mallab | tom-pc |
| hong lee | abby | will carter |
| joe cage | elvis | angelica |
| jonathan | wilbert | eric johns |
| kindsight | joe smith | john ca |
| malware | hanspeter | lebron james |
| peter miller | johnson | rats-pc |
| petermiller | placehole | robot |
| phil | tequila | serena |
| rapit | paggy sue | sofynia |
| r0b0t | klone | straz |
| cuckoo | oliver | bea-ch |
| vm-pc | stevens | |
| analyze | ieuser | |

ObliqueRAT می‌تواند با دریافت فرامین زیر از سرور فرماندهی (C2) خود اقدام به اجرای اموری همچون تصویربرداری از طریق دوربین دستگاه و جاسوسی از فعالیت‌های کاربر و اطلاعات او کند:

COMMAND CODE = “WES” ; WEBCAM SCREENSHOT

COMMAND CODE = “SSS” ; DESKTOP SCREENSHOT

<COMMAND CODE = “PIZZ” COMMAND DATA=<FILENAME> & <ZIP_FILE_NAME

<COMMAND CODE = “PLIT” COMMAND DATA=<TARGET FILEPATH

برخی منابع ارتباط ObliqueRAT با کارزارهای ناقل CrimsonRAT و گروه Transparent Tribe APT را که حمله به سفارت‌های هند در عربستان سعودی و قزاقستان را در کارنامه دارد محتمل دانسته‌اند. زیرساخت‌های سروهای C2 آن نیز اشتراکاتی با کارزارهای RevengeRAT دارد.

مشروح گزارش سیسکو در خصوص ObliqueRAT در لینک زیر قابل دریافت و مطالعه است:

https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html

# سرورهای آسیب‌پذیر Exchange
## هدف باج‌افزار DearCry

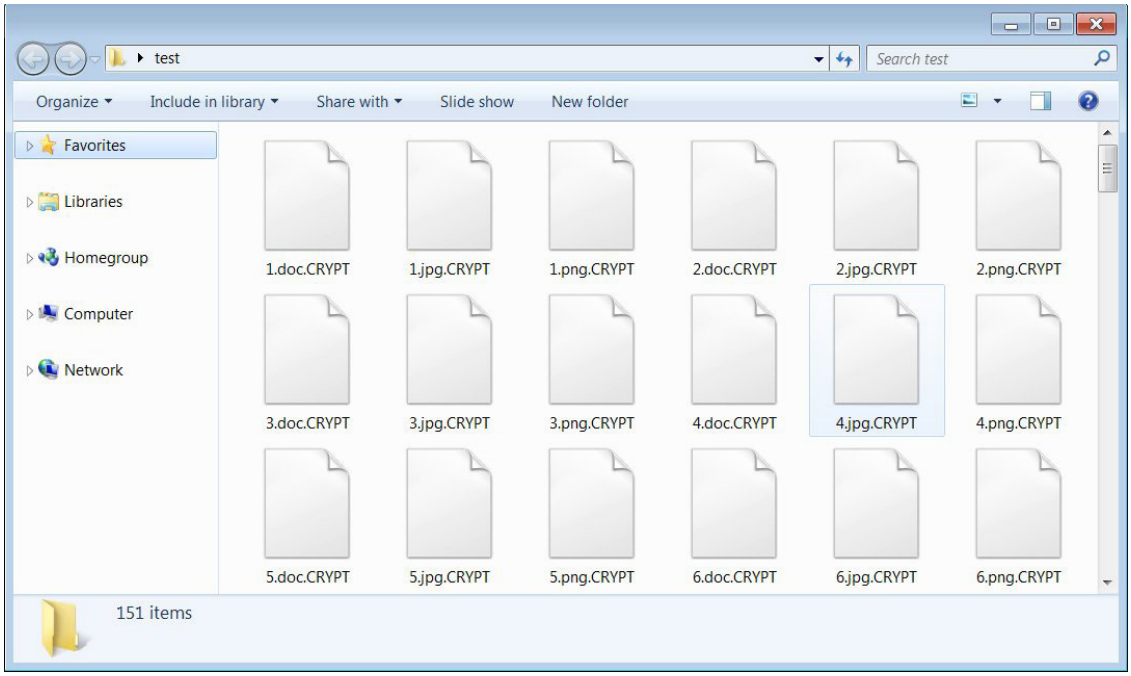

برخی منابع خبر داده‌اند مهاجمان با هک سرورهای آسیب‌پذیر MS Exchange اقدام به نفوذ به آنها و در ادامه توزیع باج‌افزار جدیدی با نام DearCry می‌کنند.

به گفته این منابع آسیب‌پذیری‌های بکار گرفته شده در جریان این حملات ProxyLogon است که ۱۲ اسفند مایکروسافت (Microsoft, Corp) اقدام به عرضه اصلاحیه‌های اضطراری برای ترمیم آنها کرده بود.

