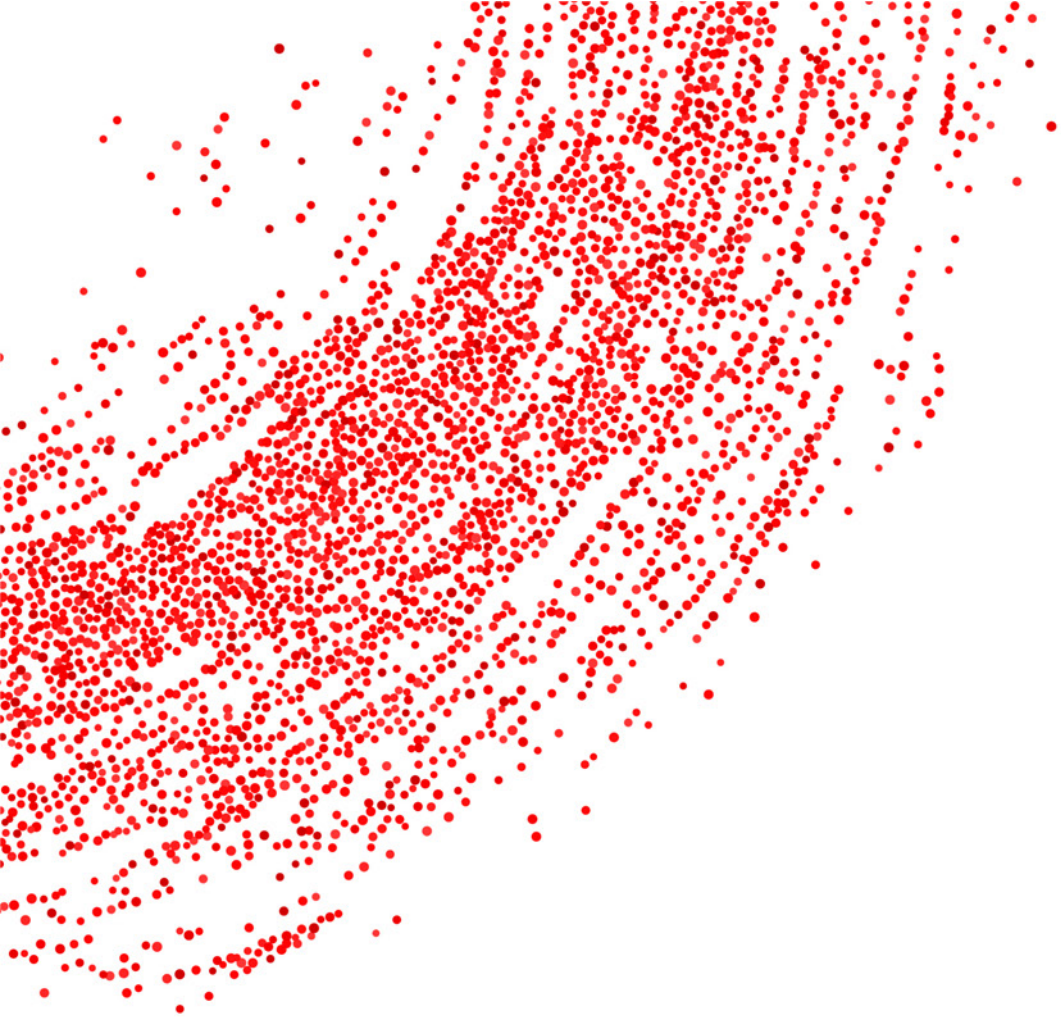
شبکه گستر

امنیت شما | وظیفه ما

ماهنامه
امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | مرداد ۱۴۰۱

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 اولین ماه از تابستان ۱۴۰۱ پرداخته شده است.

از جمله تهدیداتی که در این ماهنامه مورد بررسی قرار گرفته‌اند بدافزاری با عملکرد Wiper با عنوان Dilemma است که اخیراً در زیرساخت‌های کشور شناسایی شده است. همچنین در بخشی از این ماهنامه به بررسی حملات سایبری ۶ تیر که شرکت‌های فعال در صنعت فولاد کشور را مورد هدف قرار دادند پرداخته شده است.

Orbit، دیگر بدافزاری است که در این شماره آن را مورد بررسی قرار داده‌ایم. بدافزار مذکور با دسترسی غیرمجاز اقدام به سرقت مخفیانه اطلاعات از سیستم‌های تحت Linux و آلوده‌کردن تمام پروسه‌های در حال اجرا بر روی دستگاه‌های مبتنی بر این سیستم عامل می‌کند.

در این شماره به گزارش‌های جدیدی که چند شرکت امنیت سایبری درباره برخی باج‌افزارهای فعال همچون BlackCat و MedusaLocker منتشر کرده‌اند خواهیم پرداخت و ترفندهایی که هر یک از این تهدیدات مخرب برای دستیابی و نفوذ به شبکه استفاده می‌کنند، تشریح خواهیم کرد. همچنین به بررسی نسخه دوم باج‌افزار AstraLocker که برخلاف دیگر نمونه‌های مشابه، به جای سوءاستفاده از قابلیت ماکروهای VBA در نرم‌افزارهای Word، کد مخرب را از طریق OLE Object اجرا می‌کند، می‌پردازیم.

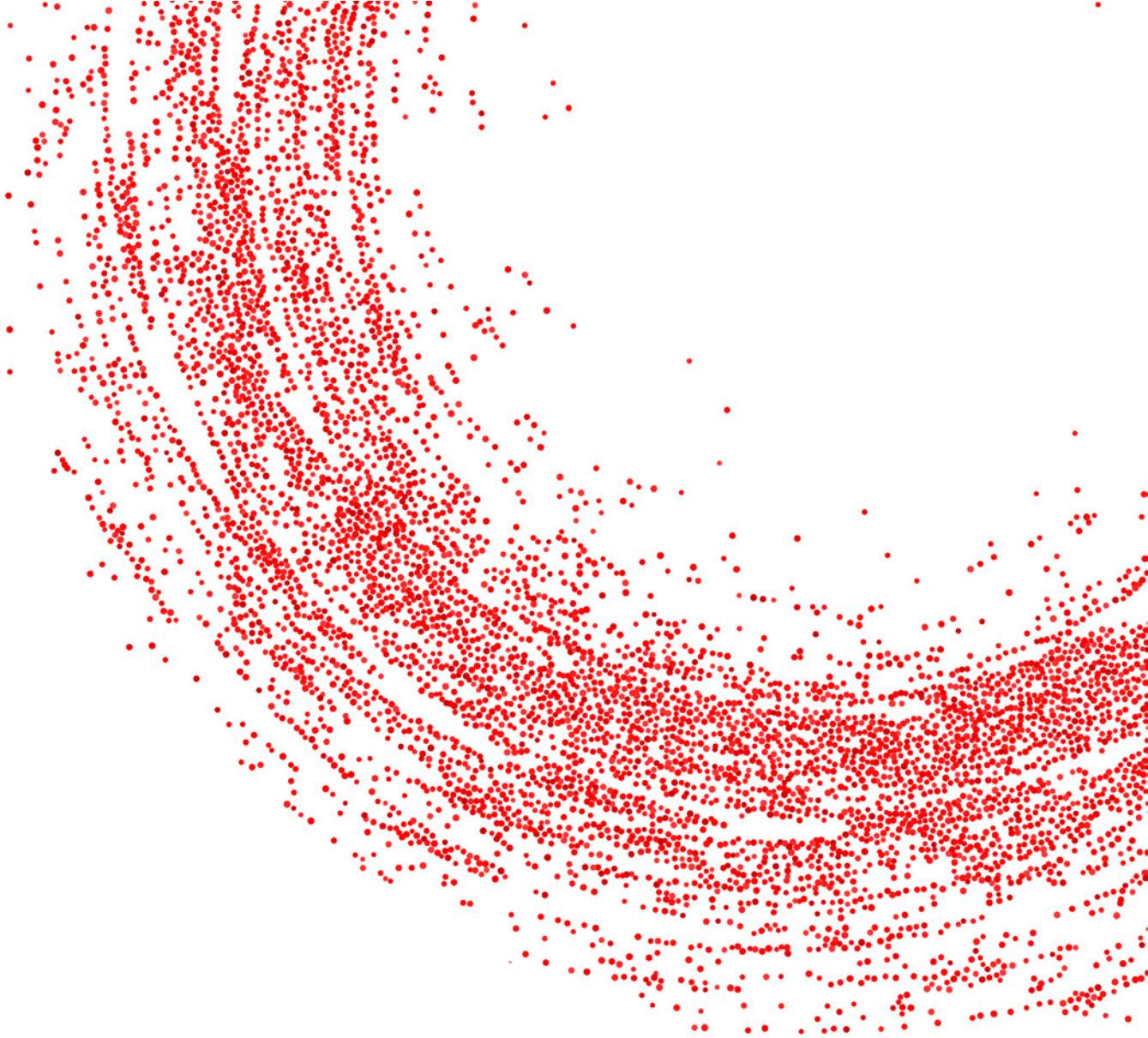
دیگر تهدید سایبری که در این ماهنامه به آن پرداخته شده، کارزاری رو به رشد به نام Raspberry Robin است که اقدام به توزیع بدافزاری با عملکرد کرم (Worm) بر روی سیستم‌های تحت Windows می‌کند.

جزئیات یک کارزار فیشینگ (Phishing) نیز که در آن مهاجمان اقدام به جعل هویت شرکت‌های برجسته در حوزه امنیت سایبری می‌کنند، مورد بررسی قرار گرفته است. همچنین به کارزاری دیگر خواهیم پرداخت که از سال ۲۰۲۱ سازمان‌های دولتی در کشورهای مختلف از جمله افغانستان و هند را مورد هدف قرار داده است. در جریان کارزار مذکور، مهاجمان از موضوعات سیاسی جهت فریب کاربران به منظور کلیک کردن روی یک لینک مخرب یا بازکردن پیوست ایمیل استفاده می‌کنند. جزئیات و نشانه‌های آلودگی این حملات فیشینگ هدفمند در این ماهنامه قابل مطالعه است.

نحوه عملکرد دکمه Mute میکروفون در نرم‌افزارهای کنفرانس از راه دور از نظر حفظ محرمانگی و حریم خصوصی از موضوعات دیگری است که در این شماره به تفصیل بررسی شده است.

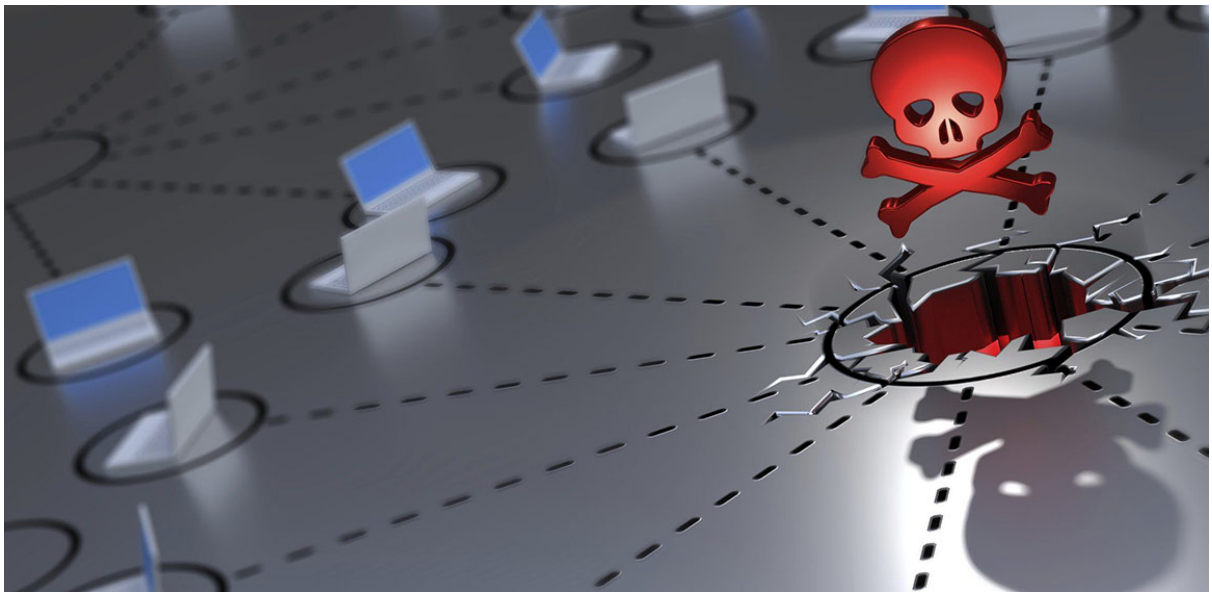
طبق معمول هر ماه، شرکت‌های مختلف فناوری اطلاعات اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. جزییات اصلاحیه‌های تیر ماه شرکت‌های مایکروسافت، سیسکو، مک‌آفی اینترپرایز، بیت‌دیفندر، وی‌ام‌ور، ادوبی، گوگل، موزیلا، اپل، دروپال، سیتریکس، س‌ای‌پی، جونیپر نت‌ورکز، اپن‌اس‌اس‌ال و اوراکل را می‌توانید 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 تلاش کارشناسان این شرکت است قدمی در جهت ارتقای دانش کاربران این حوزه باشد.



رویدادها و وقایع امنیتی

نگاهی به بدافزار مخرب Dilemma



۲۱ خرداد ۱۴۰۱، مرکز مدیریت راهبردی افتا با انتشار اطلاعیه‌ای از شناسایی یک بدافزار جدید با نام Dilemma در زیرساخت‌های کشور خبر داد [۱]. در این مطلب، نگاهی گذرا به پیشینه و عملکرد این بدافزار مخرب انداخته‌ایم.

پیشینه

Dilemma بدافزاری با عملکرد Wiper است. این نوع بدافزارها با رونویسی بخش MBR و در برخی موارد فایل‌ها عملاً موجب از کار افتادن دستگاه و معدوم شدن اطلاعات ذخیره شده بر روی آن می‌شوند.

هر چند نمونه‌هایی از باج‌افزارها نیز بجای رمزگذاری فایل‌ها، اقدام به رمزنگاری بخش MBR می‌کنند اما در بسیاری از موارد آن چه مهاجمان انجام می‌دهند نه رمزنگاری که معدوم‌سازی کامل MBR است. برای مثال، درسال ۱۳۹۵ بدافزار NotPetya توانست تعداد زیادی دستگاه را در کشورهای مختلف از جمله اوکراین دچار اختلال کند. اگر چه پیام نمایش داده شده بر روی دستگاه‌های آلوده به NotPetya تداعی‌کننده حمله‌ای باج‌افزاری بود اما بررسی‌های بیشتر نشان داد که این بدافزار فاقد هر گونه سازوکار برای بازگرداندن اطلاعات بوده و هدف آن صرفاً از کاراندازی دستگاه‌های سازمان‌های قربانی بوده است [۲].

گردانندگان این حملات، قربانیان خود را به‌صورت کاملاً هدفمند انتخاب می‌کنند. فرایند نفوذ و آلوده‌سازی نیز معمولاً محدود به چند ساعت و حتی چند روز نبوده و در مواردی هفته‌ها زمان برده است [۳]. هدف، شناسایی دقیق سرورهای حاوی اطلاعات حساس و در نتیجه وارد آوردن حداکثر خسارت و البته جلب بیشترین توجه است.

گزارش‌های منتشر شده از سوی نهادها و شرکت امنیتی در خصوص حملات چند سال اخیر نشان می‌دهد که گسترش دامنه نفوذ و توزیع بدافزار در سطح شبکه در بسیاری موارد مشابه بوده است [۱][۴][۵][۶]. برای مثال در اکثر موارد فایل‌های Batch و فرامین Scheduled Task علیرغم سادگی ماهیت آنها نقشی کلیدی در حمله داشته‌اند.

همچنین مهاجمان این گونه حملات تلاش می‌کنند تا با اعمال تغییرات مکرر بر روی فایل‌های مخرب خود احتمال شناسایی آنها توسط محصولات امنیتی را به حداقل برسانند.

نسخه اخیر

بدافزار با عملکرد Wiper که در اطلاعیه اخیر مرکز مدیریت راهبردی افتا به آن اشاره شده فایلی با نام dilemma.exe و مشخصات زیر است:

File Description: Dilemma
File Version: 1.0.0.0
Internal Name: dilemma.exe
Original Filename: dilemma.exe
Copyright: Copyright 2020
Product Name: Dilemma de modify
Product Version: 1.0.0.0
SHA-1: 2ce90ab46c620f84dfb36a3e97ae8f27122b142a

در برخی حملات پیشین، مهاجمان از نام msdskint.exe برای پروسه این بدافزار استفاده کرده بودند [۵].

Dilemma علاوه بر معدوم‌سازی بخش MBR اقدام به رونویسی فایل‌ها نیز می‌کند.

این بدافزار در یکی از سه حالت زیر قابل اجرا است:

- default – در این حالت هر فایل به بخش‌های ۱۰۲۴ بایتی تقسیم شده و بدافزار ۲۰۰ بایت از هر کدام از این بخش‌ها را رونویسی می‌کند؛
- light-wipe – تنها به تعداد تعیین‌شده در پارامتر مربوطه بخش‌های فایل را مورد دست‌درازی قرار می‌دهد؛
- full_purge – کل محتوای فایل را رونویسی می‌کند.

پروسه Dilemma از طریق پارامترهای زیر قابل فراخوانی است:

پارامتر	شرح
mbr	فعالسازی فلگ معدوم‌کننده MBR
fork-bomb	اجرای دو Instance دیگر از Wiper
sessions	متوقف کردن Session سایر کاربران بر روی دستگاه
delete-users	حذف نام کاربری افراد مورد نظر از طریق فرمان net user
break-users	رونویسی کردن گذرواژه نام‌های کاربری مورد نظر
logs	حذف سوابق Windows Event Log
passwords	در حال حاضر فاقد عملکرد
shadows	معدوم‌سازی رونوشت‌های موسوم به Shadow Copies
start-iis	اجرای سرویس IIS از طریق پروسه iisreset
stop-iis	متوقف کردن سرویس IIS از طریق پروسه iisreset
config	استخراج تنظیمات از فایل معرفی شده
light-wipe	معدوم کردن بخشی از فایل به میزان تعیین شده به همراه مؤلفه
wipe-exclude	پوشه‌های معرفی شده به همراه این مؤلفه از گزند Wiper در امان خواهند بود
delete	پس از رونویسی، فایل از روی دستگاه حذف خواهد شد
processes	پروسه‌های تعیین شده را توسط فرمان taskkill حذف خواهد کرد

wipe-stage-2	فایل‌ها را با روش پیش‌فرض رونویسی کرده و سپس حذف می‌کند
purge	کل فایل - و نه فقط بخشی از آن - را رونویسی می‌کند
wipe-only	فایل‌های تعیین شده را رونویسی می‌کند
wipe-all	تمامی فایل‌ها را رونویسی می‌کند

برای مثال، در جریان یکی از این حملات مهاجمان از طریق پارامترهای زیر اقدام به مستثنی‌سازی مسیرهای مرتبط با ضدویروس سیمانتک کرده بودند تا دست‌درازی به فایل‌های آن موجب حساسیت این محصول امنیتی نشود:

"-wipe-exclude", "C:\\\\Program Files\\\\Symantec*"
"-wipe-exclude", "C:\\\\Program Files (x86)\\\\Symantec*"

نکته قابل توجه این که مهاجمان پیش از معدوم‌سازی MBR و فایل‌ها از طریق بدافزارهای دیگر اقدام به سرقت اطلاعات می‌کنند.

