ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | آذر 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 آبان ماه محققان سیسکو اعلام نمودند که کارزارهایی مخرب را شناسایی نموده‌اند که با سوءاستفاده از مجموعه ضعف‌های امنیتی ProxyShell در سرورهای Exchange به شبکه‌های سازمانی نفوذ و آن‌ها را به باج‌افزار Babuk آلوده می‌کردند. محققان شرکت ترند میکرو نیز حملاتی موسوم به Reply Chain Attack را در سازمان‌ها شناسایی کرده‌اند که مهاجمان در آن با سوءاستفاده از ضعف‌های امنیتی ProxyShell و ProxyLogon، سرورهای Exchange را هک کرده و اقدام به توزیع بدافزار می‌کنند. جزییات این حملات در این ماهنامه مورد بررسی قرار گرفته است.

دیگر موضوعی که در این ماهنامه با استناد به گزارش یکی از شرکت‌های امنیتی به آن پرداخته شده، هک شدن نزدیک به ۳۰۰ سایت WordPress برای نمایش اعلان‌های رمزگذاری جعلی است. مهاجمان در این حملات سعی دارند صاحبان سایت را فریب دهند تا برای بازیابی فایل‌ها باج مطالبه شده را بپردازند.

در ماه گذشته محققان شرکت امنیتی سوفوس در گزارشی با بازبینی حملات باج‌افزاری به بررسی روش‌هایی پرداخته‌اند که مهاجمان از طریق آن‌ها قربانیان را برای پرداخت باج تحت فشار قرار می‌دهند. همچنین محققان مذکور به راه‌های مقابله با پروتکل RDP که مدیران و راهبران شبکه اغلب برای اتصال به سرورها و ایستگاه‌های کاری سازمان به کار می‌گیرند، پرداخته‌اند. برگردان مشروح گزارش‌های سوفوس در این ماهنامه قابل مطالعه است.

در این ماهنامه به روش کار نسخه اخیر بدافزار BazarLoader پرداخته شده که از طریق روش‌های مختلفی از جمله ایمیل منتشر می‌شود. علاوه بر بدافزار مذکور، اخیراً مهاجمانی ناشناس سه نسخه از کتابخانه محبوب JavaScript به نام UAParser.js را با تزریق کد مخرب آلوده کرده‌اند. همچنین گونه جدیدی از بات‌نت DDoS به نام Abcbot که دارای قابلیت کرم بوده و سیستم‌های تحت Linux را جهت اجرای حملات DDoS مورد تسخیر قرار می‌دهد، توسط محققان شرکت چیهو ۳۶۰ کشف شده است. روش کار بدافزارهای مذکور در این ماهنامه مورد بررسی قرار گرفته است.

از دیگر رخدادهای مهم یک ماه اخیر که در این ماهنامه به آن پرداخته شده، رمزگشایی فایل‌های قربانیان باج‌افزار BlackMatter بوده که توسط محققان شرکت امنیتی امسی‌سافت، انجام شده است. شرکت امنیت سایبری آواست نیز دو ابزار رمزگشایی منتشر کرد که به قربانیان باج‌افزارهای LockFile، AtomSilo و Babuk کمک می‌کند تا برخی از فایل‌های خود را به صورت رایگان و بدون نیاز به پرداخت باج بازیابی کنند.

در ماهی که گذشت، CRN، شرکت مک‌آفی اینترپرایز را به عنوان فینالیست دریافت جایزه CRN Tech Innovator Award در سال ۲۰۲۱ انتخاب کرد. این جایزه سالانه به ارائه‌دهندگان فناوری که به توانمندسازی کاربران نهایی به صورت مداوم متعهد هستند و در عین حال با ارائه پیشرفته‌ترین محصولات و خدمات، آن‌ها را در رشد مستمر کسب‌وکار کمک می‌کنند، اعطاء می‌شود.

همانطور که در این ماهنامه خواهید خواند، نوامبر ۲۰۲۱، نقطه عطف بزرگی برای شرکت بیت‌دیفندر بود چرا که بیستمین سالگرد تاسیس یکی از قابل اعتمادترین پیشگامان امنیت سایبری در جهان را جشن گرفتند.

در دومین ماه از پاییز ۱۴۰۰، مایکروسافت، سیسکو، مک‌آفی‌اینترپرایز، بیت‌دیفندر، کسپرسکی، وی‌ام‌ور، ادوبی، گوگل، اپل، موزیلا، اس‌آپ، سیتریکس، پالو آلتو نتورکس و دروپال اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند. جزییات این به‌روزرسانی‌ها و گزارش‌های متنوع دیگر را در این ماهنامه بخوانید.

شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی

مسدود کردن پروتکل
ریموت دسکتاپ (RDP)

پروتکل RDP یا Remote Desktop Protocol که با عناوین دیگری نظیر خدمات ترمینال (Terminal Services) یا سرویس دسکتاپ از راه دور (Remote Desktop Service) نیز شناخته می‌شود، به کاربران اجازه می‌دهد تا از راه دور به کامپیوتر دیگری متصل شوند و همان تجربه کاربری را داشته باشند که گویی حضور فیزیکی دارند.

علاوه بر مدیران و راهبران شبکه که این پروتکل را برای اتصال به سرورها و ایستگاه‌های کاری سازمان به کار می‌گیرند، در بسیاری از سازمان‌های کوچک و متوسط نیز از RDP برای برقرار نمودن ارتباط از راه دور پیمانکاران حوزه فناوری اطلاعات، به سرورهایی همچون حقوق و دستمزد، اتوماسیون اداری و غیره استفاده می‌شود.

این قابلیت به علت سهولت بکارگیری بسیار محبوب است و به هر کسی اجازه می‌دهد که به سادگی سیستمی را از راه دور مدیریت کند همچون یک ارائه دهنده خدمات مدیریت شده (Managed Service Provider) که برای مدیریت سرورهای مشتریان یا یک دندانپزشک برای دسترسی به سیستم مطب خود از خانه از این پروتکل استفاده می‌کند.

این پروتکل به طور اختصاصی متعلق به شرکت مایکروسافت است و طبق گزارش Active Adversary Playbook 2021 شرکت سوفوس (Sophos, Ltd.) در سال ۲۰۲۱، در ۳۲ درصد از حملات، از پروتکل RDP جهت دسترسی به سازمان‌های متصل به اینترنت سوءاستفاده شده است. پروتکل مذکور را به عنوان روش شماره یک بکارگرفته شده توسط مهاجمان جهت نفوذ و دسترسی اولیه رتبه‌بندی کرده‌اند.

برخلاف برخی دیگر از ابزارهای دسترسی از راه دور، RDP معمولاً به چیزی فراتر از نام کاربری و رمز عبور نیاز ندارد و اغلب نام کاربری برای سهولت در ورود بعدی به سیستم، در معرض نمایش گذاشته می‌شود. حتی پروتکل RDP در طول زمان شامل آسیب‌پذیری‌هایی شده که امکان دسترسی بدون نام کاربری و رمز عبور را نیز فراهم می‌کند.

چارچوب MITRE ATT&CK که مخفف Adversarial Tactics, Techniques, and Common Knowledge بوده و توسط MITRE Corporation ارائه شده، یک پایگاه‌دانش در حال رشد است که تاکتیک‌ها و تکنیک‌های مهاجمان را براساس حملات مشاهده شده در دنیای واقعی شناسایی نموده و در دسترس همگان قرار می‌دهد.

این چارچوب هم برای مهاجمان و هم برای مدافعان سایبری قابل فهم بوده و در موقعیت‌های بسیاری مثل تشخیص نفوذ، شکار تهدید، مهندسی امنیت، هوش تهدید و مدیریت ریسک مورد استفاده قرار می‌گیرد.

در چارچوب مذکور، مکانیزم‌های بکارگرفته شده توسط مهاجمان در RDP ارائه شده است که اصلی‌ترین آن T1133 (سرویس از راه دور خارجی) است. سایر تکنیک‌های MITER ATT&CK که در RDP استفاده می‌شوند عبارتند از:

- T1563، هایجک RDP (RDP Hijacking)
- T1021، توسعه دامنه آلودگی با سوءاستفاده از RDP (Lateral Movement using RDP)
- T1572، تونل زدن به شبکه با سوءاستفاده از RDP (RDP Tunneling)
- T1573، کنترل و فرمان‌دهی با سوءاستفاده از RDP (Command and Control over RDP)
- T1078، بکارگیری حساب‌های کاربری معتبر با سوءاستفاده از RDP (Using Valid Accounts with RDP)
- T1049، کشف اتصالات شبکه سیستم (System Network Connections Discovery)
- T1071، پروتکل لایه کاربردی (Application Layer Protocol)

هنگامی که مهاجم با موفقیت وارد یک Session از RDP شد، می‌تواند آلودگی را توسعه داده و به کل سیستم نفوذ کند و حتی امن‌ترین مرکز داده در جهان نمی‌تواند از نظر فیزیکی کمکی کند.

پیشگیری از حملات RDP فقط یک راه‌حل ساده دارد، RDP را در معرض دید قرار ندهید.

پورت TCP:3389 روی فایروال خود را به هر چیزی فوروارد نکنید و تصور نکنید که استفاده از یک پورت متفاوت دیگر، کمک‌کننده است. محققان، دوازده هزار RDP را بر روی پورت ۳۳۸۸ شناسایی کرده‌اند.

سرورهای با RDP باز به‌سادگی از طریق جستجوگرهایی همچون Shodan قابل شناسایی هستند. آمار موتور جستجوگر Shodan (Shodan.IO) بیش از ۳.۳ میلیون پورت RDP 3389 را نشان می‌دهد که در سطح جهانی بر روی اینترنت قابل دسترس هستند و به راحتی یافت می‌شوند و ممکن است هر یک از آنها مورد نفوذ مهاجمان قرار گرفته یا در آینده‌ای نزدیک قرار بگیرند.

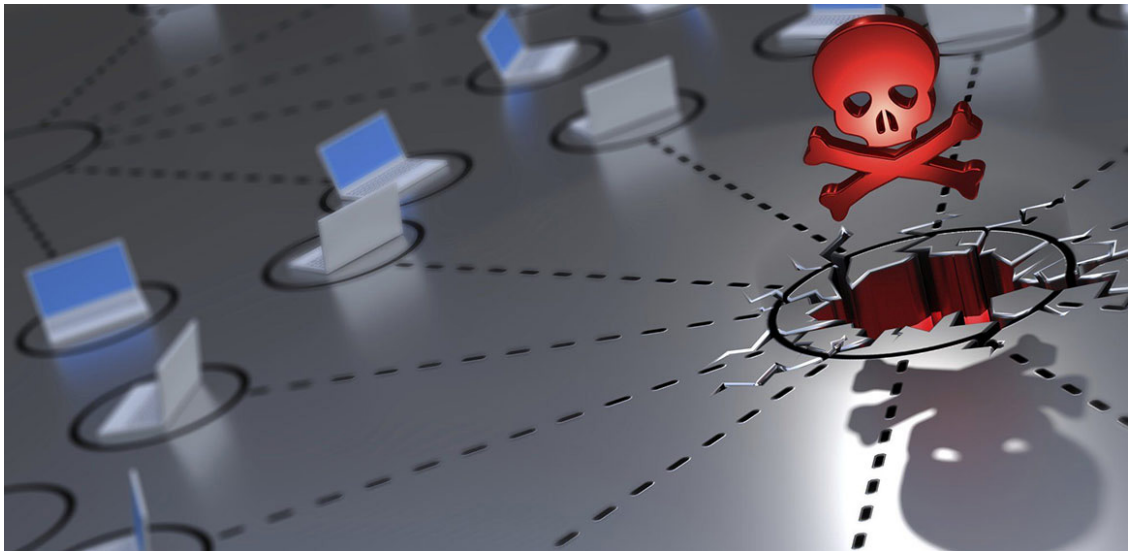
راهکار مقابله با سوءاستفاده از RDP بسیار ساده است. اگر دسترسی از راه دور و RDP مورد نیاز است، این پروتکل را فقط باید از طریق یک اتصال VPN امن همراه با احراز هویت چند عاملی جهت اتصال از راه دور به شبکه شرکت استفاده نمود. همچنین می‌توان از طریق یک Gateway دسترسی از راه دور مبتنی بر اعتماد-صفر (Zero-trust) پروتکل RDP را بکار گرفت.