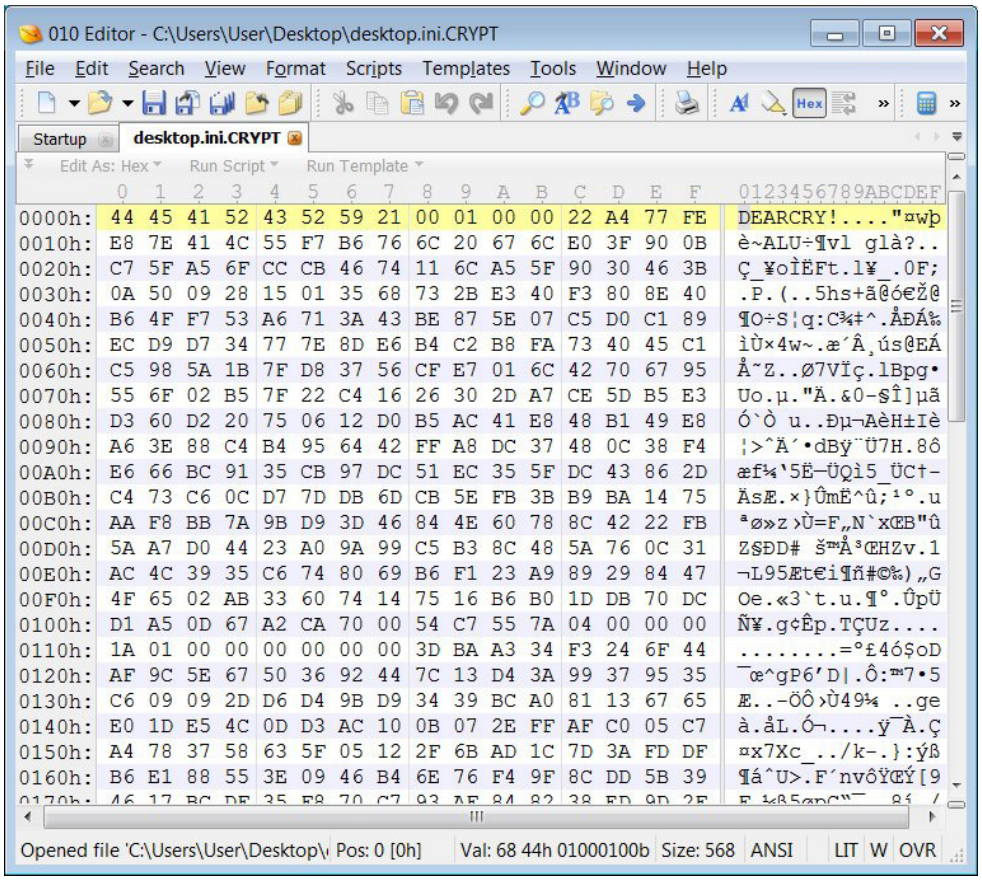
در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به چکیده‌ای از گزارش‌های منتشر در خصوص این حملات پرداخته شده است.

جمعه، ۲۲ اسفند مایکروسافت نیز اجرای حملات باج‌افزاری بر ضد سرورهای آسیب‌پذیر Exchange را تایید کرد.

بر طبق گزارشی که سایت Bleeping Computer آن را منتشر کرده DearCry پس از رمزگذاری فایل اقدام به الصاق پسوند CRYPT به آن می‌کند.




در فرایند رمزگذاری DearCry از الگوریتم‌های AES-256 و RSA-2048 استفاده می‌شود. همچنین رشته !DEARCRY نیز به ابتدای هر فایل رمز شده افزوده می‌شود.



نام فایل اطلاعیه باج‌گیری (Ransom Note) این باج‌افزار readme.txt گزارش شده است. در فایل مذکور از قربانی خواسته می‌شود تا درهم‌ساز درج شده در فایل را به مهاجم ارسال کند. به نظر می‌رسد که کد درج شده درهم‌ساز MD٤ کلید عمومی RSA قربانی است.

گفته می‌شود مبلغ اخاذی شده از یکی از قربانیان ۱۶ هزار دلار بوده است.

انتظار می‌رود که بهره‌گیری از آسیب‌پذیری‌های ProxyLogon در MS Exchange مورد توجه مهاجمان بیشتری قرار گیرد. لذا توجه به نکات اشاره شده در اطلاعیه زیر به منظور ایمن ساختن سرورهای MS Exchange به تمامی سازمان‌ها توصیه می‌شود:

https://newsroom.shabakeh.net/22058/

**نشانه‌های آلودگی (IoC)**

- 0e55ead3b8fd305d9a54f78c7b56741a
- cdda3913408c4c46a6c575421485fa5b
- c6eeb14485d93f4e30fb79f3a57518fc

# آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

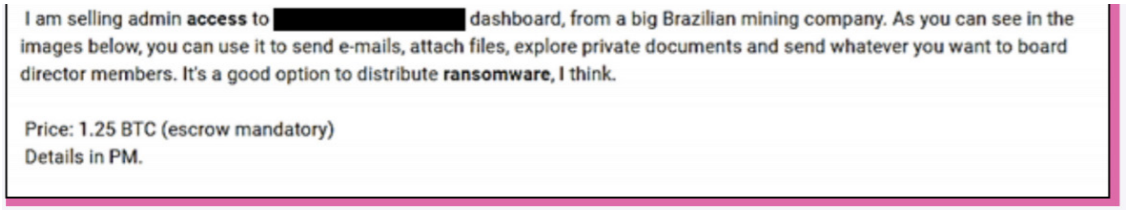
# روزگار پررونق دلال‌های
## دسترسی اولیه

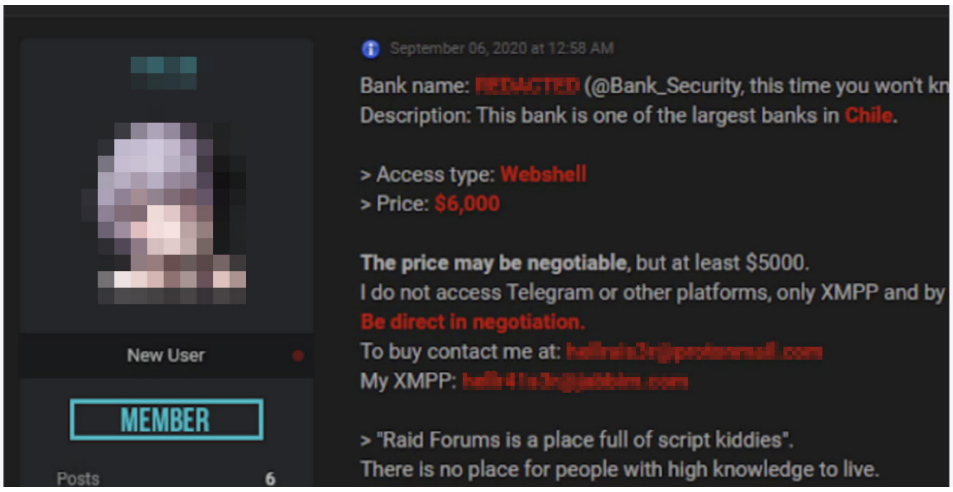
خرید و فروش اطلاعات اصالت‌سنجی (Credential) دسترسی‌های از راه دور مدتهاست که بخشی از اکوسیستم وب تاریک (Dark Web) شده است. اما بر اساس گزارشی که شرکت دیجیتال شدوز (Digital Shadows Ltd) آن را منتشر کرده سرقت و فروش دسترسی به شبکه سازمان‌ها در سال ۲۰۲۰ و در پی فراگیری دورکاری کارکنان افزایشی چشم‌گیر داشته است.