مقابله

همان طور که اشاره شد که گردانندگان این حملات هدفمند با صرف زمان و منابع قابل‌توجه سعی در به حداکثر رساندن خسارات به سازمان قربانی را دارند. رعایت موارد زیر می‌تواند شانس موفقیت این تبهکاران سایبری را به حداقل برساند:

- بکارگیری محصولات امنیت نقاط پایانی قدرتمند و به‌روز
- محدودسازی سطوح دسترسی
- بهره‌گیری از دیواره آتش با قواعد سخت‌گیرانه
- اطمینان از نصب کامل اصلاحیه‌های امنیتی
- اعمال سیاست‌های سخت‌گیرانه در خصوص گذرواژه تمامی نام‌های کاربری
- رصد و بررسی هر گونه رخداد مشکوک یا غیرعادی به خصوص بر روی سرورها
- آموزش کاربران در نحوه برخورد با تهدیدات سایبری مبتنی بر مهندسی اجتماعی

توضیح این که نسخه‌ای از بدافزار Dilemma که در این گزارش به آن پرداخته شد با نام‌های زیر قابل شناسایی می‌باشد:

Bitdefender: IL:Trojan.MSILZilla.15370
McAfee: RDN/Wiper
Sophos: Mal/Generic-S

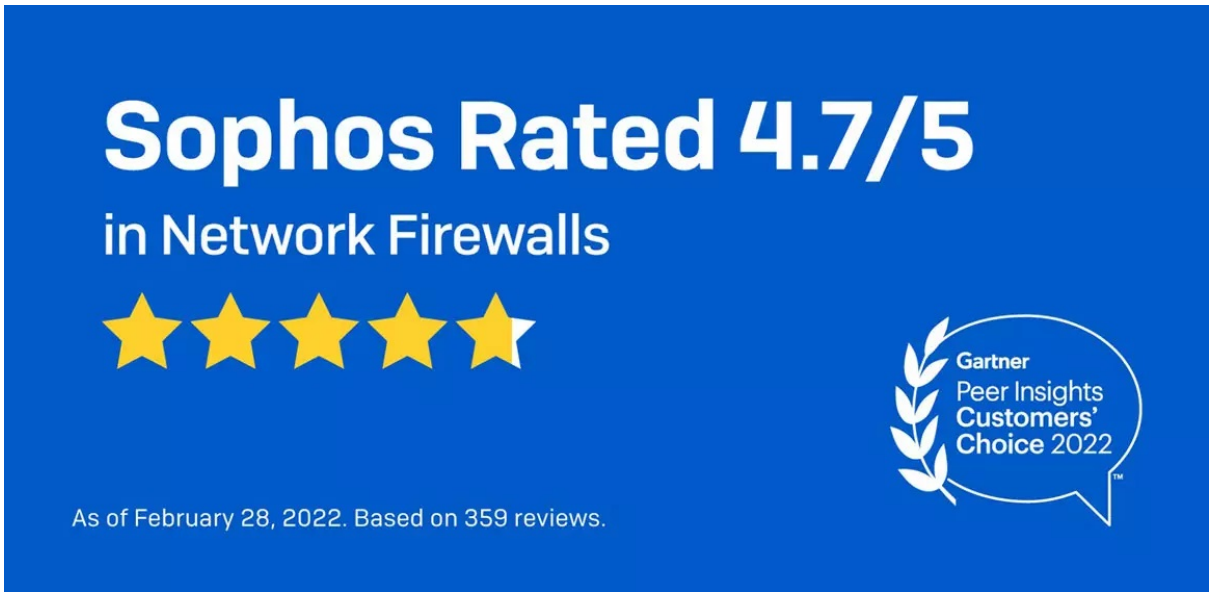
لازم به ذکر است علیرغم درخواست تبادل بیشتر اطلاعات در این زمینه از مراکز امنیتی کشور، فقط بر اساس اطلاعات جمع‌آوری شده شرکت مهندسی شبکه گستر، این خبر در این زمان، تنظیم شده است. در صورت دریافت اطلاعات بیشتر این خبر به‌روز خواهد شد.

منابع:

https://www.afta.gov.ir/fa-IR/Portal/4927/news/view/14608/2129
https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/
https://www.afta.gov.ir/fa-IR/Portal/1/news/view/14594/1889/
https://www.sentinelone.com/labs/meteorexpress-mysterious-wiper-paralyzes-iranian-trains-with-epic-troll/
https://research.checkpoint.com/2022/evilplayout-attack-against-irans-state-broadcaster/
https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/

اعطای نشان Peer Insights Customers’ Choice

به سوفوس توسط مؤسسه گارتنر



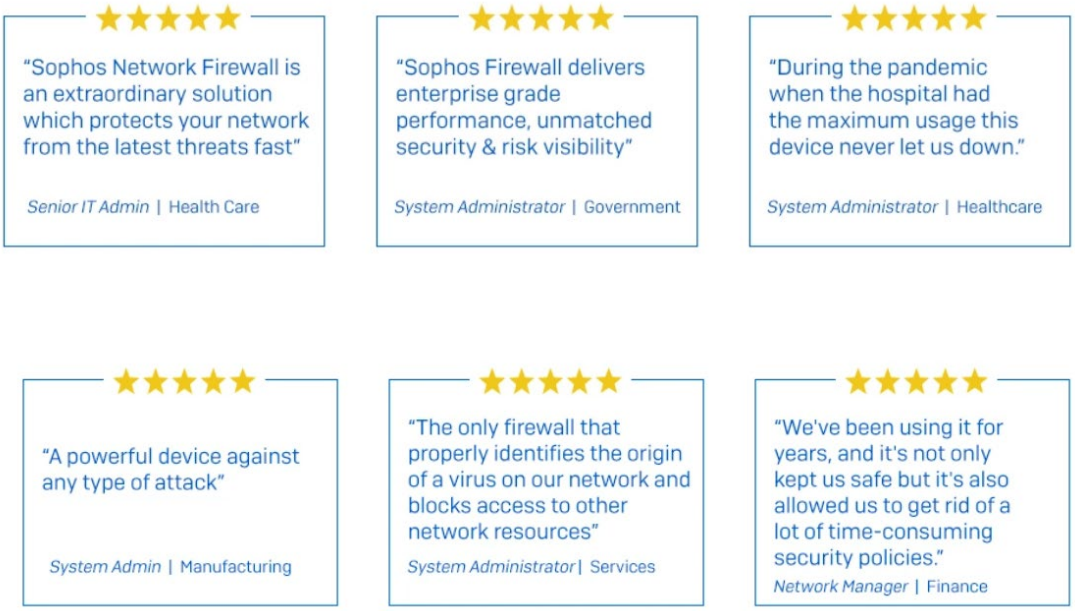
شرکت سوفوس موفق به دریافت نشان Peer Insights Customers’ Choice 2022 از مؤسسه گارتنر در بخش Network Firewalls شد.

این شرکت در سال میلادی گذشته نیز موفق به کسب نشان Peer Insights Customers’ Choice در حوزه Endpoint Protection Platforms شده بود.

گارتنر، یکی از معتبرترین مؤسسات بین‌المللی ارزیابی محصولات فناوری اطلاعات است که نشان Peer Insights Customers’ Choice را بر اساس نظرات کاربران متخصص به سازندگان برتر محصولات حوزه مورد بررسی اعطا می‌کند.

بر اساس گزارشی که گارتنر در بهار امسال آن را منتشر کرد در بازه‌ای ۱۸ ماهه صدها متخصص مستقل در نظرسنجی محصولات فایروال شرکت کردند که امتیاز شرکت سوفوس از نگاه این متخصصان به طور میانگین ۴/۷ از ۵ بوده است.

نصب و راه‌اندازی آسان، قابلیت‌های جامع رقابتی و یکپارچگی بالای محصولات فایروال سوفوس همراه با خدمات پشتیبانی عالی این شرکت از عوامل مؤثر در کسب این امتیاز درخشان و دریافت نشان Peer Insights Customers’ Choice بوده است.



نظر و بازخورد متخصصان در خصوص فایروال‌های سوفوس در لینک زیر قابل مطالعه است:

https://www.gartner.com/reviews/market/network-firewalls/vendor/sophos

فایروال‌های سوفوس، حفاظتی قدرتمند را همراه با کارایی بالا حتی برای پرترافیک‌ترین شبکه‌ها فراهم می‌کند. از جمله قابلیت‌های بی‌نظیر فایروال‌های سوفوس می‌توان به موارد زیر اشاره کرد:

افشای ریسک‌های پنهان – فایروال‌های سوفوس ریسک‌های مخفی را از طریق انواع داشبوردها و گزارش‌های بصری و جامع بهتر از سایر رقبا افشا می‌کنند.

مسدودسازی تهدیدات ناشناخته – فایروال‌های سوفوس با بررسی‌های سریع و بهینه مبتنی بر TLS و مجموعه‌ای از قابلیت‌ها حفاظتی پیشرفته که به‌سادگی هم قابل مدیریت هستند تهدیدات ناشناخته را سریع‌تر، ساده‌تر و مؤثرتر از سایر فایروال‌ها مسدود می‌کنند.

واکنش خودکار به رخدادها – دیواره های آتش سوفوس با بکارگیری ویژگی Synchronized Security و تکیه بر قابلیت بی‌نظیر Sophos Security Heartbeat به‌صورت خودکار اطلاعات تهدید را با محصولات امنیت نقاط پایانی این شرکت که بر روی سرورها و ایستگاه‌های کاری سازمان نصب هستند همسان کرده و نسبت به آن تهدید واکنشی مؤثر نشان می‌دهند.

به‌تازگی نیز شرکت سوفوس SFOS v19 را ارائه کرده که فایروال‌های این شرکت را مجهز به نوآوری‌ها و ویژگی‌هایی خاص و بی‌نظیر می‌کند. جزییات سیستم عامل SFOS v19 در لینک زیر در دسترس است:

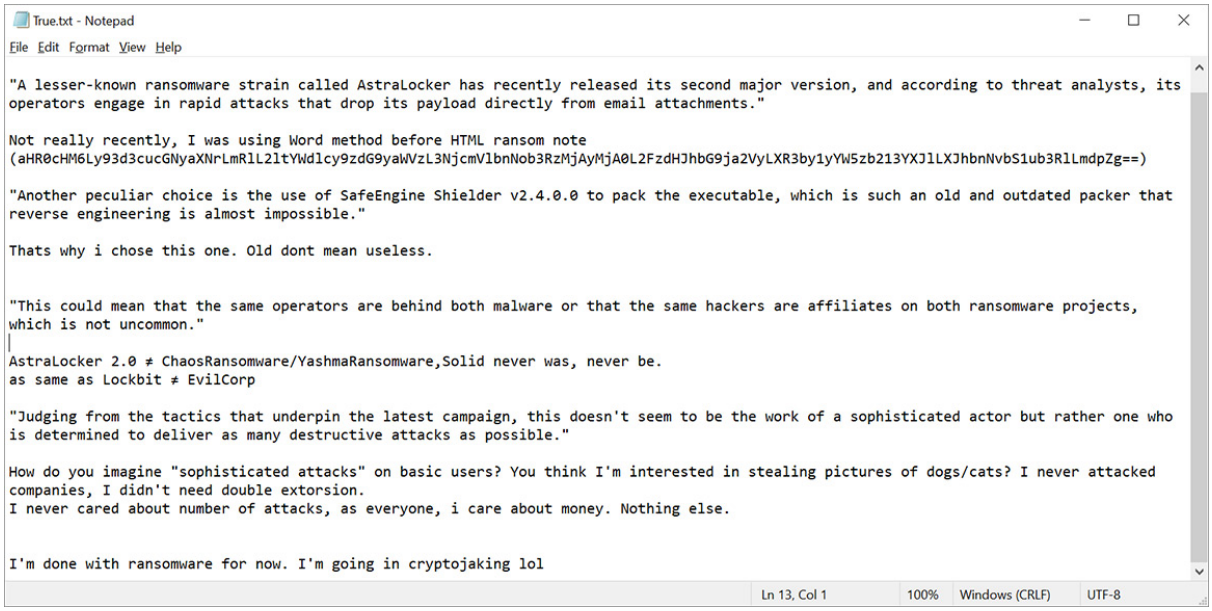
https://newsroom.shabakeh.net/24156/xstream-fastpath-sfos-v19.html

کارشناسان فروش شرکت مهندسی شبکه گستر از طریق شماره ۴۲۰۵۲ – ۰۲۱ آماده ارائه اطلاعات بیشتر در خصوص فایروال‌های سوفوس هستند.

خبر خوش برای قربانیان باج‌افزار

AstraLocker

گرداننده AstraLocker ضمن اعلام توقف فعالیت‌های باج‌افزاری خود، اقدام به انتشار کلیدهای رمزگشایی این باج‌افزار نموده است. همچنین او در گفتگو با سایت BleepingComputer عنوان نموده که در آینده بر روی استخراج رمزارز بر روی دستگاه‌های هک شده (Cryptojacking) تمرکز خواهد کرد. همچنین او یک فایل فشرده ZIP که حاوی کلیدهای رمزگشای AstraLocker است را به سایت تحلیل بدافزار VirusTotal ارسال کرده است.


True.txt - Notepad

File Edit Format View Help

"A lesser-known ransomware strain called AstraLocker has recently released its second major version, and according to threat analysts, its operators engage in rapid attacks that drop its payload directly from email attachments."

Not really recently, I was using Word method before HTML ransom note
(aHR0cHM6Ly93d3cucGNyaXNrLmRlL2ltYWdlcy9zdG9yaWVzL3NjcmVlbnNob3RzMjAyMjA0L2FzdHJhbG9ja2VyLXR3by1yYW5zb213YXJlLXJhbnNvbS1ub3RlLmdpZg==)

"Another peculiar choice is the use of SafeEngine Shielder v2.4.0.0 to pack the executable, which is such an old and outdated packer that reverse engineering is almost impossible."

Thats why i chose this one. Old dont mean useless.

"This could mean that the same operators are behind both malware or that the same hackers are affiliates on both ransomware projects, which is not uncommon."

AstraLocker 2.0 ≠ ChaosRansomware/YashmaRansomware,Solid never was, never be.
as same as Lockbit ≠ EvilCorp

"Judging from the tactics that underpin the latest campaign, this doesn't seem to be the work of a sophisticated actor but rather one who is determined to deliver as many destructive attacks as possible."

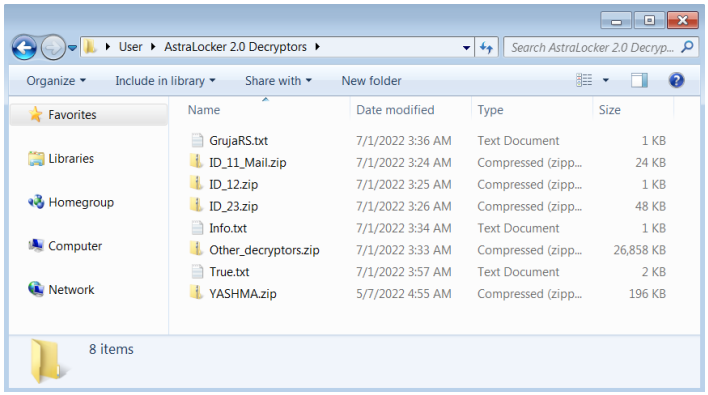
How do you imagine "sophisticated attacks" on basic users? You think I'm interested in stealing pictures of dogs/cats? I never attacked companies, I didn't need double extorsion.
I never cared about number of attacks, as everyone, i care about money. Nothing else.

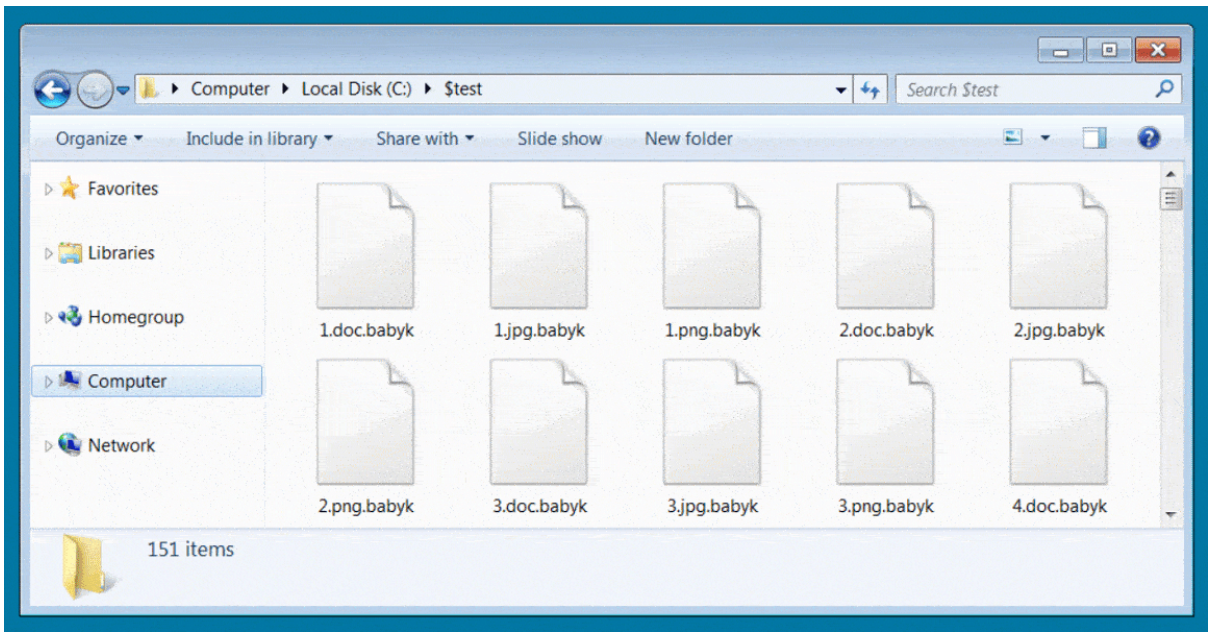
I'm done with ransomware for now. I'm going in cryptojaking lol

Ln 13, Col 1 | 100% | Windows (CRLF) | UTF-8

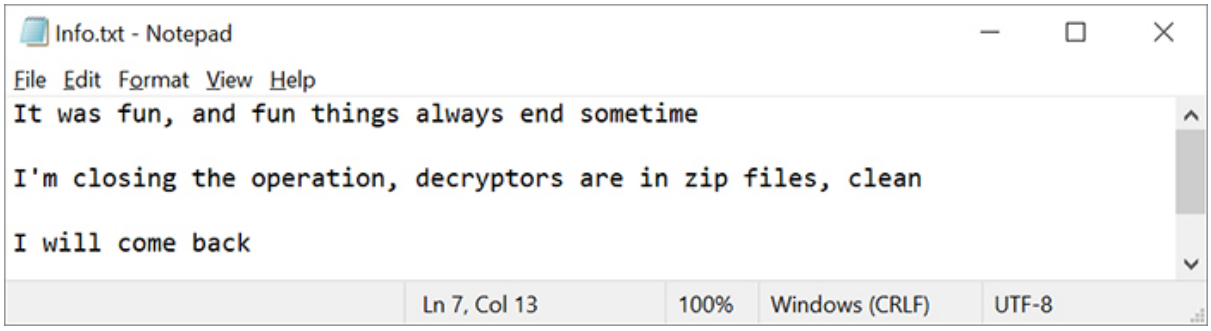
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، این گزارش مورد بررسی قرار گرفته است.

محققان با دانلود فایل مذکور و بکارگیری کلیدهای آن، موفق شدند برخی از فایل‌های رمزگذاری شده در کارزار اخیر AstroLocker را رمزگشایی کنند و تایید نمودند که این رمزگشا کاملاً معتبر می‌باشد. احتمالاً دیگر کلیدهای رمزگشای موجود در این فایل فشرده جهت رمزگشایی فایل‌های رمزگذاری شده در کارزارهای قبلی طراحی شده است.





توسعه‌دهنده باج‌افزار AstraLocker در این خصوص اعلام نموده که با انتشار فایل فشرده حاوی کلیدهای رمزگشا، فعالیت باج‌افزاری را خاتمه داده و این باج‌افزار برای او حکم یک سرگرمی را داشته و چیزهای سرگرم کننده همیشه زمانی به پایان می‌رسند. او دلیل اصلی توقف فعالیت باج‌افزار AstraLocker را فاش نکرد. احتمال آن می‌رود که به دلیل سروصدای زیاد گزارش کارزار اخیر و ترس از تحت پیگرد قرار گرفتن توسط نهادهای قانونی، فعالیت خود را متوقف کرده باشد.