برای کسب اطلاعات بیشتر و راه‌های مقابله با سوءاستفاده از RDP، مطالعه مقالات زیر توصیه می‌شود:

- حفاظت از سازمان در برابر تهدیدات مبتنی بر RDP
- روزگار پررونق دلال‌های دسترسی اولیه
- سوءاستفاده از RDP در حملات گسترده باج‌افزاری، کاوش رمزارز و سرقت اطلاعات
- سوءاستفاده از RDP در جریان حملات DDoS

FiveSys؛

روت‌کیتی مخرب با امضای مایکروسافت



به گزارش شرکت مهندسی شبکه گستر، محققان شرکت ضدویروس بیت‌دیفندر (Bitdefender)، در گزارشی جزییات روت‌کیت جدیدی به نام FiveSys را که دارای امضای دیجیتالی معتبر WHQL صادر شده توسط مایکروسافت است، منتشر کرده‌اند. روت‌کیت مذکور بیش از یک سال است که کاربران کامپیوترها را مورد هدف قرار داده است.

بیش از یک دهه پیش روت‌کیت‌ها به عنوان نوعی بدافزار طراحی شده‌اند تا مهاجمان از طریق آن‌ها به سطوح پایین سیستم‌عامل‌های هک شده دسترسی داشته باشند. شرکت مایکروسافت (Microsoft Corp) با اعمال برخی تغییرات از زمان ارائه Windows Vista، انتشار روت‌کیت‌ها را بسیار دشوارتر کرد. راهکارهای امنیتی امروزی نیز با استفاده از فناوری‌های جدیدی که ۱۰ سال پیش تنها یک رویا بودند، بسیار کارآمدتر شده‌اند.

در تغییرات اخیر، شرکت مایکروسافت الزامات جدید Driver Signing را جهت نصب راه‌اندازهای سخت‌افزاری (Driver) وضع نموده که می‌خواهد قبل از نصب در سیستم‌عامل، یک پروسه دقیق اعتبارسنجی طی شده و راه‌اندازها به صورت دیجیتالی توسط مایکروسافت امضاء شوند. هدف مایکروسافت از وضع تغییرات جدید در این سیستم اعتبارسنجی، بی‌اثر نمودن تلاش مهاجمان برای دورزدن پروسه اعتبارسنجی بوده تا احتمال موفقیت آن‌ها را بسیار کاهش دهد.

این قابلیت جدید تضمین می‌کند که همه راه‌اندازها به جای توسعه‌دهنده اصلی سخت‌افزار، توسط شرکت ارائه‌دهنده سیستم‌عامل تأیید و امضاء شوند و به این ترتیب، امضاهای دیجیتال هیچ نشانه‌ای از هویت توسعه‌دهنده واقعی را ارائه نمی‌دهند.

محققان شرکت بیت‌دیفندر نیز در تحقیقات خود پی بردند که نویسندگان روت‌کیت FiveSys به نوعی توانسته‌اند پروسه اعتبارسنجی مایکروسافت را فریب داده و به نوعی آن را بی‌اثر کنند.

محققان بیت‌دیفندر در گزارش خود اعلام نموده‌اند که در چند ماه گذشته، شاهد افزایش راه‌اندازهای مخرب با امضای دیجیتالی معتبر WHQL صادر شده توسط مایکروسافت بوده‌اند. علاوه بر این، این واقعیت که راه‌اندازهای مذکور دارای امضاهای دیجیتالی صادر شده توسط مایکروسافت هستند، ممکن است کاربران ناآگاه را فریب دهد تا تصور کنند که آن راه‌اندازها قانونی بوده و نصب آن‌ها را بپذیرند.

محققان بیت‌دیفندر پس از شناسایی روت‌کیت FiveSys با شرکت مایکروسافت تماس گرفته و سوءاستفاده روت‌کیت مذکور از امضای دیجیتالی WHQL مایکروسافت را اعلام کردند. مایکروسافت نیز مدت کوتاهی پس از آن این امضاء را لغو کرد.

هدف روت‌کیت ساده است؛ هدف آن هدایت ترافیک اینترنت در ماشین‌های هک شده از طریق یک پروکسی شخصی‌سازی شده است که از لیست تعبیه شده داخلی که حاوی ۳۰۰ دامنه است، استخراج می‌شود. در واقع از روت‌کیت برای انتقال و هدایت قربانیان به سمت نشانی‌های اینترنتی مورد علاقه مهاجمان استفاده می‌شود. این تغییر مسیر هم برای HTTP و هم HTTPS به خوبی عمل می‌کند. روت‌کیت یک گواهی‌نامه root شخصی‌سازی شده (custom root certificate) برای تغییر مسیر HTTPS نصب می‌کند. به این ترتیب، مرورگر در مورد هویت ناشناخته سرور پروکسی هشدار نمی‌دهد.

روت‌کیت علاوه بر هدایت ترافیک اینترنتی، از استراتژی‌های مختلفی جهت مسدود کردن توانایی ویرایش Registry و توقف دانلود راه‌اندازهای سایر گروه‌های بدافزاری استفاده می‌کند. روت‌کیت تلاش می‌کند که با توقف نصب سایر روت‌کیت‌ها و بدافزارهای گروه‌های مختلف، دسترسی مهاجمان رقیب را به سیستم هک شده مسدود کرده و از خود محافظت کند.

سازندگان Rootkit معمولاً جهت مسدود کردن بدافزارهای رقیب از لیست‌سیاه امضاءها و گواهی‌نامه‌های دیجیتالی سرقت شده توسط سایر بدافزارها استفاده می‌کنند. برای رسیدن به این هدف، آن‌ها دسترسی به هر فایل را نظارت کرده و امضای دیجیتالی را در صورت وجود بررسی می‌کنند. اگر امضای مذکور در آن لیست‌سیاه باشد، از دسترسی به فایل جلوگیری می‌کنند.

لیست‌سیاه امضاهای دیجیتالی به صورت دوره‌ای به‌روزرسانی می‌شود. در حال حاضر لیست مذکور دارای ۶۸ هش است که بخشی از آن در زیر نمایش داده شده است؛ هر هش مربوط به امضاهای سرقت شده/نشت شده توسط بدافزار است.

00000478	186.51918030	[MY-1]MD5-0:9D9F343EAA8FB4045A4B7D05437AC02B
00000480	186.51918030	[MY-1]MD5-1:A269121725987B766740D43964E83CF3
00000482	186.51918030	[MY-1]MD5-2:698FD84F0AABAA65F8BD3E7AD417F4D4
00000484	186.51919556	[MY-1]MD5-3:CE7D7EE076A74D3C532265D8F6BBFF09
00000486	186.51919556	[MY-1]Sign-0:Zhang Zhengqi
00000488	186.51921082	[MY-1]Sign-1:Haining shengdun Network Information Technology Co., Ltd
00000490	186.51921082	[MY-1]Sign-2:SHENZHEN LIRINUOS
00000492	186.51921082	[MY-1]Sign-3:Shanghai easy kradar Information Consulting Co.Ltd

مشروح گزارش بیت‌دیفندر در خصوص جزئیات فنی و فهرست کاملی از نشانه‌های آلودگی (indicators of Compromise- به اختصار IoC) روت‌کیت مذکور، در نشانی زیر قابل دریافت و مطالعه است:

https://www.bitdefender.com/files/News/CaseStudies/study/405/Bitdefender-DT-Whitepaper-Fivesys-creat5699-en-EN.pdf

فهرست نام‌های شناسایی ضدبدافزار بیت‌دیفندر به شرح زیر می‌باشد:

Gen:Trojan.Heur.JP.kQW@ayWx7Nnj

Gen:Variant.Cerbu.111684

Gen:Variant.Doina.11362

Gen:Variant.Doina.21224

Gen:Variant.Doina.8523

Gen:Variant.Graftor.891814

Gen:Variant.Mikey.126771

Gen:Variant.Mikey.128072

Gen:Variant.Mikey.129746

Gen:Variant.Ulise.265712

Gen:Variant.Ulise.269396

Gen:Variant.Ulise.269440

Gen:Variant.Ulise.269496

Gen:Variant.Ulise.315678

Rootkit.Agent.AJIN

Rootkit.Agent.AJIQ

Rootkit.Agent.AJIR

Rootkit.Agent.AJIT

Trojan.Agent.FKUL

Trojan.Agent.FLBC

Trojan.Agent.FLFR

Trojan.Agent.FLTM

Trojan.Agent.FLYE

Trojan.Generic.30029659

Trojan.Generic.30030153

Trojan.Generic.30034021

Trojan.Generic.30121716

Trojan.Generic.30287863

Trojan.GenericKD.36470692

Trojan.GenericKD.37303188

Trojan.GenericKD.37919591

Trojan.GenericKD.46709798

Trojan.GenericKD.47346686

فهرست نام‌های شناسایی ضدبدافزار مک‌آفی نیز به شرح زیر می‌باشد:

Artemis!191FAD43EF6C

Generic .rc

Generic .rd

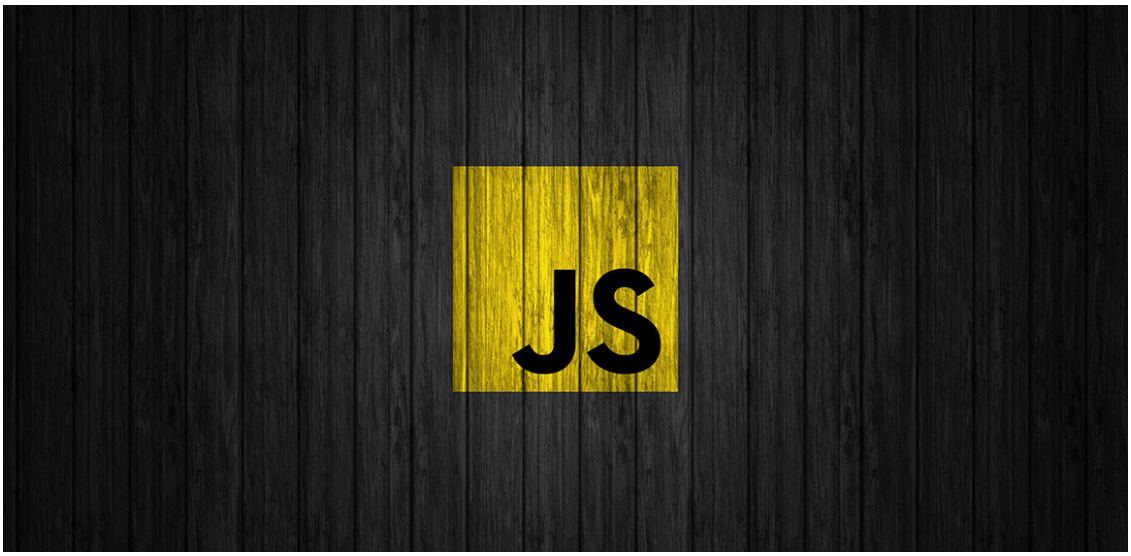
Generic .re

Generic .rf

Generic .rg

GenericRXNRBV!B518AEF15358

آلودگی کتابخانه محبوب JavaScript



کتابخانه UAParser.js که بر روی ده‌ها میلیون کامپیوتر در سراسر جهان نصب شده است، به بدافزاری آلوده شده که رمزهای عبور را سرقت کرده و اقدام به استخراج رمزارز می‌کند.