در ادامه این مطلب که با مشارکت شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، چکیده‌ای از گزارش دیجیتال شدوز ارائه گردیده است.

هک شبکه‌ها و فروش دسترسی به آنها، توسط افرادی که از آنها با عنوان "دلال‌های دسترسی اولیه" (Initial Access Broker) یاد می‌شود صورت می‌گیرد. این افراد با هک سرور یا سامانه سازمان، پس از دستیابی به اطلاعات لازم جهت رخنه به آنها، اقدام به فروش دسترسی فراهم شده به سایر تبهکاران سایبری می‌کنند.

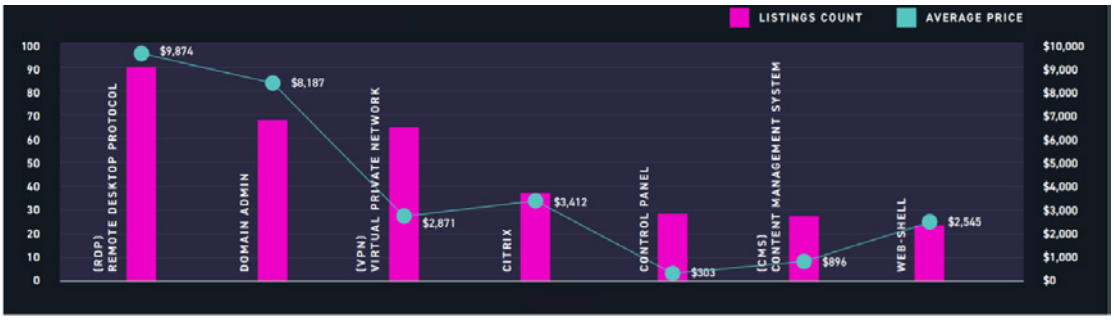
دو نمونه از تبلیغات این واسطه‌ها در تصاویر زیر قابل مشاهده است.



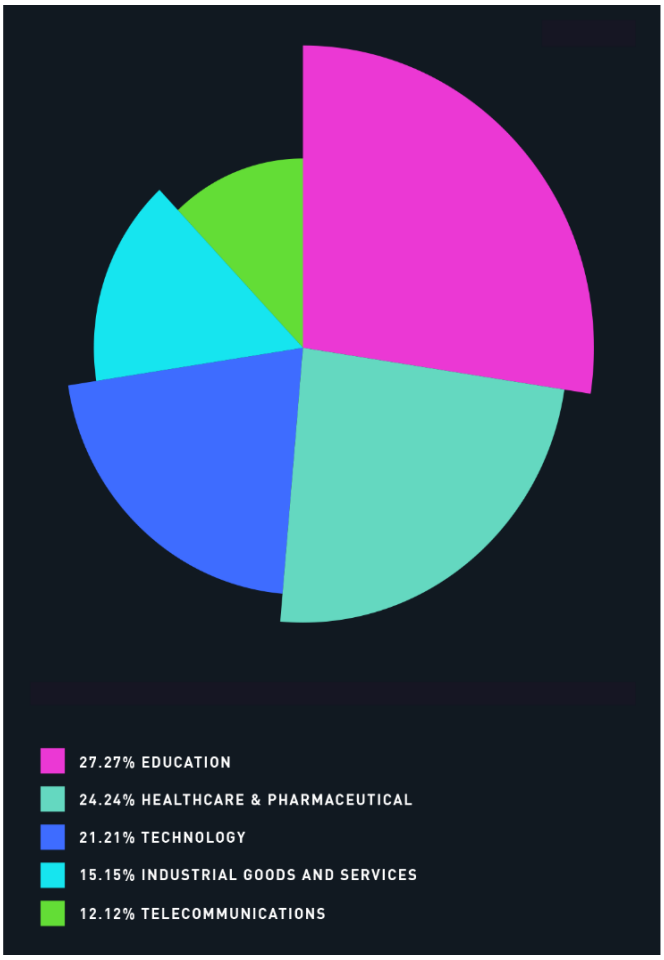
دیجیتال شدوز میانگین قیمت یک دسترسی اولیه ۷۱۰۰ دلار گزارش کرده است. این مبلغ بسته به سازمان، نوع و سطح دسترسی و تعداد دستگاه‌های قابل دسترس از طریق آن می‌تواند متفاوت باشد.

دسترسی از طریق پودمان Remote Desktop Protocol - به اختصار RDP - با ۱۷ درصد، بیشترین سهم از دسترسی‌های اولیه فروخته شده در سال ۲۰۲۰ را به خود اختصاص داده است. RDP با میانگین قیمت ۹۸۰۰ دلار جایگاه گران‌ترین روش را نیز کسب کرده است.




رخنه به شبکه قربانی از طریق پودمان RDP یکی از متداول‌ترین روش‌های استفاده شده توسط گردانندگان باج‌افزاری است که قربانیان خود را به‌صورت کاملاً هدفمند انتخاب می‌کنند. در جریان برخی از این حملات صدها هزار دلار و بعضاً میلیون‌ها دلار از قربانی اخاذی می‌شود که مبلغ ۱۰ هزار دلار صرف شده برای خرید دسترسی در برابر آن مبالغ هنگفت اصلاً به چشم نمی‌آید.

رصد برخی فاروم‌هایی که در آنها دسترسی‌های RDP به فروش می‌رسد نشان می‌دهد که بخش‌های آموزش، بهداشت و درمان، فناوری، صنعت و ارتباطات اصلی‌ترین اهداف حملات مبتنی بر RDP هستند. سازمان‌های فعال در هر یک از این حوزه‌ها می‌توانند هدفی پرسود از نگاه باج‌گیران سایبری باشند.