شرکت امنیتی امسی‌سافت (Emsisoft, Ltd.) نیز اعلام کرده که به‌زودی در آینده با انتشار ابزار رمزگشا به قربانیان باج‌افزار در رمزگشایی داده‌ها کمک می‌کند.

در گذشته نیز برای باج‌افزارهایی همچون Avaddon، Ragnarok، SynAck، TeslaCrypt، Crysis، AES-NI، Shade، FilesLocker، Ziggy و FonixLocker ابزارهای رمزگشایی منتشر شده بود.

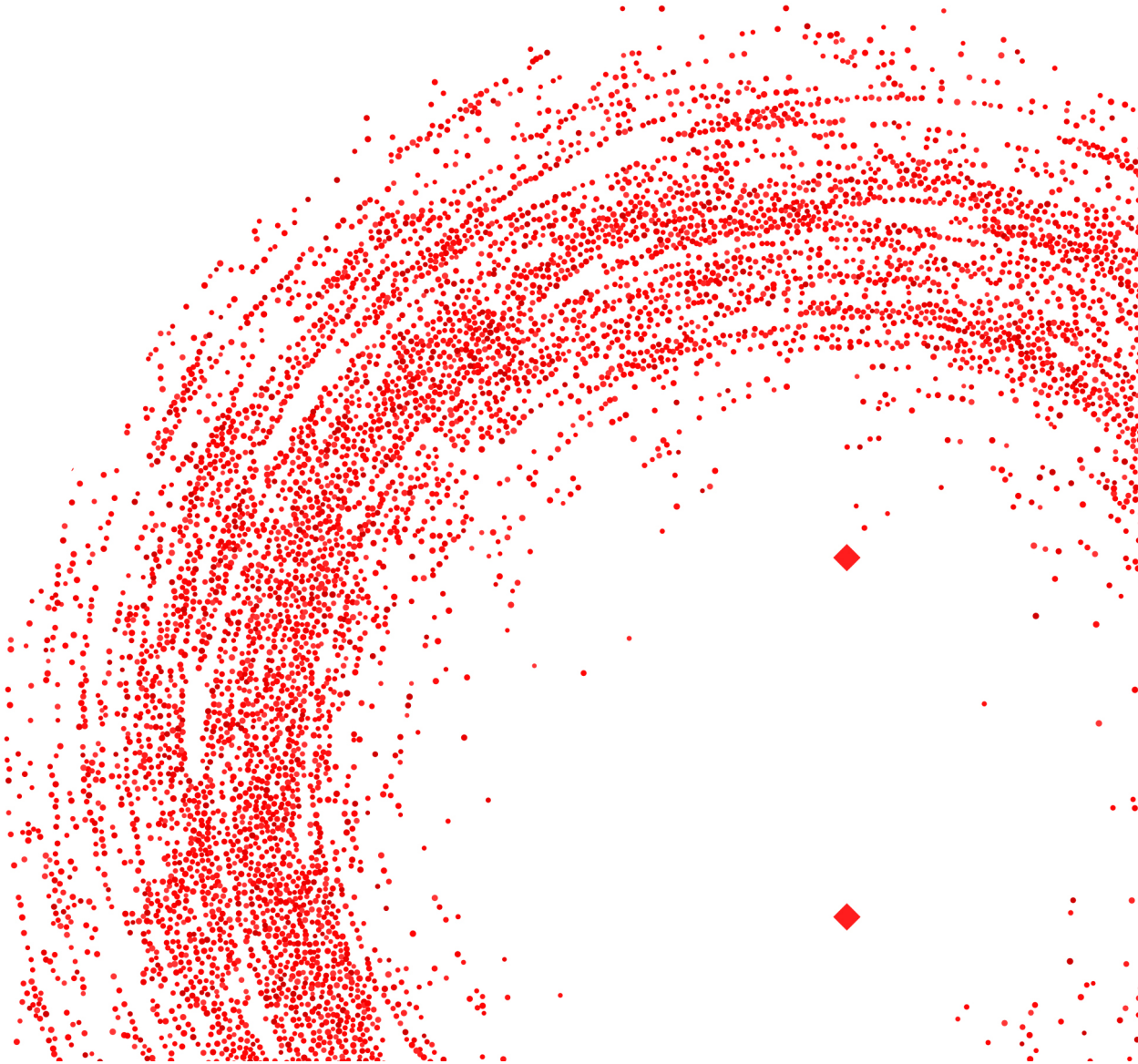
AstraLocker باج‌افزاری است که مستقیماً کد مخرب خود را از طریق فایل Word پیوست شده در ایمیل‌های فیشینگ مستقر می‌کند و به جای ماکروهای VBA از OLE Object استفاده می‌کند. هنگامی که کاربر روی نماد موجود در سند Word دوبار کلیک می‌کند و در پنجره باز شده دکمه Run را انتخاب می‌کند، کد مخرب تعبیه شده اجرا می‌شود. جزئیات بیشتر باج‌افزار AstraLocker در نشانی زیر قابل مطالعه است:

https://newsroom.shabakeh.net/24736/astralocker-v2.html

منبع:

https://www.bleepingcomputer.com/news/security/astralocker-ransomware-shuts-down-and-releases-decryptors/

هشدارهای امنیتی



بهره‌جویی باج‌افزار BlackCat

از سرورهای آسیب‌پذیر Exchange

به گزارش شرکت مایکروسافت (Microsoft Corp.)، گردانندگان باج‌افزار BlackCat با سوءاستفاده از آسیب‌پذیری‌های اصلاح نشده، سرورهای Microsoft Exchange را مورد هدف قرار می‌دهند.

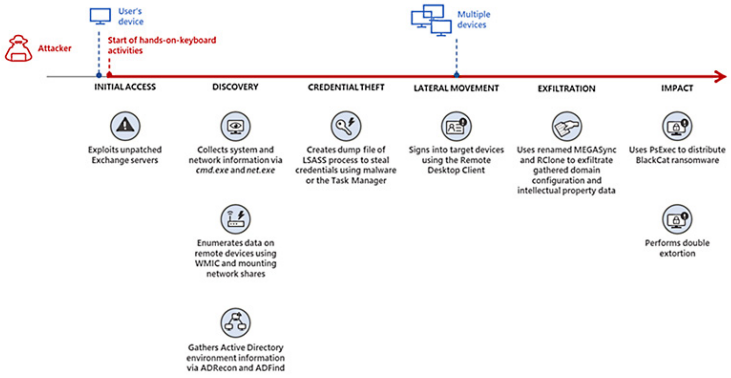
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، گزارش مذکور مورد بررسی قرار گرفته است.

کارشناسان امنیتی مایکروسافت حداقل در یکی از حملات اخیر مشاهده کردند که مهاجمان با نفوذ تدریجی در شبکه قربانی، اطلاعات اصالت‌سنجی و داده‌های سیستم‌ها را به منظور اخاذی مضاعف، استخراج و جمع‌آوری می‌کنند. دو هفته پس از سوءاستفاده از یک سرور Exchange ترمیم نشده به عنوان نقطه ورودی و نفوذ اولیه، مهاجمان کدهای مخرب باج‌افزار BlackCat را از طریق PsExec در سراسر شبکه توزیع کردند.

تیم تحقیقاتی مایکروسافت اعلام نموده در حالی که روش‌های ورودی رایج باج‌افزار BlackCat، برنامه‌های Remote Desktop و اطلاعات اصالت‌سنجی سرقت شده، هستند، در حملات اخیر مشاهده شده که مهاجمان از آسیب‌پذیری‌های سرور Exchange برای دستیابی و نفوذ به شبکه موردنظر خود استفاده می‌کنند.

اگرچه مایکروسافت در گزارش خود به شناسه آسیب‌پذیری Exchange که جهت دسترسی اولیه مورد سوءاستفاده قرار گرفته، اشاره‌ای نکرده، اما این شرکت در اسفند ۱۴۰۰ اقدامات مهارسازی و توصیه‌نامه‌ای امنیتی در خصوص حملات ProxyLogon که در آن نیز از ضعف‌های امنیتی Exchange سوءاستفاده شده، منتشر نموده بود. همچنین با وجود اینکه مایکروسافت در این تحقیق از گروهی که باج‌افزار BlackCat را توزیع

کرده، نامی نبرده، این شرکت می‌گوید چندین گروه مهاجم سایبری اکنون در حملات خود از این باج‌افزار به صورت یک سرویس اجاره‌ای (Ransomware-as-a-Service – به اختصار RaaS) استفاده می‌کنند.



نفوذ از طریق سرور آسیب‌پذیر Exchange

یکی از این گروه‌های مهاجم سایبری با انگیزه‌های مالی، FIN12 است که قبلاً نیز سابقه توزیع باج‌افزارهای Ryuk، Conti و Hive را در حملاتی که عمدتاً سازمان‌های حوزه سلامت را هدف قرار می‌دادند، دارد. با این حال، همانطور که شرکت امنیتی Mandiant در گزارش خود اعلام نموده، گردانندگان FIN12 بسیار سریع‌تر عمل می‌کنند، زیرا گاهی اوقات با صرف نظر نمودن از مرحله سرقت داده، طی کمتر از دو روز برنامه‌های مخرب رمزگذاری خود را در شبکه مورد نظر قرار می‌دهند.

شرکت مایکروسافت در گزارش خود به نشانی زیر اعلام نموده که گروه سایبری FIN12، از اسفند ۱۴۰۰، باج‌افزار BlackCat را به فهرست برنامه‌های مخرب خود جهت توزیع اضافه کرده است.

https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

گمان می‌رود تغییر رویه گروه FIN12 و روی‌آوردن به باج‌افزار BlackCat بجای باج‌افزار Hive، به دلیل افشای عمومی روش‌های رمزگذاری باج‌افزار Hive باشد.

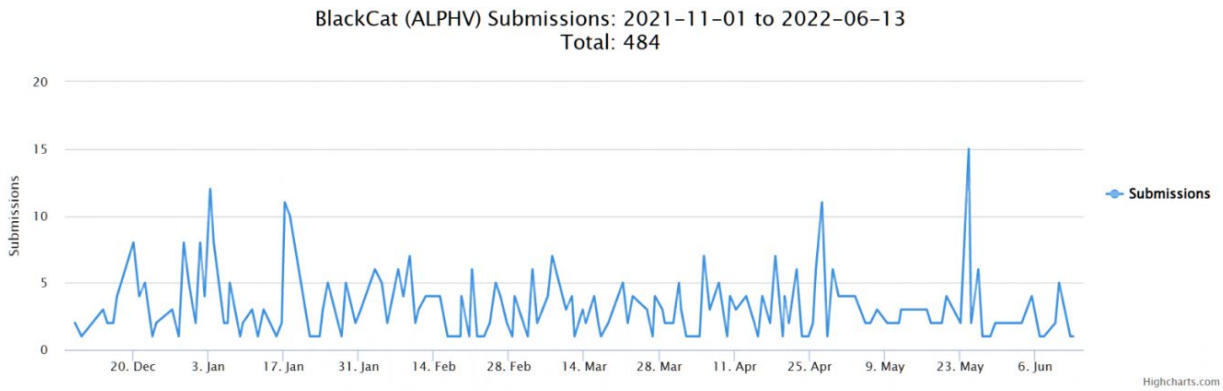
باج‌افزار BlackCat همچنین توسط گروهی به‌عنوان DEV-0504 بکار گرفته شده است. این گروه معمولاً داده‌های سرقت شده را از طریق Stealbit - ابزار مخربی که گروه LockBit به عنوان بخشی از سرویس RaaS خود در اختیار تبهکاران سایبری قرار می‌دهند - استخراج می‌کند.
همچنین از آذر ۱۴۰۰، DEV-0504 از سایر باج‌افزارها نظیر BlackMatter، Conti، LockBit 2.0، Revil و Ryuk استفاده کرده است.
به منظور پیشگیری از حملات باج‌افزار BlackCat، مایکروسافت به مدیران فناوری اطلاعات سازمان‌ها توصیه می‌کند که ضمن بررسی ساختار هویتی خود، هرگونه دسترسی از بیرون به شبکه‌های خود را رصد نموده و همه سرورهای آسیب‌پذیر Exchange سازمان را در اسرع وقت بروزرسانی کنند.

در فروردین ۱۴۰۱، «پلیس فدرال امریکا» (Federal Bureau of Investigation – به اختصار FBI) طی اطلاعیه‌ای به نشانی زیر، درخصوص باج‌افزار BlackCat که در بازه زمانی آبان ۱۴۰۰ تا اسفند ۱۴۰۰، برای رمزگذاری شبکه‌های حداقل ۶۰ سازمان در سراسر جهان مورد استفاده قرار گرفته، هشدار داد.

https://www.ic3.gov/Media/News/2022/220420.pdf

FBI در آن زمان اعلام نمود که بسیاری از برنامه‌نویسان باج‌افزار BlackCat/ALPHV و افرادی که باج‌های دریافتی آن را پولشویی می‌کنند، با گردانندگان باج‌افزار Darkside/Blackmatter در ارتباط می‌باشند که این امر نشان دهنده ارتباط گسترده مهاجمان BlackCat و تجربه و تبحر

آنها در حملات باج‌افزاری است. با این حال، به احتمال زیاد، تعداد واقعی قربانیان BlackCat بسیار بیشتر از ۴۸۰ موردی است که بین آبان ۱۴۰۰ و خرداد ۱۴۰۱ به سایت ID-Ransomware ارسال شده است.



مشروح گزارش مایکروسافت درخصوص اقدامات کاهشی در سرورهای Exchange در نشانی زیر قابل مطالعه می‌باشد:

https://msrc-blog.microsoft.com/2021/03/16/guidance-for-responders-investigating-and-remediating-on-premises-exchange-server-vulnerabilities/

منبع:

https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-blackcat-ransomware/

مهاجمان همچنان به دنبال
بهره‌جویی از Follina

در ۶ خرداد ۱۴۰۱، محققان تیم nao_sec یک آسیب‌پذیری روز صفر جدید را در MSDT گزارش کردند که تمامی نسخ Windows از آن تاثیر می‌پذیرند.

این ضعف امنیتی به مهاجمان اجازه می‌دهد تا کد مخرب را از راه دور (Arbitrary Code Execution) بر روی سیستم‌های آسیب‌پذیر اجرا کنند. این در حالی است که برای اجرای کد مخرب آن حتی به فعال بودن امکانات ماکروها در نرم‌افزارهای Office نیازی نمی‌باشد و مهاجمان با بهره‌جویی از این آسیب‌پذیری، قادر به عبور از تمام محافظت‌های امنیتی، از جمله گزینه Protected View بوده و فرامین مخرب PowerShell از طریق ابزار MSDT اجرا می‌شوند.

این ضعف امنیتی که محققان آن را Follina نامیدند، بعداً شناسه CVE-2022-30190 را دریافت کرد. جزئیات بیشتر درخصوص نحوه عملکرد Follina در نشانی زیر قابل مطالعه می‌باشد:

https://newsroom.shabakeh.net/24338/new-microsoft-office-zero-day-exploit.html

جزئیات فنی ضعف امنیتی CVE-2022-30190:

عملکرد این آسیب‌پذیری در برخی از حملات صورت گرفته را می‌توان به صورت خلاصه اینطور تشریح نمود.

مهاجم یک سند MS Office با پیوندی به یک OLE مخرب خارجی نظیر یک فایل HTML که در سروری راه دور است، ایجاد می‌کند. داده‌های مورد استفاده برای توصیف پیوند در تگی که حاوی پارامترهای (Attribute) خاص می‌باشد، قرار می‌گیرد.

پیوند موجود در ویژگی Target به فایل HTML مذکور اشاره دارد که در داخل آن یک اسکریپت مخرب با بکارگیری یک URL خاص نوشته شده است. هنگامی که اسکریپت باز می‌شود، سند ایجاد شده توسط مهاجم، MSDT را اجرا می‌کند. سپس مهاجم می‌تواند از طریق مجموعه‌ای از پارامترها، هر فرمانی را به این ابزار برای اجرا در سیستم قربانی با امتیازات کاربری که سند را باز کرده است، ارسال کند.

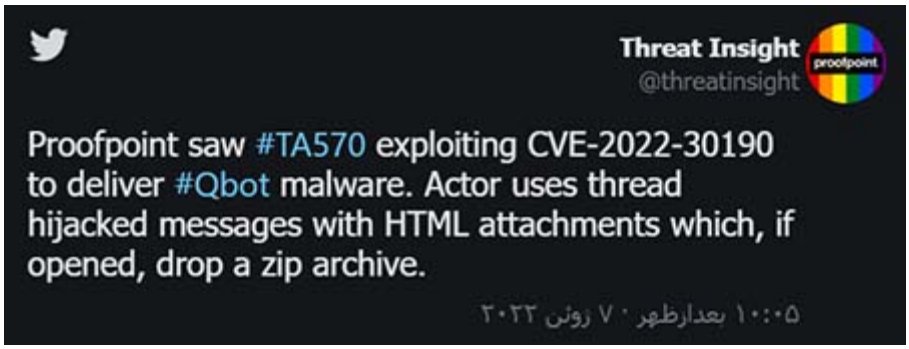
علاوه بر این، حتی اگر سند در حالت محافظت شده (Protected View) باز شود و ماکروها نیز غیرفعال باشند، فرمان را می‌توان ارسال کرد. تا تاریخ ۱۶ خرداد، از دو قالب Microsoft Word (.docx) و قالب (.rtf) جهت بهره‌جویی از ضعف امنیتی CVE-2022-30190 استفاده شده است.

قالب rtf. برای قربانی احتمالی خطرناک‌تر است زیرا اجازه اجرای فرمان مخرب را حتی بدون باز کردن سند به مهاجم می‌دهد و برای این منظور فقط پیش نمایش آن در Windows Explorer کافی است.

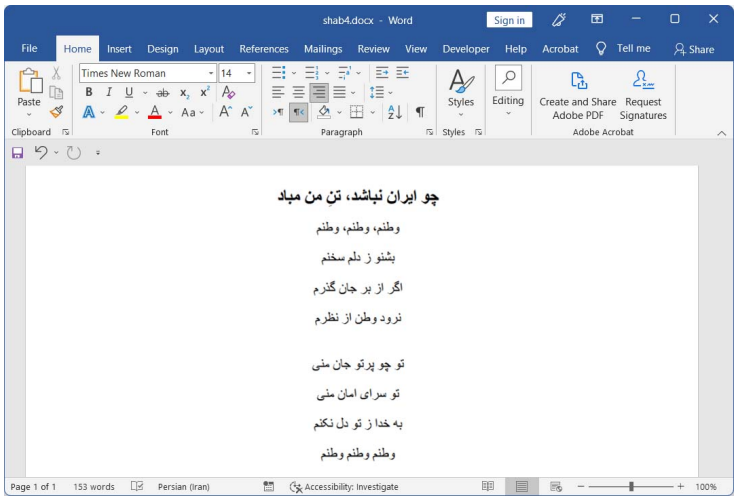
به نقل از محققان، در صورت بهره‌جویی موفقیت آمیز، مهاجمان می‌توانند از ضعف امنیتی Follina برای نصب برنامه‌ها، مشاهده، تغییر یا حذف داده‌ها یا حتی ایجاد حساب‌های کاربری جدید در سطح دسترسی کاربر قربانی، استفاده کنند.

بهره‌جویی گسترده مهاجمان از Follina

پس از افشای این آسیب‌پذیری، ۱۷ خرداد ماه شرکت پروف‌پوینت (Proofpoint, Inc.) از بکارگیری Follina توسط گروه هکری TA570 در حملات گسترده فیشینگ (Phishing) برای توزیع بدافزار QBot که از جمله بدافزارهای ناقل تهدیدات باج‌افزاری هستند، خبر داد که سازمان‌های بسیاری را در جهان مورد هدف قرار داده است.



اخیراً نمونه فایل‌هایی با محتوای فارسی با پسوند docs و با نام shab4.docx به دست کارشناسان شرکت شبکه گستر رسیده که ناقل بهره‌جوی ضعف امنیتی CVE-2022-30190 می‌باشند. اجرای فایل مذکور بر روی دستگاه‌های آسیب‌پذیر منجر به آلوده شدن آن به نوعی جاسوس‌افزار می‌شود. تصویر زیر این نمونه فایل را نشان می‌دهد.



