ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | تیر ۱۴۰۰

شبکه گستر

امنیت شما | وظیفه ما

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.

در ماه‌های اخیر، موارد متعددی از سوءاستفاده مهاجمان از آسیب‌پذیری محصولات مختلف وی‌ام‌ور با هدف رخنه به شبکه سازمان‌ها گزارش شده است. یکی از جدیدترین نمونه از این حملات که در جریان آن، بدافزاری با نام FreakOut اقدام به آلوده‌سازی سرورهای آسیب‌پذیر VMware vCenter می‌کند در این ماهنامه مورد بررسی قرار گرفته است.

در این ماهنامه جزییات بدافزاری ارائه شده که حداقل از سال ۲۰۱۷ دیپلمات‌ها را در نقاط مختلف جهان از جمله کشورهایی در آفریقا و خاورمیانه هدف قرار می‌داده است. اصلی‌ترین قابلیت‌های این بدافزار، استخراج داده‌ها از روی دستگاه، تصویربرداری از فعالیت‌های کاربر و رونویسی، حذف/انتقال و سرقت فایل گزارش شده است.

باج‌افزار REvil که با نام Sodinokibi نیز شناخته می‌شود از جمله تهدیداتی است که در قالب خدمات موسوم به RaaS ارائه می‌شود و توانسته طرفداران زیادی را در بازارهای زیرزمینی تبهکاران سایبری به خود جلب کند. یافته‌های شرکت امنیتی سوفوس نشان می‌دهد نمی‌توان دو گروه از مهاجمان را یافت که از سرویس RaaS باج‌افزار REvil به‌نحوی یکسان در جریان حملات خود استفاده کرده باشند. مشروح گزارش سوفوس در خصوص این باج‌افزار مخرب را در این ماهنامه بخوانید.

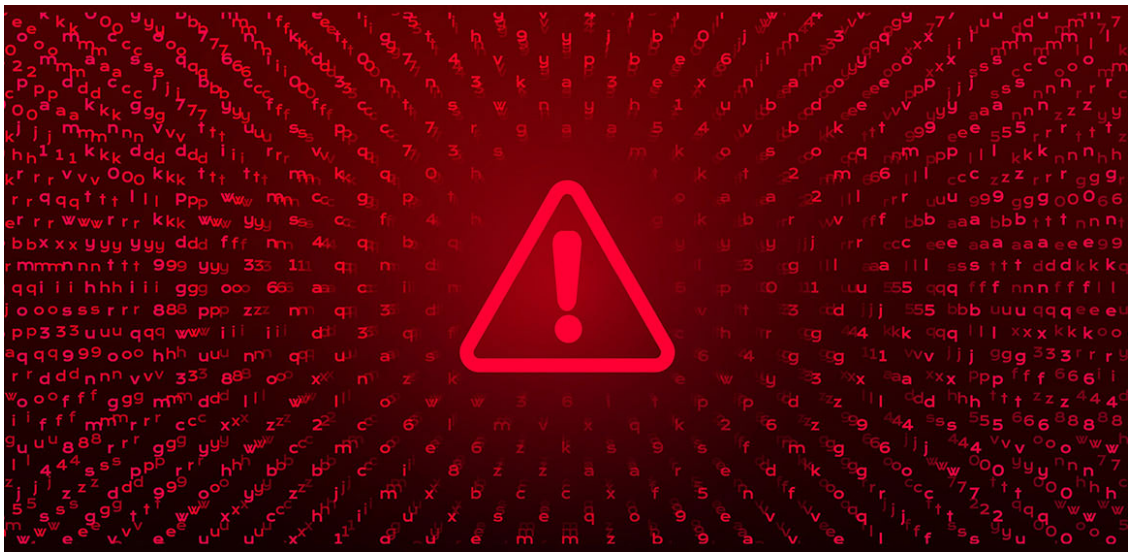
افزایش اجرای حملات نه چندان پیچیده و مبتنی بر روش‌های معمول بر ضد پروسه‌های کنترلی در سامانه‌های صنعتی، دیگر موضوعی است که در این ماهنامه با استناد به گزارش یکی از شرکت های امنیتی به آن پرداخته شده است.

در سومین ماه از سال ۱۴۰۰، مایکروسافت، رد هت، سیسکو، مک‌آفی، وی‌ام‌ور، بیت‌دیفندر، ادوبی، اس‌آپ، گوگل، اپل، موزیلا و دروپل اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از 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

سوءاستفاده مهاجمان
از آسیب‌پذیری‌های Fortinet



چند نهاد امنیتی، نسبت به سوءاستفاده حداقل یک گروه از مهاجمان APT از آسیب‌پذیری‌های Fortinet برای رخنه به اهداف خود هشدار داده‌اند.

در یکی از موارد، مهاجمان تقریباً موفق به بهره‌جویی از Fortigate به‌منظور دسترسی یافتن به سرور وبی که دامنه حساسی را میزبانی می‌کرده شده بودند.

به نظر می‌سد در جریان حمله، این مهاجمان اقدام به ایجاد یک حساب کاربری با نام elie یا WADGUtilityAccount جهت گسترش دامنه نفوذ و اجرای اقدامات مخرب در سطح شبکه می‌کنند.

بر اساس گزارش‌های منتشر شده، مهاجمان با برقراری ارتباط بر روی درگاه‌های ۴۴۴۳، ۸۴۴۳ و ۱۰۴۴۳ از آسیب‌پذیری‌های زیر سوءاستفاده می‌کنند:

- CVE-2018-13379
- CVE-2019-5591
- CVE-2020-12812

این آسیب‌پذیری‌ها، FortiOS، سیستم عامل مورد استفاده در محصولات Fortinet را متأثر می‌کنند.

توجه ویژه مهاجمان به این سه آسیب‌پذیری احتمالا به دلیل اطلاع آنها از استفاده از محصولات Fortinet در شبکه قربانی بوده است.

پس از رخنه به شبکه، مهاجمان قادر به استخراج اطلاعات، رمزگذاری داده‌ها و یا سایر امور مخرب خواهند بود.

اجرای این حملات بر ضد زیرساخت‌های حساس در حالی صورت می‌پذیرد که حداقل یک سال از وصله شدن آسیب‌پذیری‌های مذکور توسط شرکت سازنده می‌گذرد. باید توجه داشت که آسیب‌پذیری‌های مورد سوءاستفاده مهاجمان، محدود به موارد مذکور نیست و اعمال مستمر وصله‌های جدید می‌بایست همواره در دستور کار مسئولان و دست‌اندرکاران امنیت سازمان قرار داشته باشد. همچنین بکارگیری راهکارهای امنیتی قدرتمند، مسدوسازی درگاه‌ها و سرویس‌های غیرضرور، در حداقل نگاه داشتن سطوح دسترسی، بخش‌بندی شبکه (Network Segmentation)، تهیه نسخ پشتیبان از داده‌های بااهمیت و مقاوم‌سازی فرایند ثبت ورود (Login) از دیگر مواردی است که همگی در کنار یکدیگر شانس موفقیت تبهکاران سایبری را در نفوذ به شبکه سازمان به حداقل می‌رسانند.

نشانه‌های آلودگی (IoC)

نام فایل:

Audio.exe

frpc.exe

هش:

b90f05b5e705e0b0cb47f51b985f84db

نام کاربری:

elie

WADGUtilityAccount

منابع

https://www.ic3.gov/Media/News/2021/210402.pdf

https://www.ic3.gov/Media/News/2021/210527.pdf

سرورهای Exchange

هدف باج‌افزار Epsilon Red

بر اساس گزارشی که شرکت امنیتی Sophos آن را منتشر کرده گردانندگان باج‌افزار Epsilon Red با هدف قرار دادن سرورهای آسیب‌پذیر Exchange اقدام به رخنه به شبکه قربانی و رمزگذاری فایل‌ها می‌کنند.

چکیده گزارش مذکور در ادامه این مطلب توسط شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده ارائه شده است.

در جریان حملات این باج‌افزار از چندین اسکریپت و یک ابزار تجاری دسترسی از راه دور بهره گرفته شده است.

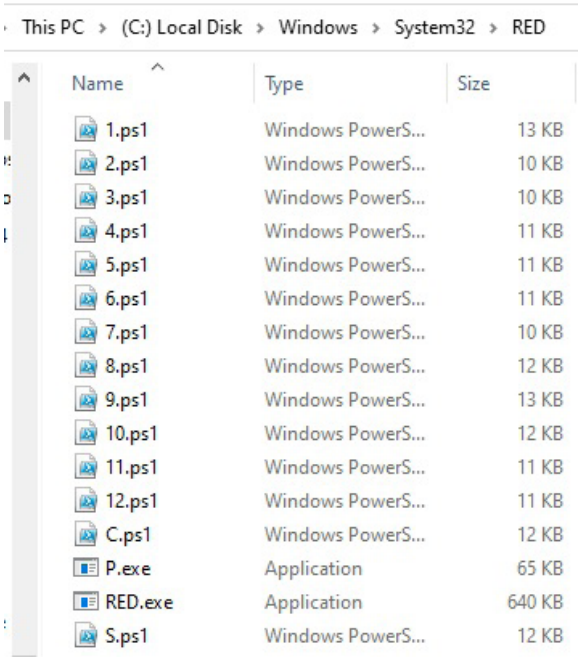
احتمال داده می‌شود که مهاجمان، ProxyLogon را به‌منظور سوءاستفاده از چندین آسیب‌پذیری حیاتی در Exchange به خدمت گرفته باشند.

ProxyLogon مجموعه آسیب‌پذیری‌هایی در سرویس‌دهنده ایمیل MS Exchange است که Microsoft در ۱۲ اسفند اصلاحیه‌هایی اضطراری برای ترمیم آنها منتشر کرد. از زمان انتشار اصلاحیه‌ها و افشای جزییات آن، هکرهای مستقل و گردانندگان APT متعددی، ProxyLogon را به فهرست تکنیک‌های نفوذ خود اضافه کرده‌اند.

Epsilon Red به زبان Golang یا همان Go نوشته شده و با استفاده از مجموعه‌ای از اسکریپت‌های منحصربه‌فرد PowerShell اقدامات زیر را انجام می‌دهد:

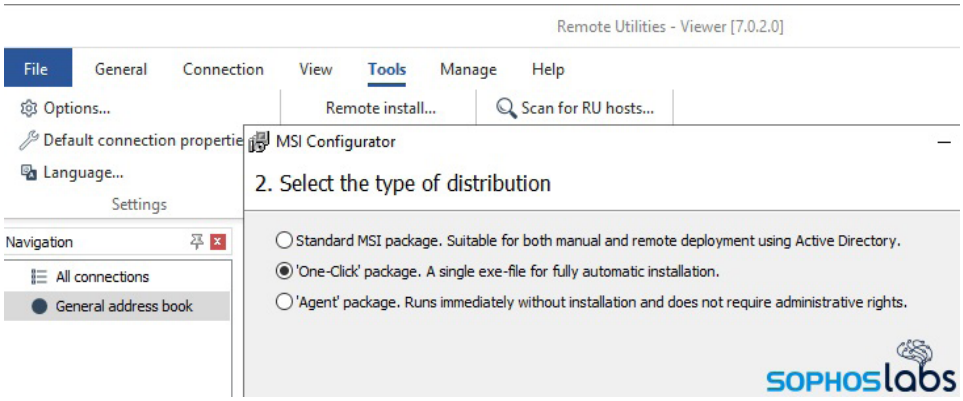
- از کار انداختن پروسه‌ها و سرویس‌های مرتبط با ابزارهای امنیتی، پایگاه‌های داده، برنامه‌های مدیریت نسخ پشتیبان، مجموعه نرم‌افزاری Office و برنامه‌های مدیریت ایمیل
- حذف اطلاعات مربوط به Volume Shadow Copies
- سرقت فایل Security Account Manager - به اختصار SAM - که شامل درهم‌ساز رمزهای عبور است
- حذف سوابق رویدادها در Windows
- غیرفعال کردن Windows Defender
- حذف ابزارهای امنیتی با هر یک از برندهای Sophos، Trend Micro، Cylance، MalwareBytes، Sentinel One، Vipre و Webroot
- گسترده کردن سطح دسترسی بر روی دستگاه

نام اکثر اسکریپت‌های مذکور عددی بین ۱ تا ۱۲ است. اما نام برخی از آنها نیز شامل تنها یک کاراکتر الفبایی است. به نظر می‌رسد یکی از آنها با نام c.ps1 رونوشتی از ابزار تست نفوذ Copy-VSS است.