مهاجمان ناشناسی، سه نسخه ۰.۷.۲۹، ۰.۸.۰ و ۱.۰.۰ از کتابخانه محبوب JavaScript به نام UAParser.js را با تزریق کد مخرب آلوده کرده‌اند. بنا بر آمار صفحه توسعه‌دهندگان نرم‌افزار، در بسیاری از پروژه‌ها از این کتابخانه استفاده شده و هر هفته کتابخانه مذکور، ۶ تا ۸ میلیون بار دانلود می‌شود.

شرکت مهندسی شبکه گستر اکیداً توصیه می‌کند که در اسرع وقت تمامی کاربران و راهبران، کتابخانه‌های مذکور را به ترتیب به نسخ ۰.۷.۳۰، ۰.۸.۱ و ۱.۰.۱ به‌روزرسانی کنند.

UAParser.js چیست و چرا اینقدر محبوب است؟

توسعه‌دهندگان JavaScript از کتابخانه UAParser.js برای پردازش و تحلیل (Parse) اطلاعات User-Agent ارسالی مرورگرها استفاده می‌کنند. کتابخانه مذکور در بسیاری از سایت‌ها بکارگرفته شده و در پروسه تولید و توسعه نرم‌افزار شرکت‌های مختلفی همچون Mozilla، Oracle، Dell، HPE، IBM، Slack، Microsoft، Amazon، Apple، Facebook و غیره استفاده می‌شود.

علاوه بر این، برخی از توسعه‌دهندگان نرم‌افزار از ابزارهای ثالث (Third-party instruments) همچون چارچوب Karma برای تست کد استفاده می‌کنند که به کتابخانه مذکور وابسته است و با افزودن یک پیوند اضافی به زنجیره تأمین، وسعت و دامنه حمله را بیشتر می‌کند.

مهاجمان، اسکریپت‌های مخرب را در کتابخانه UAParser.js جاسازی کرده‌اند تا کدهای مخرب را در کامپیوترهای قربانیان، هم در سیستم‌های Linux و هم در سیستم‌های تحت Windows دانلود و آن را اجرا کنند.

اهداف یکی از ماژول‌های جاسازی شده در اسکریپت مذکور، استخراج رمز ارز (Cryptocurrency) بوده و هدف دیگر (فقط برای سیستم‌های تحت Windows) سرقت اطلاعات اصالت‌سنجی مانند کوکی‌های مرورگر، رمزهای عبور و اطلاعات اصالت‌سنجی سیستم‌عامل می‌باشد. با این حال، ممکن است فعالیت اسکریپت‌ها تنها به این موارد منتهی نشود. طبق هشدار آژانس امنیت سایبری و حفاظت از زیرساخت ایالات متحده (CISA)، مهاجمان با نصب کتابخانه‌های آلوده می‌توانند کنترل سیستم‌های هک شده را در اختیار بگیرند.

بنا بر اظهارات کاربران در GitHub، این بدافزار فایل‌های باینری jsextension (در Linux) و jsextension.exe (در Windows) را ایجاد می‌کند. وجود فایل‌های مذکور نشانه بارزی است از این که سیستم، هک شده است.

مهاجمان چگونه کد مخرب را وارد کتابخانه UAParser.js کرده‌اند؟

توسعه‌دهنده پروژه UAParser.js، اظهار داشت که پس از دریافت تعداد زیادی ایمیل حاوی هرزنامه (Spam)، گویا مهاجمی ناشناس به حساب کاربری او در Npm Repository دسترسی پیدا کرده و سه نسخه مخرب از کتابخانه UAParser.js را منتشر کرده است.

با این که کتابخانه‌های مذکور ظاهراً تنها کمی بیشتر از چهار ساعت از ساعت ۱۴:۱۵ تا ۱۸:۲۳ به وقت اروپای مرکزی (Central European Time - به اختصار CET) روز ۳۰ مهر ۱۴۰۰ به صورت آنلاین در دسترس بوده‌اند، تعداد قابل توجهی از ماشین‌ها توانسته بودند آن را دانلود کنند.

عصر همان روز، توسعه‌دهنده کتابخانه مذکور، متوجه فعالیت غیرمعمول هرزنامه در صندوق ورودی خود شده ودر مورد وقوع فعالیتی مشکوک هشدار داد و به دنبال آن علت اصلی مشکل را کشف کرد. توسعه‌دهنده مذکور بلافاصله با پشتیبانی Npm تماس گرفته و به آن‌ها درخصوص سه نسخه آلوده شده از کتابخانه UAParser.js هشدار داده است و توصیه نموده که به سرعت نسخ آلوده شده را حذف کنند. وی همچنین اظهار داشته که به سختی می‌توان فهمید که در این مدت چند بار کتابخانه‌های آلوده دانلود شده‌اند.

در صورت دانلود کتابخانه‌های آلوده، چه کاری باید انجام داد؟

اولین قدم این است که کامپیوترها را به منظور شناسایی بدافزار بررسی کنید. سپس کتابخانه‌های خود را به نسخ وصله شده ۰.۷.۳۰، ۰.۸.۱ و ۱.۰.۱ به روزرسانی کنید.

اما این به‌روزرسانی کافی نیست، بنا بر توصیه‌نامه‌ای که در نشانی زیر قابل دریافت است، هر کامپیوتری که نسخ آلوده کتابخانه مذکور روی آن نصب یا اجرا شده باید کاملاً در معرض خطر تلقی شود. بنابراین، کاربران و راهبران امنیتی باید تمام اطلاعات اصالت‌سنجی (رمزهای عبور) را که در آن کامپیوترها بکارگرفته شده، تغییر دهند.

https://github.com/advisories/GHSA-pjwm-rvh2-c87w

به طور کلی، محیط‌های توسعه یا پیاده‌سازی، اهداف مناسبی برای مهاجمانی هستند که از آن جهت سازماندهی حملات زنجیره تامین سوءاستفاده می‌کنند. این بدان معناست که چنین محیط‌هایی همواره به رصد و محافظت نرم‌افزارهای ضدویروس نیاز دارند.

Abcbot؛
باتنت جدید DDoS

شرکت چیهو ۳۶۰ (Qihoo ۳۶۰, Ltd.)، در گزارشی در خصوص گونه جدیدی از باتنت DDoS به نام Abcbot هشدار داده است.

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

به نقل از محققان شرکت چیهو ۳۶۰، باتنت مذکور دارای قابلیت‌های کرم (Wormable Capabilities) بوده و سیستم‌های تحت Linux را جهت اجرای حملات DDoS مورد تسخیر قرار می‌دهد. شرکت امنیتی مذکور در مجموع شش نسخه از باتنت Abcbot را تا به امروز تحلیل کرده است.

در ۲۳ تیر ۱۴۰۰، متخصصان امنیتی یک فایل ELF ناشناخته را کشف کردند که پویش گسترده‌ای را جهت شناسایی سیستم‌های تحت Linux انجام می‌دهد؛ تحلیل فایل مذکور نشان داد که پیاده‌سازی پویشگر (Scanner) مذکور با زبان برنامه‌نویسی Go انجام شده است. نامگذاری Abcbot، از مسیر منبع آن یعنی "abc-hello" الهام گرفته شده است.

وجود رشته "dga.go" در مسیر منبع Abcbot نشان می‌دهد که نویسندگان DGA را در نسخه‌های بعدی پیاده‌سازی خواهند کرد.

نسخه‌های اولیه بدافزار فوق بسیار ساده بودند. Abcbot در نسخه‌های ابتدایی به عنوان پویشگر برای نفوذ به سیستم‌های تحت Linux، از رمزهای عبور ضعیف و آسیب‌پذیری‌های روز صفر سوءاستفاده نموده و بدافزار را همانند کرم منتشر می‌کرد. با گذشت زمان، Abcbot به تکامل خود ادامه داد و همانطور که انتظار می‌رفت، ویژگی DGA را در نمونه‌های بعدی اضافه کرد. جدیدترین نسخه‌ها (۸ آبان ۱۴۰۰)، پایگاه داده‌های رایج و سرورهای WEB را هدف قرار می‌دهند.

امروزه Abcbot توانایی خود به‌روزرسانی، راه‌اندازی Webserver، اجرایی حملات DDoS و همچنین انتشار کرم مانند را دارد.

شرکت ترند میکرو (Trend Micro, Inc.) در ماه اکتبر مؤلفه‌های (Component) مورد استفاده در زنجیره حمله خانواده این بدافزار را در گزارش زیر تحلیل کرد.

https://www.trendmicro.com/en_us/research/۲۱/j/actors-target-huawei-cloud-using-upgraded-linux-malware-.html

در گزارش مذکور به تفصیل حملات صورت گرفته علیه Huawei Cloud برای استخراج رمز ارز (Cryptocurrency mining) بررسی شده است.

بدافزار مذکور پس از نصب بر روی سیستم هدف، اطلاعات سیستم را به سرور کنترل و فرمان‌دهی (C2) گزارش می‌کند و شروع به پویش درگاه‌های باز می‌کند تا دستگاه‌های دیگر را آلوده کند. این بدافزار زمانی که گردانندگان بات (botmasters) ویژگی‌های جدیدی را اضافه می‌کنند، خود را به‌روزرسانی می‌کند.

Abcbot از تابع "abc_hello_web_StartServer" برای راه‌اندازی یک WebServer در سیستم‌های آلوده استفاده می‌کند و درگاه ۲۶۸۰۰ را شنود می‌کند.

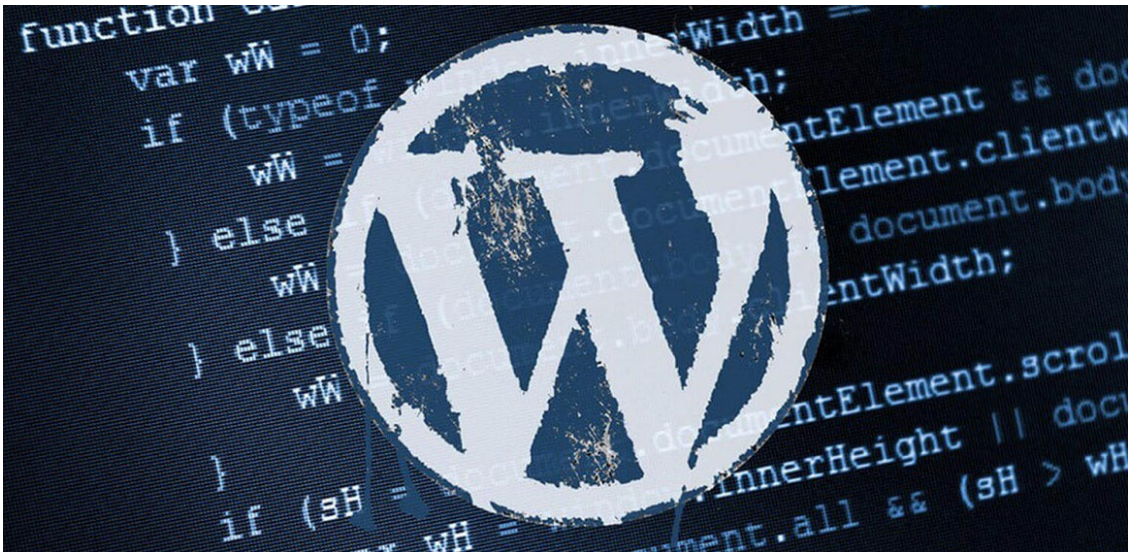
در ۲۹ مهر ۱۴۰۰، گردانندگان آن، یک به‌روزرسانی را به منظور افزودن روت‌کیت منبع باز ATK برای پشتیبانی از اجرای حملات DDoS اعمال کردند، اما با به‌روزرسانی جدید در ۸ آبان ۱۴۰۰، به‌روزرسانی قبلی کنار گذاشته شد، زیرا گردانندگان قابلیت حملات DDoS خود را پیاده‌سازی کردند.