کد مخرب تعبیه شده در این فایل که اسکریپتی Powerhell است، امکاناتی نظیر تصویربرداری از صفحه نمایش کاربر را برای آنها فراهم می‌کند.

اصلاحیه Follina

شرکت مایکروسافت (Microsoft Corp.) ۲۴ خرداد در بروزرسانی ماه ژوئن خود اصلاحیه این ضعف امنیتی را منتشر نمود. بنابراین اکنون که وصله این ضعف امنیتی موجود است و با توجه به بهره‌جویی گسترده مهاجمان از ضعف امنیتی CVE-2022-30190 در سراسر جهان، اکیداً به راهبران امنیتی سازمان‌ها توصیه می‌شود که در اسرع وقت با مراجعه به نشانی‌های زیر بروزرسانی مربوطه را اعمال نمایند.

https://msrc.microsoft.com/update-guide/vulnerability

https://newsroom.shabakeh.net/24462/microsoft-security-update-june-2022.html

منابع:

https://securelist.com/cve-2022-30190-follina-vulnerability-in-msdt-description-and-counteraction/106703/

https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e

https://www.theregister.com/2022/06/09/qbot-malware-microsoft-follina/

https://threatpost.com/follina-exploited-by-state-sponsored-hackers/179890/

https://www.rpnegar.com/blog/follina-and-farsi-docs/

https://www.rpnegar.com/blog/follina-is-widely-being-exploited/

اطلاعیه در خصوص

حملات سایبری ۶ تیر

بر اساس گزارش‌های دریافتی، روز گذشته، ۶ تیر ماه، برخی شرکت‌های فعال در صنعت فولاد کشور هدف حمله سایبری قرار گرفتند.

بر اساس نمونه فایل‌هایی که از سوی تعدادی از مراکز مورد حمله در اختیار شرکت مهندسی شبکه گستر گذاشته شده، سه فایل مخرب با نام‌های Chaplin.exe، Screen.exe و mapping.dat توسط مهاجمان بکار گرفته شده است.

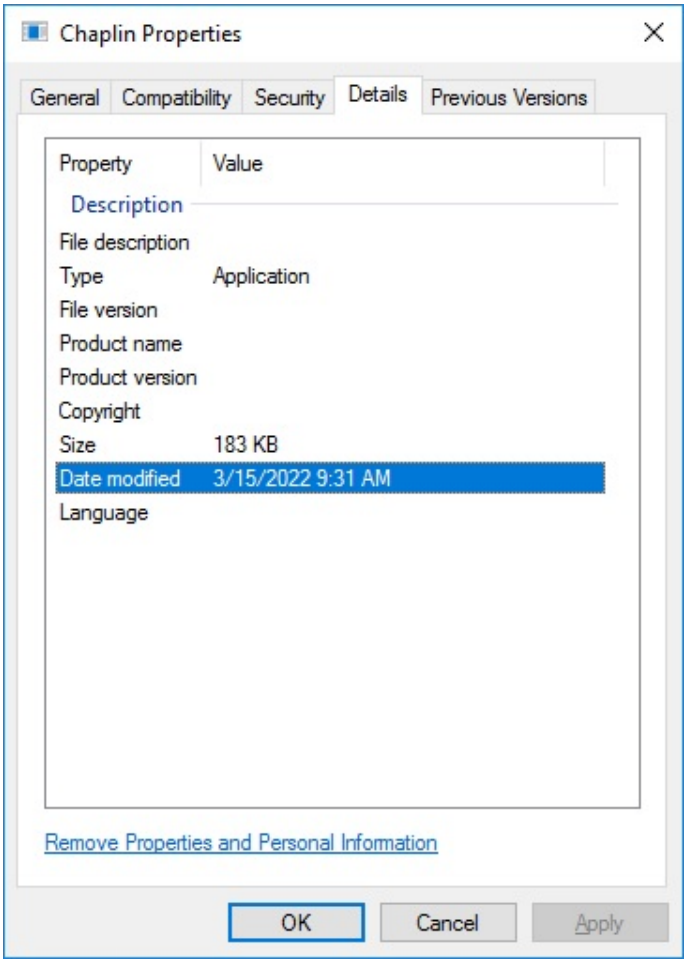
فایل‌های مذکور با نام‌های زیر قابل شناسایی هستند:

McAfee:
RDN/Real Protect-LS
RDN/Generic.dx

Sophos:
Mal/Generic-S

Bitdefender:
Trojan.GenericKD.49256673
Trojan.GenericKD.49258420
Trojan.GenericFCA.Agent.42536

تاریخ ساخت دو فایل Chaplin.exe و Screen.exe به بیش از سه ماه قبل باز می‌گردد که می‌تواند نشانه‌ای از برنامه‌ریزی بلندمدت مهاجمان برای اجرای این حملات باشد.



در جریان حملات روز گذشته تلاش شده بخش Master Boot Record – به اختصار MBR – دستگاه‌های آلوده تخریب شود تا در نتیجه آن فرایند راه‌اندازی دستگاه قربانی دچار اختلال گردد. همچنین، تصویری حاوی پیام مهاجمان نیز بر روی صفحه نمایش دستگاه قربانی ظاهر می‌شود.

به نظر می‌رسد هدف اصلی این مهاجمان رخنه به سامانه‌های صنعتی و سرقت اطلاعات آنها بوده است. مرکز مدیریت راهبردی افتا نیز در این خصوص اطلاعیه‌ای منتشر کرده که در اینجا قابل مطالعه است.

توزیع فایل‌های مخرب، پس از نفوذ اولیه مهاجمان به حداقل یک سرور یا ایستگاه کاری درون شبکه صورت گرفته است. لذا مقاوم‌سازی هر درگاه بالقوه ورودی می‌تواند شانس موفقیت اجرای این گونه حملات را به حداقل برساند. رعایت موارد زیر به راهبران توصیه اکید می‌شود:

- بکارگیری محصولات امنیت نقاط پایانی قدرتمند و به‌روز
- محدودسازی سطوح دسترسی
- بهره‌گیری از دیواره آتش با قواعد سخت‌گیرانه و همچنین بخش‌بندی (Segmentation) شبکه
- اطمینان از نصب کامل اصلاحیه‌های امنیتی
- اعمال سیاست‌های سخت‌گیرانه در خصوص گذرواژه تمامی نام‌های کاربری
- رصد و بررسی هر گونه رخداد مشکوک یا غیرعادی به خصوص بر روی سرورها و دستگاه‌های حساس
- آموزش کاربران در نحوه برخورد با تهدیدات سایبری مبتنی بر مهندسی اجتماعی

شماره تلفن ۴۲۰۵۲ در ساعات اداری و سامانه خدمات پس از فروش و پشتیبانی شرکت مهندسی شبکه گستر به نشانی my.shabakeh.net در طول شبانه روز نیز در اختیار مشترکین گرامی است تا مشکلات و مسائل خود را مطرح کرده و پاسخ‌ها و راهنمایی‌های لازم را دریافت نمایند.

هشدار در خصوص
ادامه بهره‌جویی از Log4Shell

به تازگی مرکز CISA ایالت متحده در گزارشی هشدار داده که مهاجمان همچنان در حال بهره‌جویی از آسیب‌پذیری Log4Shell در محصولات VMware Horizon و VMware Unified Access Gateway - به اختصار UAG - می‌باشند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، گزارش مذکور مورد بررسی قرار گرفته است.

Log4Shell یا LogJam آسیب‌پذیری است که در کتابخانه Log4j در اواخر پاییز سال گذشته کشف شد و دارای شناسه CVE-2021-44228 می‌باشد. بهره‌جویی گسترده از ضعف امنیتی مذکور، پس از انتشار یک نمونه اثبات‌گر (Proof-of-Concept – به اختصار PoC) از حدود ۱۸ آذر ۱۴۰۰ آغاز شد.

این آسیب‌پذیری، امکان اجرای کد از راه دور (Remote Code Execution – به اختصار RCE) را برای مهاجمان فراهم می‌کند و سوءاستفاده از آن نیازی به تخصص فنی بالا و احراز هویت ندارد. مهاجمان می‌توانند با بهره‌جویی از Log4Shell بصورت از راه دور کنترل سرورهای آسیب‌پذیر را در اختیار گرفته و در ادامه اقدام به انجام انواع امور مخرب نظیر گسترش آلودگی در سطح شبکه نمایند.

بر اساس گزارش اخیر CISA، مهاجمان در حال بهره‌جویی از Log4Shell برای نفوذ به محصولات آسیب‌پذیر VMware و در ادامه رخنه به شبکه سازمان‌ها می‌باشند.

این مهاجمان پس از نفوذ به شبکه، اقدام به استقرار انواع مختلفی از بدافزارها نموده و در مواردی صدها گیگابایت اطلاعات حساس قربانیان را سرقت می‌کنند. برخی از این بدافزارها امکان برقراری ارتباط با سرورهای کنترل و فرمان‌دهی (Command and Control – به اختصار C2) را برای مهاجمان فراهم می‌کنند.

اکیداً به راهبران سرورهای VMware توصیه می‌شود تا نسبت به اعمال بروزرسانی‌های مرتبط با ضعف‌امنیتی CVE-2021-44228 اطمینان حاصل کنند. همچنین ضروری است راهبران امنیتی در اسرع وقت سیستم‌های بالقوه هک شده را از شبکه جدا کرده و لاگ‌ها و سوابق مربوطه را جمع‌آوری و بررسی نمایند.

مشروح توصیه‌نامه امنیتی CISA در نشانی زیر قابل مطالعه می‌باشد:

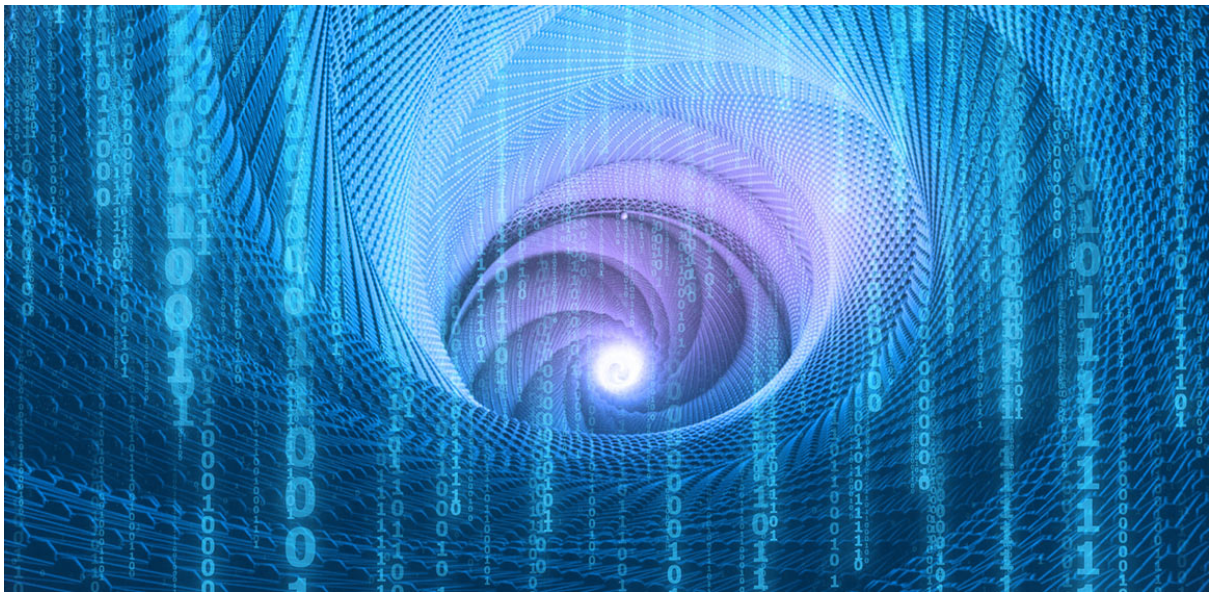
https://www.cisa.gov/uscert/ncas/alerts/aa22-174a

منبع:

https://www.bleepingcomputer.com/news/security/cisa-log4shell-exploits-still-being-used-to-hack-vmware-servers/

CVE-2022-26925؛

مهاجمان در حال بهره‌جویی از آن



مرکز CISA، جمعه ۱۰ تیر، یک ضعف امنیتی دیگر را به «فهرست آسیب‌پذیری‌های در حال بهره‌جویی» یا همان Known Exploited Vulnerabilities Catalog اضافه کرد.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، ضعف امنیتی مذکور مورد بررسی قرار گرفته است.

آسیب‌پذیری مذکور، ضعفی به شناسه CVE-2022-26925 است که همان‌طور که پیش‌تر نیز در این خبر به آن پرداختیم در ۲۰ اردیبهشت سال جاری توسط مایکروسافت وصله شد.

این آسیب‌پذیری، ضعفی از نوع «جعل» (Spoofing) در بخش LSA سیستم عامل Windows است و از قبل از عرضه اصلاحیه توسط مایکروسافت، مورد بهره‌جویی مهاجمان قرار گرفته است.

بر طبق توصیه‌نامه مایکروسافت تمامی نسخ سیستم عامل Windows از آسیب‌پذیری مذکور متأثر می‌شوند.

جزییات بیشتر در خصوص CVE-2022-26925 و وصله‌های آن در اینجا قابل دریافت و مطالعه است.

فهرست کامل Known Exploited Vulnerabilities Catalog نیز در اینجا در دسترس است.

انتشار باج‌افزار؛
این بار از طریق OLE Object

اخیراً نسخه دوم باج‌افزاری به نام AstraLocker از طریق فایل‌های Word پیوست شده به ایمیل‌های فیشینگ در حال انتشار است. برخلاف نمونه‌های مشابه، کد مخرب نه با بکارگیری ماکرو بلکه با استفاده از OLE Object در سند Word اجرا می‌شود.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، این باج‌افزار مورد بررسی قرار گرفته است.

محققان پس از تحلیل کد باج‌افزار AstraLocker بر این باورند که از کد باج‌افزار Babuk که در شهریور ۱۴۰۰ افشا شد، بر گرفته شده است. علاوه بر این، یکی از نشانی‌های کیف پول Monero که در اطلاعیه باج‌گیری (Ransom Note) باج‌افزار AstraLocker آمده است به گردانندگان باج‌افزار Chaos مرتبط است. این می‌تواند به این معنی باشد که گردانندگان، شرکا و هکرهای یکسانی پشت هر دو باج‌افزار هستند که چندان هم غیر معمول نیست. با مقایسه تاکتیک‌های بکارگرفته شده آن با کارزارهای جدید، به نظر نمی‌رسد این باج‌افزار پیچیده باشد بلکه مهاجمان آن بیشتر مصمم هستند تا حد امکان حداکثر تعداد کاربر را در سریع‌ترین زمان مورد حمله قرار دهند.

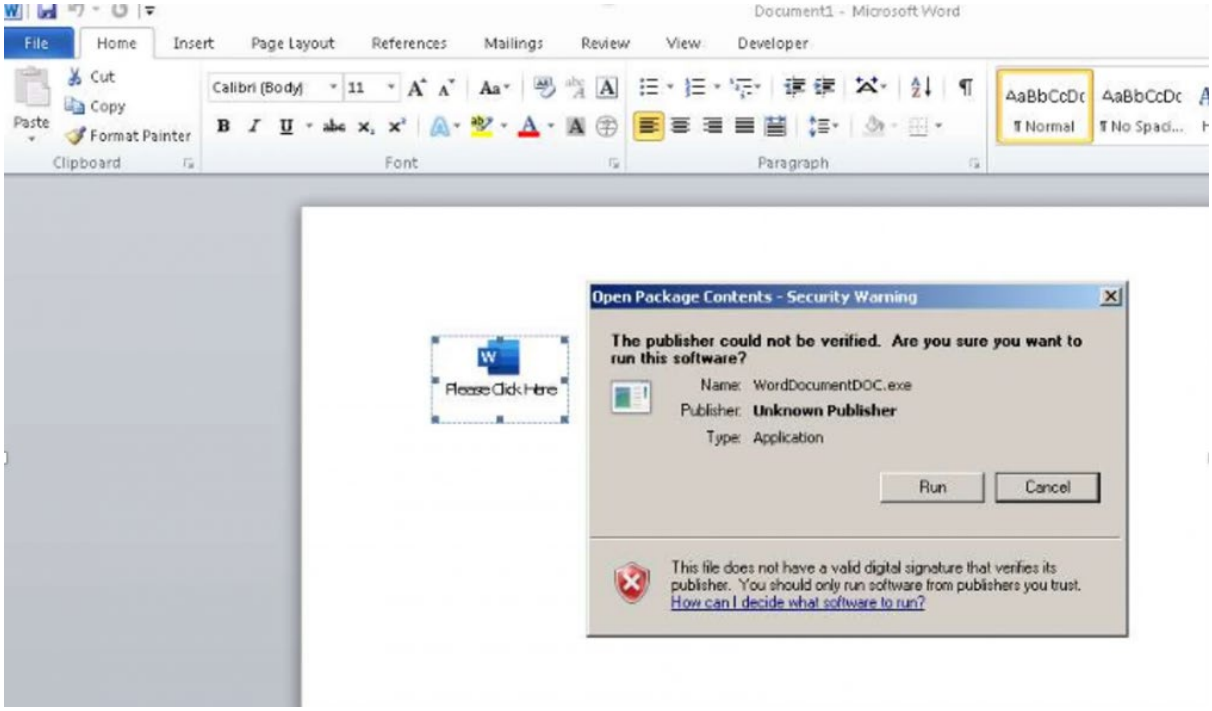
تصویر زیر نمونه‌ای از اطلاعیه باج‌گیری این باج‌افزار را نمایش می‌دهد:

این باج‌افزار به جای سوءاستفاده از قابلیت ماکروهای VBA در نرم‌افزارهای Word که در توزیع بدافزارها متداول است، از OLE Object بهره می‌گیرد.

یکی دیگر از انتخاب‌های عجیب گردانندگان این باج‌افزار، استفاده از یک فشرده‌ساز قدیمی به نام SafeEngine Shielder v2.4.0.0 برای مبهم‌سازی و فشرده‌سازی فایل اجرایی است که مهندسی معکوس را تقریباً غیرممکن می‌سازد. این فشرده‌ساز آنقدر قدیمی است که نسخه معتبر آن دیگر به فروش نمی‌رسد، به این معنی که مهاجمان احتمالاً نسخه قفل شکسته و غیرمجاز آن را دریافت کرده‌اند.

محققان با بررسی حملات این باج‌افزار به این نکته پی بردند که تکنیک استفاده شده توسط گردانندگان آن، ارسال انبوه ایمیل‌های فیشینگ به دنبال آلوده‌سازی حداکثر دستگاه‌ها و دریافت سریع باج می‌باشد. به عبارت دیگر مهاجمان AstraLocker زمانی را صرف شناسایی اهداف خود و کشف فایل‌های ارزشمند آنها نکرده و در عوض به‌صورت انبوه اقدام به ارسال ایمیل‌های ناقل این باج‌افزار می‌کنند.

گردانندگان AstraLocker 2.0 در حملات خود از یک فایل Microsoft Word که یک OLE Object حاوی کد باج‌افزار را در خود جای داده است، استفاده می‌کنند. فایل اجرایی تعبیه شده دارای نام «WordDocumentDOC.exe» می‌باشد. تنها در صورتی باج‌افزار فعال می‌شود که کاربر روی نماد موجود در سند دوبار کلیک کند و با کلیک روی دکمه Run با اجرای فایل تعبیه شده مذکور موافقت کند.



این باج‌افزار پروسه‌هایی را که می‌توانند مانع رمزگذاری شوند، متوقف نموده و تلاش می‌کند نسخ Shadow Copy و سایر نسخ پشتیبان را حذف کند تا برگرداندن اطلاعات برای قربانی امکان‌پذیر نباشد. همچنین پروسه‌های مربوط به محصولات امنیتی نظیر ضدویروس را متوقف می‌سازد. محتویات Recycle Bin را نیز به جای رمزگذاری به سادگی حذف می‌کند.