پس از رخنه به شبکه، مهاجمان تلاش می‌کنند تا از طریق پودمان RDP به دستگاه‌های دیگر دسترسی یافته و با بکارگیری Windows Management Instrumentation، ابزارها و اسکریپت‌های مورد نظر خود و در نهایت باج‌افزار Epsilon Red را بر روی آنها اجرا کنند.

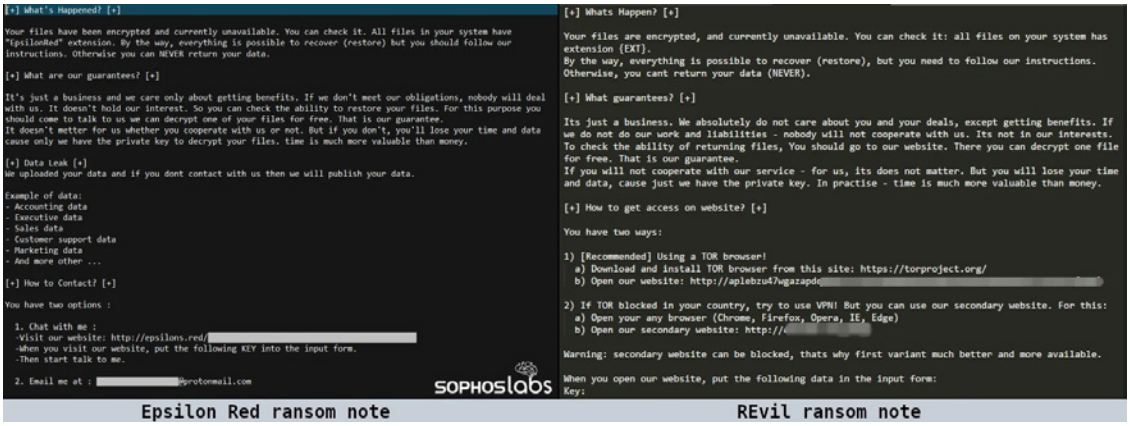
بررسی محققان Sophos نشان می‌دهد که مهاجمان از یک ابزار تجاری با نام Remote Utilities نیز برای برقراری ارتباطات از راه دور در کنار Tor Browser استفاده می‌کنند. با این رویکرد حتی در صورت مسدود شدن نقطه رخنه اولیه همچنان یک درگاه، باز باقی خواهد ماند.



همچنین Epsilon Red از Godirwalk جهت پویش دیسک و معرفی مسیرها به پروسه‌های فرزند و در ادامه رمزگذاری مستقل زیرپوشه‌ها استفاده می‌کند. به همین خاطر تا خاتمه کار، رونوشت‌های متعددی از پروسه های باج‌افزار بر روی دستگاه اجرا می‌شوند.

این باج‌افزار به فایل‌های رمزگذاری شده پسوند epsilonred را الصاق می‌کند. ضمن آن که بر خلاف بسیاری از باج‌افزارها که برای جلوگیری از بروز اشکال در فرایند بالا آمدن دستگاه، از رمزگذاری فایل‌های با پسوند EXE و DLL پرهیز می‌کنند، Epsilon Red این فایل‌ها را نیز مورد دست‌درازی قرار می‌دهد.

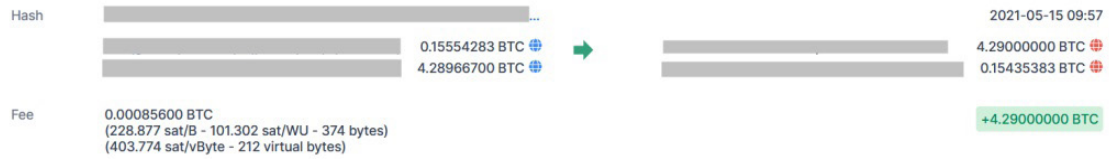
مشابه سایر باج افزارها، Epsilon Red نیز در پوشه پردازش شده، فایل موسوم به اطلاعیه باج‌گیری (Ransom Note) را که متن آن از اطلاعیه باج‌گیری REvil الگوبرداری شده کپی می‌کند.



Epsilon Red ransom note | REvil ransom note

علیرغم جدید بودن این باج‌افزار، تاکنون شرکت‌های مختلفی هدف آن قرار گرفته‌اند.

تحقیقات Sophos نشان می‌دهد که حداقل یکی از قربانیان در تاریخ ۲۵ اردیبهشت مبلغ ۴.۲۸ بیت‌کوین را به گردانندگان این باج افزار پرداخت کرده.



Epsilon Red برگرفته شده از شخصیتی با همین نام در دنیای مارول است که نقش یک ابرسرباز روسی دارای چهار شاخک با توانایی تنفس در فضا را ایفا می‌کند.

Sophos معتقد است که حداقل این نسخه از Epsilon Red، محصول برنامه‌نویسان حرفه‌ای نیست؛ به‌خصوص آن که بجز رمزگذاری، قابلیت‌های بسیار محدودی در آن به چشم می‌خورد. اما در هر صورت اجرای موفق آن در هر شبکه‌ای می‌تواند موجب رمزگذاری بدون محدودیت فایل‌ها و در نهایت بروز اختلالات جدی شود.

مشروح گزارش Sophos در لینک زیر قابل مطالعه است:

https://news.sophos.com/en-us/2021/05/28/epsilonred/

نشانه‌های آلودگی این باج‌افزار نیز در لینک زیر در دسترس قرار گرفته است:

https://github.com/sophoslabs/IoCs/blob/master/Ransomware-EpsilonRed.csv

منبع

https://www.bleepingcomputer.com/news/security/new-epsilon-red-ransomware-hunts-unpatched-microsoft-exchange-servers/

سرورهای آسیب‌پذیر vCenter،
هدف بدافزار FreakOut

تحقیقات جدید نشان می‌دهد نسخ جدید بدافزار FreakOut قادر به آلوده‌سازی سرورهای آسیب‌پذیر VMware vCenter هستند.

در ادامه این مطلب توسط شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده پیشینه این بدافزار و یافته های جدید محققان در خصوص آن ارائه شده است.

FreakOut که با نام‌های Necro و N3Cr0m0rPh نیز شناخته می‌شود، بدافزاری مبتنی بر Python است که دستگاه‌های با هر یک از بسترهای Windows و Linux را هدف قرار می‌دهد.

اولین بار در زمستان ۱۳۹۹، شرکت چک‌پوینت با انتشار گزارش زیر جزییات این بدافزار را به‌صورت عمومی منتشر کرد:

https://research.checkpoint.com/2021/freakout-leveraging-newest-vulnerabilities-for-creating-a-botnet/

FreakOut اسکریپتی مبهم‌سازی شده (Obfuscated) است که هسته چندشکلی (Polymorphic) و قابلیت روت‌کیتی مبتنی بر کاربر (User-mode Rootkit) آن، فایل‌های مخرب ایجاد شده توسط بدافزار را از دید محصولات امنیتی مخفی نگاه می‌دارد.

این بدافزار با بهره‌گیری از چندین آسیب‌پذیری در سیستم‌های عامل و برنامه‌ها و اجرای حملات موسوم به Brute-force در بستر SSH، دستگاه‌ها را به شبکه مخرب (Botnet) خود ملحق می‌کند.

قابلیت‌های پایه این بدافزار مهاجمان را قادر به اجرای حملات DDoS، راه‌اندازی درب‌پشتی بر روی سامانه‌های آلوده، اجرای باج‌افزار، شنود ترافیک شبکه و اجرای ابزارهای استخراج‌کننده نظیر XMRig می‌کند.

بر اساس گزارشی که شرکت سیسکو ۱۳ خرداد آن را منتشر کرد گردانندگان FreakOut از اواخر اردیبهشت که فعالیت شبکه مخرب آن ناگهان افزایش یافته در حال تکامل امکانات انتشار این بدافزار بوده‌اند.

از جمله این تغییرات می‌توان به برقراری ارتباطات متفاوت با سرور فرماندهی (C2) و افزوده شدن قابلیت سوءاستفاده از آسیب‌پذیری‌هایی علاوه بر موارد پیشین اشاره کرد.

دستگاه‌های آلوده بهFreakOut ، دستگاه‌های دیگر را بر اساس نشانی‌هایی که به‌صورت تصادفی استخراج شده‌اند یا نشانی‌هایی که از سوی سرور فرماندهی در بستر IRC ارسال می‌شوند شناسایی می‌کنند.

به ازای هر نشانی IP استخراج شده، دستگاه آلوده تلاش می‌کند تا با بکارگیری یکی از اکسپلویت‌های خود یا اطلاعات اصالت‌سنجی SSH درج شده در کد بدافزار، به آن رخنه کند.

نسخ اولیه FreakOut تنها آسیب‌پذیری‌های زیر را هدف قرار می‌دادند:

- Lifearay - Liferay Portal - Java Unmarshalling via JSONWS RCE
- Laravel RCE (CVE-2021-3129)
- WebLogic RCE (CVE-2020-14882)
- TerraMaster TOS
- Laminas Project laminas-http before 2.14.2, & Zend Framework 3.0.0

اما در نسخ جدید موارد زیر نیز به این فهرست افزوده شده‌اند:

- VestaCP - VestaCP 0.9.8 - ‘v_sftp_licence’ Command Injection
- ZeroShell 3.9.0 - ‘cgi-bin/kerbynet’ Remote Root Command Injection
- SCO Openserver 5.0.7 - ‘outputform’ Command Injection
- Genexis PLATINUM 4410 2.1 P4410-V2-1.28 - Remote Command Execution vulnerability
- OTRS 6.0.1 - Remote Command Execution vulnerability
- VMWare vCenter - Remote Command Execution vulnerability
- Nrdh.php remote code execution

در فهرست بالا، آسیب‌پذیری CVE-2021-21972 در VMware vCenter بیش از سایر موارد جلب توجه می‌کند. این آسیب‌پذیری در اسفند ۱۳۹۹ وصله شد. اما بر اساس آمار سایت‌هایی همچون Shodan و BinaryEdge، هزاران سرور vCenter آسیب‌پذیر همچنان در بستر اینترنت قابل دسترس هستند.