نتایج تحلیل مذکور حاکی از آن است که پروسه به‌روزرسانی در این شش ماه، جهت ارتقاء مداوم ویژگی‌ها نیست، بلکه توازنی بین فناوری‌های مختلف است. Abcbot به آرامی به تکامل می‌رسد. البته همچنان این مرحله، شکل نهایی بات‌نت مذکور نیست، بدیهی است که در این مرحله ویژگی‌های زیادی وجود دارند که باید توسعه یابند.

مشروح گزارش شرکت چیهو ۳۶۰ و همچنین فهرست نشانه‌های آلودگی (Indicators of Compromise - به اختصار IoC) بات‌نت Abcbot در حملات اخیر در نشانی زیر قابل دریافت است:

https://blog.netlab.360.com/abcbot_an_evolving_botnet_en/

سایت‌های WordPress،
هدف حملات باج‌افزاری جعلی



مهاجمان در موج جدیدی از حملات که از اواخر هفته گذشته شروع شده، نزدیک به ۳۰۰ سایت WordPress را برای نمایش اعلان‌های رمزگذاری جعلی هک کرده‌اند. مهاجمان در این حملات سعی دارند صاحبان سایت را فریب دهند تا ۰.۱ بیت کوین برای بازیابی فایل‌ها بپردازند.

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

این درخواست باج‌خواهی همراه با یک تایمر شمارش معکوس ارائه می‌شود تا احساس فوریت را القاء کند و احتمالاً مدیر سایت را برای پرداخت باج دستپاچه کند. این در حالی است که مقدار باج ۰.۱ بیت کوین (تقریباً معادل ۶.۲۳.۰۶۹ دلار) در مقایسه با آنچه که در حملات باج‌افزارهای شناخته‌شده و باسابقه می‌بینیم، چندان قابل توجه نیست، اما هنوز هم می‌تواند برای بسیاری از صاحبان سایت‌ها مقدار قابل توجهی باشد.

ترفند مهاجمان سایت‌های WordPress برای القاء وقوع حملات باج‌افزاری

این حملات توسط شرکت امنیت سایبری Sucuri بررسی شد. محققان Sucuri شروع به تحقیق در مورد سایت کردند و معلوم شد که هیچ چیزی رمزگذاری نشده است! آن‌ها دریافتند که سایت‌ها رمزگذاری نشده‌اند، بلکه مهاجمان یک پلاگین (افزونه) نصب‌شده در WordPress را جهت نمایش یادداشت اطلاعیه باج‌گیری (Ransom Note) و شمارش معکوس تغییر داده‌اند.

معمولاً وقتی باج‌افزار، فایل‌های سایت را مورد رمزگذاری قرار می‌دهد، پسوند آن‌ها را به lock. یا چیزی مشابه این تغییر می‌دهد و دیگر فایل‌های رمزگذاری‌شده، قابل خواندن نمی‌باشند. اما در این حملات اینطور نیست. اخطار باج کاملاً ساختگی بود. هیچ فایلی رمزگذاری نشده بود! این یک صفحه HTML ساده بود که تنها توسط یک افزونه جعلی تولید شده بود و نه چیزی بیشتر.

```
<div class="bgimg">
 <div class="middle">
   <h1>SITE ENCRYPTED</h1>
   <hr>
   <p id="demo"></p>

   <p id="INFO">
   FOR RESTORE SEND 0.1 BITCOIN: 3BkiGYFh6QtjtNCPNNjGwszoqqCka2SDEc
   </p>
   <p id="INFO"><small style="font-size:14px;">
   (create file on site /unlock.txt with transaction key inside)
   </small></p>
 </div>
</div>
```

برای تولید ساعت شمارش معکوس نیز از تعدادی اسکریپت PHP اولیه استفاده شده است.

```
<script>
// Set the date we're counting down to
var countDownDate = new Date("Nov 20, 2021 00:00:00").getTime();

// Update the count down every 1 second
var x = setInterval(function() {

  // Get todays date and time
  var now = new Date().getTime();

  // Find the distance between now an the count down date
  var distance = countDownDate - now;

  // Time calculations for days, hours, minutes and seconds
  var days = Math.floor(distance / (1000 * 60 * 60 * 24));
  var hours = Math.floor((distance % (1000 * 60 * 60 * 24)) / (1000 * 60 * 60));
  var minutes = Math.floor((distance % (1000 * 60 * 60)) / (1000 * 60));
  var seconds = Math.floor((distance % (1000 * 60)) / 1000);

  // Display the result in an element with id="demo"
  document.getElementById("demo").innerHTML = days + "d " + hours + "h "
  + minutes + "m " + seconds + "s ";

  // If the count down is finished, write some text
  if (distance < 0) {
    clearInterval(x);
    document.getElementById("demo").innerHTML = "EXPIRED";
  }
}, 1000);
</script>
```

برای حذف این آلودگی، تنها باید افزونه را از wp-content/plugins directory حذف نمود. با این حال، هنگام مراجعه به صفحه اصلی سایت، در همه صفحات و پست‌های آنها، خطای 404 Not Found مشاهده می‌شود. دلیل این امر آخرین قطعه از افزونه مخرب است، که در تصویر زیر نمایش داده شده است:

```
126  <?php
127  global $wpdb;
128  $wpdb->query("UPDATE $wpdb->posts SET post_status='null' WHERE post_status='publish' ");
129  include(dirname(__FILE__)."/azz_encrypt.php");
130  exit;
```

علاوه بر نمایش اطلاعیه باج‌گیری، مهاجمان با دستکاری یکی از دستورات اولیه SQL، یعنی با تغییر گزینه "Post_status"، تمام پست‌ها و صفحات وبلاگ WordPress را از "publish" به "null" تغییر می‌دهند که منجر می‌شود آن‌ها به وضعیت "منتشر نشده" بروند. با اعمال این تغییر، همه محتواها هنوز در پایگاه داده هستند، فقط قابل مشاهده نمی‌باشند! این در حالی است که مهاجمان با تغییر وضعیت صفحات سایت و انتشار اطلاعیه باج‌گیری، این را به قربانیان القاء کرده‌اند که سایت آن‌ها رمزگذاری شده است.

دستور مذکور را می‌توان با یک دستور SQL به آسانی همانند آنچه در زیر نمایش داده شده، معکوس کرد. با این کار هر محتوایی که در پایگاه‌داده به صورت null علامت‌گذاری شده است، به حالت قبل برگشته و منتشر می‌شود.

```
UPDATE `wp_posts` SET `post_status` = 'publish' WHERE `post_status` = 'null';
```

بنابراین با حذف افزونه و اجرای دستور بازنشر پست‌ها و صفحات، سایت به وضعیت عادی خود برمی‌گردد.

پس از تحلیل بیشتر گزارش‌های ترافیک شبکه، محققان Sucuri دریافتند که اولین نقطه‌ای که آدرس IP مهاجمان در آن مشاهده می‌شود، پنل wp-admin است. این بدان معنی است که مهاجمان به عنوان سرپرست سایت از طریق اجرای حملات موسوم به Brute-Force یا بواسطه جستجو در بازارهای Dark Web جهت دستیابی به اطلاعات اصالت‌سنجی سرقت شده، در سایت وارد شده‌اند.

به نظر می‌رسد این یک حمله انفرادی نبوده، بلکه به نظر می‌رسد بخشی از کارزاری گسترده‌تر باشد.

افزونه‌ای که محققان Sucuri در این حملات مشاهده کردند، افزونه Directorist بوده که ابزاری برای ایجاد فهرستی در فهرست‌های کسب‌وکار آنلاین (online business directories) موجود در سایت‌ها می‌باشد.

محققان مذکور تقریباً ۲۹۱ سایت را که تحت تأثیر این حملات قرار گرفته بودند، شناسایی کرده‌اند. سایت‌های متاثر از این حمله در نشانی زیر، در موتور جستجوی Google، نشان داده شده است. بعضی از این سایت‌ها، عملیات پاکسازی را انجام داده‌اند، ولی در برخی دیگر هنوز اطلاعیه‌های باج‌گیری قابل نمایش است.

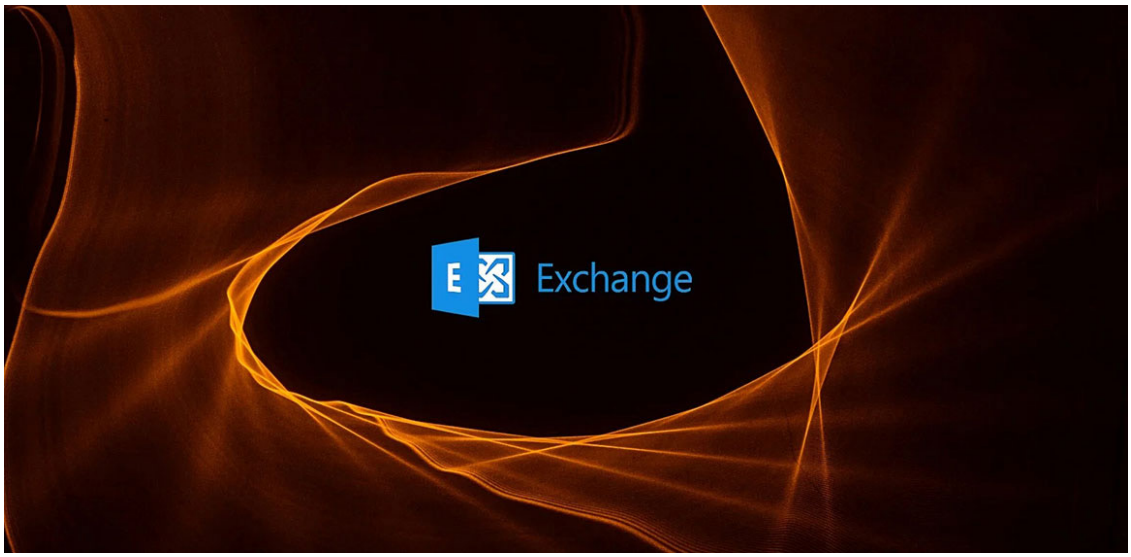
https://www.google.com/search?q=%E2%80%9CFOR+RESTORE+SEND+0.1+BITCOIN%E2%80%9D

به نقل از سایت اینترنتی BleepingComputer، همه سایت‌هایی که در نتایج جستجو نشانی بالا، مشاهده می‌شوند، با استناد به لینک زیر، از آدرس بیت‌کوین 3BkiGYFh6QtjtNCPNNjGwszoqqCka2SDEc استفاده می‌کنند که تاکنون هیچ باجی پرداخت نشده است.

https://www.blockchain.com/btc/address/3BkiGYFh6QtjtNCPNNjGwszoqqCka2SDEc

مهاجمان

باز هم در پی سرورهای Exchange



اخیراً مهاجمان با سوءاستفاده از ضعف‌های امنیتی ProxyShell و ProxyLogon، سرورهای Microsoft Exchange را هک کرده و از طریق تکنیک جدیدی موسوم به Reply Chain Attack اقدام به توزیع بدافزار کرده‌اند.