باج‌افزار همچنین دارای سازوکارهای ضد تحلیل نظیر عدم اجرا بر روی ماشین‌های مجازی (Virtual Machines) می‌باشد.

برخی از علائم آلودگی (Indicators-of-Compromise – به اختصار IoC) این باج‌افزار به صورت است:

SHA256 Hash:	File Type
cf3bdf0f8ea4c8ece5f5a76524ab4c81fea6c3a1715b5a86b3ad4d397fca76f3	AstraLocker 2.0 Ransomware
b0a010e5a9b353a11fb664501de91fc47878d89bf97cb57bc03428c7a45981b9	AstraLocker 2.0 Ransomware
17ea24ce8866da7ef4a842cba16961eafba89d526d3efe5d783bb7a30c5d1565	AstraLocker 2.0 Ransomware
08565f345878369fdbbcf4a064d9f4762f4549f67d1e2aa3907a112a5e5322b6	AstraLocker 2.0 Ransomware

5c061e188979d3b744a102d5d855e845a3b51453488530ea5dca6b098add2821	AstraLocker 2.0 Ransomware
60167b6a14b7da2257cb6cbdc7f1ebcb4bdfa16c76cc9a7539c9b8d36478d127	Malicious Word Document
71ba916a7f35fe661cb6affc183f1ce83ee068dbc9a123663f93acf7b5a4263e	Malicious Word Document

ضمن بکارگیری راهکارهای امنیتی قدرتمند و به‌روز در گام نخست به مدیران فناوری اطلاعات توصیه می‌شود که به طور منظم در آموزش انواع حملات باج‌افزاری، اصول و تکنیک‌های امنیت اطلاعات، خطرات، آسیب‌پذیری‌ها و حملات فیشینگ به کاربران سازمان بکوشند. آگاهی‌سازی کاربران نقش کلیدی در بی‌اثر کردن این نوع تهدیدات دارد.

جزئیات بیشتر حملات این باج‌افزار در نشانی زیر قابل مطالعه می‌باشد:

https://blog.reversinglabs.com/blog/smash-and-grab-astralocker-2-pushes-ransomware-direct-from-office-docs

منبع:

https://blog.reversinglabs.com/blog/smash-and-grab-astralocker-2-pushes-ransomware-direct-from-office-docs

نگاهی به باج‌افزار

MedusaLocker

باج‌افزاری با نام MedusaLocker در حال انتشار است که مهاجمان آن از طریق پودمان Remote Desktop Protocol – به اختصار RDP – یا کارزارهای ایمیل، به شبکه قربانیان نفوذ می‌کنند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، باج‌افزار مذکور مورد بررسی قرار گرفته است.

باج‌افزار MedusaLocker در حملات خود اقدام به رمزگذاری داده‌های قربانیان نموده و در هر یک از پوشه‌های حاوی فایل رمزگذاری شده، یک اطلاعیه باج‌گیری (Ransom Note) به همراه اطلاعات تماس و دستورالعمل نحوه ارتباط با مهاجمان را در اختیار قربانی قرار می‌دهد. در این اطلاعیه باج‌گیری از قربانیان خواسته می‌شود تا مبلغ باج مطالبه شده را به یک آدرس کیف پول بیت کوین خاص ارسال کنند. به نظر می‌رسد MedusaLocker یک سرویس اجاره‌ای (Ransomware-as-a-Service – به اختصار RaaS) است که باج پرداخت شده را تقسیم می‌کند. مدل‌های معمولی RaaS شامل توسعه‌دهنده باج‌افزار و شرکای مختلف آنها است که باج‌افزار را در سیستم‌های قربانی مستقر می‌کنند. به نظر می رسد در MedusaLocker باج پرداخت شده همواره بین آنها تقسیم می‌شود به گونه‌ای که ۵۵ تا ۶۰ درصد باج را شرکا و باقی‌مانده مبلغ را توسعه‌دهنده باج‌افزار دریافت می‌کند.

جزییات فنی

گردانندگان این باج‌افزار اغلب از طریق پیکربندی‌های آسیب‌پذیر در پودمان RDP، ایمیل‌های فیشینگ و یا کارزارهای ایمیلی به شبکه قربانیان نفوذ پیدا می‌کنند.

این باج‌افزار از فایلی از نوع Batch برای اجرای یک اسکریپت مبتنی بر PowerShell (invoke-ReflectivePEInjection) استفاده می‌کند. اسکریپت مذکور، با ویرایش مقدار EnableLinkedConnections در رجیستری دستگاه قربانی، باج‌افزار را در سراسر شبکه منتشر می‌کند. سپس از روی دستگاه آلوده، با بکارگیری پودمان‌های Internet Control Message Protocol - به اختصار ICMP – و Server Message Block – به اختصار SMB – اقدام به شناسایی سرورها و شبکه‌های متصل و پوشه‌های اشتراکی می‌کند.

در ادامه باج‌افزار MedusaLocker:

- با راه‌اندازی مجدد سرویس LanmanWorkstation، امکان ویرایش رجیستری را برای خود فراهم می‌کند.
- پروسه‌های برنامه‌های متداول حسابداری و نرم‌افزارهای امنیتی را متوقف می‌کند.
- برای جلوگیری از شناسایی شدن توسط راهکارهای امنیتی، دستگاه را در حالت Safe Mode راه‌اندازی مجدد می‌کند.
- فایل‌های قربانی را با الگوریتم AES-256 رمزگذاری نموده و سپس کلید حاصل را با یک کلید عمومی RSA-2048 رمزنگاری می‌کند.
- هر ٦٠ ثانیه مجدداً اجرا شده و همه فایل‌ها را به جز آنهایی که برای عملکرد دستگاه قربانی حیاتی هستند و آنهایی که قبلاً رمزگذاری شده را رمزنگاری می‌کند.
- با کپی کردن یک فایل اجرایی (svhost.exe یا svhostt.exe) در مسیر %APPDATA%\Roaming از طریق فرامین Schedule Task پروسه مخرب باج‌افزار را هر ۱۵ دقیقه فراخوانی می‌کند تا بدین ترتیب موجب ماندگاری باج‌افزار بر روی دستگاه شود.
- نسخه‌های پشتیبان محلی و نسخه‌های Shadow را حذف کرده و با غیرفعال کردن گزینه‌های بازیابی موجب غیرممکن ساختن بازگردانی سیستم می‌شود.

اطلاعیه باج‌گیری که باج‌افزار در هر یک از پوشه‌های حاوی فایل رمزگذاری شده قرار می‌دهد، نحوه ارتباط با مهاجمان را تشریح می‌کند که معمولاً در آن یک یا چند آدرس ایمیل را برای قربانیان ارسال می‌کند که از طریق آن می‌توانند با مهاجمان تماس بگیرند. به نظر می‌رسد میزان باج مطالبه شده توسط این باج‌افزار بسته به وضعیت مالی قربانی، متفاوت است.

از جمله پسوندهایی که در جریان این حملات به فایل‌های رمزگذاری شده الصاق می‌شود، می‌توان به موارد زیر اشاره کرد:

Encrypted File Extensions:			
.1btc	.matlock20	.marlock02	.readinstructions
.bec	.mylock	.jpz.nz	.marlock11
.cn	.NET1	.key1	.fileslocked
.datalock	.NZ	.lock	.lockfilesUS
.deadfilesgr	.tyco	.lockdata7	.rs
.faratak	.uslockhh	.lockfiles	.tyco
.fileslock	.zoomzoom	.perfection	.uslockhh
.marlock13	n.exe	.Readinstruction	.marlock08
.marlock25	nt_lock20	.READINSTRUCTION	
.marlock6	.marlock01	.ReadInstructions	

همچنین اسامی فایل‌های مربوط به اطلاعیه باج‌گیری که این باج‌افزار از آنها استفاده کرده، عبارتند از:

Ransom Note File Names:

how_to_ recover_data.html	how_to_recover_data.html.marlock01
instructions.html	READINSTRUCTION.html
!!!HOW_TO_DECRYPT!!!	How_to_recovery.txt
readinstructions.html	readme_to_recover_files
recovery_instructions.html	HOW_TO_RECOVER_DATA.html
recovery_instruction.html	

برخی از نشانی‌هایی که مهاجمان این باج‌افزار برای ارسال ایمیل به قربانیان خود از آن استفاده کرده‌اند، به شرح زیر می‌باشد:

Email Addresses:	
willyhill1960@tutanota[.]com	unlockfile@cock[.]li
zlo@keem[.]ne	unlockmeplease@airmail[.]cc
zlo@keemail[.]me	unlockmeplease@protonmail[.]com
zlo@tfwno[.]gf	willyhill1960@protonmail[.]com
support@ypsotecs[.]com	support@imfoodst[.]com
traceytevin@protonmail[.]com	support@itwgset[.]com
unlock_file@aol[.]com	support@novibmaker[.]com
unlock_file@outlook[.]com	support@securycasts[.]com
support@exoprints[.]com	rewmiller-1974@protonmail[.]com
support@exorints[.]com	rpd@keemail[.]me
support@fanbridges[.]com	soterissylla@wyseil[.]com
support@faneridges[.]com	support@careersill[.]com
perfection@bestkoronavirus[.]com	karloskolorado@tutanota[.]com
pool1256@tutanota[.]com	kevynchaz@protonmail[.]com
rapid@aaathats3as[.]com	korona@bestkoronavirus[.]com
rescuer@tutanota[.]com	lockPerfection@gmail[.]com
ithelp01@decorous[.]cyou	lockperfection@gmail[.]com
ithelp01@wholeness[.]business	mulierfagus@rdhos[.]com
ithelp02@decorous[.]cyou	[rescuer]@cock[.]li
ithelp02@wholness[.]business	107btc@protonmail[.]com
ithelpresotre@outlook[.]com	33btc@protonmail[.]com
cmd@jitjat[.]org	777decoder777@protonmail[.]com
coronaviryz@gmail[.]com	777decoder777@tfwno[.]gf
dec_helper@dremno[.]com	andrewmiller-1974@protonmail[.]com
dec_helper@excic[.]com	angelomartin-1980@protonmail[.]com
dec_restore@prontonmail[.]com	ballioverus@quocor[.]com
dec_restore1@outlook[.]com	beacon@jitjat[.]org
bitcoin@sitesoutheat[.]com	beacon@msgsafe[.]io
briansalgado@protonmail[.]com	best666decoder@tutanota[.]com
bugervongir@outlook[.]com	bitcoin@mobtouches[.]com
best666decoder@protonmail[.]com	encrypt2020@outlook[.]com
decoder83540@cock[.]li	fast-help@inbox[.]lv
decra2019@gmail[.]com	fuc_ktheworld1448@outlook[.]com

diniaminius@winrof[.]com	fucktheworld1448@cock[.]li
dirhelp@keemail[.]me	gartaganisstuffback@gmail[.]com
emaila.elaich@iav.ac[.]ma	gavingonzalez@protonmail[.]com
emd@jitjat[.]org	gsupp@onionmail[.]org
encrypt2020@cock[.]li	gsupp@techmail[.]info
best666decoder@protonmail[.]com	helper@atacdi[.]com
ithelp@decorous[.]cyou	helper@buildingwin[.]com
ithelp@decorous[.]cyoum	helprestore@outlook[.]com
ithelp@wholeness[.]business	helptorestore@outlook[.]com

بعضی از نشانی‌های IP مورد استفاده توسط این باج‌افزار به شرح زیر است با این توضیح که بسیاری از این نشانی‌های مذکور چندین سال قدمت دارند و ممکن است در زمان حال دیگر تحت کنترل مهاجمان این باج‌افزار قرار نداشته باشند.

IP Addresses:
195.123.246.138
138.124.186.221
159.223.0.9
45.146.164.141
185.220.101.35
185.220.100.249
50.80.219.149
185.220.101.146
185.220.101.252
179.60.150.97
84.38.189.52
94.232.43.63
108.11.30.103
194.61.55.94
198.50.233.202
40.92.90.105
188.68.216.23

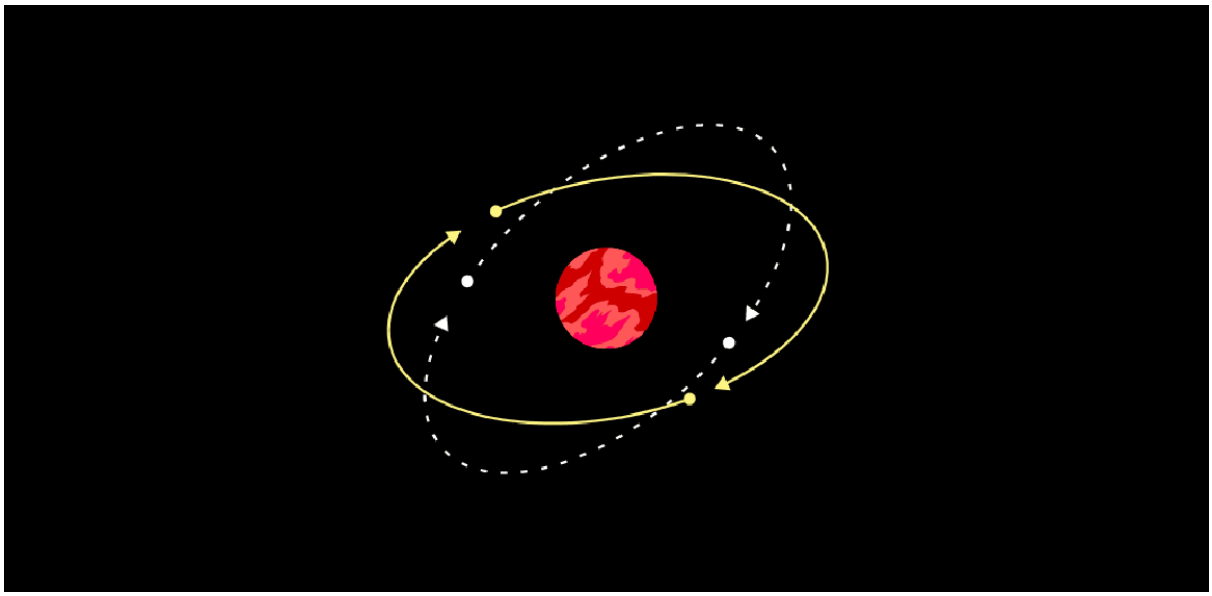
87.251.75.71
196.240.57.20
198.0.198.5
194.5.220.122
194.5.250.124
194.5.220.124
104.210.72.161

منبع:

https://www.cisa.gov/uscert/ncas/alerts/aa22-181a

بدافزار OrBit؛

سارق اطلاعات دستگاه‌های تحت Linux



به تازگی بدافزاری کشف شده که با دسترسی غیرمجاز (Backdoor) اقدام به سرقت مخفیانه اطلاعات از سیستم‌های تحت Linux و آلوده‌کردن تمام پروسه‌های در حال اجرا در این دستگاه‌ها می‌کند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، بدافزار مذکور مورد بررسی قرار گرفته است.

این بدافزار که توسط محققان امنیتی، OrBit نامیده شده، کنترل کتابخانه‌های مشترک را در اختیار گرفته و با تغییر متغیر LD_PRELOAD در دستگاه‌های آسیب‌پذیر، فراخوانی‌های توابع را رهگیری می‌کند.

بدافزار OrBit با بکارگیری دو روش مختلف ضمن مخفی نمودن خود از دید راهکارهای امنیتی، از شناسایی و حذف شدن خود جلوگیری نموده و در سیستم آسیب‌پذیر ماندگار می‌شود. OrBit همچنین می‌تواند به عنوان یک مولفه موقتی در هنگام کپی در حافظه موسوم به Shim-memory مورد استفاده قرار گیرد. در برنامه‌نویسی کامپیوتری، حافظه موسوم به Shim-memory، کتابخانه‌ای است که بی‌واسطه فراخوانی‌های API را رهگیری نموده و آرگومان‌های ارسال شده را تغییر می‌دهد، خود عملیات را مدیریت نموده یا عملیات را به جای دیگری هدایت می‌کند.

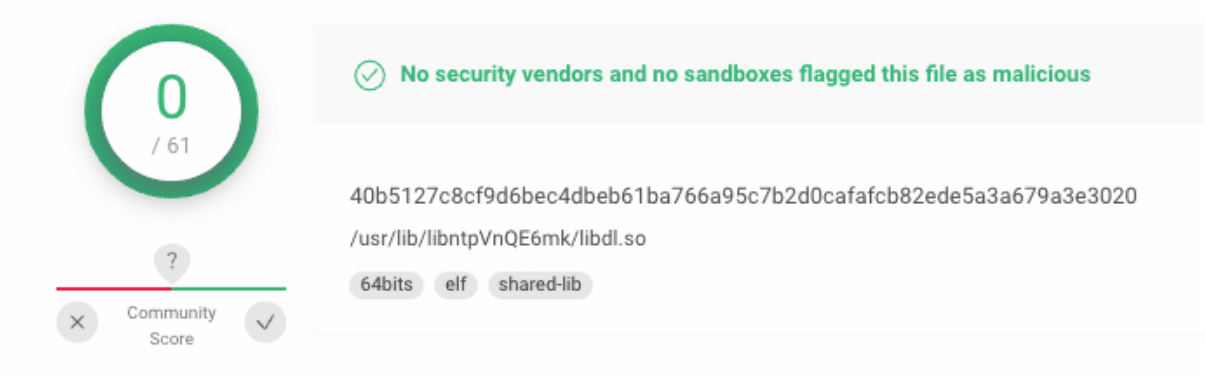
همچنین این بدافزار متکی به توابع مختلفی برای دورزدن ضدویروس‌ها، کنترل رفتار پروسه‌ها و حفظ ماندگاری در سیستم از طریق آلوده کردن پروسه‌های جدید و پنهان کردن فعالیت و حضور در سطح شبکه می‌باشد.

به عنوان مثال، هنگامی که OrBit به یک پروسه در حال اجرا نفوذ می‌کند، می‌تواند با دستکاری خروجی و فیلتر کردن موارد لاگ شده، هرگونه اثر و ردپای خود را پنهان کند.

محققان امنیتی بر این باورند که این بدافزار تکنیک‌های پیشرفته‌ای را جهت فرار از راهکارهای تشخیصی پیاده‌سازی نموده و با بکارگیری توابع کلیدی روی دستگاه ماندگار می‌شود.

همچنین از طریق پودمان SSH دسترسی از راه دور را برای مهاجمان فراهم نموده و ضمن جمع‌آوری اطلاعات اصالت‌سنجی، فرامین TTY را تحت رصد قرار می‌دهد.

هنگامی که بدافزار نصب شد، تمامی پروسه‌ها از جمله پروسه‌های جدیدی که بر روی دستگاه در حال اجرا هستند، آلوده می‌شود. در ابتدا زمانی که بدافزار کشف شد، فایل‌های مرتبط با آن توسط ضدویروس‌ها قابل شناسایی نبود. اما به مرور تعداد محصولات ضدویروسی که قادر به شناسایی آن هستند، افزایش یافت. به نحوی که در زمان انتشار این خبر و به استناد از سایت VirusTotal بیش از نیمی از محصولات ضدویروس قادر به شناسایی آن می‌باشند.



گزارش پویش فایل‌های مذکور در سایت VirusTotal در نشانی‌های زیر قابل مشاهده می‌باشد.

https://www.virustotal.com/gui/file/40b5127c8cf9d6bec4dbeb61ba766a95c7b2d0cafafcb82ede5a3a679a3e3020

https://www.virustotal.com/gui/file/f1612924814ac73339f777b48b0de28b716d606e142d4d3f4308ec648e3f56c8

OrBit اولین بدافزار تحت Linux نیست که از قابلیت‌های متعددی جهت مخفی شدن از راهکارهای تشخیصی استفاده می‌کند و ترفندهایی را جهت آلوده‌سازی کامل دستگاه‌ها و دسترسی غیرمجاز بکار می‌گیرد.