پیش‌تر و در پی انتشار نمونه کد بهره‌جو (Proof-of-Concept) آن نیز گزارش‌هایی مبنی بر پویش انبوه سرورهای آسیب‌پذیر vCenter منتشر شده بود. برخی نهادها هم قبلا در خصوص مورد سوءاستفاده قرار گرفتن CVE-2021-21972 توسط مهاجمان هشدار داده بودند.

در موارد متعددی در جریان حملات هدفمند باج‌افزاری آسیب‌پذیری‌های VMware به استخدام مهاجمان درآمده‌اند.

اعمال فوری وصله‌ها و به‌روزرسانی‌های امنیتی به تمامی راهبران توصیه می‌شود.

مشروح گزارش سیسکو در لینک زیر قابل مطالعه است:

https://blog.talosintelligence.com/2021/06/necro-python-bot-adds-new-tricks.html

دیپلمات‌ها؛

هدف BackdoorDiplomacy

ای‌ست (ESET) در گزارشی به بررسی بدافزار یک گروه APT پرداخته که به گفته این شرکت حداقل از سال ۲۰۱۷ دیپلمات‌ها را در نقاط مختلف جهان از جمله کشورهایی در آفریقا و خاورمیانه هدف قرار می‌داده است.

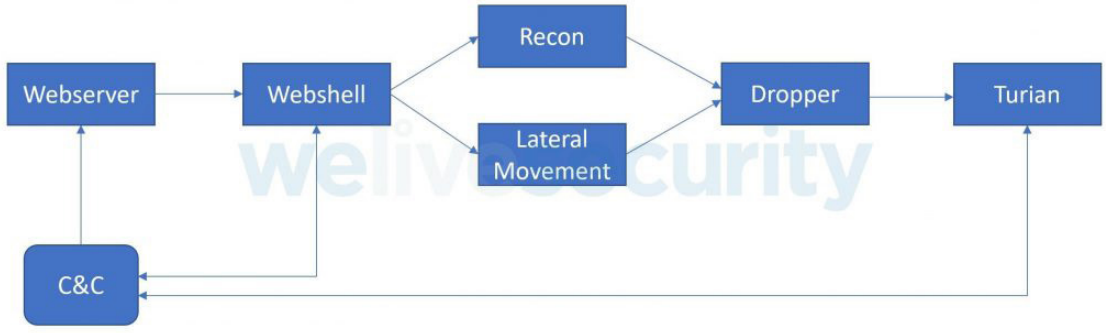
این گروه که از آن با عنوان BackdoorDiplomacy یاد شده، از بدافزاری سفارشی با نام Turian برای آلوده‌سازی اهداف خود بهره می‌گرفته است.

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

به نظر می‌رسد اصلی‌ترین روش نفوذ اولیه BackdoorDiplomacy، در هر دو بستر Windows و Linux، سوءاستفاده از آسیب‌پذیری سرویس‌ای قابل دسترس بر روی اینترنت است. چنانچه سرورهای وب یا واسط‌های مدیریت شبکه‌ای قربانی به دلیل وجود ضعف امنیتی نرم‌افزاری یا عدم مقاوم‌سازی صحیح آسیب‌پذیر تشخیص داده شوند، این مهاجمان اقدام به اجرای حمله می‌کنند.

در یکی از موارد، مهاجمان از آسیب‌پذیری CVE-2020-5902 در F5 برای توزیع یک درب‌پشتی Linux استفاده کرده بودند. یا در نمونه‌ای دیگر مهاجمان از باگ‌های امنیتی Exchange برای توزیع China Chopper Webshell بهره برده بودند.

به‌محض فراهم شدن دسترسی اولیه، مهاجمان اقدام به پوش دستگاه‌ها برای گسترش دامنه آلودگی می‌کنند. در ادامه نیز با نصب Turian و توزیع مجموعه‌ای از ابزارها، فعالیت کاربران قربانی را تحت رصد قرار داده و در نهایت داده‌ها را سرقت می‌کنند.



فهرست ابزارهای مورد استفاده در جریان انتشار BackdoorDiplomacy به‌شرح زیر گزارش شده است:

- EarthWorm که یک تونل شبکه‌ای ساده مبتنی بر SOCKS v۵ است؛
- Mimikatz و نسخ مختلف ابزارهای مبتنی بر آن از جمله SafetyKatz؛
- Nbtscan که یک پویشگر خط‌فرمان NetBIOS برای Windows است؛
- NetCat که یک ابزار شبکه‌ای برای خواندن و نوشتن داده‌ها در بستر ارتباطات شبکه‌ای است؛
- PortQry که برای شناسایی دستگاه‌های آسیب‌پذیر به EternalBlue مورد استفاده قرار می‌گیرد.

ضمن آنکه از ابزارهای مختلف ShadowBrokers شامل موارد زیر نیز بهره گرفته شده است:

- DoublePulsar
- EternalBlue
- EternalRocks
- EternalSynergy

همچنین مهاجمان از VMProtect برای مبهم‌سازی (Obfuscation) کدها و ابزارها استفاده کرده‌اند.

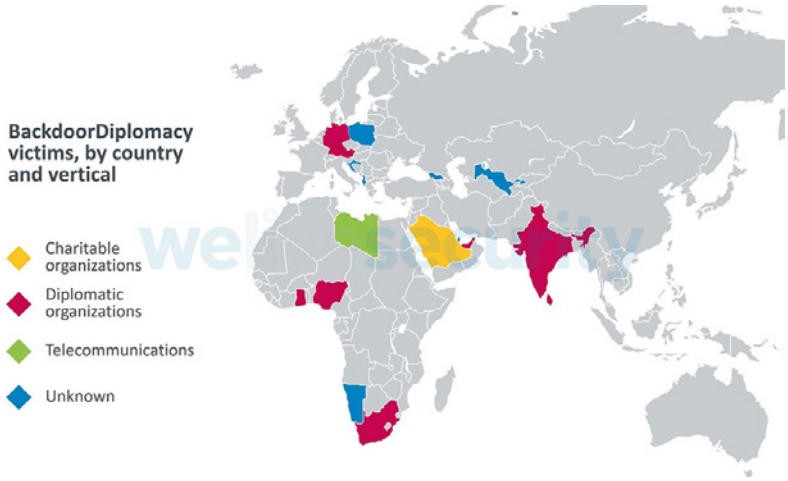
از دیگر فعالیت‌های مخرب BackdoorDiplomacy می‌توان به پویش حافظه‌های USB Flash متصل به دستگاه و در ادامه ارسال تمامی فایل‌های آنها به سرور فرماندهی (C2) در قالب یک فایل فشرده حاوی رمز عبور (Password-protected Archive) اشاره کرد.

اصلی‌ترین قابلیت Turian استخراج داده‌ها از روی دستگاه، تصویربرداری از فعالیت‌های کاربر و رونویسی، حذف/انتقال و سرقت فایل‌هاست.

بررسی‌ها نشان می‌دهد Turian بر پایه Quarian توسعه داده شده است. از Quarian در سال ۲۰۱۳ برای اجرای حمله سایبری بر ضد دیپلمات‌های سوری و آمریکایی استفاده شده بود.

روش رمزگذاری بکار گرفته شده توسط BackdoorDiplomacy بسیار مشابه با درب پشتی Whitebird است که گروه Calypso در سال‌های ۲۰۱۷ تا ۲۰۲۰ از آن برای حمله به دیپلمات‌های قزاقستان و قرقیزستان استفاده کرده بود. ضمن آن که شباهت‌هایی نیز با گروه CloudComputating/Platinum که حمله به دیپلمات‌ها، دولت‌ها و سازمان‌های نظامی در آسیا را در کارنامه دارد مشاهده می‌شود. تشابهاتی نیز در سازوکار و کدنویسی گروه‌های Rehashed Rat و MirageFox/APT15 گزارش شده است.

به گفته ای‌ست، BackdoorDiplomacy، موفق به حمله به وزارت خارجه کشورهایی در آفریقا، آسیا و اروپا، چند شرکت فعال در حوزه مخابرات در آفریقا و خاورمیانه و یک نهاد خیریه در عربستان سعودی شده است.



کمتر از دو هفته قبل نیز شرکت چک‌پوینت (Check Point Software Technologies) در گزارش زیر از شناسایی یک درب‌پشتی نو با نام VictoryDll_x86.dll خبر داد که مهاجمان چینی از آن برای نفوذ به وزارت خارجه کشورهایی در جنوب شرق آسیا استفاده کرده بودند:

https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/

مشروح گزارش ای‌ست در لینک زیر قابل مطالعه است:

https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

WinRM نیز

آسیب‌پذیر در برابر CVE-2021-31166

نتایج بررسی محققان نشان می‌دهد که آسیب‌پذیری CVE-2021-31166، سرویس WinRM در نسخ ۲۰۰۴ و 20H2 سیستم‌های عامل Windows 10 و Windows Server را نیز متأثر می‌کند. پیش‌تر تصور می‌شد دامنه این آسیب‌پذیری محدود به سرویس IIS است.

CVE-2021-31166 از HTTP Protocol Stack یا همان فایل HTTP.sys که سرویس‌دهنده Windows Internet Information Services - به اختصار IIS - از آن به‌عنوان یک شنودکننده (Listener) به‌منظور پردازش درخواست‌های HTTP استفاده می‌کند ناشی می‌شود.

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

مایکروسافت ۲۱ اردیبهشت وصله CVE-2021-31166 را منتشر کرد. این شرکت اعلام کرده که سوءاستفاده از این آسیب‌پذیری امکان "اجرای کد به‌صورت از راه دور" را در "بسیاری مواقع" میسر می‌کند. مایکروسافت اعمال وصله را با اولویت بالا توصیه کرده است.

به‌تازگی نیز نمونه اثبات‌گر (Proof-of-Concept) آن به‌صورت عمومی در دسترس قرار گرفته است.

پس از انتشار جزییات CVE-2021-31166، یک محقق امنیتی خبر داد که دستگاه‌های با هر یک از سیستم‌های عامل Windows 10 و Windows Server که سرویس WinRM بر روی آنها فعال است هم نسبت به این ضعف امنیتی آسیب‌پذیر هستند.

Windows Remote Management - به اختصار WinRM - جزیی از Windows Hardware Management محسوب می‌شود.

WinRM به‌صورت پیش‌فرض بر روی Windows 10 غیرفعال است. اما بر روی سرورها این سرویس به‌طور پیش‌فرض در وضعیت فعال قرار دارد و استفاده از آن نیز در بسترهای سازمانی متداول است.

بر طبق آمار سایت shodan.io در حال حاضر بیش از ۲ میلیون سامانه Windows که WinRM بر روی آنها فعال است در اینترنت قابل دسترس هستند. با این توضیح که تنها نسخ ۲۰۰۴ و ۲۰H2 سیستم‌های عامل Windows 10 و Windows Server آسیب‌پذیر گزارش شده‌اند.

با توجه به انتشار نمونه اثبات‌گر و گسترده بودن دامنه این آسیب‌پذیری، به کلیه راهبران توصیه می‌شود چنانچه هنوز نسبت به اعمال وصله امنیتی مربوطه اقدام نکرده‌اند، انجام آن را با اولویت بالا در دستور کار قرار دهند.