محققان شرکت ترند میکرو (Trend Micro, Inc.) تکنیک مذکور را که مهاجمان از آن جهت توزیع ایمیل‌های مخرب میان کاربران داخلی یک سازمان استفاده می‌کنند، مورد بررسی قرار داده‌اند.

ProxyShell عنوانی است که به مجموعه سه آسیب‌پذیری زیر اطلاق می‌شود:

- CVE-2021-34473 - که ضعفی از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution - به اختصار RCE) است و در ۲۲ تیر ۱۴۰۰ توسط مایکروسافت وصله شد.
- CVE-2021-34523 - که ضعفی از "ترفیع امتیازی" (Elevation of Privilege) است. این آسیب‌پذیری نیز در ۲۲ تیر ۱۴۰۰ توسط مایکروسافت وصله شد.
- CVE-2021-31207 - که ضعفی از نوع "عبور از سد کنترل‌های امنیتی" (Security Feature Bypass) است و در ۲۱ اردیبهشت ۱۴۰۰ توسط مایکروسافت وصله شد.
- ProxyLogon نیز عنوانی است که به مجموعه ضعف‌های امنیتی با شناسه‌های CVE-2021-26855، CVE-2021-26857، CVE-2021-26858 و CVE-2021-27065 اطلاق می‌شود.

هنگام راه‌اندازی کارزار ایمیل‌های بدافزاری توسط مهاجمان، سخت‌ترین بخش آن فریب‌دادن و متقاعد کردن دریافت‌کنندگان ایمیل است. مهاجمان باید ایمیل را به گونه‌ای طراحی کنند که دریافت‌کنندگان به فرستنده ایمیل اعتماد کرده و لینک‌ها یا پیوست‌های موجود در آن را باز کنند.

اخیراً محققان حملاتی موسوم به Reply Chain Attack را در سازمان‌ها شناسایی کرده‌اند که در آن زنجیره پاسخ ایمیل توسط مهاجمان ربوده شده و کاربر دریافت کننده ایمیل مخرب، پاسخ (Reply) ایمیل ارسالی خود را به ظاهر از همکار خود دریافت می‌کند. به عبارتی مهاجمان، ایمیل‌های قانونی و موجود بین کاربران سازمان را مورد نفوذ قرار داده و سپس با زدن گزینه Reply به آن‌ها پاسخ می‌دهند و بدافزار خود را در قالب لینک یا فایل‌های ضمیمه شده به ایمیل ارسال می‌کنند.

اعتقاد بر این است که مهاجمان پشت این حمله، مهاجمان معروف "TR" هستند که ایمیل‌های حاوی پیوست‌های مخرب را ارسال می‌کنند. پیوست‌های موجود در ایمیل‌های مذکور، کدهای بدافزاری همچون Qbot، IcedID، Cobalt Strike و SquirrelWaffle را منتشر می‌کنند.

نحوه اجرای حملات Reply Chain Attack

مهاجمان به منظور فریب دادن کاربران سازمان‌ها برای باز کردن پیوست‌های مخرب، با سوءاستفاده از آسیب‌پذیری‌های ProxyShell و ProxyLogon، سرورهای Microsoft Exchange را مورد نفوذ قرار می‌دهند. سپس آن‌ها از این سرورهای Exchange هک شده برای پاسخ‌دادن به ایمیل‌های داخلی سازمان استفاده نموده و لینک‌های حاوی اسناد مخرب را جهت نصب بدافزارهای مختلف ارسال می‌کنند.

محققان شرکت ترند میکرو، Header ایمیل‌ها را در ایمیل‌های مخرب دریافتی سازمان مورد تحلیل قرار داده‌اند. آن‌ها در گزارشی اعلام نموده‌اند که مسیر ایمیل مربوط به داخل سازمان بوده است (بین صندوق‌های پستی سه سرور Exchange داخلی). این امر نشان می‌دهد ایمیل‌ها از یک فرستنده خارجی، open mail relay یا Message Transfer Agent - به اختصار MTA نشات نگرفته است.


Mon 11/8/2021 11:31 AM

[redacted]

Re: [redacted]

To [redacted]

Greeting! Our specialists composed desired document and I send it to you. Document can be found through this link:

1)aayomsolutions.co.in/etiste/quasnam-4966787

2)aparnashealthfoundation.aayom.com/quasisuscipit/totamet-4966787

☺

From: [redacted]
Sent: Sunday, November 7, 2021 1:41 PM
To: [redacted]
Subject: Breakfast

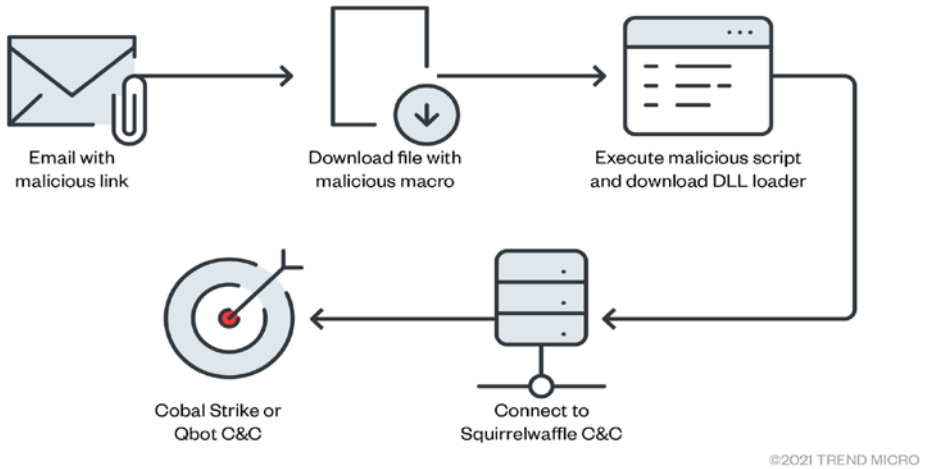
Dear All,

Breakfast on me tomorrow!!

Regards,
Ali

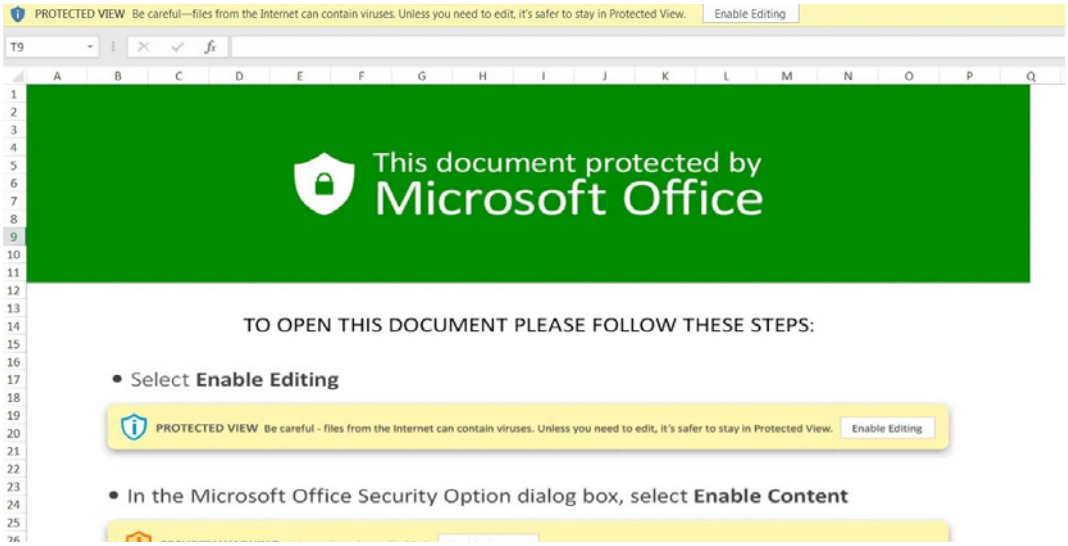
از آنجایی که گیرنده ایمیل مخرب، قبلاً به فرستنده (همکار خود) ایمیل ارسال کرده و به او اعتماد دارد، احتمال باز کردن فایل مخرب ضمیمه شده یا کلیک کردن روی پیوند بدافزاری جاسازی شده در ایمیل پاسخ به شدت افزایش می‌یابد. از طرفی این تکنیک موجب بی‌اثر شدن سیستم‌های حفاظتی ایمیل سازمان شده و اعلان هشداردهی نیز توسط راهکارهای امنیتی سازمان نمایش داده نمی‌شود.

ساختار حملات موسوم به Reply Chain Attack در تصویر زیر نمایش داده شده است.



مهاجمان در حملات موسوم به Reply Chain Attack مجبور نیستند برای ایجاد قالب‌های ایمیل به ظاهر قانونی زمان زیادی صرف کنند، زیرا آنها به کل زنجیره ایمیل‌های سازمان دسترسی داشته و می‌توانند متناسب با موضوع مکالمات زنجیره ایمیل‌های واقعی، پیام‌های خود را تنظیم نموده و کدهای بدافزاری خود را در قالب فایل یا لینک در ایمیل پاسخ ضمیمه و منتشر کنند.

پیوست‌هایی که با این ایمیل‌ها می‌آیند یا به آن‌ها لینک داده می‌شوند، اغلب از الگوهای مخرب استاندارد Microsoft Excel پیروی می‌کنند که در آن به گیرندگان پیامی نمایش داده می‌شود که جهت مشاهده فایل محافظت‌شده، بر روی «Enable Content» کلیک نمایند. در این حالت، هنگامی که کاربر با کلیک بر روی دگمه مذکور، محتوا را فعال می‌کند، ماکروهای مخرب اجرا شده و بدافزار جاسازی شده در پیوست، دانلود و نصب می‌شود، خواه این بدافزار Qbot، Cobalt Strike و SquirrelWaffle یا هر بدافزار دیگری باشد.



بنا بر گزارش محققان، در این حملات، راه‌انداز (Loader) SquirrelWaffle توزیع می‌شود که بدافزار Qbot را نصب می‌کند.

همچنین برخی محققان معتقدند که سند مخرب مورد استفاده در این حملات، به جای توزیع Qbot توسط راه‌انداز SquirrelWaffle، هر دو بدافزار را به عنوان کدهای مجزا منتشر می‌کند.

> *Some of this name confusing might come from initial phrases like "SquirrelWaffle drops QakBot", however as far as I know this has never happened. The maldoc has dropped both DLLs, but the timing is att the qbot traffic starts later than SqWa, so just looks that way in pcaps.*
>
> *— TheAnalyst (@ffforward) November 19, 2021*

سرورهای Exchange خود را همواره به روز نگه دارید

شرکت مایکروسافت (Microsoft Corp) ضعف‌های امنیتی ProxyLogon و ProxyShell را در ماه‌های گذشته ترمیم کرده است. در آن زمان آسیب‌پذیری‌های مذکور از نوع "روز-صفر" اعلام شده بودند.