انتظار می‌رود سوءاستفاده گسترده مهاجمان از پودمان RDP همچنان ادامه خواهد یافت. موارد زیر از جمله اقدامات مؤثر در ایمن‌سازی این پودمان است:

- دسترسی به RDP در بستر اینترنت مسدود شود. سرورهای با RDP باز به‌سادگی از طریق جستجوگرهایی همچون Shodan قابل شناسایی هستند.
- از تغییر درگاه (Port) پیش‌فرض RDP اطمینان حاصل شود.
- از پودمان TCP بجای UDP استفاده شود.
- از اصالت‌سنجی موسوم به Network Level Authentication - به اختصار NLA - استفاده شود.
- اطمینان حاصل شود که سیاست‌های مدیریت رمز عبور از جمله الزام پیچیده و غیرتکراری بودن آنها شامل حساب‌های کاربری RDP نیز می‌شود تا احتمال هک شدن آنها در جریان حملات Brute-force به حداقل برسد.
- حتی‌الامکان از اصالت‌سنجی‌های دوعاملی (2FA) جهت دسترسی به RDP استفاده شود.
- دسترسی به RDP محدود به نشانی‌های IP مجاز و حساب‌های کاربری خاص شود.
- ارتباطات RDP از طریق SSH یا IPSec امن شود.
- سطح دسترسی کاربران محلی و تحت دامنه در حداقل ممکن تنظیم شود. استفاده از سامانه‌های کنترل دسترسی نقش-محور (Role-based Access Control - به اختصار RBAC) توصیه می‌شود.
- از اعمال سریع اصلاحیه‌های (Patch) عرضه شده اطمینان حاصل شود.
- در نامگذاری‌ها تلاش شود که اطلاعات سازمان افشا نشود.

مشروح گزارش دیجیتال شدوز با عنوان Initial Access Brokers - An Excess of Access در لینک زیر قابل دریافت و مطالعه است:

https://resources.digitalshadows.com/whitepapers-and-reports/initial-access-brokers-report

# آسیب‌پذیری برخی تجهیزات سوپرمایکرو به بدافزار TrickBoot

شرکت سوپرمایکرو (Super Micro Computer, Inc) با انتشار توصیه‌نامه‌ای، نسبت به آسیب‌پذیر بودن برخی مادربردهای خود به بدافزار TrickBoot هشدار داده است.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به برخی ویژگی‌های TrickBoot و توصیه‌نامه منتشر شده از سوی سوپرمایکرو پرداخته شده است.

در اواسط آذر ماه، اعلام شد که نویسندگان TrickBot ماژول 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. این ماژول TrickBot به TrickBoot معروف شد.

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.

در گزارش زیر که ۱۳ آذر ماه منتشر شد جزییات فنی TrickBoot مورد بررسی قرار گرفت:

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

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

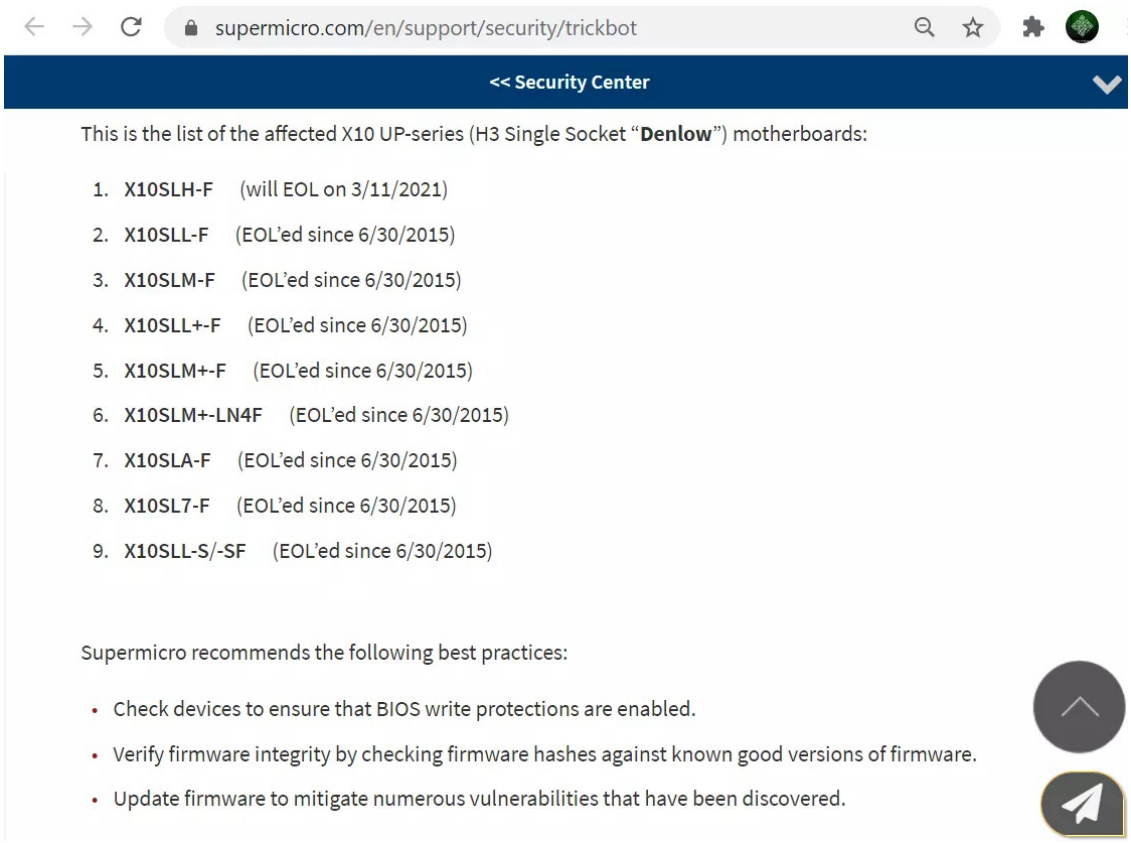
در آن زمان اعلام شد که تنها بسترهای ساخت شرکت Intel شامل Coffee Lake، Kaby Lake، Skylake و Comet Lake در فهرست اهداف آن قرار دارند.

هر چند در نمونه‌های بررسی شده در آن دوران، ماژول مذکور تنها به تشخیص آسیب‌پذیر بودن UEFI بسنده می‌کرد اما این احتمال نیز از سوی آنها مطرح شده بود که دامنه فعالیت آن بر روی اهداف باارزش‌تر ممکن است گسترده‌تر و مخرب‌تر باشد.