بدافزار Symbiote نیز از LD_PRELOAD برای راه‌اندازی خود در پروسه‌های در حال اجرا استفاده نموده و علاوه بر آلوده‌سازی آنها، هیچ نشانه‌ای از خود باقی نمی‌گذارد. BPFDoor، بدافزار دیگری است که اخیراً شناسایی شده و سیستم‌های تحت Linux را هدف قرار می‌دهد. این بدافزار با تظاهر کردن به عنوان یک Linux daemon اقدام به مخفی شدن نموده و به این دلیل تا بیش از پنج سال شناسایی نشد. هر دوی این سویه‌ها از تکنیکی موسوم به Berkeley Packet Filter - به اختصار BPF - برای رصد و دستکاری ترافیک شبکه استفاده می‌کنند که موجب پنهان شدن کانال‌های ارتباطی آنها از راهکارهای امنیتی می‌شود.

سومین بدافزار تحت Linux، روت‌کیتی به نام Syslogk است که اخیراً توسط محققان آواست (Avast Software s.r.o) شناسایی شده و می‌تواند ماژول‌های خود را به اجبار در هسته Linux ماشین آلوده قرار داده و پوشه‌ها و ترافیک شبکه را پنهان کند تا بدین ترتیب از شناسایی شدن جلوگیری کند.

با وجود اینکه OrBit اولین یا اصلی‌ترین بدافزاری نیست که Linux را مورد هدف قرار می‌دهد، اما همچنان دارای قابلیت‌هایی است که آن را از سایر بدافزارها متمایز می‌کند. این بدافزار اطلاعات را با بکارگیری فرامین و ابزارهای مختلفی سرقت نموده و آنها را در فایل‌های خاص روی دستگاه ذخیره می‌کند. علاوه بر این، به صورت گسترده‌ای از فایل‌ها به منظور ذخیره حجم زیادی از داده‌ها بهره می‌گیرد؛ چیزی که قبلاً در میان بدافزارهای تحت Linux چندان متداول نبوده است.

برخی از علائم آلودگی (Indicators-of-Compromise – به اختصار IoC) این بدافزار به شرح زیر است:

Hash:	File:
f1612924814ac73339f777b48b0de28b716d606e142d4d3f4308ec648e3f56c8	Dropper
40b5127c8cf9d6bec4dbeb61ba766a95c7b2d0cafafcb82ede5a3a679a3e3020	Payload

جزئیات بیشتر این بدافزار در نشانی زیر قابل مطالعه می‌باشد:

https://www.intezer.com/blog/incident-response/orbit-new-undetected-linux-threat/

منبع:

https://www.bleepingcomputer.com/news/linux/new-stealthy-orbit-malware-steals-data-from-linux-devices/

Raspberry Robin؛

مدت‌ها پنهان از نگاه محصولات امنیتی

محققان امنیت سایبری نسبت به وقوع کارزاری رو به رشد به نام Raspberry Robin که اقدام به توزیع بدافزاری با عملکرد کرم (Worm) در سیستم‌های تحت Windows می‌کند، هشدار داده‌اند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، این بدافزار مورد بررسی قرار گرفته است.

محققان شرکت سایبریزن (Cybereason, Inc.) این کرم را تهدیدی «مستمر» و «درحال گسترش» توصیف نموده‌اند که تعدادی قربانی نیز در اروپا داشته است.

این بدافزار کرم مانند از طریق حافظه‌های قابل حمل همچون دستگاه‌های USB که حاوی یک فایل مخرب LNK. می‌باشند، منتشر می‌شود و از دستگاه‌های آسیب‌پذیر ذخیره‌سازی متصل به شبکه (Network Attached Storage – به اختصار NAS) ساخت شرکت کیونپ (QNAP Systems, Inc.) برای کنترل و فرمان‌دهی استفاده می‌کند. این بدافزار اولین بار توسط محققانی از Red Canary در اردیبهشت ۱۴۰۱ شناسایی شد.

بدافزار مذکور که برخی آن را کرم QNAP نیز نامیده‌اند از یک Windows Installer Binary معتبر به نام «msiexec.exe» برای دانلود و اجرای یک فایل DLL بر روی دستگاه‌های آسیب‌پذیر QNAP استفاده می‌کند.

محققان بر این باورند که به منظور دور زدن راهکارهای امنیتی، Raspberry Robin از تکنیک تزریق کد مخرب به سه پروسه سیستمی معتبر Windows استفاده می‌کند.

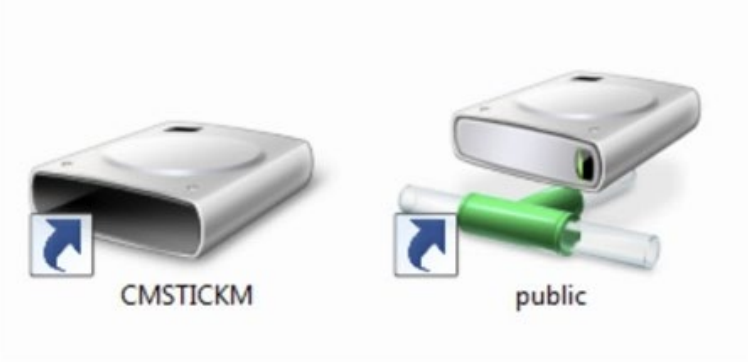
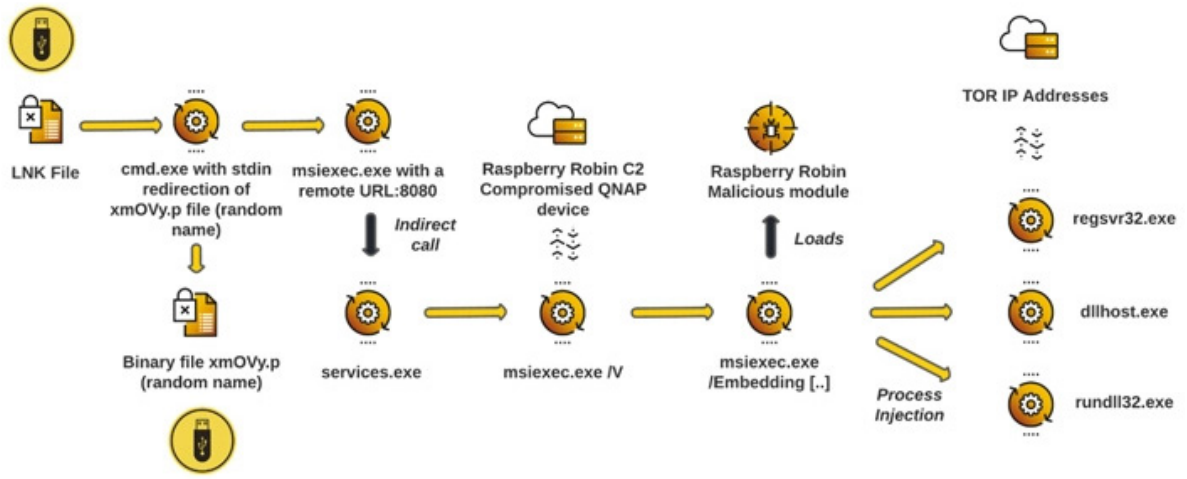


Figure 1. Sample of LNKs used by the threat actor

در مراحل ابتدایی، بدافزار به منظور ماندگاری در دستگاه آلوده و فراخوانی کد مخرب، تغییراتی را در Windows Registry از طریق پروسه معتبر «rundll32.exe» ایجاد می‌کند.

این کارزار تا پیش از شناسایی توسط شرکت سایبریزن بصورت رمز و راز باقی مانده بود و هیچ سرنخی در مورد مهاجمان یا اهداف نهایی آن وجود نداشت.



جزئیات این کارزار هنگامی منتشر شد که QNAP اعلام کرد که به طور فعال در حال بررسی موج جدیدی از آلودگی‌های باج‌افزاری پس از حملات AgeLocker، eCh0raix و DeadBolt است که دستگاه‌هایش را هدف قرار داده است.

تحقیقات اولیه شرکت کیونپ حاکی از آن است که مهاجمان از طریق سرویس‌های SMB آسیب‌پذیر حمله می‌کنند و از فهرستی از رمزهای عبور کشف شده در حملات قبلی (Dictionary Attack) جهت نفوذ به حساب‌های دارای رمزهای عبور ضعیف استفاده می‌کنند.

هنگامی که مهاجمان موفق به ورود به دستگاهی می‌شود، داده‌ها را در پوشه‌های اشتراکی رمزگذاری نموده و یک اطلاعیه باج‌گیری (Ransom Note) با نام فایل «!CHECKMATE_DECRYPTION_README» در هر پوشه قرار می‌دهند.

این شرکت تایوانی به کاربران دستگاه‌های QNAP توصیه می‌کند به منظور پیشگیری و در امان ماندن از این حملات، ضمن بکارگیری رمزهای عبور پیچیده، تهیه نسخ پشتیبان از داده‌های حساس و حیاتی به طور منظم و دوره‌ای، سرویس SMB را به اینترنت متصل نکنند و دستگاه‌های QNAP خود را به آخرین نسخه موجود به‌روز کنند.

جزئیات بیشتر این بدافزار در نشانی‌های زیر قابل دریافت و مطالعه می‌باشد:

https://www.cybereason.com/blog/threat-alert-raspberry-robin-worm-abuses-windows-installer-and-qnap-devices

https://7095517.fs1.hubspotusercontent-na1.net/hubfs/7095517/FLINT%202022-016%20-%20QNAP%20worm_%20who%20benefits%20from%20crime%20(1).pdf

منبع:

https://thehackernews.com/2022/07/researchers-warn-of-raspberry-robins.html

جعل هویت شرکت‌های برجسته امنیتی؛

ترفند جدید مهاجمان

به تازگی شرکت کراوداسترایک (CrowdStrike Holdings, Inc.) نسبت به اجرای یک کارزار فیشینگ (Phishing) که در آن مهاجمان اقدام به جعل هویت شرکت‌های برجسته در حوزه امنیت سایبری می‌کنند، هشداری صادر کرده است.

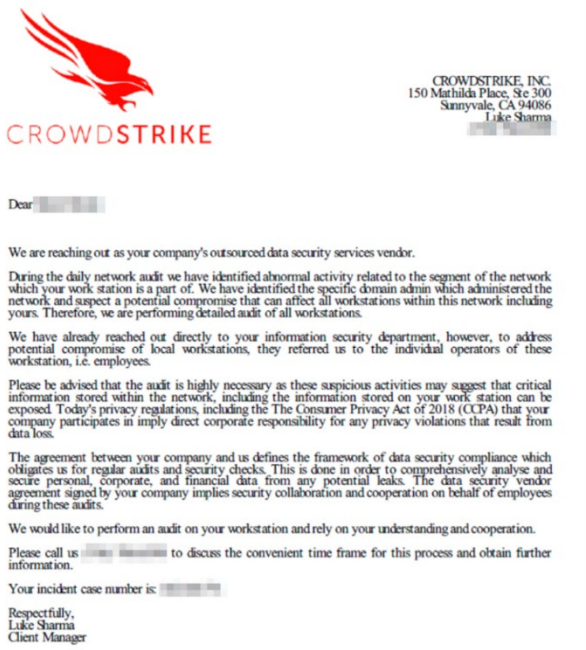
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، کارزار مذکور مورد بررسی قرار گرفته است.

در ایمیل‌های فیشینگ کارزار مذکور اینطور وانمود می‌شود که شرکت دریافت‌کننده ایمیل هک شده و قربانی می‌بایست با شماره تلفن درج شده در ایمیل تماس بگیرد.

این کارزار از تاکتیک‌های مهندسی اجتماعی مشابه که در کارزارهای اخیر همچون BazarCall 2021 بکارگرفته شده، استفاده می‌کند.

احتمال داده شده که در جریان این کارزار مهاجمان از ابزارهای معمول همکاری از راه دور (Remote Collaboration Tool – به اختصار RAT) جهت دسترسی و نفوذ اولیه، ابزارهای متداول تست نفوذ برای گسترش آلودگی به دستگاه‌های مجاور در شبکه و در نهایت اجرای کدهای مخرب به منظور آلوده‌سازی دستگاه‌ها به باج‌افزار یا سرقت اطلاعات استفاده می‌کنند.

در این کارزارها که به «برگردان تماس» (Callback) معروف هستند، مهاجمان ایمیل‌هایی در ظاهر از جانب شرکت‌های امنیتی برجسته ارسال می‌کنند. آنها در متن ایمیل ادعا می‌کنند که شرکت امنیتی مذکور خطری احتمالی را در شبکه آنها شناسایی کرده و همچون سایر کارزارهای «برگردان تماس»، همانند شکل یک شماره تلفن برای دریافت کننده ایمیل ارسال می‌کنند.



CROWDSTRIKE

CROWDSTRIKE, INC.
150 Mathilda Place, Ste 300
Sunnyvale, CA 94086
Luke Sharma
[redacted]

Dear [redacted]

We are reaching out as your company's outsourced data security services vendor.

During the daily network audit we have identified abnormal activity related to the segment of the network which your work station is a part of. We have identified the specific domain admin which administered the network and suspect a potential compromise that can affect all workstations within this network including yours. Therefore, we are performing detailed audit of all workstations.

We have already reached out directly to your information security department, however, to address potential compromise of local workstations, they referred us to the individual operators of these workstation, i.e. employees.

Please be advised that the audit is highly necessary as these suspicious activities may suggest that critical information stored within the network, including the information stored on your work station can be exposed. Today's privacy regulations, including the The Consumer Privacy Act of 2018 (CCPA) that your company participates in imply direct corporate responsibility for any privacy violations that result from data loss.

The agreement between your company and us defines the framework of data security compliance which obligates us for regular audits and security checks. This is done in order to comprehensively analyse and secure personal, corporate, and financial data from any potential leaks. The data security vendor agreement signed by your company implies security collaboration and cooperation on behalf of employees during these audits.

We would like to perform an audit on your workstation and rely on your understanding and cooperation.

Please call us [redacted] to discuss the convenient time frame for this process and obtain further information.

Your incident case number is: [redacted]

Respectfully,
Luke Sharma
Client Manager

Figure 1. Example of CrowdStrike-Themed Phishing Email

نمونه‌ای از ایمیل فیشینگ که ظاهراً از سوی شرکت کراوداستراید ارسال شده

در حملات قبلی، در زمان تماس قربانیان با شماره درج شده در این گونه ایمیل‌ها، مهاجم آنها را متقاعد می‌کرد تا به بهانه بررسی اولیه نرم‌افزارهای RAT را در شبکه خود نصب کنند.

به عنوان مثال، محققان شرکت کراوداستراید کارزار «برگردان تماس» مشابه‌ای را در اسفند ۱۴۰۰ شناسایی کردند که در آن مهاجمان، AteraRMM و سپس Cobalt Strike را جهت گسترش آلودگی به دستگاه‌های مجاور در شبکه و اجرای بدافزار نصب کردند.

این در حالی است که در حال حاضر این محققان نمی‌دانند دقیقاً از چه نوع بدافزاری در این کارزار استفاده شده اما احتمالاً هدف مهاجمان انتشار باج‌افزار به منظور کسب درآمد می‌باشد.

کارزارهایی نظیر BazarCall 2021 در نهایت منجر به آلودگی به باج‌افزار Conti شده است، اگرچه اخیراً این باج‌افزار به عنوان یک سرویس اجاره‌ای (Ransomware-as-a-Service – به اختصار RaaS) فعالیت خود را متوقف کرده است. کارزار BazarCall 2021 اولین موردی بود که هویت نهادهای امنیت سایبری را جعل کرده بود و با توجه به ماهیت اضطراری آن، احتمال موفقیت بالقوه بیشتری داشت.

منبع:

https://www.crowdstrike.com/blog/callback-malware-campaigns-impersonate-crowdstrike-and-other-cybersecurity-companies/

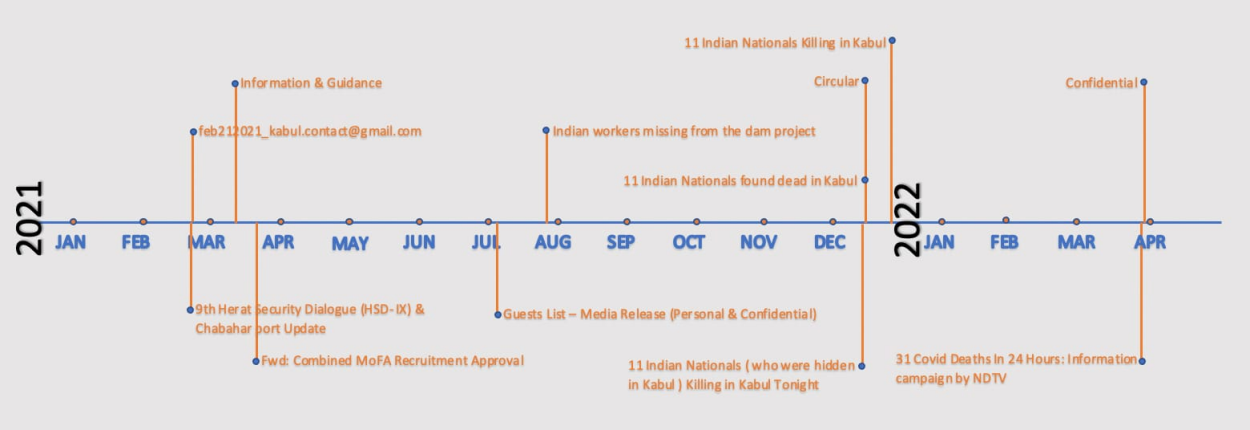
حملات هدفمند

از طریق فایل Excel مخرب

شرکت ترلیکس (Trellix, LLC.) جزییات کارزاری مخرب را منتشر کرده که از سال ۲۰۲۱ سازمان‌های دولتی در کشورهای مختلف از جمله افغانستان و هند را هدف قرار می‌داده است.

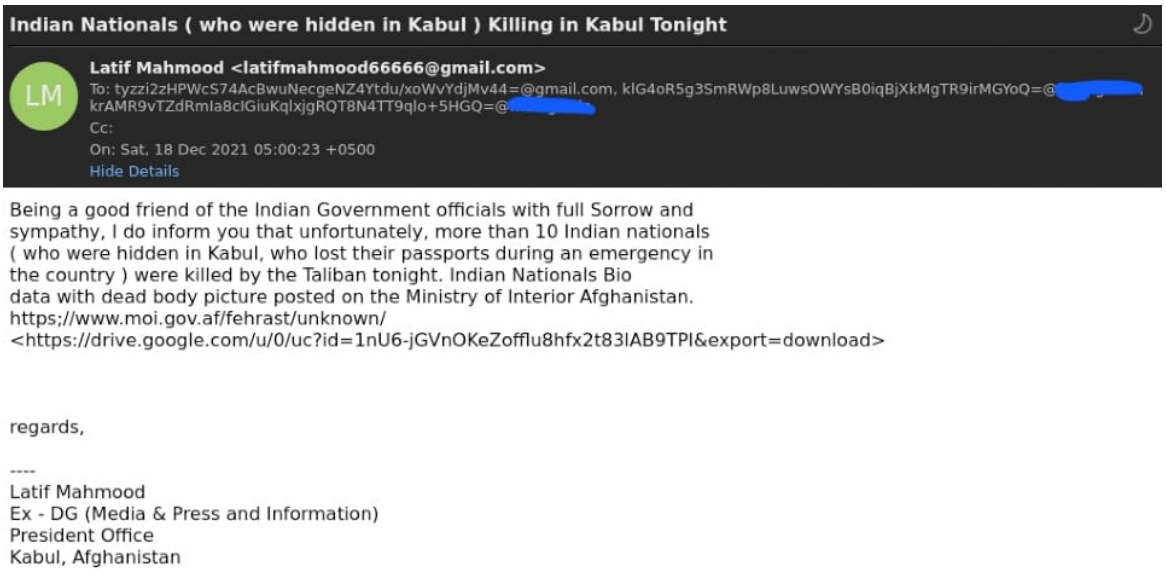
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، این کارزار مورد بررسی قرار گرفته است.

تصویر زیر خط زمانی کارزار این مهاجمان را نشان می‌دهد.



این مهاجمان معمولاً از موضوعات سیاسی جهت فریب کاربران به منظور کلیک کردن روی یک لینک مخرب یا بازکردن پیوست ایمیل استفاده می‌کنند.