از آنجایی که مهاجمان از هر دو آسیب‌پذیری مذکور برای استقرار باج‌افزار یا نصب پوسته‌های وب جهت دسترسی به درب‌پشتی (Backdoor) سوءاستفاده می‌کنند، وصله نکردن سرورهای Exchange، پس از گذشت چند ماه و با وجود اطلاع‌رسانی گسترده، همانند ارسال کارت دعوتی برای مهاجمان است.

شرکت مهندسی شبکه گستر اکیداً توصیه می‌کند، راهبران امنیتی در صورت وصله نکردن حفره‌های امنیتی مذکور، با مراجعه به اتاق خبر شرکت مهندسی شبکه گستر و دریافت به‌روزرسانی‌ها و اصلاحیه‌های هر ماه، سرورهای خود را به آخرین نسخه ارتقا داده تا از حملات مهاجمان در امان باشند.

مشروح گزارش شرکت ترند میکرو در نشانی زیر قابل مطالعه است:

https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLog-on-to-Hijack-Email-Chains.html

رویدادها و وقایع امنیتی

رمزگشای مخفی

فایل‌های قربانیان BlackMatter

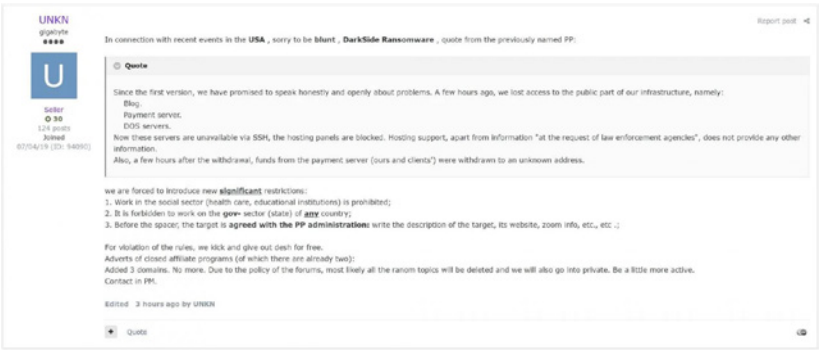
محققان شرکت امنیتی امسی‌سافت (Emsisoft, Ltd.)، از تابستان امسال بی‌سروصدا در حال رمزگشایی فایل‌های قربانیان باج‌افزار BlackMatter بوده‌اند.

BlackMatter یک گروه باج‌افزاری نسبتاً جدید است که حملات آن از تابستان امسال بلافاصله پس از اینکه باج‌افزار دیگری به نام DarkSide فعالیت خود را تعطیل کرد، آغاز شده است. ۳۰ تیر، گردانندگان این باج‌افزار در یکی از تالارهای گفتگوی اینترنتی هکرها، اقدام به انتشار پیام‌هایی در خصوص خرید اطلاعات دسترسی شبکه‌های سازمانی کردند.

با بررسی پیام‌های مهاجمان و نحوه عملکرد آن‌ها به نظر می‌رسد که گردانندگان باج‌افزار BlackMatter افرادی بسیار حرفه‌ای بوده و به احتمال زیاد باج‌افزار آن‌ها، بر پایه باج‌افزاری مطرح و سابقه‌دار توسعه داده شده است. برخی محققان نیز معتقدند باج‌افزار BlackMatter محصول گروهی است که قبلاً با DarkSide و REvil همکاری داشته‌اند. پس از یافتن نمونه‌های این باج‌افزار توسط محققان، مشخص شد که روال‌ها و روش رمزگذاری مورد استفاده در این باج‌افزار، همان شیوه منحصربه‌فرد مورد استفاده در DarkSide است.

سال گذشته گزارش شد که گردانندگان باج‌افزار REvil، برای فرار از پیگیردهای قانونی، اقدام به تغییر نام خود به DarkSide کرده‌اند. در عین حال ظهور DarkSide موجب افول REvil نشد و طی یک سال گذشته هر دوی آنها فعال ماندند.

گروه باج‌افزاری DarkSide حملات باج‌افزاری متعددی را در آگوست ۲۰۲۰ علیه سازمان‌ها در سراسر جهان انجام دادند. حمله آنها به شرکت خط لوله کولونیال، بزرگترین خط لوله سوخت در ایالات متحده، حساسیت نهادهای قانونی به جرایم سایبری را تشدید کرد. این حمله منجر به توقف سرورهای آنها و پرداخت ۴ میلیون دلار به عنوان باج جهت دریافت کلید رمزگشا و بازیابی سرورهای خط لوله کولونیال شد.



گروه باج‌افزاری DarkSide پس از حمله مذکور، در پی اعمال فشار از سوی نهادهای قانونی ایالات متحده، فعالیت خود را تعطیل کردند. با این حال، همواره باج‌افزارها پس از توقف فعالیت خود، با نام‌های جدید بازمی‌گردند. در مورد DarkSide نیز این مساله صادق است و در ماه ژوئیه با نام BlackMatter بازگشته است.

از آن زمان تا کنون، تیم‌های تحقیقاتی از جمله شرکت امسی‌سافت در پی یافتن باگ‌هایی در الگوریتم‌های رمزگذاری باج‌افزار بوده‌اند تا امکان ساخت رمزگشا را فراهم کنند و به قربانیان باج‌افزار کمک کنند تا فایل‌های رمزگذاری شده خود را بازیابی کنند.

با این حال، به منظور جلوگیری از رفع باگ‌های موجود در الگوریتم‌های رمزگذاری باج‌افزارها توسط نویسندگان باج‌افزار، محققان به صورت بی‌سروصدا با شرکا و نهادهای قانونی مورد اعتماد و تیم پاسخ به رویداد همکاری کرده‌اند. در این راستا، اخبار این رمزگشاها در دسترس عموم قرار نگرفته است.

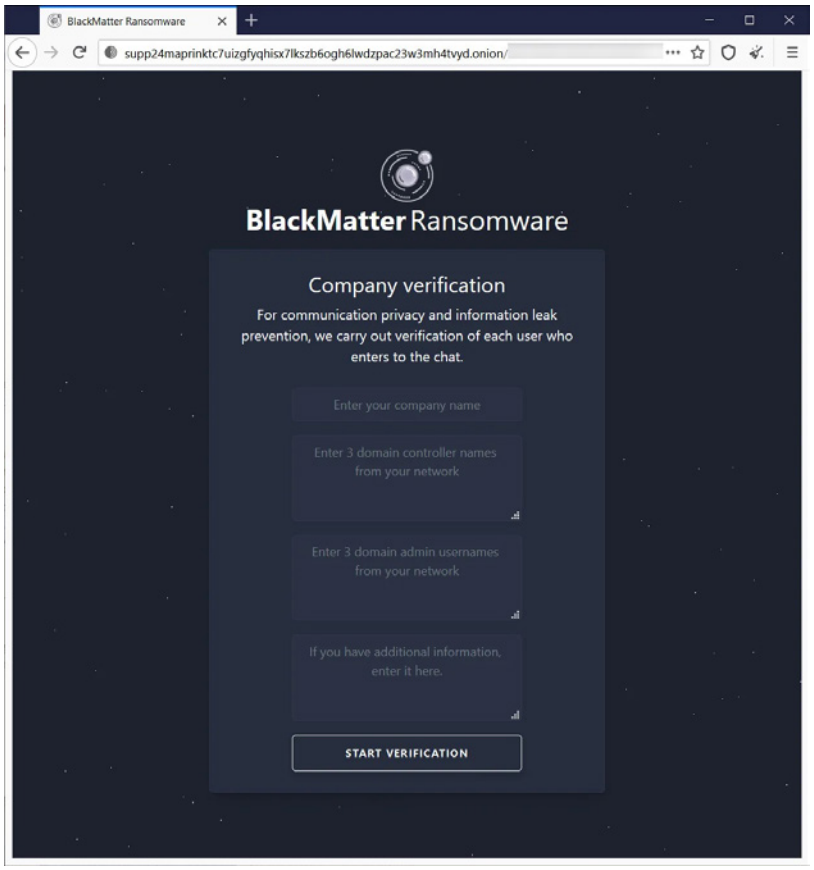
بلافاصله پس از شروع حملات باج‌افزار BlackMatter، محققان امسی‌سافت، باگی را کشف کردند که آن‌ها را قادر می‌ساخت بدون پرداخت باج، کلید رمزگشایی را جهت بازیابی فایل‌های رمزگذاری شده قربانیان ایجاد کنند. پس از آن امسی‌سافت نهادهای قانونی، شرکت‌های مذاکره کننده باج‌افزار، شرکت‌های پاسخگویی به رویدادها و شرکای مورد اعتماد خود را در سراسر جهان در خصوص این رمزگشا مطلع ساخت.

نهادهای مذکور، پس از این اطلاع‌رسانی، قربانیان BlackMatter را جهت بازیابی فایل‌های رمزگذاری شده بدون پرداخت باج، به شرکت امسی‌سافت ارجاع می‌دادند. از آن زمان آن‌ها مشغول کمک به قربانیان این باج‌افزار جهت بازیابی اطلاعات بوده و به آن‌ها کمک نموده که از پرداخت میلیون‌ها دلار باج مطالبه شده، اجتناب کنند. به غیر از موارد ارجاع داده شده توسط نهادهای فوق، شرکت امسی‌سافت نیز با قربانیانی که نمونه‌های باج‌افزار و اطلاعیه‌های باج‌گیری (Ransom Note) را به صورت عمومی در سایت‌های مختلف بارگذاری می‌کردند، تماس می‌گرفت.

پس از انتشار نمونه باج‌افزار BlackMatter به صورت عمومی، قابلیت استخراج اطلاعیه‌های باج‌گیری فراهم شد و محققان شرکت از طریق آن به مذاکرات بین قربانی و گروه باج‌افزاری دسترسی پیدا کردند. پس از شناسایی قربانی، امسی‌سافت به طور خصوصی با مهاجمان باج‌افزاری در خصوص رمزگشا تماس گرفته و مذاکره می‌نمودند تا قربانیان مجبور به پرداخت باج نباشند.

حال که محققان توانسته بودند به نمونه‌ها و اطلاعیه‌های باج‌گیری باج‌افزار BlackMatter دسترسی پیدا کنند، افراد دیگر نیز می‌توانستند این اطلاعات را بدست آورند و از آن‌ها برای ربودن چت‌های مذاکره یا تصاویر اشتراک‌گذاری شده چت‌ها در توییتر استفاده کنند.

این امر در نهایت باعث شد نویسندگان باج‌افزار BlackMatter، سایت مذاکرات خود را قفل کنند تا فقط قربانیان بتوانند به آن‌ها دسترسی پیدا کنند و دیگر محققان نتوانند قربانیان را از این طریق پیدا کنند. قفل کردن سایت مذاکرات توسط گروه باج‌افزاری، منجر به متوقف شدن فعالیت محققان امسی‌سافت و سایر افراد در این روند شده است.



هنگامی که قربانیان از پرداخت باج امتناع کردند، نویسندگان باج‌افزار به طور فزاینده‌ای به مذاکره‌کنندگان باج‌افزار مشکوک و عصبانی شدند. به نقل از یکی از مذاکره‌کنندگان، بعد از اینکه هیچ یک از قربانیان حاضر به پرداخت باج نشدند، از طرف مهاجمان BlackMatter به مرگ نیز تهدید شدند.