به‌روزرسانی‌ها و اصلاحیه‌ها؛

در خرداد ۱۴۰۰

در خرداد ۱۴۰۰، مایکروسافت، رد هت، سیسکو، مک‌آفی، وی‌ام‌وِر، بیت‌دیفندر، ادوبی، اس‌آپ، گوگل، اپل، موزیلا و دروپل اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

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

مـایـکـروسـافـت

۱۸ خرداد، شرکت مایکروسافت (Microsoft Corp)، مجموعه‌اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی ژوئن منتشر کرد. اصلاحیه‌های مذکور در مجموع ۵۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند.

درجه اهمیت ۵ مورد از این آسیب‌پذیری‌ها "حیاتی" (Critical) و ۴۵ مورد "مهم" (Important) اعلام شده است.

از این میان، ۷ آسیب‌پذیری ترمیم شده از نوع روز-صفر گزارش شده که حداقل ۶ مورد از آنها از مدتی قبل مورد سوءاستفاده مهاجمان قرار گرفته‌اند. لذا اعمال فوری به‌روزرسانی‌ها و وصله‌های امنیتی مربوطه در اسرع وقت توصیه اکید می‌شود.

فهرست آسیب پذیری‌های روز-صفری که سوءاستفاده از آنها از سوی برخی منابع امنیتی گزارش شده به شرح زیر است:

- CVE-2021-31955 - ضعفی از نوع "نشت اطلاعات" (Information Disclosure) است که Windows Kernel از آن تأثیر می‌پذیرد.
- CVE-2021-31956 - ضعفی از نوع "ترفیع امتیازی" (Elevation of Privilege) است که سیستم فایل NTFS در سیستم عامل Windows از آن متأثر می‌شود.
- CVE-2021-33739 - ضعفی از نوع "ترفیع امتیازی" است که از Microsoft DWM Core Library ناشی می‌شود.
- CVE-2021-33742 - ضعفی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) در MSHTML Platform است.
- CVE-2021-31199 و CVE-2021-31201 - هر دو، ضعفی از نوع "ترفیع امتیازی" در Microsoft Enhanced Cryptographic هستند.

CVE-2021-31968، دیگر آسیب‌پذیری روز-صفر این ماه است که علیرغم افشای جزییات آن، تا این لحظه موردی از بهره‌جویی از آن توسط مهاجمان، حداقل به‌صورت عمومی گزارش نشده است. آسیب پذیری مذکور ضعفی از نوع "منع سرویس" (Denial of Service) است که Windows Remote Desktop Services از آن تأثیر می‌پذیرد.

بر اساس گزارشی که آزمایشگاه کسپرسکی (Kaspersky Lab) در ۱۸ خرداد آن را منتشر کرد CVE-2021-31955 و CVE-2021-31956 از ماه‌ها پیش مورد سوءاستفاده گروه PuzzleMaker قرار گرفته بوده است. PuzzleMaker، در جریان حملاتی کاملا هدفمند، ابتدا از یک ضعف امنیتی روز-صفر در Chrome در زنجیره Exploit بهره گرفته و در ادامه با ترکیب دو آسیب‌پذیری مذکور سطح دسترسی خود را در Windows ارتقا می‌داده است. در نهایت نیز مهاجمان با ایجاد یک به اصطلاح Remote Shell بر روی آن، امکان آپلود و دانلود فایل‌ها و اجرای فرامین را برای خود فراهم می‌کرده‌اند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های ژوئن ۲۰۲۱ مایکروسافت در گزارش زیر که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده قابل مطالعه است:

https://afta.gov.ir/portal/home/?news/235046/237266/243924/

رد هت

به تازگی محققان از شناسایی ضعفی در polkit خبر داده‌اند که سوءاستفاده از آن، مهاجم، با دسترسی محدود را قادر به دستیابی به سطح دسترسی root می‌کند. polkit یک سرویس اصالت‌سنجی است که به‌صورت پیش‌فرض بر روی بسیاری از توزیع‌های اخیر Linux نصب شده است. باگ مذکور با شناسه CVE-2021-3560 در دسته آسیب‌پذیری‌های Local Privilege Escalation قرار می‌گیرد. وصله این آسیب‌پذیری که اکنون جزییات آن به‌صورت عمومی منتشر شده از ۱۳ خرداد توسط شرکت رد هت (Red Hat, Inc) در دسترس قرار گرفته است. در گزارش زیر که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده خلاصه‌ای از جزییات این ضعف امنیتی ارائه شده است:

https://afta.gov.ir/portal/home/?news/235046/237266/243942/

سیسکو

شرکت سیسکو (Cisco Systems, Inc) در خرداد ماه در چندین نوبت اقدام به عرضه اصلاحیه‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها ۴۵ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۱۵ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "تزریق فرمان" (Command Injection)، "نشت اطلاعات"، "ترفیع امتیازی" و "منع سرویس" 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

مک‌آفی

در خرداد ۱۴۰۰، شرکت مک‌آفی (McAfee, LLC)، با انتشار نسخه جدید، چندین آسیب‌پذیری امنیتی را در محصولات زیر ترمیم کرد:

McAfee Agent: https://kc.mcafee.com/corporate/index?page=content&id=SB10362

McAfee Data Loss Prevention Endpoint:
https://kc.mcafee.com/corporate/index?page=content&id=SB10360

McAfee Database Security: https://kc.mcafee.com/corporate/index?page=content&id=SB10359

McAfee GetSusp: https://kc.mcafee.com/corporate/index?page=content&id=SB10363

از مجموع ۹ آسیب‌پذیری ترمیم شده توسط نسخ جدید، شدت حساسیت ۲ مورد "حیاتی"، ۲ مورد "بالا"، ۴ مورد "متوسط" و ۱ مورد "کم" گزارش شده است.

وی‌اِم‌وِر

در خرداد شرکت وی‌اِم‌وِر (VMware, Inc) با انتشار توصیه‌نامه، نسبت به وجود یک آسیب‌پذیری "حیاتی" در یکی از افزونه‌های پیش‌فرض vCenter Server هشدار داد. آسیب‌پذیری مذکور با شناسه CVE-2021-21985 ضعفی از نوع "اجرای کد به‌صورت از

راه دور" (RCE) است که از عدم اعتبارسنجی صحیح ورودی‌های افزونه Virtual SAN Health Check ناشی می‌شود. افزونه مذکور به‌طور پیش‌فرض بر روی سرورهای vCenter فعال است. شدت این آسیب‌پذیری ۹.۸ از ۱۰ (بر طبق استاندارد CVSSv3) گزارش شده است. vSAN، حتی در صورت فعال نبودن، نسخ ۶.۵، ۶.۷ و ۷.۰ سرور vCenter را در معرض خطر قرار می‌دهد. جزییات بیشتر در خصوص آسیب‌پذیری مذکور در گزارش زیر که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری قابل مطالعه است:

https://afta.gov.ir/portal/home/?news/235046/237266/243788/

بـیـت‌دیـفـنـدر

در سومین ماه سال ۱۴۰۰ شرکت بیت‌دیفندر (Bitdefener, Inc) اقدام به انتشار نسخ جدید زیر کرد:

Bitdefender GravityZone version 6.24.1-1:
https://www.bitdefender.com/support/bitdefender-gravityzone-6-24-1-1-release-notes-2705.html

Bitdefender Endpoint Security Tools 7.1.2.33:
https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-7-1-2-33-release-notes-(windows)-2706.html

Bitdefender Endpoint Security Tools 6.6.100.397:
https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-6-100-397-release-notes-(windows)-2710.html

Bitdefender Endpoint Security Tools for Linux 6.2.21.160:
https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-2-21-160-release-notes-(linux)-2711.html

Endpoint Security for Mac 4.17.26.200176:
https://www.bitdefender.com/support/endpoint-security-for-mac-version-4-17-26-200176-release-notes-2709.html

لازم به ذکر است در نسخه جدید Bitdefender Endpoint Security Tools for Linux ضعفی با شناسه CVE-2021-3485 وصله شده که سوءاستفاده از آن مهاجم را قادر به اجرای کد به صورت از راه دور می‌کند. شدت حساسیت این آسیب‌پذیری ۶.۴ از ۱۰، بر طبق استاندارد CVSS:3.1 گزارش شده است. جزییات بیشتر در لینک زیر قابل دریافت است:

https://www.bitdefender.com/support/security-advisories/improper-input-validation-in-bitdefender-endpoint-security-tools-for-linux-va-9769/

ادوبـی

در خرداد، شرکت ادوبی (Adobe, Inc) اقدام به انتشار به‌روزرسانی برای ۱۰ محصول خود از جمله Adobe Acrobat & Reader کرد که جزییات آن در لینک زیر قابل مطالعه است:

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

اس‌آپ

اس‌آپ (SAP SE) نیز در خرداد ۱۴۰۰ با انتشار مجموعه‌اصلاحیه‌های ماه ژوئن، نزدیک به ۲۰ آسیب‌پذیری را در چندین محصول خود برطرف کرد. شدت دو مورد از این ضعف‌های امنیتی بیش از ۹ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده است. بهره‌جویی از بعضی از 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=578125999

گـوگـل

شرکت گوگل (Google, LLC) در خرداد، در چندین نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۷ خرداد انتشار یافت ۹۱.۰.۴۴۷۲.۱۱۴ است. دو آسیب‌پذیری ترمیم شده، ضعف‌هایی روز-صفر با شناسه‌های CVE-2021-30551 و CVE-2021-30554 هستند که از قبل انتشار اصلاحیه‌های مربوطه، مورد سوءاستفاده مهاجمان قرار گرفته‌اند. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html

https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_14.html

https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop.html

اپـل

در خرداد ماه، شرکت اپل (Apple, Inc) با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در چندین محصول خود از جمله سیستم عامل macOS ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

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

مـوزیـلا

در ماهی که گذشت شرکت موزیلا (Mozilla, Corp) با ارائه به‌روزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد. درجه حساسیت برخی از این آسیب‌پذیری‌های ترمیم شده، "بالا" گزارش شده است. توضیحات بیشتر در لینک زیر قابل مطالعه است:

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

دروپـال

۵ خرداد، جامعه دروپال (Drupal Community) با عرضه به‌روزرسانی‌های امنیتی، یک آسیب‌پذیری با شناسه CVE-2021-33829 را در برخی نسخ Drupal اصلاح کرد؛ سوءاستفاده از آن، مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توضیحات کامل در این خصوص در لینک زیر قابل دسترس است:

https://www.drupal.org/sa-core-2021-003

گزارش‌ها

سامانه‌های صنعتی،
هدف مهاجمان بیشتر

یافته‌های جدید نشان می‌دهد که اجرای حملات نه چندان پیچیده و مبتنی بر روش‌های معمول بر ضد پروسه‌های کنترلی در سامانه‌های صنعتی، رو به افزایش است.

شرکت فایرآی (FireEye, Inc) سه‌شنبه، ۴ اردیبهشت گزارشی را منتشر کرد که در آن به حملاتی پرداخته شده که در جریان آنها پروسه‌های کنترلی به‌ویژه نرم‌افزارها و سخت‌افزارهای موسوم به OT (فناوری عملیاتی) نظیر PLC و SCADA هدف قرار گرفته‌اند.

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

در حالی که در برهه‌ای، حمله به پروسه‌های کنترلی، به دلیل دشواری دسترسی به آنها پیچیده به‌نظر می‌آمد، اکنون مدتی است که در معرض قرار گرفتن این پروسه‌ها و وجود آسیب‌پذیری در آنها و به‌طور کلی گسترده‌تر شدن دامنه اهداف، هک و بروز اختلال در فناوری‌های اختصاصی صنعتی را تسهیل کرده است.