برای نمونه، در جریان یکی از این حملات فیشینگ هدفمند (Spear-phishing) به کشتن یکی از اتباع هند در افغانستان اشاره شده است.



Indian Nationals (who were hidden in Kabul) Killing in Kabul Tonight

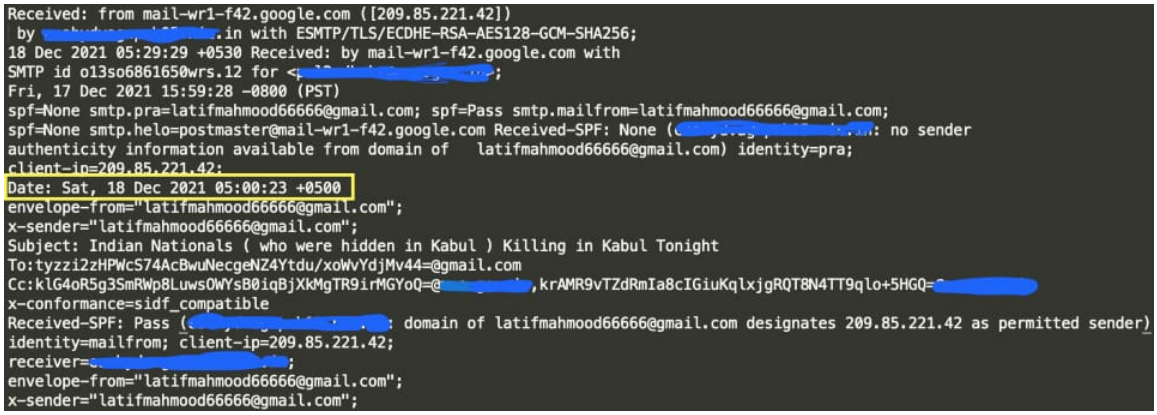
LM **Latif Mahmood <latifmahmood66666@gmail.com>**
To: tyzzi2zHPWcS74AcBwuNecgeNZ4Ytdu/xoWvYdjMv44=@gmail.com, klG4oR5g3SmRWp8LuwsOWYsB0iqBjXkMgTR9irMGYoQ=@[redacted]
krAMR9vTZdRmIa8cIGiuKqlxjgRQT8N4TT9qlo+5HGQ=@[redacted]
Cc:
On: Sat, 18 Dec 2021 05:00:23 +0500
Hide Details

Being a good friend of the Indian Government officials with full Sorrow and sympathy, I do inform you that unfortunately, more than 10 Indian nationals (who were hidden in Kabul, who lost their passports during an emergency in the country) were killed by the Taliban tonight. Indian Nationals Bio data with dead body picture posted on the Ministry of Interior Afghanistan.
https;//www.moi.gov.af/fehrast/unknown/
<https://drive.google.com/u/0/uc?id=1nU6-jGVnOKeZoffIu8hfx2t83IAB9TPI&export=download>

regards,

Latif Mahmood
Ex - DG (Media & Press and Information)
President Office
Kabul, Afghanistan

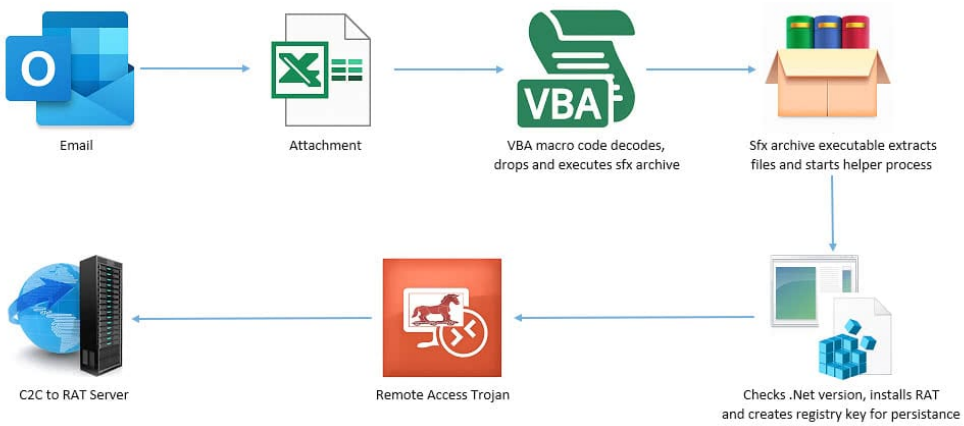
منطقه زمانی دستگاهی که ایمیل از آن ارسال شده است، UTC 0500+ (منطقه جنوب آسیا) بوده که احتمالاً نشانه ملیت مهاجمان این کارزار می‌باشد.



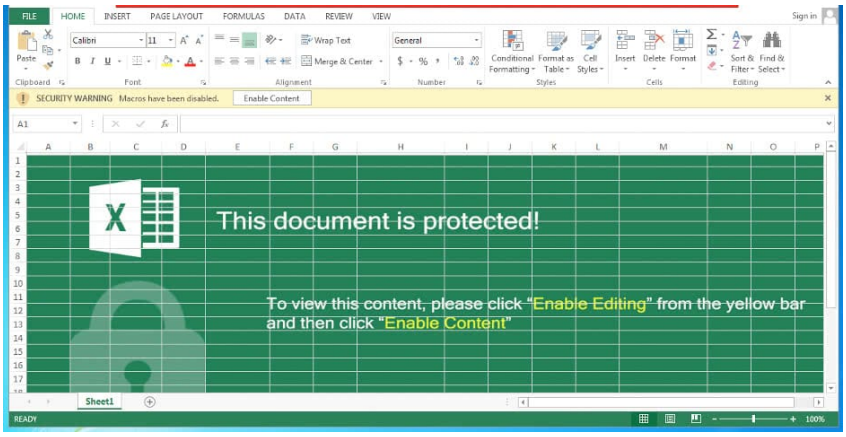
```
Received: from mail-wr1-f42.google.com ([209.85.221.42])
 by [redacted].in with ESMTP/TLS/ECDHE-RSA-AES128-GCM-SHA256;
18 Dec 2021 05:29:29 +0530 Received: by mail-wr1-f42.google.com with
SMTP id o13so6861650wrs.12 for <[redacted]>;
Fri, 17 Dec 2021 15:59:28 -0800 (PST)
spf=None smtp.pra=latifmahmood66666@gmail.com; spf=Pass smtp.mailfrom=latifmahmood66666@gmail.com;
spf=None smtp.helo=postmaster@mail-wr1-f42.google.com Received-SPF: None ([redacted]: no sender
authenticity information available from domain of   latifmahmood66666@gmail.com) identity=pra;
client-ip=209.85.221.42;
Date: Sat, 18 Dec 2021 05:00:23 +0500
envelope-from="latifmahmood66666@gmail.com";
x-sender="latifmahmood66666@gmail.com";
Subject: Indian Nationals ( who were hidden in Kabul ) Killing in Kabul Tonight
To:tyzzi2zHPWcS74AcBwuNecgeNZ4Ytdu/xoWvYdjMv44=@gmail.com
Cc:klG4oR5g3SmRWp8LuwsOWYsB0iqBjXkMgTR9irMGYoQ=@[redacted],krAMR9vTZdRmIa8cIGiuKqlxjgRQT8N4TT9qlo+5HGQ=[redacted]
x-conformance=sidf_compatible
Received-SPF: Pass ([redacted]: domain of latifmahmood66666@gmail.com designates 209.85.221.42 as permitted sender)
identity=mailfrom; client-ip=209.85.221.42;
receiver=[redacted];
envelope-from="latifmahmood66666@gmail.com";
x-sender="latifmahmood66666@gmail.com";
```

یا در یکی دیگر از نمونه‌های اخیر آن، مهاجمان ایمیلی با موضوعی مرتبط با کووید-۱۹ را ارسال کرده‌اند.

این ایمیل‌ها که از سرویس رایگان ایمیل Gmail ارسال شده‌اند یا حاوی لینکی مخرب به Google Drive بوده یا یک فایل ZIP مخرب را دارا می‌باشند که هر دوی آنها قربانی را به یک فایل Excel مخرب هدایت می‌کند. فایل مذکور حاوی یک صفحه مخرب (Sheet) به نام FE_APT_Dropper_Macro_DoubleHide_1 می‌باشد.



پس از باز کردن فایل Excel، ماکروی مخرب جاسازی شده در آن اجرا شده و سپس جهت ماندگاری در سیستم یک تروجان دسترسی از راه دور (AysncRAT / LimeRAT) نصب می‌شود. هنگامی که تروجان دسترسی از راه دور بر روی ماشین قربانی نصب شد، به یک سرور کنترل و فرمان‌دهی (Command-and-Control – به اختصار C2) متصل شده و برای استخراج داده‌های قربانی مورد استفاده قرار می‌گیرد.



تروجان دسترسی از راه دور بکارگرفته شده در این کارزار، قادر به جمع‌آوری اطلاعات حساس نظیر کلیدهای فشرده شده روی صفحه کلید (Keystroke)، تصاویر گرفته شده از صفحه نمایش (Screenshot)، ضبط اطلاعات کاربری/اطلاعات اصالت‌سنجی و افزودن دستگاه به شبکه مخرب (Botnet) تحت کنترل مهاجمان می‌باشد. همچنین می‌تواند سیستم‌های آسیب‌پذیر موجود در شبکه را شناسایی نموده و آلودگی را در سطح شبکه سازمان گسترش دهد.

مشروح گزارش ترلیکس در لینک زیر قابل مطالعه است:

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/targeted-attack-on-government-agencies.html

نشانه‌های آلودگی:

از جمله اسامی فایل‌های مربوط به این کارزار می‌توان به موارد زیر اشاره کرد:

File info	File name
LimeRAT [Runtime: .Net Framework 2.0]	3_5
AsyncRAT [Runtime: .Net Framework 4]	4
AsyncRAT [Runtime: .Net Framework 4.5]	4_5
AsyncRAT [Runtime: .Net Framework 4.5.1]	4_5_1
AsyncRAT [Runtime: .Net Framework 4.5.2]	4_5_2
AsyncRAT [Runtime: .Net Framework 4.6]	4_6
AsyncRAT [Runtime: .Net Framework 4.6.1]	4_6_1
AsyncRAT [Runtime: .Net Framework 4.7	4_7
AsyncRAT [Runtime: .Net Framework 4.7.2]	4_7_2
Delphi compiled file installs RAT file according to available .Net version	igfx.exe

درهم‌ساز (Hash) فایل‌های مخرب این کارزار به شرح زیر می‌باشد:

SHA256	File Name
7a6b87a7ba79160232579157b8ebcaea7660392d98cb6b8b3d562a383a0894bc	3_5
5e44f769aa9a745ade82589bbbd17c3687f2fb7c08b1043d8c5c44d28eaa20a9	4
fe1c8b01f5abc62551b0a3f59fe1675c66dd506d158f5de495a5d22d7445e6e9	4_5
fa9cb5608841f023052379818a9186496526039bc47cac05a6866f5fb0e70fc5	4_5_1
080fcc70c11248eaf34bd30c0dc9800b0b1742fe92c96c9995a1c73c0adf2336	4_5_2
465a59b7a97364bc933703a8fda715090c6a927f814bc22a0057e6a7134cb69f	4_6
5e082d1c85e591aebb380d7d7af56000ac0ef5fc32e216cb5fe7027bb9861743	4_6_1
f59dc209ee236e5ed78f83117865164e57a223f742c75f57c20d3da4cbe179e0	4_7
f32b0d71274ea93f27527079371e5e926e8d6a6f29d84ac602e48da0332c9f4c	4_7_2
8248432bcba6e8bb8731c0b8f2fbe4aae2e2d0fee2157477c83343743c39c1a8	igfx.exe
06064b3b0158efbfa9d849c853a9783c7e9d07c5924275d0d33c6ac74c78eec7	msword.exe
886c5883113d279d97caaca2714860dfceb421c7297dbb3ee04a00b7d50b821b	Unknown.xls
b9584cf67e73a759d6c412962d4a9d7471c703f72e056cd24742a4b78c68ff2d	Unknown.ZIP

همچنین عناوین ایمیل‌هایی که مهاجمان در حملات از آن استفاده کرده‌اند، عبارتند از:

9th Herat Security Dialogue (HSD- IX) & Chabahar port Update
feb212021_kabul.contact@gmail.com
Information & Guidance
Fwd: Combined MoFA Recruitment Approval
Guests List - Media Release (Personal & Confidential)
Indian workers missing from the dam project
Indian Nationals (who were hidden in Kabul) Killing in Kabul Tonight
11 Indian Nationals found dead in Kabul
Circular
Indian Nationals Killing in Kabul

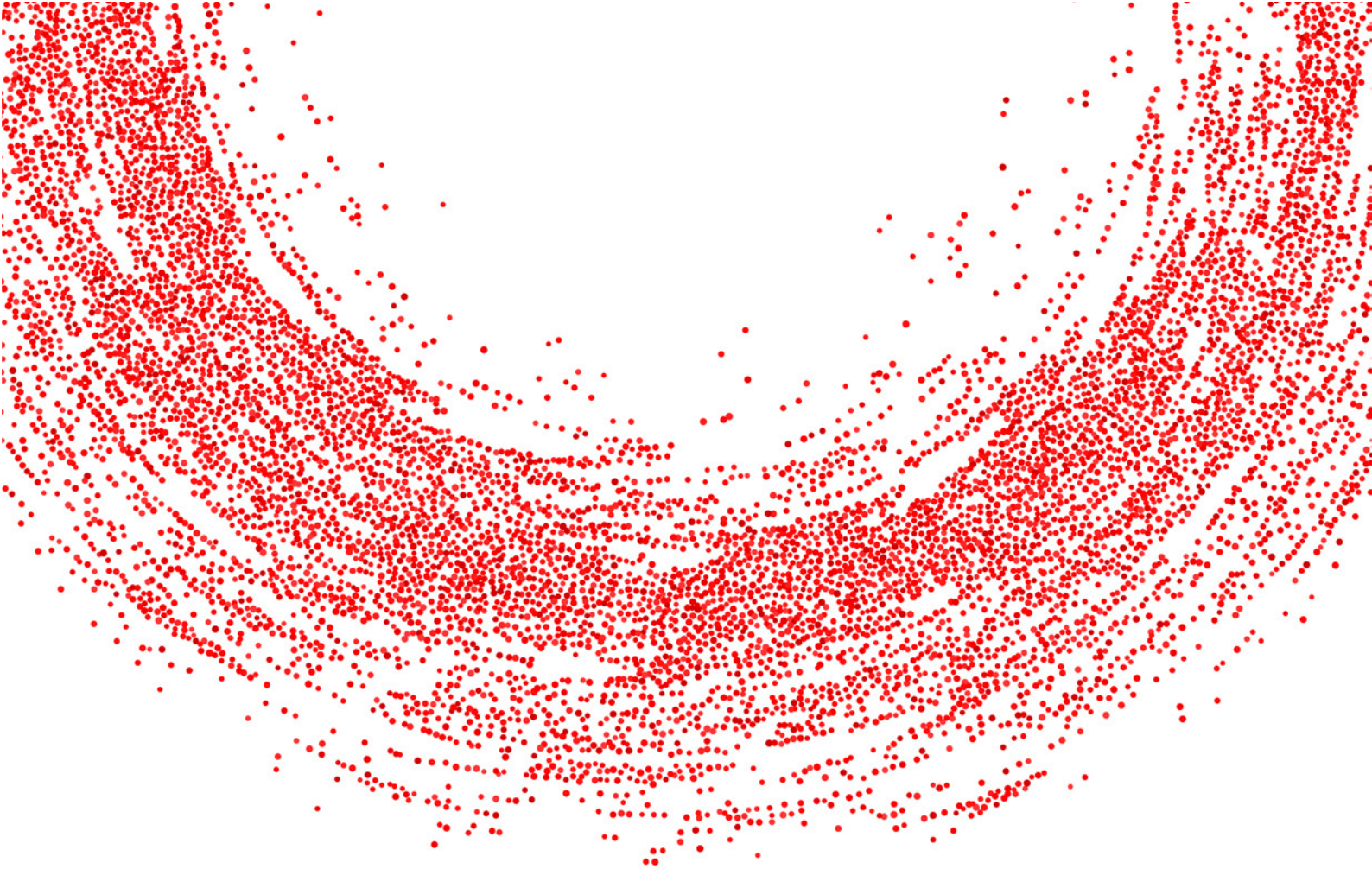
31 Covid Deaths In 24 Hours: Information campaign by NDTV

برخی از نشانی‌هایی که مهاجمان این کارزار برای ارسال ایمیل به قربانیان خود از آن استفاده کرده‌اند، به شرح زیر است:

kabul.contact@gmail.com
mashrefhaideri@gmail.com
latifmahmood66666@gmail.com
fscon.kab@gmail.com
admn.kabul@gmail.com
ravish49.ndtv@gmail.com

منبع:

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/targeted-attack-on-government-agencies.html



آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

بروزرسانی‌ها و اصلاحیه‌های

مرداد ۱۴۰۱

در تیر ۱۴۰۱ شرکت‌های زیر اقدام به عرضه بروزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

مایکروسافت	وی‌ام‌ور	اپل	جونیپر نت‌ورکز
سیسکو	ادوبی	دروپال	اپن‌اس‌اس‌ال
مک‌آفی اینترپرایز	گوگل	سیتریکس	اوراکل
بیت‌دیفندر	موزیلا	اس‌ای‌پی	

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به برخی از بااهمیت‌ترین اصلاحیه‌های تیر ماه پرداخته شده است.

مایکـروسافت

شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی جولای ۲۰۲۲ منتشر کرد. اصلاحیه‌های مذکور بیش از ۸۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. تنها درجه اهمیت ۴ مورد از آسیب‌پذیری‌های ترمیم شده ماه جولای «حیاتی» (Critical) و اکثر موارد دیگر «مهم» (Important) اعلام شده است.

این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را در محصولات مایکروسافت ترمیم می‌کنند.

- «ترفیع اختیارات» (Elevation of Privilege)
- «اجرای کد از راه دور» (Remote Code Execution)

- «افشای اطلاعات» (Information Disclosure)
- «از کارانداری سرویس» (Denial of Service - به اختصار DoS)
- «عبور از سد امکانات امنیتی» (Security Feature Bypass)
- «دست‌درازی» (Tampering)
- «جعل» (Spoofing)

یک مورد از آسیب‌پذیری‌های ترمیم شده ماه جولای، از نوع «روز-صفر» با شناسه CVE-2022-22047 می‌باشد و به طور گسترده در حملات مورد سوءاستفاده قرار گرفته است. مایکروسافت آن دسته از آسیب‌پذیری‌هایی را از نوع روز-صفر می‌داند که پیش‌تر اصلاحیه رسمی برای ترمیم آن‌ها ارائه نشده، جزییات آن‌ها به‌طور عمومی منتشر شده یا در مواقعی مورد سوءاستفاده مهاجمان قرار گرفته است.

آسیب‌پذیری CVE-2022-22047 دارای درجه اهمیت «مهم» بوده و از نوع «ترفیع اختیارات» است. این ضعف امنیتی بر روی Windows CSRSS تاثیر می‌گذارد و مهاجم با سوءاستفاده از آن قادر خواهد بود امتیازات در سطح System را بدست آورد. مهاجم معمولاً در کنار این آسیب‌پذیری از باگی از نوع اجرای کد از راه دور که اغلب از طریق یک سند دستکاری شده Office یا Adobe ساخته‌شده، نیز سوءاستفاده می‌کند تا سیستم را تحت کنترل قرار دهد.

چهار مورد از آسیب‌پذیری‌های ترمیم شده دارای درجه اهمیت «حیاتی» با شناسه‌های CVE-2022-30221، CVE-2022-22029، CVE-2022-22039 و CVE-2022-22038 می‌باشند که در ادامه به بررسی جزئیات این ضعف‌های امنیتی می‌پردازیم.

- ضعف امنیتی با شناسه CVE-2022-22029، از نوع «اجرای کد از راه دور» می‌باشد. مهاجم می‌تواند بدون نیاز به احراز هویت در بستر شبکه، Network File System – به اختصار NFS – را مورد بهره‌جویی قرار دهد. با این حال، به نقل از مایکروسافت، سوءاستفاده از آن پیچیدگی بالایی دارد و به تلاش های مکرر مهاجم از طریق ارسال داده‌های ثابت یا متناوب نیاز دارد.