TrickBoot 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.

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

اکنون شرکت سوپرمایکرو اعلام کرده که مدل Denlow مادربردهای X10 UP این شرکت نیز در برابر TrickBoot آسیب‌پذیر هستند.




سوپرمایکرو این آسیب‌پذیری را در BIOS 3.4 ترمیم و اصلاح کرده است. اما در عین حال این نسخه تنها برای مادربرد X10SLH-F به‌صورت عمومی منتشر شده و صاحبان سایر مادربردهای آسیب‌پذیر باید برای دریافت نسخه مذکور با سوپرمایکرو تماس بگیرند.

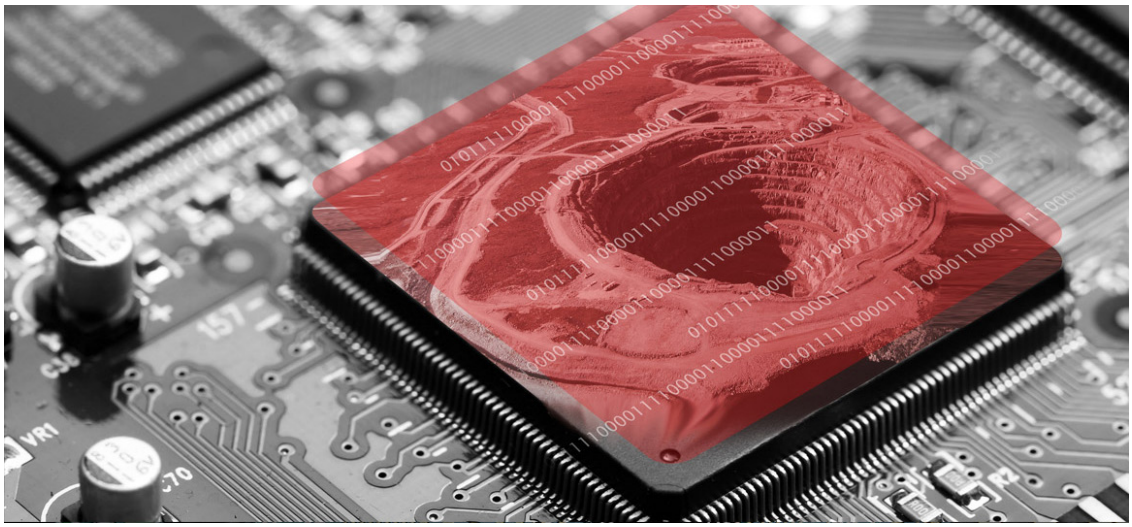
توصیه‌نامه سوپرمایکرو در لینک زیر قابل دریافت و مطالعه است:

https://www.supermicro.com/en/support/security/trickbot

لازم به ذکر است شرکت پالس سکیور (Pulse Secure, LLC) نیز اقدام به انتشار توصیه‌نامه زیر در خصوص تجهیزات PSA-5000 و PSA-7000 که در آنها از مدل آسیب‌پذیر سخت‌افزار سوپر مایکرو استفاده شده کرده است:

https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44712

# دستگاه‌های QNAP،
## باز هم هدف حملات سایبری



بر اساس گزارشی که شرکت چیهو ۳۶۰ آن را منتشر کرده دستگاه‌های NAS ساخت QNAP هدف حملات موسوم به Cryptojacking قرار گرفته‌اند. در جریان این حملات، مهاجمان بدافزاری را بر روی دستگاه هک‌شده اجرا می‌کنند که امکان استخراج ارز رمز را با استفاده از منابع دستگاه برای آنها فراهم می‌کند.

چیهو ۳۶۰، بدافزار استفاده شده در این حملات را UnityMiner نامگذاری کرده است.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده چکیده‌ای از گزارش چیهو ۳۶۰ ارائه شده است.

در حملات مذکور از دو آسیب‌پذیری RCE (اجرای فرمان به‌صورت از راه دور) به شناسه‌های CVE-2020-2506 و CVE-2020-2507 برای هک دستگاه QNAP بهره گرفته می‌شود. این در حالی است که اصلاحیه این دو آسیب‌پذیری از ماه‌ها قبل در دسترس قرار داشته است.

در گزارش چیهو ۳۶۰ اشاره شده که مهاجمان با مخفی‌سازی پروسه و اطلاعات واقعی میزان استفاده از CPU، عملاً فعالیت‌های غیرعادی دستگاه را از دید کاربران در هنگام استفاده از رابط کاربری مخفی می ماند.

تمامی دستگاه‌های QNAP که تاریخ انتشار فرمور آنها به پیش از آگوست ۲۰۲۰ باز می‌گردد نسبت به این حملات آسیب‌پذیر گزارش شده‌اند. لذا اطمینان از آسیب‌پذیر نبودن نسخه فرمور تجهیزات NAS ساخت QNAP به تمامی راهبران توصیه می‌شود.

تعداد دستگاه‌های آسیب‌پذیر قابل دسترس بر روی اینترنت بیش از ۴ میلیون عدد تخمین زده شده است.

در سال‌های اخیر تجهیزات NAS ساخت شرکت QNAP به کرات هدف حملات سایبری از جمله حملات باج‌افزاری قرار گرفته‌اند.

مشروح گزارش چیهو ۳۶۰ در لینک زیر قابل دریافت و مطالعه است:

https://blog.netlab.360.com/qnap-nas-users-make-sure-you-check-your-system/

## نشانه‌های آلودگی (IoC)

**IP:**

۲۱۰.۲۰۱.۱۳۶.۱۷۰ | Taiwan | ASN9311 | HITRON TECHNOLOGY INC.

**Miner Proxy:**

aquamangts.tk:12933

a.aquamangts.tk:12933

b.aquamangts.tk:12933

**URL:**

http://c.aquamangts.tk:8080/QFS/install/unity_install.sh

http://c.aquamangts.tk:8080/QFS/arm64/Quick.tar.gz

http://c.aquamangts.tk:8080/QFS/amd64/Quick.tar.gz

**MD5:**

0f40086c9e96c9c11232a9175b26c644

1eb01a23a122d077540f83b005abdbfc

97015323b4fd840a40a9d40d2ad4e7af

# به‌روزرسانی‌ها و اصلاحیه‌های منتشر شده
## در آخرین ماه ۱۳۹۹


در اسفند ۱۳۹۹، شرکت‌های مایکروسافت، سیسکو، وی‌ام‌وِر، اف‌فایو، سونیک‌وال، بیت‌دیفندر، گوگل، موزیلا، ادوبی، اس‌آپ و اپل اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند که در ادامه این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به آنها پرداخته شده است.