به گفته فایرآی، تعداد حملات غیرپیچیده بر ضد محصولات حوزه OT روندی افزایشی داشته و این شرکت شاهد اجرای حمله توسط هکرهایی با سطوح توانایی و منابع مختلفی است که با استفاده از ابزارها و تکنیک‌های معمول برای دسترسی یافتن و رخنه کردن به سامانه‌های صنعتی تلاش می‌کنند.

شبکه پنل‌های انرژی خورشیدی، سامانه‌های کنترل آب و سامانه‌های اتوماسیون ساختمان (BAS) نمونه‌هایی هستند که هدف این گونه حملات قرار گرفته‌اند. زیرساخت‌های حیاتی در حالی در فهرست این مهاجمان قرار دارند که از تکنیک‌هایی یکسان برای حمله به تجهیزات موسوم به اینترنت اشیاء (IoT) در مراکز آکادمیک و منازل افراد استفاده می‌شود.

محققان فایرآی معتقدند از جمله دلایل افزایش حمله به سامانه‌های OT، ورود مهاجمانی است که با گرایش‌های ایدئولوژیک، خودپرستی افراطی یا مالی برای ایجاد اختلال‌های هر چند کوچک - بجای در اختیار گرفتن هسته زیرساخت - تقلا می‌کنند.

طی چند سال گذشته، تجهیزات OT از روش‌های مختلفی همچون سرویس‌های دسترسی از راه دور و بسترهای VNC هدف هکرها قرار گرفته‌اند.

بسیاری از این مهاجمان صرفاً در پی دسترسی یافتن به کنسول مدیریتی در تجهیزات OT هستند. کنسول‌هایی که بر پایه آسان ساختن مدیریت تنظیمات پیچیده این تجهیزات طراحی شده‌اند و عملاً مهاجم را قادر می‌کنند تا با دانش هر قدر اندک خود در حوزه این تجهیزات مقادیر متغیرهای صنعتی را تغییر دهد.

نکته قابل توجه دیگر، گرایش هکتیویسم است که به سبب منابع آموزشی گسترده‌ای که به رایگان بر روی اینترنت قابل دسترس است روز به روز افراد بیشتری را به خود جلب می‌کند.

برخی مهاجمان کم‌تجربه نیز علیرغم دانش کم در خصوص اهدافشان بر روی بدنام کردن اهداف خود تمرکز دارند.

برای مثال، در یکی از حملات ادعا شده بود که یک سامانه خط آهن در آلمان هک شده است. در حالی که دستاورد هکرها محدود به یک ایستگاه کنترلی مدل‌سازی قطارها بود. یا در نمونه‌ای دیگر مهاجمان مدعی هک سامانه سوخت یکی از کشورها شده بودند؛ در صورتی که فقط سامانه تهویه یک رستوران را هک کرده بودند.

آنچه که نباید از نظرها دور بماند عواقب بعضاً جبران‌ناپذیر و فاجعه‌بار اجرای هر حمله مخرب به تجهیزات OT است. حمله باج‌افزاری اخیر به Colonial Pipeline که منجر به بروز بحران و کمبود سوخت در ایالات متحده شد نمونه‌ای از اثرات چنین حملاتی است.

با افزایش تعداد حملات، ریسک بروز اختلال نیز بیشتر می‌شود. افشای عمومی این رخدادها هم می‌تواند به نوعی منجر به عادی پنداشته شدن اجرای عملیات سایبری بر ضد سامانه‌های OT و تشویق مهاجمان بیشتر به ورود به این حوزه شود. ضمن آنکه باید انتظار داشت که گروه‌های قدرتمندتر با انگیزه‌های مالی از جمله گردانندگان باج‌افزار بیش از قبل بر روی سامانه‌های OT تمرکز کنند.

فایرآی پیشنهاد کرده که تا حد امکان سامانه‌های OT از شبکه‌های متصل به اینترنت دور نگاه داشته شوند، شبکه مقاوم‌سازی شده، ممیزی‌های امنیتی شامل کشف دستگاه‌های غیرمجاز در دوره‌های زمانی مرتب انجام شده و اجزای سامانه‌های OT به نحوی پیکربندی شوند که در برابر اعمال تنظیمات بالقوه مخرب در امان باشند.

پیش‌تر نیز برخی نهادها و سازمان‌های امنیتی و نظارتی در ایالات متحده در خصوص حمله به بسترهای حیاتی OT هشدار داده بودند. این نهادها وجود دستگاه‌های قدیمی، اتصال به اینترنت و روش‌های پیشرفته حمله را عامل ظهور "یک طوفان تمام‌عیار" توصیف کرده بودند.

مشروح گزارش فایرآی در لینک زیر قابل مطالعه است:

https://www.fireeye.com/blog/threat-research/2021/05/increasing-low-sophistication-operational-technology-compromises.html

نگاهی نزدیک

به حملات یک باج‌افزار بی‌رحم

یافته‌های شرکت امنیتی سوفوس (Sophos Ltd) نشان می‌دهد نمی‌توان دو گروه از مهاجمان را یافت که از سرویس RaaS باج‌افزار REvil به‌نحوی یکسان در جریان حملات خود استفاده کرده باشند.

روی آوردن به سرویس‌های RaaS تغییراتی اساسی در روش کار باج‌افزارها ایجاد کرده است.

در خدمات باج‌افزار به‌عنوان سرویس (Ransomware-as-a-Service) - به اختصار RaaS -، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به نویسنده و بخشی دیگر به متقاضی می‌رسد.

بدین‌ترتیب از یک سو برنامه‌نویسان آنها بر روی توسعه امکانات باج‌افزار تمرکز می‌کنند و از سویی دیگر وظیفه انتشار به گروه‌هایی با تجربه، متخصص و مجهز به منابع لازم سپرده می‌شود.

REvil که با نام Sodinokibi نیز شناخته می‌شود از جمله باج‌افزارهایی است که به‌صورت RaaS ارائه می‌شود و توانسته طرفداران زیادی را در بازارهای زیرزمینی تبهکاران سایبری به خود جلب کند.

شرکت امنیتی سوفوس در گزارشی به بررسی REvil و روش‌های بکار گرفته شده در جریان انتشار این باج‌افزار پرداخته که برگردان آن که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده در ادامه این مطلب ارائه شده است.

```
------ Welcome. Again. ------

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion
[[CODE INDICATING ENCRYPTED FILES]].
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you
cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do
our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free.
That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,
cause just we have the private key. In practise - time is much more valuable than money.
```

در حملات هدفمند باج‌افزاری، معمولا توزیع فایل مخرب باج‌افزار، آخرین مرحله از فرایند حمله است. در بسیاری مواقع تاریخ آغاز رخنه مهاجمان بسیار قبل‌تر از زمانی است که کاربران فایل اطلاعیه باج‌گیری (Ransom Note) را بر روی دسکتاپ خود می‌بینند.

در این گزارش ضمن مرور قابلیت‌های REvil، بر روی اقدامات تکثیرکنندگان، به‌طور خاص تمرکز شده است. اگر محصولات امنیتی یا راهبران شبکه بتوانند به‌سرعت این الگوها را کشف کنند در همان زمانی که مهاجمان در حال محکم کردن جای خود در شبکه هستند می‌توان پیش از وارد آمدن هر گونه خسارت تلاش آنها را ناکام گذاشت.

مهاجمان از ترکیبی از اسکریپت‌ها (که در برخی موارد بر روی انباره‌های فایلی نظیر Github یا Pastebin میزبانی می‌شوند) و در بسیاری موارد با استفاده از پودمان Remote Desktop Protocol - به اختصار RDP - یا دیگر ابزارهای دسترسی از راه دور امور را در شبکه قربانی مدیریت می‌کنند.

برای مثال در یکی از حملات، توزیع‌کنندگان REvil، اسکریپت‌های زیر را که همگی جزیی از یک مجموعه تست نفوذ (Penetration Tester Tools) هستند مستقیما از Github دریافت کرده بودند.

File path and name
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/nc.exe
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/privesc.exe
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/SharpByeBear.exe
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/SharpPolarbearx86.exe
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/schedsvc.dll
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/schtasks.exe
https://github[.]com/S3cur3Th1sSh1t/Creds/raw/master/exeFiles/winexploits/test.job
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Invoke-Sharpcradle/master/Invoke-Sharpcradle.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/cve-2020-0683.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/cve-2019-1215.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/m15-077.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/juicypotato64.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/invoke-juicypotato.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/cve-2018-8120.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/ms16-32.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/ms16-135.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/view.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/viewdevobfs.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/adpass.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/Invoke-Sharp.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/locksher.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/UpPower.ps1
https://raw.githubusercontent[.]com/S3cur3Th1sSh1t/Creds/master/obfuscatedps/GPpass.ps1

SOPHOSlabs

سوفوس یک حمله معمول REvil را به مراحل زیر تقسیم می‌کند:

- نفوذ و فراهم کردن دسترسی اولیه
- استخراج اطلاعات اصالت‌سنجی و ارتقای سطح دسترسی
- آماده‌سازی بستر
- توزیع باج‌افزار

همچنین در اغلب اوقات در مرحله‌ای از حمله، مهاجمان با تکیه بر اطلاعات اصالت‌سنجی به دست آمده اقدام به کشف و سرقت داده‌های حساس قربانی قبل از توزیع باج‌افزار می‌کنند.

نـفوذ بـه شـبکه

رخنه، بر خلاف آن چه که بسیاری تصور می‌کنند کار سختی برای هکرهای حرفه‌ای نیست. یکی از اصلی‌ترین روش‌های به کار گرفته شده در این مرحله اجرای حملات سعی‌وخطا (Brute-force) بر ضد سرویس‌های قابل دسترس بر روی اینترنت نظیر RDP و VNC و حتی برخی سامانه‌های رایانش ابری است.
سوءاستفاده از اطلاعات اصالت‌سنجی که پیش‌تر از طریق جاسوس‌افزارها و حملات فیشینگ به دست مهاجمان رسیده نیز یکی از روش‌های به کار گرفته شده در این مرحله است.

متاسفانه تلاش‌های سعی‌وخطا بخش زیادی از ترافیک تقریبا هر سرویس قابل دسترس بر روی اینترنت را تشکیل می‌دهد. هزینه اجرای حمله سعی‌وخطا اگر چه برای مهاجمان ناچیز است اما در صورت موفقیت عملا نقش دربی را خواهد داشت که به روی آنها برای ورود به شبکه باز شده است. به همین خاطر استفاده از سازوکارهای اصالت سنجی چندمرحله‌ای (MFA) راهکاری مؤثر در مقابله با این تهدیدات است. در این مرحله از ابزارهایی نظیر Shodan یا Censys نیز به‌منظور کشف درگاه‌های باز بهره گرفته می‌شود.