متأسفانه مهاجمان در پایان سپتامبر از رمزگشا مطلع شدند و توانستند باگ‌هایی را که به امسی‌سافت اجازه رمزگشایی فایل‌های قربانیان را می‌داد، برطرف کنند. یکی از روش‌هایی که مهاجمان ممکن است از وجود این باگ آگاه شوند، رصد شبکه‌ها و ارتباطات شرکت پس از نفوذ است. به همین دلیل است که محققان امسی‌سافت همیشه به قربانیان توصیه می‌کنند که از یک کانال ارتباطی امن، مانند گروه سیگنال اختصاصی (Dedicated Signal Group) استفاده کنند و همچنین اطمینان حاصل کنند که هیچ یک از شبکه‌های آلوده شده در فرآیندهای بازیابی عمومی دخیل نیستند.

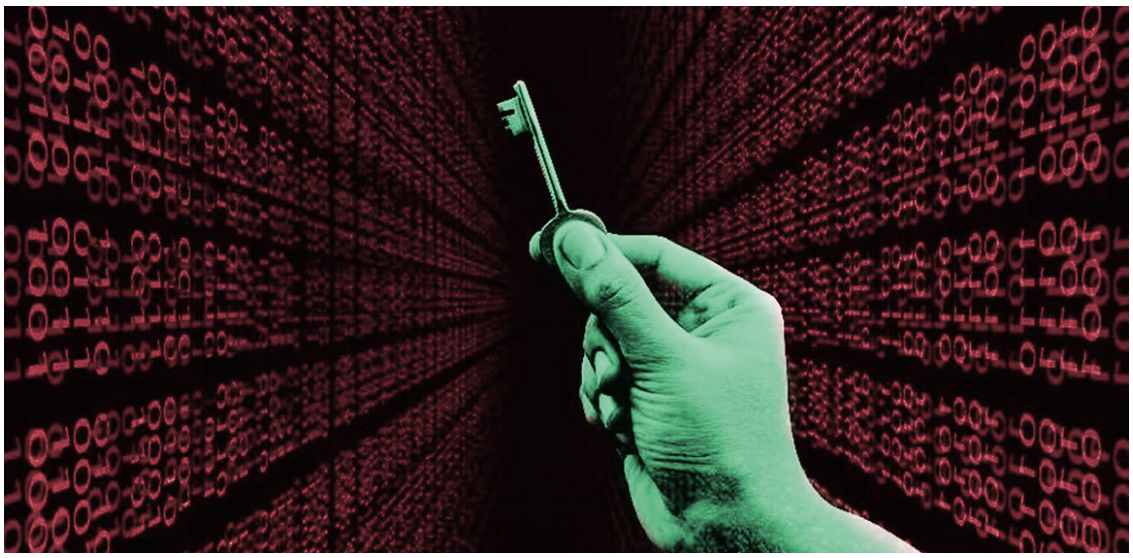
> *"Unlike most of the industry, we don't charge per hour but operate on a fixed price basis. The exact fee is usually in the mid 4 figures, but may depend on the exact circumstances. If a victim can't afford to pay us, we generally waive the fee or come to an alternative arrangement. Ultimately, the fee is not designed to make us rich." - Fabian Wosar.*

پس از این که نویسندگان باج‌افزار BlackMatter، باگ‌ها را برطرف نمودند، شرکت امسی‌سافت دیگر قادر به رمزگشایی فایل‌هایی که پس از آن تاریخ مزگذاری شده نیست، اما همچنان این شرکت به قربانیان پیشنهاد می‌کند که با محققان و شرکت‌های امنیتی تماس بگیرند تا ببینند آیا از نمونه‌های جدیدتر این باج‌افزار می‌توانند باگی کشف کنند.

محققان به قربانیان توصیه می‌کنند تا حملات باج‌افزاری را به نیروهای امنیتی و نهادهای قانونی اطلاع دهند. این نهادها می‌توانند شاخص‌های ارزشمندی از آلودگی را به منظور تحقیق بر روی آن‌ها، جمع‌آوری نموده و در صورت موجود بودن رمزگشا، قربانیان را به شرکت‌های ارائه دهنده کلید رمزگشا ارجاع دهند.

خبر خوش

برای قربانیان سه باج‌افزار



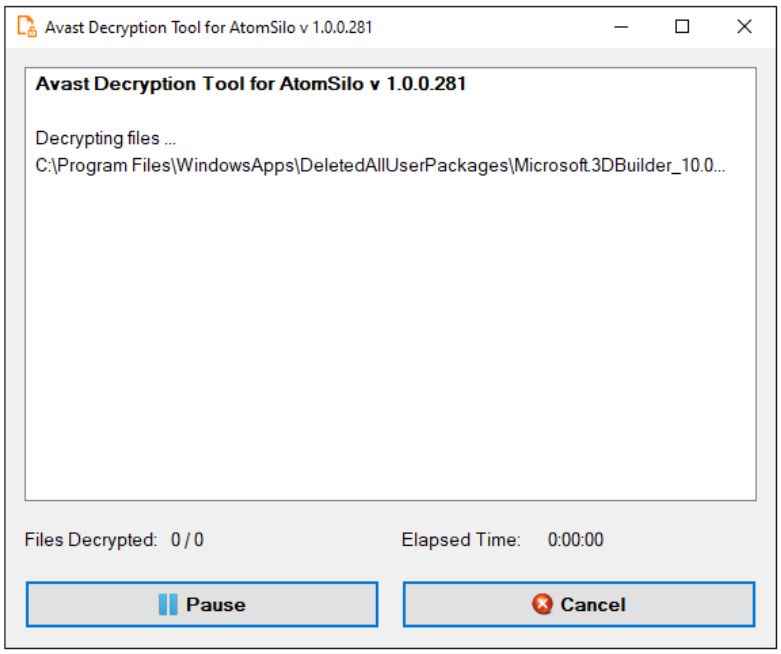
شرکت امنیت سایبری آواست (Avast Software s.r.o) به تازگی دو ابزار رمزگشایی منتشر کرده است که به قربانیان باج‌افزارهای LockFile، AtomSilo و Babuk کمک می‌کند تا برخی از فایل‌های خود را به صورت رایگان و بدون نیاز به پرداخت باج بازیابی کنند.

AtomSilo و LockFile بسیار شبیه به یکدیگر هستند. با وجود این که مهاجمان از تاکتیک‌های مختلفی در حملات این دو باج‌افزار استفاده می‌کنند ولی به علت تشابه بین دو باج‌افزار مذکور، رمزگشای واحدی برای آن‌ها ارائه شده است.

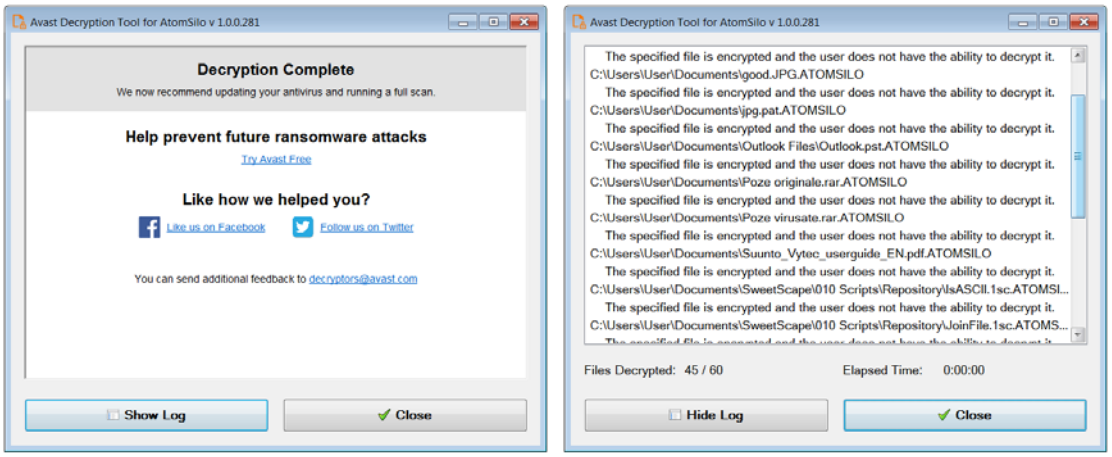
محققان آواست پس از شناسایی نقطه ضعفی در کد باج‌افزار AtomSilo موفق به ارائه این رمزگشا شدند و عنوان نموده‌اند که این رمزگشا ممکن است قادر به رمزگشایی فایل‌های ناشناخته، اختصاصی یا فاقد فرمت نباشد.

ابزار رمزگشای مذکور از طریق نشانی زیر قابل دریافت است:

https://files.avast.com/files/decryptor/avast_decryptor_atomsilo.exe



قربانیان AtomSilo و LockFile می‌توانند ابزار رمزگشایی را از نشانی بالا دانلود کرده و مطابق با دستورالعمل‌های نمایش داده شده در رابط کاربری ابزار رمزگشا، رمزگشایی کنند.



برای اولین بار به دنبال کشف آسیب‌پذیری‌های ProxyShell سرورهای Microsoft Exchange در اردیبهشت، در تیر ماه منتشر شد. به نظر می‌رسد که باج‌افزار LockFile از آسیب‌پذیری‌های ProxyShell برای نفوذ به اهداف بدون وصله در سرورهای Microsoft Exchange و آسیب‌پذیری‌های PetitPotam در Windows جهت تحت اختیار گرفتن کنترل دامنه و رمزگذاری دستگاه‌ها سوءاستفاده می‌کند.

باج‌افزار LockFile، هنگام رمزگذاری فایل‌ها، پسوند lockfile. را به نام فایل‌های رمزگذاری‌شده اضافه می‌کند و اطلاعیه باج‌گیری (Ransom Note) را با فرمت زیر ایجاد می‌کند:

[victim_name]-LOCKFILE-README.hta

جالب توجه این است که طرح رنگ LockFile و طرح اطلاعیه باج‌گیری بسیار شبیه باج‌افزار LockBit است. با این حال، به نظر می‌رسد هیچ رابطه‌ای بین این دو باج‌افزار وجود ندارد.

AtomSilo نیز باج‌افزاری است که جدیداً کشف شده و مهاجمان این باج‌افزار Confluence Server و Data Center را هدف قرار داده‌اند.

در ۳ شهریور ۱۴۰۰، شرکت اطلسین (Atlassian Corporation Plc.) به‌روزرسانی‌های امنیتی را برای ترمیم آسیب‌پذیری در Confluence Server با شناسه CVE-2021-26084 که از نوع "اجرای کد از راه دور" (Remote Code Execution - به اختصار RCE) می‌باشد، منتشر کرد. جزییات و وصله منتشر شده توسط این شرکت در نشانی زیر قابل مطالعه است.

https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html

ضعف امنیتی مذکور به طور فعال توسط مهاجمان مورد سوءاستفاده قرار گرفته است. مهاجمان باج‌افزاری AtomSilo، با سوءاستفاده از ضعف مذکور در موارد غیروصله شده Confluence Server، قادر خواهند بود از راه دور به سرورها دسترسی داشته باشند.