- دیگر آسیب‌پذیری حیاتی، CVE-2022-22038 می‌باشد که بهره‌جویی از آن نیز به دلیل فراهم نمودن اقدامات اضافی توسط مهاجم نسبتاً دشوار به نظر می‌رسد. این ضعف امنیتی از نوع «اجرای کد از راه دور» بوده و بر Remote Procedure Call Runtime در همه نسخه‌های Windows تاثیر می‌گذارد.

- سومین ضعف امنیتی با درجه اهمیت «حیاتی» ماه جولای نیز از نوع «اجرای کد از راه دور» و دارای شناسه CVE-2022-22039 می‌باشد که NFS از آن تاثیر می‌پذیرد. مهاجم تنها با برنده شدن در شرایط رقابتی (Race Condition) می‌تواند موفق به سوءاستفاده از آن شود لذا احتمالاً این ضعف امنیتی کمتر مورد بهره‌جویی قرار خواهد گرفت.

- آخرین آسیب‌پذیری ترمیم شده با درجه اهمیت «حیاتی» در ماه جولای ۲۰۲۲، ضعفی با شناسه CVE-2022-30221 و از نوع «اجرای کد از راه دور» است. این ضعف امنیتی بر Windows Graphics Component تاثیر می‌گذارد. مهاجم باید کاربر را متقاعد کند که به یک سرور RDP مخرب متصل شود. پس از اتصال، سرور مخرب می تواند کدی را از راه دور در سیستم قربانی اجرا کند.

در ادامه به بررسی جزئیات دیگر آسیب‌پذیری‌های اصلاح شده ماه جولای شرکت مایکروسافت و به ویژه به مواردی که ممکن است بیشتر مورد توجه مهاجمان قرار گیرند، می‌پردازیم.

در میان ضعف‌های ترمیم شده از نوع «دست‌درازی» در ماه جولای ۲۰۲۲، شناسه CVE-2022-30216 بر Windows Server و CVE-2022-33637 بر Microsoft Defender for Endpoint for Linux تاثیر می‌گذارد. هر دوی این ضعف‌های امنیتی دارای درجه اهمیت «مهم» می‌باشند.

دیگر ضعف امنیتی رفع شده CVE-2022-22048 با درجه اهمیت «مهم» است که قابلیت BitLocker Device Encryption را در سیستم‌عامل Windows تحت تاثیر قرار می‌دهد. بهره‌جویی از آسیب‌پذیری مذکور، مهاجمی را که به دستگاه دسترسی فیزیکی دارد قادر به دستیابی به داده‌های رمزشده خواهد کرد.

علاوه بر این، بروزرسانی ماه جولای ۲۰۲۲ مایکروسافت شامل اصلاحاتی برای چهار آسیب‌پذیری با شناسه‌های CVE-2022-22022، CVE-2022-22041، CVE-2022-30206 و CVE-2022-30226 است که همگی از نوع «ترفیع اختیارات» می‌باشند و Windows Print Spooler از آنها تاثیر می‌پذیرد. CVE-2022-22022 و CVE-2022-30226 فقط امکان حذف فایل‌های موردنظر را برای مهاجم فراهم نموده در حالی که CVE-2022-22041 و CVE2022-30206 می‌توانند مهاجم را قادر به کسب امتیاز در سطح SYSTEM نمایند.

تقریباً یک سوم از وصله‌های منتشر در ماه جولای مربوط به ضعف‌های Microsoft Azure Site Recovery می‌باشند که مهم‌ترین آنها دارای شناسه CVE-2022-33675 می‌باشد. این آسیب‌پذیری از نوع «ترفیع اختیارات» بوده و به علت وجود باگی در Directory Permission مهاجم را قادر به ارتقای امتیازات خود تا سطح SYSTEM از طریق DLL Hijacking خواهد کرد.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های جولای ۲۰۲۲ مایکروسافت در گزارش زیر قابل مطالعه است.

https://newsroom.shabakeh.net/24834/newsroom-microsoft-security-update-july-2022.html

سیسکو

شرکت سیسکو (Cisco Systems, Inc.) در تیر ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ۲۵ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت چهار مورد از آنها «حیاتی»، دو مورد از آنها از نوع «بالا» (High) و ۱۹ مورد از نوع «متوسط» (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون «تزریق کد از طریق سایت» (Cross-Site Scripting)، «خواندن و نوشتن فایل دلخواه» (Arbitrary File Read and Write)، «افشای اطلاعات»، «تزریق فرمان» (Command Injection)، «از کاراندازی سرویس»، «اجرای کد از راه دور» و «ترفیع اختیارات» از جمله مهمترین اشکالات مرتفع شده توسط بروزرسانی‌های جدید هستند. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. اطلاعات بیشتر در نشانی زیر قابل دسترس می‌باشد.

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

مک‌آفی اینترپرایز

در تیر ۱۴۰۱، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) اقدام به انتشار نسخه ۶/۴/۲۲ نرم‌افزار Application and Change Control for Linux و نسخه ۲/۲ نرم‌افزار Endpoint Security Storage Protection کرد. جزییات کامل در خصوص باگ‌های برطرف‌شده و قابلیت‌های جدید افزوده‌شده در این نسخ در لینک‌های زیر قابل مطالعه است.

https://docs.trellix.com/bundle/application-change-control-6.4.x-release-notes-linux/
https://kcm.trellix.com/corporate/index?page=content&id=SNS3572

همچنین این شرکت در ماهی که گذشت از ترمیم ضعفی از نوع «ترفیع اختیارات»، با شناسه CVE-2022-2188 و با شدت «متوسط» در Data Exchange Layer Broker خبر داد. اطلاعات بیشتر در مورد بروزرسانی عرضه‌شده در لینک زیر قابل دسترس است.

https://kcm.trellix.com/corporate/index?page=content&id=SB10383

بیت‌دیفندر

شرکت بیت‌دیفندر (Bitdefender) در تیر ماه اقدام به انتشار نسخ جدید زیر کرد.

- GravityZone Control Center 6.29.1-2
- Bitdefender Endpoint Security Tools for Windows 7.6.1.203
- Bitdefender Endpoint Security Tools for Linux 7.0.3.2004
- Bitdefender Endpoint Security for Mac 7.6.14.200022

اطلاعات کامل در خصوص تغییرات و بهبودهای لحاظ شده در نسخ مذکور در نشانی زیر قابل مطالعه است.

https://www.bitdefender.com/business/support/en/77212-48453-release-notes.html

وی‌ام‌ور

در ماه گذشته، شرکت وی‌ام‌ور (VMware, Inc.) با انتشار توصیه‌نامه‌ها و بروزرسانی‌های امنیتی، نسبت به ترمیم ضعف‌های امنیتی با شناسه‌های CVE-2022-29901، CVE-2022-28693، CVE-2022-23816، CVE-2022-23825، CVE-2022-31654، CVE-2022-31655، CVE-2022-22982 و CVE-2021-22048 در محصولات زیر اقدام کرد.

- VMware ESXi
- VMware vRealize Log Insight
- VMware vCenter Server (vCenter Server)
- VMware Cloud Foundation (Cloud Foundation)

سوءاستفاده از ضعف‌های امنیتی ترمیم شده توسط این بروزرسانی‌ها، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر و دستیابی به اطلاعات حساس می‌کند. جزییات بیشتر آن در لینک زیر قابل مطالعه است.

https://www.vmware.com/security/advisories.html

ادوبی

شرکت ادوبی (Adobe, Inc.) مجموعه اصلاحیه‌های امنیتی ماه جولای ۲۰۲۲ را منتشر کرد. اصلاحیه‌های مذکور، ضعف‌های امنیتی را در محصولات زیر ترمیم می‌کنند:

- Adobe RoboHelp
- Adobe Acrobat and Reader
- Adobe Character Animator
- Adobe Photoshop

بیشترین تعداد آسیب‌پذیری ترمیم شده ماه جولای ادوبی، متعلق به Adobe Acrobat and Reader با ۲۲ مورد است. ۱۵ مورد از این ضعف‌های امنیتی «حیاتی» و ۷ مورد از آن «مهم» گزارش شده‌اند. بهره‌جویی موفق مهاجم از ضعف‌های امنیتی مذکور منجر به «اجرای کد از راه دور» (Arbitrary Code Execution) یا «نشت حافظه» (Memory Leak) خواهد شد. فریب کاربر به باز نمودن سند PDF دستکاری شده، از جمله سناریوهای قابل تصور برای سوءاستفاده از ضعف‌های امنیتی مذکور می‌باشد.

در بروزرسانی ماه جولای ۲۰۲۲، ادوبی یک ضعف امنیتی با درجه اهمیت «حیاتی» و یک مورد با درجه اهمیت «مهم» را در نرم‌افزار Photoshop ترمیم نموده است. آسیب‌پذیری برطرف شده از نوع «حیاتی» مربوط به مشکلات آزادسازی فضای حافظه پس از استفاده از آن (Use-After-Free – به اختصار UAF) می‌باشد که منجر به اجرای کد از راه دور می‌شود. وصله Character Animator دو آسیب‌پذیری «اجرای کد از راه دور» با درجه اهمیت «حیاتی» را برطرف می‌کند یکی از نوع «سرریز حافظه» (Heap Overflow) و دیگری مرتبط با Out-of-Bounds Read (OOB Read) می‌باشند.

در نهایت، وصله RoboHelp تنها یک ضعف با درجه اهمیت «مهم» از نوع «تزریق اسکریپت از طریق سایت» (Cross-site Scripting یا XSS) را ترمیم می‌کند. ادوبی به مشتریان خود توصیه می‌کند که در اسرع وقت اقدام به نصب بروزرسانی‌ها کنند. اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه جولای ۲۰۲۲ در نشانی زیر قابل مطالعه است.

https://helpx.adobe.com/security/security-bulletin.html

گـوگـل

شرکت گوگل (Google, LLC) در تیر ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۸ تیر ماه انتشار یافت، نسخه ۱۰۳/۰/۵۰۶۰/۱۳۴ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است.

https://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop_19.html

مـوزیـلا

در ماه گذشته، شرکت موزیلا (Mozilla, Corp) با ارائه بروزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار مدیریت ایمیل Thunderbird برطرف کرد. این اصلاحیه‌ها، در مجموع ۲۲ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت چهار مورد از آنها «بالا»، ۱٤ مورد «متوسط» و چهار مورد «پایین» (Low) گزارش شده است. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. توضیحات بیشتر در لینک زیر قابل مطالعه است.

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

اپـــل

در تیر ماه، شرکت اپل (Apple, Inc.) با انتشار بروزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله iOS، iPadOS، watchOS، tvOS، macOS و Safari ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. توصیه می‌شود با مراجعه به نشانی زیر، بروزرسانی‌های مربوطه هر چه سریع‌تر اعمال شود.

https://support.apple.com/en-us/HT201222

دروپـال

۲۹ تیر ۱۴۰۱، جامعه دروپال (Drupal Community) با عرضه بروزرسانی‌های امنیتی، یک ضعف امنیتی با شناسه CVE-2022-25276 با درجه اهمیت نسبتاً حیاتی (Moderately critical) را در نسخه‌های ۹٫٤ و ۹٫۳ ترمیم نمود. سوءاستفاده از این آسیب‌پذیری، مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. با نصب این بروزرسانی، نسخه نرم‌افزار Drupal نگارش ۹٫٤ به ۹٫۴٫۳ و نگارش ۹٫۳به ۹٫۳٫۱۹ تغییر خواهند کرد. توضیحات کامل در خصوص این بروزرسانی‌ها و توصیه‌نامه‌های منتشر شده پروژه Drupal Core، در آدرس زیر در دسترس می باشد.

https://www.drupal.org/sa-core-2022-015

سیتریکس

در تیر ماه، شرکت سیتریکس (Citrix Systems, Inc.) با عرضه بروزرسانی‌های امنیتی، یک آسیب‌پذیری با شناسه CVE-2022-26362 را در Citrix Hypervisor 7.1 LTSR CU2 ترمیم کرد. مهاجم می‌تواند از این ضعف امنیتی به منظور آلودگی Host و اجرای کدهای دلخواه در یک ماشین مجازی سوءاستفاده کند. توصیه می‌شود راهبران با مراجعه به آدرس زیر بروزرسانی لازم را اعمال کنند.

https://support.citrix.com/article/CTX460064

همچنین این شرکت در ۲۲ تیر، دو ضعف امنیتی با شناسه‌های CVE-2022-23825 و CVE-2022-29900 را در Citrix Hypervisor و XenServer برطرف کرده است. توضیحات کامل درخصوص این بروزرسانی و آسیب‌پذیری‌های مربوطه در نشانی زیر قابل مطالعه است.

https://support.citrix.com/article/CTX461397

اس‌ای‌پی

اس‌ای‌پی (SAP SE) نیز در ۲۱ تیر ۱٤۰۱ با انتشار مجموعه‌اصلاحیه‌هایی، ۲۳ آسیب‌پذیری را در چندین محصول خود برطرف کرد. درجه اهمیت چهار مورد از آنها «بالا» گزارش شده است. توصیه می‌شود با مراجعه به نشانی زیر، جزئیات مربوطه مطالعه و بروزرسانی اعمال شود.

https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

جونیپر نت‌ورکز

جونیپر نت‌ورکز (Juniper Networks, Inc.) هم در تیر ماه با ارائه بروزرسانی چندین ضعف امنیتی را در محصولات مختلف این شرکت ترمیم کرد. بهره‌جویی از ضعف‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است.

https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

اپن‌اس‌اس‌ال

۱۴ تیر ماه، بنیاد نرم‌افزاری اپن-اس‌اس‌ال (OpenSSL Software Foundation, Inc.) با عرضه بروزرسانی‌های امنیتی، ضعف‌های امنیتی متعددی را در نسخه‌های ۳/۰/۴، ۱/۱/۱ و ۳/۰ نرم‌افزار OpenSSL ترمیم نموده است. با نصب این بروزرسانی، نسخه نرم‌افزار OpenSSL نگارش ۳/۰/٤ به ۳/۰/۵، نگارش ۱/۱/۱ به ۱/۱/۱q و نگارش ۳/۰ به ۳/۰/۵ تغییر خواهند کرد. سوءاستفاده از بعضی از این آسیب‌پذیری‌ها مهاجم را قادر به «اجرای کد از راه دور» می‌کند. از این رو توصیه می‌شود که راهبران امنیتی در اولین فرصت نسبت به ارتقاء این نرم‌افزار اقدام کنند. توضیحات کامل در این خصوص در نشانی زیر قابل دسترس است.

https://www.openssl.org/news/secadv/20220705.txt

اوراکـل

۲۹ تیر ۱۴۰۱، شرکت اوراکل (Oracle Corp) مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار مجموعه بروزرسانی‌های موسوم به Critical Patch Update اقدام به ترمیم ۳۴۹ آسیب‌پذیری امنیتی در ده‌ها محصول ساخت این شرکت کرد. سوءاستفاده از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند.

لازم به ذکر است که شرکت اوراکل بعد از انتشار بروزرسانی Critical Patch Update Oracle ماه آوریل ۲۰۲۲، هشدار و توصیه‌نامه امنیتی برای ضعف امنیتی به شناسه CVE-2022-21500 در تاریخ ۲۹ اردیبهشت ۱۴۰۱ برای محصول Oracle E-Business Suit صادر نمود. اوراکل تاکید می‌کند که راهبران و کاربران این محصول، بروزرسانی جولای ۲۰۲۲ که شامل وصله‌های تکمیلی این ضعف امنیتی می‌باشد را بدون تأخیر اعمال کنند.

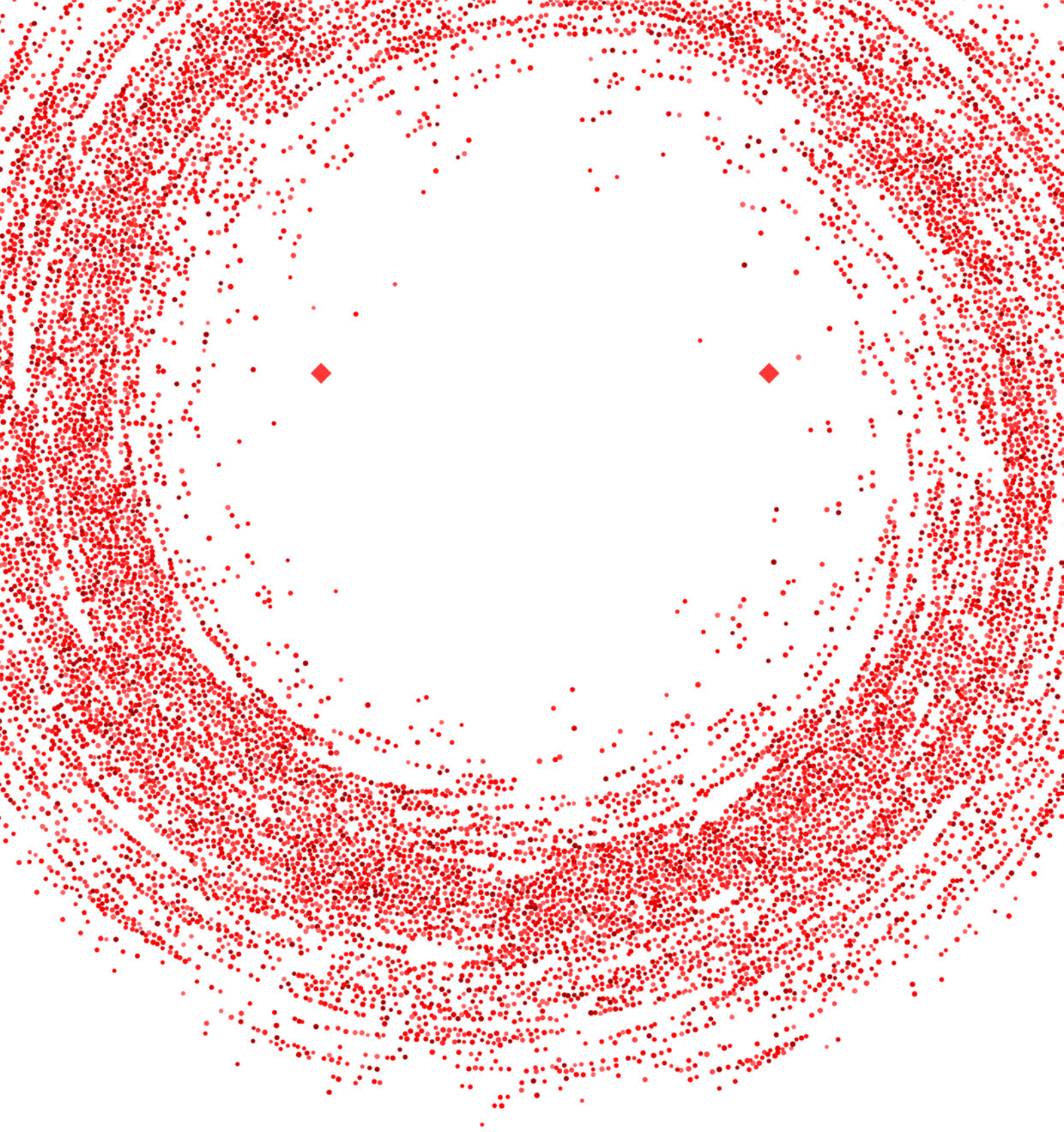
توصیه می‌شود که راهبران هر یک از محصولات اوراکل با مطالعه لینک زیر اقدام به نصب اصلاحیه‌های جدید کنند. جزییات کامل در خصوص آنها در لینک زیر قابل دریافت است.

https://www.oracle.com/security-alerts/cpujul2022.html

اطلاعات فناوری امنیت اخبار آخرین

@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم افزارهای 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 بین المللی فعالیت خود را بر روی نرم افزارهای 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 Managment) 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 شرکت Sophos، فعالیت خود را در این زمینه ادامه داد 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 توزیع (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefendr 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 راه اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است.



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