در یکی از حملات اخیر، سازمان با حجم انبوهی از تلاش‌ها برای ثبت‌ورود (Login) در بستر RDP مواجهه شده بود که در نهایت یکی از این تلاش‌ها به سرانجام می‌رسد. بر روی یک سرور عادی لاگی که تلاش‌های ناموفق برای ورود به سرور RDP را نگهداری می‌کند بسته به تعداد رخدادها ممکن است در عرض چند روز داده‌های جدید را بر روی داده‌های نه چندان قدیمی رونویسی کند. برای مثال در این نمونه در عرض پنج دقیقه، تقریبا ۳۵۰۰۰ تلاش ناموفق از سوی ۳۴۹ نشانی IP منحصربه فرد از مبدا کشورهای مختلف ثبت شده بوده است. فهرست نام‌های کاربری که در جریان این حملات برای هک کردن آنها تلاش شده بود در تصویر زیر قابل مشاهده است:

Username	Failed login attempts
ADMINISTRATOR	12,638
ADMIN	10,360
USER	439
SERVER	420
ADMINISTATOR1	167
TRAINING	33
CORPORATE	24
OPERATION	24
STATION	24
LIBRARY	22

RDP یکی از متداول‌ترین درگاه‌هایی است که مهاجمان از آن برای رخنه به شبکه بهره می‌گیرند. لذا از کار انداختن دسترسی از راه دور در بستر اینترنت یکی از کلیدی‌ترین راهکارها در مقابله با این تهدیدات است. اما RDP تنها پودمانی نیست که مورد سوءاستفاده قرار می‌گیرد. در بسیاری موارد نیز مهاجمان از طریق دیگر سرویس‌های قابل دسترس بر روی اینترنت و اجرای حملات سعی‌وخطا بر ضد آنها یا سوءاستفاده از آسیب‌پذیری‌های امنیتی راه رخنه به شبکه را پیدا می‌کنند. در یکی از این حملات، مهاجمان از باگی در نرم‌افزار یک سرور خاص VPN برای دسترسی به شبکه قربانی سوءاستفاده کرده بودند. در ادامه هم از یک باگ Apache Tomcat که پنج سال از شناسایی آن می‌گذشت بر روی همان سرور بهره‌جویی شده و در نهایت یک حساب کاربری با سطح دسترسی Administrator بر روی آن سرور ثبت شده بود.

در دو حمله به دو سازمان متفاوت نقطه اولیه دسترسی چیزی بود که از گروهی دیگر از مهاجمان بجا مانده بود که نشان می‌داد ماه‌ها پیش از دخالت محققان سوفوس آنها قربانی شده بودند. در یکی از این دو مورد، کارشناسان سوفوس، Cobalt Strike را که یک مجموعه ابزار تجاری تست نفوذ پرطرفدار است و به کرات مورد سوءاستفاده مهاجمان قرار می‌گیرد کشف کرده بودند. این ابزار توسط گروهی دیگر که پیش‌تر باج‌افزار Le Chiffre را شبکه قربانی توزیع کرده بودند جا مانده بود.

یا در نمونه‌ای دیگر به نظر می‌رسد مهاجمان اقدام به اجرای حمله "سعی‌و خطا" بر ضد ماشینی کردند که ردپای حضور مهاجمانی دیگر تنها سه هفته قبل از حمله REvil بر روی آن به چشم می‌خورد.

Initial Access	Execution	Persistence	Defense Evasion	Lateral Movement	Command & Control	Impact
Valid accounts ID: T1078	Command and Scripting Interpreter ID: T1059	Valid accounts ID: T1078	Impair Defenses ID: T1562	T1570 - Lateral Tool Transfer ID: T1570	Application Layer Protocol ID: 1071	Data Encrypted for Impact ID: T1486
	Scheduled Task/Job ID: T1053	Create or Modify System Process ID: T1543		Remote Services: Remote Desktop Protocol ID: T1021.001		Data Destruction ID: T1485

SOPHOSlabs

اسـتخراج اطلاعـات اصـالت‌سنجی و ارتـقای سطح دسـترسی

گردانندگان باج‌افزار ترجیح می‌دهند که از ابزارهای داخلی سازمان قربانی نظیر سرورهای Domain Controller برای توزیع کد مخرب استفاده کنند. اگر اطلاعات اصالت‌سنجی سرقت/کشف شده در جریان حملات فیشینگ را خریداری نکرده باشند معمولا ارتباطات را بر روی اولین دستگاه آلوده رصد می‌کنند. ضمن آن‌که ممکن است از ابزارهایی که به رایگان در دسترسند و لزوما مخرب محسوب نمی‌شوند برای استخراج رمزهای عبور ذخیره شده از روی دیسک سخت و/یا ابزارهای پیشرفته‌ای همچون Mimikatz برای دستیابی به اطلاعات اصالت‌سنجی یک حساب کاربری با سطح دسترسی Domain Admin دامنه بهره بگیرند. لازمه این کار صبوری مهاجمان است؛ به‌خصوص آن که تضمینی نیست که لزوما در زمان صرف شده به اطلاعات اصالت‌سنجی دست پیدا کنند. اما به محض دستیابی می‌توانند به‌سرعت وارد مرحله بعد شوند.

آمـاده‌سـازی بسـتر

آماده سازی یک شبکه سازمانی برای اجرای حمله‌ای باج‌افزاری پیچیده‌تر از آن است که به نظر می رسد. مهاجمان قبل از هر چیز نیاز به در اختیار داشتن سطح دسترسی Domain Admin برای از کاراندازی هر چیزی که مانع از اجرای موفق حمله آنها می‌شود دارند. از Windows Defender گرفته تا محصولات امنیتی دیگر؛ به‌طور معمول هکرها زمانی را صرف شناخت ابزارهای حفاظتی اجرا شده بر روی نقاط پایانی کرده و در ادامه با اجرای یک یا چندین اسکریپت سفارشی نسبت به از کاراندازی پروسه‌ها و سرویس‌های آنها تلاش می‌کنند.

برای مثال در جریان یکی از حملات REvil مهاجمان با اجرای اسکریپت زیر برای متوقف کردن سرویس‌ها و پروسه‌های سوفوس و حتی حذف آنها تلاش کرده بودند که البته قابلیت Sophos Tamper Protection مانع از موفقیت آنها شده بود.

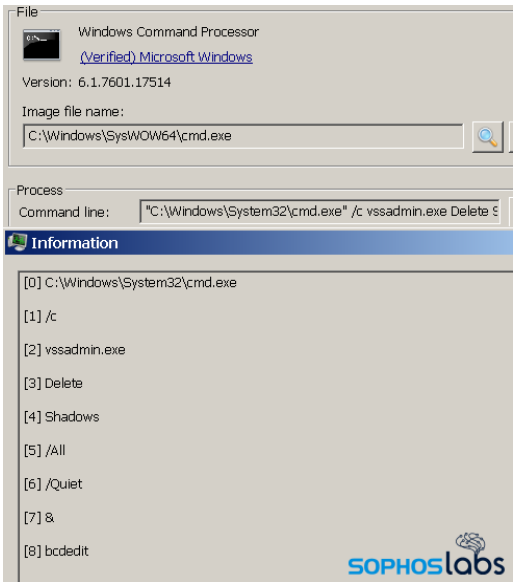
```
net stop "Sophos AutoUpdate Service"
net stop "Sophos Agent"
net stop "SAVService"
net stop "SAVAdminService"
net stop "Sophos Message Router"
net stop "Sophos Web Control Service"
net stop "swi_service"
net stop "SntpService"
net stop "sophossps"
net stop "swi_filter"

MsiExec.exe /X{66967E5F-43E8-4402-87A4-04685EE5C2CB} /qn
MsiExec.exe /X{1093B57D-A613-47F3-90CF-0FD5C5DCFFE6} /qn
MsiExec.exe /X{66967E5F-43E8-4402-87A4-04685EE5C2CB} /qn REBOOT=SUPPRESS
MsiExec.exe /X{1093B57D-A613-47F3-90CF-0FD5C5DCFFE6} /qn REBOOT=SUPPRESS
net stop "Sophos Anti-Virus"
net stop "Sophos AutoUpdate Service"
"C:\program files\Sophos\Sophos Endpoint Agent\uninstallcli.exe"
:Sophos AutoUpdate
MsiExec.exe /qn /X{7CD26A0C-9B59-4E84-B5EE-B386B2F7AA16} REBOOT=ReallySuppress
```

SOPHOSlabs

در حداقل یک حمله REvil نیز مهاجمان با بررسی دقیق، دریافته بودند که قربانی از فایروال سوفوس استفاده کرده و امنیت نقاط پایانی خود را از طریق Sophos Central مدیریت می‌کند. این هکرها با پشتکار فراوان، پس از دستیابی به اطلاعات اصالت‌سنجی کارکنان واحد فناوری اطلاعات برای دسترسی یافتن به کنسول Sophos Central تلاش کرده بودند و در نهایت اطلاعات اصالت‌سنجی یکی از کارکنان، آنها را موفق به ورود به کنسول کرده بود. بدین‌ترتیب آنها قادر بودند تا هر امکان امنیتی را که مانع از توزیع باج‌افزار می‌شده به‌صورت مرکزی و از راه دور غیرفعال کنند.

به‌طور معمول، مهاجمان با بکارگیری اسکریپت‌های PowerShell، فایل‌های Batch و یا سایر کدهای بسترساز برای غیرفعال کردن قابلیت‌های امنیتی و حفاظتی نقاط پایانی قربانی تلاش می‌کنند. به عنوان نمونه Volume Shadow Copy در اکثر موارد توسط اسکریپت حذف می‌شود تا امکان بازگردانی فایل‌های حذف شده یا رمزگذاری شده از طریق آن ممکن نباشد.



تعداد فرامین مختلفی که مهاجمان می‌توانند از آنها برای اجرای این گونه اقدامات استفاده کنند اگر چه محدود است اما روش اجرای آنها در هر حمله متفاوت است. به گفته سوفوس در نامگذاری این اسکریپت‌ها، مهاجمان از اعداد و نام‌هایی که به آنها جلوه‌ای معتبر می‌دهد بهره می‌گیرند.

استخراج و ارسال داده‌ها

در نیمی از رخدادهای مرتبط با REvil که توسط محققان سوفوس مورد بررسی قرار گرفته‌اند مهاجمان حجم زیادی از داده‌های خصوصی، حساس و باارزش را از سازمان‌های مورد حمله سرقت کردند. در تئوری، ارسال این حجم از داده‌ها باید خیلی زود، توجه مسئولان فناوری اطلاعات سازمان قربانی را به خود جلب کند اما در عمل در هیچ کدام از رخدادهایی که مورد بررسی محققان سوفوس قرار گرفته‌اند تا پیش از رمزگذاری فایل‌ها کسی متوجه خروج این حجم عظیم اطلاعات نشده بوده است.

عملا پس از فراهم شدن دسترسی‌های مورد نیاز، مهاجمان چندین روز را صرف کشف سرورهای فایل، استخراج حجم زیادی از اسناد و جاسازی آنها در یک یا چند فایل فشرده شده بر روی یکی از دستگاه‌های قربانی می‌کنند. به‌محض آنکه هر آنچه که به دنبال آن هستند را جمع‌آوری کردند ارسال آنها را آغاز می‌کنند که بسته به سرعت شبکه قربانی و حجم داده‌های سرقت شده می‌تواند از چند ساعت تا یک روز به طول بیانجامد.

مهاجمان از انواع سرویس‌های ذخیره‌سازی ابری بهره می‌گیرند. به‌نظر می‌رسد Mega.nz یکی از سرویس‌های رایانش ابری مورد علاقه مهاجمان است. به‌نحوی که در سه‌چهارم حملات مبتنی بر REvil که اطلاعات قربانی سرقت شده از Mega.nz به‌عنوان یک انباره موقت استفاده شده است.