### مایکروسافت

۱۹ اسفند، شرکت مایکروسافت (Microsoft Corp)، مجموعه‌اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی مارس منتشر کرد. اصلاحیه‌های مذکور در مجموع ۸۲ آسیب‌پذیری را در Windows و محصولات و اجزای نرم‌افزاری زیر ترمیم می‌کنند:

- Azure
- HEVC Video Extensions
- Internet Explorer
- Microsoft 365 Apps for Enterprise
- Microsoft Business Productivity Servers
- Microsoft Edge
- Microsoft Excel
- Microsoft Office
- Microsoft PowerPoint
- Microsoft Quantum Development Kit for Visual Studio Code
- Microsoft SharePoint
- Microsoft Visio
- Microsoft Visual Studio
- Power BI Report Server
- Visual Studio

درجه اهمیت ۱۰ مورد از این آسیب‌پذیری‌ها "حیاتی" (Critical) و ۷۲ مورد "مهم" (Important) اعلام شده است.

دو مورد از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها، روز-صفر (Zero-day) بوده و جزییات آنها پیش‌تر به‌صورت عمومی منتشر شده بود. فهرست این آسیب‌پذیری‌های روز-صفر به شرح زیر است:

- CVE-2021-26411 که ضعفی از نوع Memory Corruption در مرورگر Internet Explorer است. هدایت کاربر به یک صفحه حاوی کد Exploit آن می‌تواند یکی از سناریوهای احتمالی سوءاستفاده از این آسیب‌پذیری باشد. نکته بسیار مهم این که حداقل از ماه فوریه گروهی از مهاجمان از آسیب‌پذیری مذکور به منظور نصب یک Backdoor سفارشی بر روی اهداف خود استفاده کرده‌اند.
- CVE-2021-27077 که ضعفی از Elevation of Privilege است که Win32k در سیستم عامل Windows متأثر می‌شود.

همچنین چندین آسیب‌پذیری در سرویس DNS سیستم عامل Windows توسط اصلاحیه‌های این ماه ترمیم شده‌اند.
CVE-2021-26895، CVE-2021-26894، CVE-2021-26893 ، CVE-2021-26877 و CVE-2021-26897 در دسته از RCE و CVE-2021-27063 و CVE-2021-26896 در دسته آسیب‌پذیری‌های Denial of Service (از کاراندازی سرویس) قرار می‌گیرند.

لازم به ذکر است که ۱۲ اسفند ماه شرکت مایکروسافت با انتشار به‌روزرسانی اضطراری و خارج از برنامه، چهار آسیب‌پذیری بحرانی روز-صفر را در نسخ مختلف Microsoft Exchange ترمیم کرد. جزییات بیشتر در خصوص این به‌روزرسانی‌ها در لینک های زیر قابل مطالعه است:

- https://afta.gov.ir/portal/home/?news/235046/237266/243111/
- https://afta.gov.ir/portal/home/?news/235046/237266/242971/
- https://afta.gov.ir/portal/home/?news/235046/237266/243066/
- https://afta.gov.ir/portal/home/?news/235046/237266/243067/
- https://afta.gov.ir/portal/home/?news/235046/237266/243110/

به‌روزرسانی‌های ۱۲ اسفند علاوه بر موارد بالا سه آسیب‌پذیری زیر را نیز که همگی از نوع RCE (اجرای کد به صورت از راه دور) هستند در Microsoft Exchange ترمیم می‌کنند:

- CVE-2021-26412
- CVE-2021-27065
- CVE-2021-27078

جزییات بیشتر در خصوص مجموعه اصلاحیه های ماه مارس مایکروسافت را در گزارش زیر که با همکاری مرکز مدیریت راهبردی افتای ریاست جمهوری و شرکت مهندسی شبکه گستر تهیه شده بخوانید:

https://afta.gov.ir/portal/home/?news/235046/237266/243062/

## سیسکو

شرکت سیسکو (Cisco Systems Inc) در اسفند ماه در چندین نوبت اقدام به عرضه اصلاحیه‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها نزدیک به ۴۰ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۴ مورد آنها "حیاتی" و ۷ مورد "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "عبور از سد کنترل‌های اصالت‌سنجی"، "نشت اطلاعات" (Information Disclosure) و "از کاراندازی سرویس" (Denial of Service) از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید هستند. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

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

## وی‌اِم‌وِر

۵ اسفند شرکت وی‌ام‌ور (VMware, Inc) ضعفی "حیاتی" (Critical) از نوع RCE ("اجرای کد به صورت از راه دور") را در vCenter Server برطرف کرد که سوءاستفاده از آن به‌طور بالقوه کنترل سامانه آسیب‌پذیر را در اختیار مهاجم قرار می‌دهد.

به آسیب‌پذیری مذکور شناسه CVE-2021-21972 تخصیص داده شده است. سطح حساسیت آن نیز ۹.۸ از ۱۰ - بر طریق استاندارد CVSSv۳ - اعلام شده است.

اکسپلویت CVE-2021-21972 به‌صورت از راه دور و بدون نیاز به اصالت‌سنجی، با پیچیدگی کم ممکن گزارش شده است.

بر طبق توصیه‌نامه وی‌ام‌ور، vSphere Client (HTML۵) شامل ضعفی در یک افزونه vCenter Server است. مهاجم با دسترسی شبکه‌ای به پورت ۴۴۳ قادر به اکسپلویت کردن آن و اجرای فرامین با سطح دسترسی نامحدود بر روی سیستم عامل میزبان vCenter Server خواهد بود.