در برخی از حملات، برنامه Mega Client بر روی دستگاه‌های قربانی باقی مانده بود که احتمالا مهاجمان از آن جهت بالا بردن سرعت آپلودها استفاده کرده بودند. تعداد کمتری از مهاجمان نیز از روش‌هایی دیگر نظیر نصب نسخه به اصطلاح Portable نرم‌افزار FileZilla FTP Client برای آپلود داده‌ها به یک سرور در اختیار خود در خارج از شبکه استفاده کرده بودند.

هدف از سرقت داده‌ها، تهدید قربانی به انتشار آنها در صورت عدم پرداخت باج است. مهاجمان ادعا می‌کنند در صورتی که قربانی اقدام به پرداخت مبلغ اخاذی شده کند هیچ رونوشتی از داده‌ها را برای خود نگاه نخواهند داشت. ضمن آن‌که هیچ تضمینی برای انجام این کار وجود ندارد، در بسیاری موارد نیز ثابت شده که نمی‌توان روی قول مهاجمان حساب باز کرد.

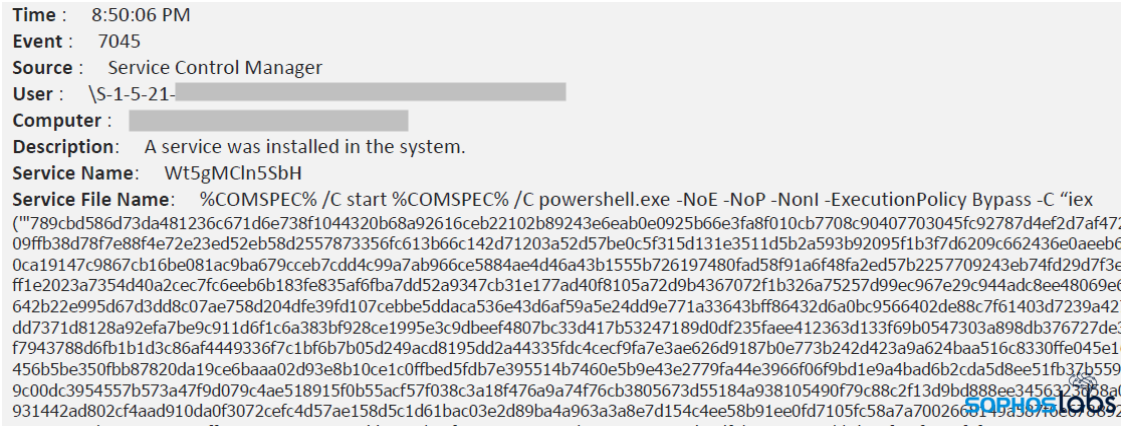
ضربه نهایی: توزیع

مهاجمان به روش‌های مختلف کد مخرب باج‌افزار را توزیع می‌کنند. از توزیع از طریق سرورهای Domain Controller گرفته تا بکارگیری فرامین مبتنی بر WMIC و PsExec برای فراخوانی و اجرای کد مخرب باج‌افزار بر روی سرورها و ایستگاه‌های کاری.

REvil مجهز به قابلیت‌هایی است که مهاجمان ممکن است در جریان توزیع باج‌افزار از آنها بهره بگیرند. در یکی از موارد، باج‌افزار دستگاه را راه‌اندازی مجدد کرده و پس از بالا آوردن آن در حالت Safe Mode عملیات رمزگذاری را آغاز می‌کند. در حالت Safe Mode درایورها و سرویس‌های ثالث اجرا نمی‌شوند. اما از آنجا که قبل از آن، REvil، پروسه خود را به فهرست بسیار کوتاه برنامه‌های قابل اجرا در حالت Safe Mode افزوده است بدون هیچ‌گونه مشکل و محدودیتی و به دور از چشم بسیاری از محصولات امنیتی به رمزگذاری فایل‌های قربانی می‌پردازد.

یا در نمونه‌ای دیگر، مهاجمان با نصب نسخه کامل VirtualBox و یک فایل دیسک مجازی حاوی Windows ۱۰ آلوده به باج‌افزار، رمزگذاری فایل‌های قربانی را از روی ماشین مجازی میهمان انجام داده بودند.

در مواردی نیز مشاهده شده که مهاجمان از WMI برای ایجاد سرویس استفاده کرده‌اند. این موارد شامل رشته فرامینی طولانی و رمز شده هستند که مگر در صورت اطلاع از متغیرهایی با مقادیر خاص تحلیل آنها ممکن نخواهد بود. این متغیرها شامل اطلاعاتی همچون نام ماشین، نشانی IP، دامنه و نام کاربری است. اگر از همه اینها بر روی دستگاهی که سرویس بر روی آن نصب شده اطلاع نداشته باشید تحلیل کد بسیار دشوار خواهد بود.



باج‌افزار؛ مروری بر عملکرد آن

REvil در قالب یک فایل اجرایی بسته‌بندی (Packed) و رمز شده کار می‌کند که در آن چندین قابلیت ضدتحلیل لحاظ شده است. فایل دودویی (Binary) آن حاوی پیکربندی‌های خاص و اطلاعیه باج‌گیری است.

پس از اولین اجرا، بدافزار، پروفایل‌های ماشین را هدف قرار داده، پروسه‌های اجرا شده را فهرست می‌کند و Volume Shadow Copy، به‌روزرسانی‌های Windows Defender، فایل‌های پشتیبان/موقت مورد استفاده توسط برخی نرم‌افزارهای ثالث را حذف می‌کند. برای مثال تصویر زیر بخشی از کدی را نشان می‌دهد که وظیفه آن حذف به‌روزرسانی‌های Windows Defender است.

```
call ce.403C1C
pop ecx
push dword ptr ss:[ebp+8]                [ebp+8]:L"\\\\?\\C:\\ProgramData\\Microsoft\\Windows Defender\\Definition Updates\\Backup\\mpasbase.v
call dword ptr ds:[<&DeleteFilew>]
```

باج‌افزار، پروسه‌های اجرا شده را شناسایی کرده و آنهایی را که با فهرست آن مطابقت دارند از کار می‌اندازد. فهرست مذکور شامل ۳۰ پروسه از جمله پروسه برنامه‌های پایگاه داده، Office، مدیریت ایمیل، پشتیبان‌گیری و مرورگر Firefox است.

```
"prc": [ // process to kill
    "tbirdconfig",
    "isqlplussvc",
    "mspub",
    "mydesktopservice",
    "xfssvccon",
    "outlook",
    "sql",
    "visio",
    "excel",
    "msaccess",
    "onenote",
    "thunderbird",
    "infopath",
    "ocomm",
    "oracle",
    "sqbcoreservice",
    "encsvc",
    "thebat",
    "steam",
    "ocssd",
    "wordpad",
    "dbeng50",
```

SOPHOSlabs

REvil فهرستی از سرویس‌های نصب شده را نیز استخراج کرده و برای متوقف کردن سرویس‌های متعلق به محصولات امنیتی تلاش می‌کند.

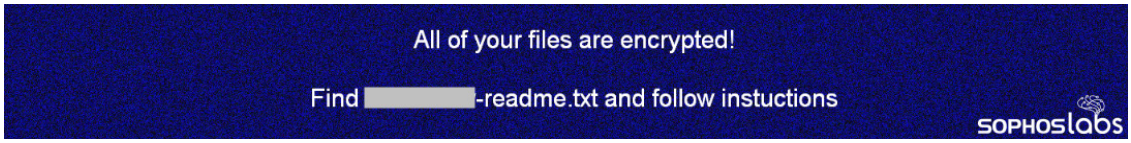
در ادامه، باج‌افزار اطلاعیه باج‌گیری را که در کد آن لحاظ شده استخراج کرده و در قالب یک فایل آن را در ریشه درایو C: ذخیر می‌کند. فایل مذکور حاوی یک نشانی در شبکه ناشناس TOR به همراه دستورالعمل نحوه برقراری ارتباط با مهاجمان است.

```
02254390 2D 00 2D 00 2D 00 3D 00 3D 00 3D 00 20 00 57 00 -.-.-.=.=.=. .W.
022543A0 65 00 6C 00 63 00 6F 00 6D 00 65 00 2E 00 20 00 e.l.c.o.m.e... .
022543B0 41 00 67 00 61 00 69 00 6E 00 2E 00 20 00 3D 00 A.g.a.i.n... .=.
022543C0 3D 00 3D 00 2D 00 2D 00 2D 00 0D 00 0A 00 0D 00 =.=.-.-.-.......
022543D0 0A 00 5B 00 2B 00 5D 00 20 00 57 00 68 00 61 00 ..[.+.]. .W.h.a.
022543E0 74 00 73 00 20 00 48 00 61 00 70 00 70 00 65 00 t.s. .H.a.p.p.e.
022543F0 6E 00 3F 00 20 00 5B 00 2B 00 5D 00 0D 00 0A 00 n.?. .[.+.].....
02254400 0D 00 0A 00 59 00 6F 00 75 00 72 00 20 00 66 00 ....Y.o.u.r. .f.
02254410 69 00 6C 00 65 00 73 00 20 00 61 00 72 00 65 00 i.l.e.s. .a.r.e.
02254420 20 00 65 00 6E 00 63 00 72 00 79 00 70 00 74 00  .e.n.c.r.y.p.t.
02254430 65 00 64 00 2C 00 20 00 61 00 6E 00 64 00 20 00 e.d.,. .a.n.d. .
02254440 63 00 75 00 72 00 72 00 65 00 6E 00 74 00 6C 00 c.u.r.r.e.n.t.l.
02254450 79 00 20 00 75 00 6E 00 61 00 76 00 61 00 69 00 y. .u.n.a.v.a.i.
02254460 6C 00 61 00 62 00 6C 00 65 00 2E 00 20 00 59 00 l.a.b.l.e... .Y.
02254470 6F 00 75 00 20 00 63 00 61 00 6E 00 20 00 63 00 o.u. .c.a.n. .c.
02254480 68 00 65 00 63 00 6B 00 20 00 69 00 74 00 3A 00 h.e.c.k. .i.t.:.
02254490 20 00 61 00 6C 00 6C 00 20 00 66 00 69 00 6C 00  .a.l.l. .f.i.l.
022544A0 65 00 73 00 20 00 6F 00 6E 00 20 00 79 00 6F 00 e.s. .o.n. .y.o.
022544B0 75 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 u. .c.o.m.p.u.t.
022544C0 65 00 72 00 20 00 68 00 61 00 73 00 20 00 65 00 e.r. .h.a.s. .e.
022544D0 78 00 70 00 61 00 6E 00 73 00 69 00 6F 00 6E 00 x.p.a.n.s.i.o.n.
022544E0 20 00 7B 00 45 00 58 00 54 00 7D 00 2E 00 0D 00  .{.E.X.T.}.....
```

SOPHOSlabs

در فایل Configuration یک فایل تصویری bmp تزریق شده که باج‌افزار آن را پس از ذخیره در مسیر زیر، جایگزین تصویر پس‌زمینه Desktop دستگاه آلوده می‌کند.

%AppData%\Local\Temp



فایل اطلاعیه باج‌گیری با همان هشت نویسه‌ای آغاز می‌شود که به نام هر فایل رمز شده نیز الصاق می‌شود.

REvil از الگوریتم curve25519/salsa20 برای رمزگذاری فایل‌ها استفاده می‌کند.