این آسیب‌پذیری در اکتبر ۲۰۲۰ توسط شرکت پازیتیو تکنالاجیز (Positive Technologies) به‌طور خصوصی به وی‌ام‌ور گزارش شده بود. پس ترمیم آن در ۵ اسفند و در پی آن انتشار حداقل دو نمونه اثبات‌گر (PoC)، جزییات فنی آن نیز در قالب لینک زیر از سوی پازیتیو تکنالاجیز منتشر شد:

https://swarm.ptsecurity.com/unauth-rce-vmware/

به دلیل حساسیت بالا و ماهیت حیاتی این آسیب‌پذیری و از همه مهمتر انتشار جزییات فنی و نمونه‌های اثبات‌گر ارتقای فوری vCenter Server به یکی از نسخ زیر توصیه می‌شود:

- U3n 5
- U3l 7
- U1c 0

نسخ بالا، یک ضعف امنیتی "متوسط" (Moderate) با شناسه CVE-2021-21973 را نیز در vCenter Server برطرف می‌کنند.

همچنین وی‌ام‌ور راهکار موقت (Workaround) زیر را برای آن دسته از راهبرانی که امکان ارتقای فوری vCenter Server را ندارند ارائه کرده است:

https://kb.vmware.com/s/article/82374

لازم به ذکر است که برخی منابع از پویش گسترده مهاجمان برای شناسایی سرورهای آسیب‌پذیر وی‌ام‌ور بر روی اینترنت خبر داده‌اند که می‌تواند نشانه‌ای از مورد اکسپلویت قرار گرفتن CVE-2021-21972 در آینده‌ای نزدیک باشد.

۵ اسفند، وی‌ام‌ور ضعفی "مهم" (Important) از نوع Heap-overflow با شناسه CVE-2021-21974 را نیز در VMware ESXi ترمیم کرد که سوءاستفاده از آن در شرایطی امکان اجرای کد به‌صورت از راه دور را ممکن می‌کند.

این شرکت ۱۲ اسفند نیز یک آسیب‌پذیری به شناسه CVE-2021-21978 و با درجه حساسیت "مهم" را در View Planner برطرف کرد. سوءاستفاده از آسیب پذیری مذکور امکان اجرای کد به‌صورت از راه دور را برای مهاجم فراهم می‌کند.

توصیه‌نامه‌های وی‌ام‌ور در خصوص آسیب‌پذیری‌های مذکور در لینک‌های زیر قابل دریافت و مطالعه است:

- https://www.vmware.com/security/advisories/VMSA-2021-0002.html
- https://www.vmware.com/security/advisories/VMSA-2021-0003.html

### اف‌فایو

۲۰ اسفند شرکت اف فایو (F5, Inc) در مجموع ۲۱ آسیب پذیری را در برخی محصولات این شرکت را ترمیم کرد. شدت حساسیت ۴ مورد از آسیب‌پذیری‌های مذکور، "حیاتی" گزارش شده است. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://support.f5.com/csp/article/K02566623

لازم به ذکر است که یکی از این آسیب پذیری ها با شناسه CVE-2021-22986 در دو محصول BIG-IP و BIG-IQ مورد سوءاستفاده مهاجمان قرار گرفته است.

### سونیک‌وال

در بهمن ماه شرکت سونیک‌وال (SonicWall Inc) با انتشار اطلاعیه‌ای از بهره‌جویی مهاجمان از یک آسیب‌پذیری روز-صفر در برخی محصولات این شرکت برای رخنه به سامانه‌های داخلی آن خبر داد. این شرکت در اسفند ماه نیز در چندین نوبت اقدام به به‌روزرسانی توصیه‌نامه امنیتی خود در خصوص این آسیب‌پذیری‌ها کرد. به کلیه راهبران محصولات سونیک‌وال از جمله محصولات Secure Mobile Access - به اختصار SMA - مطالعه اطلاعیه امنیتی زیر توصیه می شود:

https://www.sonicwall.com/support/product-notification/additional-sma-100-series-10-x-and-9-x-firmware-updates-required-updated-feb-19-2-p-m-cst/210122173415410/

### بیت‌دیفندر

در دوازدهمین ماه از سال ۱۳۹۹ شرکت بیت‌دیفندر (Bitdefender Corp) نسخه جدید راهکار Bitdefender GravityZone با شناسه ۶.۲۱.۱-۱ را منتشر کرد. از جمله تغییرات اعمال شده در نسخه ۶.۲۱.۱-۱ ارتقای سیستم عامل GravityZone Appliance به نگارش جدید است.

پشتیبانی از Ubuntu 16.04 LTS که سیستم عامل مورد استفاده در GravityZone است رسماً در ۱۰ اردیبهشت ۱۴۰۰ پایان می‌یابد. پس از آن تاریخ، ارائه اصلاحیه‌های حیاتی و به‌روزرسانی‌های امنیتی برای این نسخه از سیستم عامل Ubuntu متوقف خواهد شد. شرکت بیت‌دیفندر نیز در ۶.۲۱.۱-۱ نسخه سیستم عامل مذکور را در Appliance خود به ۲۰.۰۴ LTS ارتقا داده است.

جزییات بیشتر در خصوص GravityZone 6.21.1-1 در اینجا قابل دریافت و مطالعه است.

همچنین این شرکت نسخ ۶.۶.۲۵.۳۵۹، ۶.۲.۲۱.۱۳۷ و ۴.۱۵.۱۳۷.۲۰۰۱۳۷ را به‌ترتیب برای محصولات Endpoint Security Tools for Windows، Bitdefender Endpoint Security for Linux و Endpoint Security for Mac منتشر کرده است. جزییات بیشتر را در لینک‌های زیر بخوانید:

- https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-6-25-359-release-notes-(windows)-2675.html
- https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-2-21-137-release-notes-(linux)-2670.html
- https://www.bitdefender.com/support/endpoint-security-for-mac-version-4-15-137-200137-release-notes-2671.html

### گوگل

در اسفند ماه شرکت گوگل (Google LLC) در سه نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۲ اسفند انتشار یافت ۸۹.۰.۴۳۸۹.۹۰ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

- https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_12.html
- https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_5.html
- https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html

### موزیلا

در ماهی که گذشت شرکت موزیلا (Mozilla Corp) با ارائه به‌روزرسانی، در مجموع ۱۰ آسیب پذیری با درجه اهمیت "بالا"، ۴ ضعف امنیتی با درجه "متوسط" و ۴ آسیب پذیری با درجه "کم" را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد. توضیحات بیشتر در لینک‌های زیر قابل مطالعه است:

https://www.mozilla.org/en-US/security/advisories/mfsa2021-09/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-07/