Initial state of Salsa20

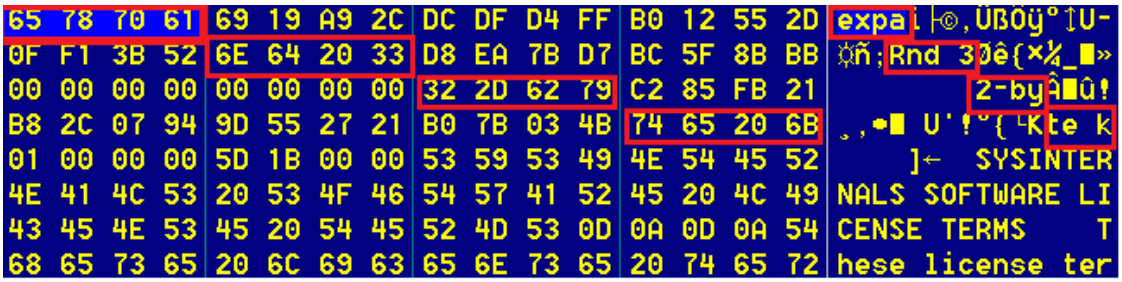
"expa"	Key	Key	Key
Key	"nd 3"	Nonce	Nonce
Pos.	Pos.	"2-by"	Key
Key	Key	Key	"te k"

پیکربندی حاوی فهرست مفصلی از پوشه‌ها، انواع فایل و نام‌های فایل خاصی است که با هدف عدم بروز اختلال در فرایند بالا آمدن دستگاه از رمزگذاری آنها پرهیز می‌شود.

```
"fls": [ // files
    "ntuser.dat.log",
    "desktop.ini",
    "ntuser.dat",
    "iconcache.db",
    "boot.ini",
    "thumbs.db",
    "ntldr",
    "bootfont.bin",
    "ntuser.ini",
    "bootsect.bak",
    "autorun.inf"
```

SOPHOSlabs

شکل زیر بخشی از یک فایل رمز شده را نشان می‌دهد که در آن نحوه رمزگذاری گام‌به‌گام Salsa20 به تصویر کشیده شده است.



باج‌افزار در حین اجرا اقداماتی به غیر از رمزگذاری نیز انجام می‌دهد. از جمله، ارسال آمار و گزارش از وضعیت رمزگذاری به دامنه‌هایی که در کد آن درج شده‌اند. برقراری ارتباط با این دامنه‌ها می‌تواند نشانه‌ای قابل اطمینان از وجود آلودگی باشد.

پرداخت باج REvil مدتی است که باید از طریق رمز ارز مونرو انجام شود. شاید یکی از دلایل آن بیشتر بودن قابلیت‌های حریم خصوصی در مونرو در مقایسه با بیت‌کوین باشد.

رعایت موارد زیر در این روزگار پررونق باج‌افزارها بیش از هر زمانی اهمیت دارد.

رصد و واکنش به رخدادهای مشکوک - اطمینان حاصل کنید که ابزارها، پروسه‌ها و منابع انسانی و تجهیزات سخت‌افزاری لازم برای رصد و پاسخدهی به تهدیدات در سازمان پیاده‌سازی شده باشد. ارزیابی و بررسی سریع یک هشدار یا رخداد امنیتی توسط یک متخصص بسیار کلیدی است. در بسیاری مواقع، مهاجمان اجرای عملیات را به ساعات کم‌ترافیک، روزهای آخر هفته و تعطیلات موکول می‌کنند؛ با این فرض که در این ساعات و ایام افراد کمتری بر رخدادها نظارت دارند.

رمزهای عبور؛ همیشه پیچیده - استفاده از رمزهای عبور قدرتمند اولین خط دفاعی است. قوانین پیچیدگی در انتخاب رمز عبور در نظر گرفته شده و طول رمزهای عبور حداقل ۱۲ نویسه باشد. استفاده از راهکارهای Password Manager در بکارگیری رمزهای عبور پیچیده که در انحصار افراد مستقل هستند کمک‌کننده خواهد بود. از یک رمز عبور هیچ‌گاه در دو جا استفاده نشود.

اصالت‌سنجی؛ چندمرحله‌ای (MFA) - حتی رمزهای عبور قدرتمند می‌توانند هک شوند. استفاده از هر نوع سازوکار اصالت‌سنجی چندمرحله‌ای برای به دسترسی به منابع حساس نظیر ایمیل‌ها، ابزارهای مدیریت از راه دور و تجهیزات شبکه‌ای بجای اتکای صرف به رمز عبور توصیه می‌شود. برنامک‌های ایجادکننده رمز یک‌بار مصرف بر روی گوشی‌های هوشمند امن‌تر از سامانه‌های اصالت‌سنجی چندمرحله‌ای مبتنی بر ایمیل یا پیامک به نظر می‌رسند. در مواقعی که مهاجمان موفق به رخنه به شبکه شده‌اند، ایمیل‌ها هم ممکن است هک شده باشند و SIM Swapping اگر چه متداول نیست اما در هر صورت می‌تواند کدهای اصالت‌سنجی چندمرحله‌ای پیامکی را مورد دست‌درازی قرار دهد. اما به هر حال اصالت‌سنجی چندمرحله‌ای به هر شکلی می‌تواند موجب افزایش امنیت شود.

مقاوم‌سازی؛ به ویژه سرویس‌های قابل دسترس - با پویش شبکه از خارج از سازمان درگاه‌های مورد استفاده به خصوص پودمان‌ها و درگاه‌های RDP و VNC و به‌طور کلی هر ابزار دسترسی از راه دور مقاوم‌سازی شود. اگر قرار است ماشینی از طریق ابزارهای مدیریت از راه دور قابل دسترس باشد در پشت VPN مجهز به اصالت‌سنجی چندمرحله ای قرار بگیرد. ضمن اینکه ماشین مذکور از طریق VLAN با سایر دستگاه‌ها جداسازی شود.

تقسیم‌بندی؛ با رویکرد اعتماد-صفر - با بهره‌گیری از VLAN و Segmentation و لحاظ کردن رویکرد اعتماد-صفر (Zero-trust)، سرورهای حیاتی از یکدیگر و از ایستگاه‌های کاری جداسازی شوند.

تهیه فهرست از تجهیزات و حساب‌های کاربری؛ به‌روزرسانی مستمر آن - دستگاه‌های حفاظت و وصله نشده در شبکه موجب افزایش ریسک و آسیب‌پذیری به انواع حملات می‌شوند. برای اطمینان از تحت حفاظت بودن دستگاه‌ها، نیاز به وجود فهرستی از کامپیوترها و تجهیزات IoT است. از پویش‌های شبکه و بررسی‌های فیزیکی برای یافتن و فهرست کردن آنها استفاده کنید.

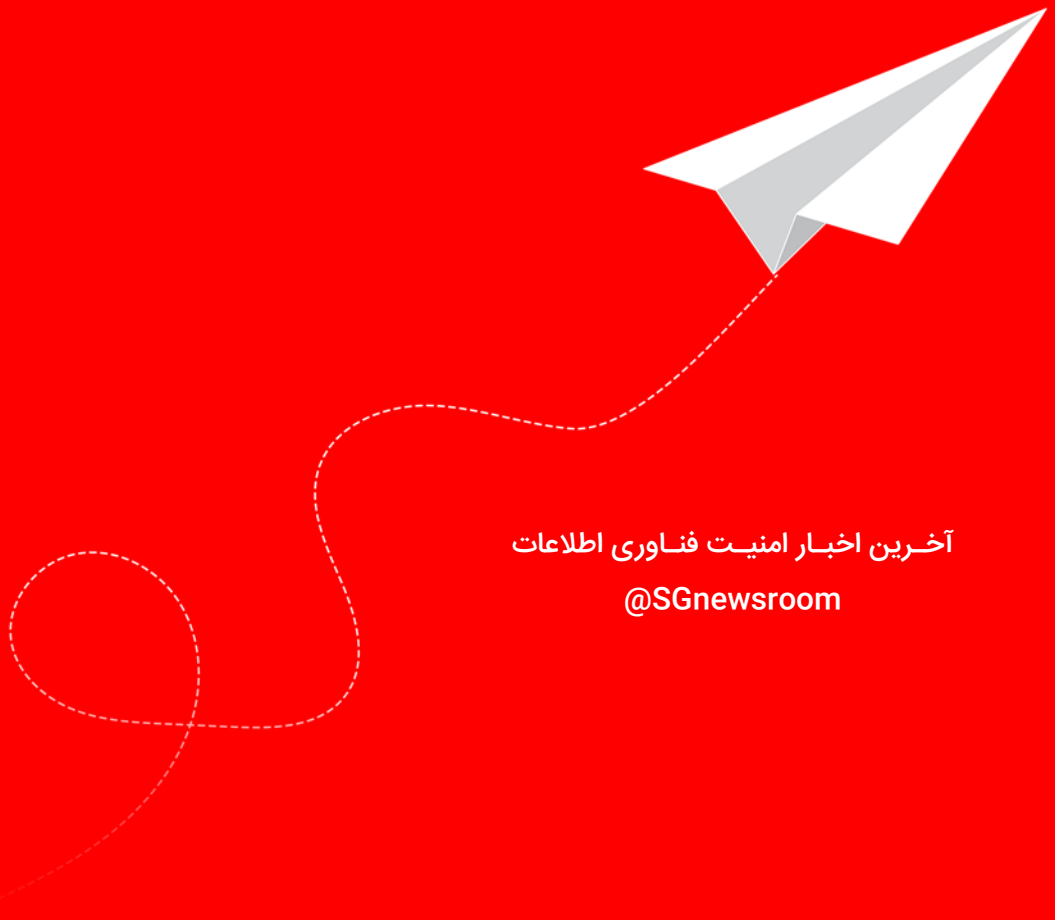
پیکربندی صحیح محصولات؛ همراه بازبینی مستمر - اطمینان حاصل شود که محصولات امنیتی بر اساس به‌روش‌ها پیکربندی شده باشند. پالیسی‌های پیکربندی و فهرست استثنائات به‌طور منظم بررسی شود. باید در نظر داشت که امکانات جدید ممکن است به‌صورت خودکار فعال نباشند.

Active Directory؛ رصد مستمر حساب‌های کاربری - با انجام ممیزی‌های مستمر تمامی حساب‌های کاربری دامنه، اطمینان حاصل شود که هیچ حساب کاربری بیشتر از حد معمول مورد استفاده قرار نگرفته باشد. حساب کاربری به‌محض جدا شدن کاربر از مجموعه غیرفعال شود.

وصله کنید؛ همه چیز را - Windows و سایر نرم‌افزارها به‌روز نگاه داشته شوند. از نصب کامل و صحیح اصلاحیه‌ها بر روی سرورهای حیاتی از جمله سامانه‌های قابل دسترس بر روی اینترنت اطمینان حاصل شود.

منبع:

https://news.sophos.com/en-us/2021/06/11/relentless-revil-revealed/



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.

شـرکـت مـهـنـدسـی شـبـکـه گـسـتـر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظـفـر)، شـماره ۲۷۳

تلفـن / دورنـگار ۰۲۱ - ۴۲۰۵۲

رایانامـه info@shabakeh.net

تارنمای شـرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکـز آمـوزش events.shabakeh.net

اتـاق خبـر newsroom.shabakeh.net