### ادوبی

۱۹ اسفند، شرکت ادوبی (Adobe Inc) مجموعه اصلاحیه‌های امنیتی ماه میلادی مارس خود را منتشر کرد. اصلاحیه‌های مذکور، در مجموع، ۱۷ ضعف امنیتی را در محصولات زیر ترمیم می‌کنند:

- Photoshop: https://helpx.adobe.com/security/products/photoshop/apsb21-17.html
- Connect: https://helpx.adobe.com/security/products/connect/apsb21-19.html
- Creative Cloud Desktop Application: https://helpx.adobe.com/security/products/creative-cloud/apsb21-18.html
- Framemaker: https://helpx.adobe.com/security/products/framemaker/apsb21-14.html
- Animate: https://helpx.adobe.com/security/products/animate/apsb21-21.html

شدت حساسیت بسیاری از آسیب‌پذیری‌های مذکور، "حیاتی" گزارش شده و اکثر آنها در دسته آسیب‌پذیری به حملات اجرای کد قرار می‌گیرند.

### اس‌آپ

اس‌آپ (SAP SE) دیگر شرکتی بود که در اسفند ماه ۹۹ با انتشار به‌روزرسانی امنیتی، آسیب‌پذیری‌هایی را در چندین محصول خود برطرف کرد. بهره‌جویی از بعضی از این آسیب‌پذیری‌های ترمیم شده مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107

### اپل

در ۱۹ اسفند ماه، شرکت اپل (Apple Inc) با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در محصولات زیر ترمیم و اصلاح کرد:

- Safari: https://support.apple.com/en-us/HT212223
- macOS Big Sur: https://support.apple.com/en-us/HT212220
- watchOS: https://support.apple.com/en-us/HT212222
- iOS & iPadOS: https://support.apple.com/en-us/HT212221

سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند.

# رویدادها و وقایع امنیتی

## Go؛

## هر روز محبوب‌تر از دیروز

بر اساس گزارشی که شرکت اینتزر (Intezer) آن را منتشر کرده تعداد بدافزارهایی که به زبان Go برنامه‌نویسی شده‌اند در فاصله سال‌های ۲۰۱۷ تا ۲۰۲۰ افزایشی ۲ هزار درصدی داشته است.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده چکیده‌ای از گزارش مذکور ارائه است.

این یافته‌ها مهاجرت ویروس‌نویسان از زبان‌های C و C++ به Go را که پیش‌تر از سوی برخی شرکت‌ها و محققان امنیتی مطرح شده بود تایید می‌کند. برای مثال، در اواسط سال ۲۰۱۹، شرکت پالو آلتو نت‌ورکز (Palo Alto Networks) در گزارش زیر از گسترش استفاده از Go توسط مهاجمان خبر داده بود:

https://unit42.paloaltonetworks.com/the-gopher-in-the-room-analysis-of-golang-malware-in-the-wild

Go - که برخی از آن با عنوان Golang یاد می‌کنند - یک زبان برنامه‌نویسی است که توسط شرکت گوگل (Google) طراحی شده و نخستین نسخه از آن ۱۱ سال قبل به‌طور عمومی منتشر شد.

در حالی که اولین بدافزار مبتنی بر Go در سال ۲۰۱۲ شناسایی شد اما چند سالی طول کشید تا این زبان توجه ویروس‌نویسان را به خود جلب کند.

رواج آن در دنیای تهدیدات سایبری از سال ۲۰۱۹ آغاز شد و اکنون Go به‌طور گسترده‌ای مورد استقبال گردانندگان این تهدیدات قرار گرفته است.

از گروه‌های هک با پشتوانه دولتی و گردانندگان APT گرفته تا تبهکاران سایبری، همگی استفاده از نمونه‌ای از بدافزارهای مبتنی بر Go را در کارنامه دارند. ضمن آن که در مواردی، محققان امنیتی نیز در ساخت ابزارهای تست نفوذ از این زبان بهره گرفته‌اند.

استقبال گسترده مهاجمان از Go بی‌دلیل نیست.

برنامه‌های نوشته شده به زبان Go را می‌توان به‌سادگی برای بسترهای مختلف کامپایل کرد؛ به‌عبارت دیگر بدون نیاز به اعمال تغییرات اساسی در کد پایه بدافزار می‌توان فایل‌هایی برای اجرا شدن در هر یک از بسترهای Mac، Windows و Linux ایجاد کرد. قابلیتی که بسیاری زبان‌های برنامه‌نویسی دیگر فاقد آن هستند.

تحلیل کدهای باینری مبتنی بر Go و مهندسی معکوس کردن آنها برای محققان امنیتی نیز همچنان دشوار است و این خود شانس شناسایی زودهنگام بدافزارهای توسعه داده شده توسط این زبان را کاهش می‌دهد.

Go مجهز به استک شبکه‌ای است که کار با آن آسان است. همچنین Go به یکی از زبان‌های برنامه‌نویسی ابری تبدیل شده که بسیاری از برنامه‌های مبتنی بر رایانش ابری (Cloud Computing) توسط آن توسعه داده شده‌اند. این ویژگی Go به‌خوبی نیاز آن دسته از کدنویسانی را که ساخت بدافزارهایی برای تغییر، استخراج، ارسال یا دریافت بسته‌های شبکه‌ای را در سر دارند برآورده می‌سازد.

بسیاری از بدافزاری مبتنی بر Go بات‌نت‌هایی هستند که دستگاه‌های Linux و IoT را برای نصب استخراج‌کنندگان ارز رمز (Cryptojacking) هدف قرار می‌دهند یا اجرای حملات DDoS را بر عهده دارند. اینتزر معتقد است که تعداد باج‌افزارهایی که با Go نوشته شده‌اند نیز در حال افزایش است.

جزییات بیشتر در خصوص گزارش اینتزر در لینک زیر قابل مطالعه است:

https://www.intezer.com/blog/malware-analysis/year-of-the-gopher-2020-go-malware-round-up

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 |