به گفته محققان سوفوس (Sophos, Ltd) که گزارش کامل آن در نشانی زیر قابل دسترس است، باج‌افزار AtomSilo تقریباً مشابه LockFile است.

https://news.sophos.com/en-us/2021/10/04/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack/

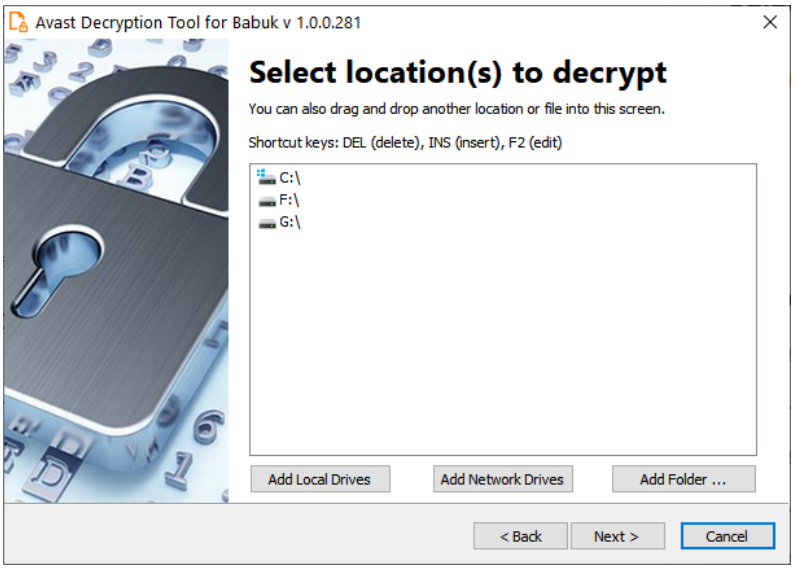
این باج‌افزار تمام داده‌های موجود در کامپیوتر کاربر از جمله (تصاویر، اسناد، جداول اکسل، موسیقی، ویدیوها و غیره) را رمزگذاری می‌کند و پسوند خاص خود را به هر فایل اضافه می‌کند.

با این حال، مهاجمان باج‌افزار AtomSilo از تکنیک‌های جدیدی همچون Side-loading malicious dynamic-link libraries استفاده می‌کنند که شناسایی حملات آنها را بسیار دشوار می‌کند و راهکارهای حفاظت نقاط پایانی را مختل می‌کند.

همچنین محققان آواست با بکارگیری کدهای افشا شده باج‌افزار Babuk، ابزار رمزگشای دیگری را نیز منتشر کرده‌اند تا به قربانیان باج‌افزار مذکور کمک کند که فایل‌های خود را به صورت رایگان بازیابی کنند. این ابزار رمزگشا می‌تواند توسط قربانیانی که فایل‌های آن‌ها با پسوندهای babyk.، babuk. و doydo. رمزگذاری شده است، مورد استفاده قرار گیرد.

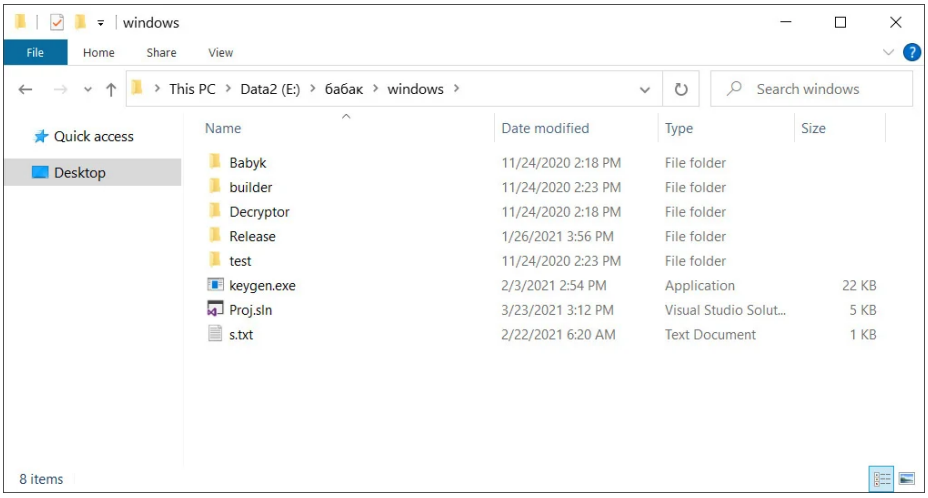
قربانیان باج‌افزار Babuk می‌توانند ابزار رمزگشایی را از نشانی زیر دانلود کرده و کل فایل‌ها را مطابق با دستورالعمل‌های نمایش داده شده در رابط کاربری رمزگشا، به طور رایگان رمزگشایی کنند.

https://files.avast.com/files/decryptor/avast_decryptor_babuk.exe



ماه گذشته، کد منبع (Source Code) کامل باج‌افزار Babuk در یکی از تالارهای گفتگوی هکرهای روسی زبان توسط یکی از مهاجمان که ادعا می‌کرد عضوی از اعضای گروه Babuk است و به نوعی سرطان علاج‌ناپذیر مبتلاست، فاش شد. متن کامل این خبر در "افشای کدهای برنامه‌نویسی باج‌افزارBabuk" قابل مطالعه است.

فایل‌های فاش شده توسط مهاجم مذکور، مربوط به پروژه‌های Visual Studio Babuk جهت رمزگذارهای VMware ESXi، NAS و Windows بود. همچنین پوشه‌ای با نام Windows وجود داشت که حاوی کد منبع کامل رمزگذار، رمزگشای Windows و چیزی شبیه به تولیدکننده‌های کلید خصوصی و عمومی بود. در این افشاگری، کدهای رمزگذاری و کدهای رمزگشایی نیز وجود داشت که گویی برای قربانیان خاص باج‌افزار، کامپایل شده بود.



پس از افشای این اطلاعات، محققان شرکت امسی‌سافت (Emsisoft, Ltd.) عنوان نمودند که کد منبع افشا شده کاملاً معتبر بوده و ممکن است حاوی کلیدهای رمزگشایی برای قربانیان گذشته باشد.

Babuk Locker، که با نام Babuk و Babyk نیز شناخته می‌شود، از ابتدای سال ۲۰۲۱ آغاز شده است و گردانندگان آن سازمان‌های فعال در حوزه‌های مختلف را به منظور سرقت و رمزگذاری داده‌ها مورد هدف قرار می‌داده‌اند. از جمله معروف‌ترین قربانیان این باج‌افزار می‌توان به اداره پلیس واشنگتن اشاره کرد که به نظر می‌رسد آخرین حمله بزرگ آنها پیش از خروج موقت از کسب‌وکار باج‌افزارها بوده است.

پس از حمله به اداره پلیس واشنگتن، این مهاجمان باج‌افزاری ادعا کردند که فعالیت خود را متوقف کرده‌اند. با این حال، چند تن از اعضا از گروه جدا شدند. مدیر اصلی، تالار گفتگوی Ramp را راه‌اندازی نمود و سایر اعضاء با راه‌اندازی نسخه جدیدی از Babuk معروف به Babuk V2، همچنان به اجرای حملات باج‌افزاری و رمزگذاری فایل‌های قربانیان ادامه دادند.

اما خیلی زود تالار گفتگوی Ramp هدف حملات DDoS قرار گرفت. گرداننده این تالار گفتگو، شرکای سابق خود را مسئول این حملات دانست، هر چند که این ادعا توسط تیم Babuk V2 رد شد. مدتی بعد نیز در پی تشدید این اختلافات، یکی از برنامه‌های سازنده Babuk با نام Babuk Ransomware Builder در یک سایت اشتراک فایل فاش شد و توسط گروه دیگری برای راه اندازی حملات باج‌افزاری مورد استفاده گرفت.

McAfee Enterprise؛ فینالیست CRN

CRN، McAfee Enterprise را به عنوان فینالیست دریافت جایزه CRN Tech Innovator Award در سال ۲۰۲۱ انتخاب کرده است.

در ماه مارس (شرکت مک‌آفی McAfee, LLC.) خدمات و محصولات سازمانی خود را به مبلغ ۴ میلیارد دلار به Symphony Technology Group - به اختصار STG - واگذار کرد که منجر به ظهور شرکت جدید McAfee Enterprise شد. در ماه ژوئیه نیز، شرکت فایرآی (FireEye, Inc.) از فروش محصولات این شرکت به STG به قیمت ۱.۲ میلیارد دلار خبر داد. در اکتبر ۲۰۲۱ با ادغام محصولات McAfee Enterprise و FireEye و تشکیل شرکتی با بیش از ۵ هزار کارمند شاهد آغاز فصلی جدید در دنیای امنیت سایبری بودیم.

راهکارهای شرکت McAfee Enterprise موسوم به "از دستگاه تا ابر" (Device-to-Cloud) و ترکیب آنها با محصولات قدرتمند و اختصاصی FireEye فرصتی طلایی برای مقابله با نفوذگران و مهاجمانی است که چند سال اخیر همواره از ارائه‌دهندگان راهکارهای امنیتی یک قدم جلوتر بوده‌اند. این شرکت جدید فناوری نوآورانه، هوشمندی و اتوماسیون را برای کمک به حل پیچیده‌ترین مشکلات امنیت سایبری برای مشتریان خود ترکیب می‌کند. اطلاعات بیشتر در این خصوص در ادغام McAfee Enterprise و FireEye؛ آغاز فصلی جدید در دنیای امنیت سایبری قابل مطالعه است.

McAfee Enterprise جایزه CRN Tech Innovator Award را به دنبال دریافت جوایزی دیگری همچون CyberSecurity Stratus Awards، Breakthrough Awards و Expert Insights "Best of" Fall Awards دریافت کرده است.

جوایز سالانه CRN Tech Innovator Award به ارائه‌دهندگان فناوری که به فعال‌سازی و توانمندسازی کاربران نهایی به صورت مداوم متعهد هستند و در عین حال با ارائه پیشرفته‌ترین محصولات و خدمات هدفمند به عرضه‌کنندگان محصولات فناوری، آن‌ها را در رشد مستمر کسب‌وکار کمک می‌کنند، اعطاء می‌شود.

این جایزه سالانه، شرکت‌های عرضه‌کننده نوآور را در حوزه فناوری اطلاعات (IT) در ۴۷ دسته مختلف تکنولوژی، در حوزه‌های کلیدی از بستر ابری تا ذخیره‌سازی، شبکه و امنیت به نمایش می‌گذارد. برای تعیین برندگان، گروهی از داوران CRN صدها محصول از ارائه‌دهندگان مذکور را با استفاده از معیارهای متعددی همچون قابلیت‌های کلیدی، منحصربه‌فرد بودن، نوآوری در فناوری ارائه شده و توانایی پاسخگویی به نیازهای مشتری و شرکای آنان بررسی می‌کنند.

سازمان‌ها در هر مقیاس و وسعتی که باشند به یک معماری ساده نیاز دارند. آن‌ها به معماری نیاز دارند که آنها را قادر سازد تا با هزینه و پیچیدگی محصولات مختلف نقاط پایانی با موفقیت روبرو شوند و از امکانات محصولات حفاظتی ارائه شده مبتنی بر ابر بدون سرمایه‌گذاری عمده در ابزارهای موجود یا نیروهای توسعه‌دهنده بهره‌مند شوند.

بنا بر اظهارات رئیس Global Sales شرکت McAfee Enterprise، برنامه‌های کاربردی ارائه‌شده در بستر ابری و حفاظت از نقاط پایانی برای محافظت از شرکت‌ها، کسب‌وکارهای تجاری و بخش عمومی در سطح جهانی بسیار مهم هستند. وی در ادامه عنوان نموده که شرکای آنان بخش کلیدی از کسب‌وکار آن‌ها بوده و برای آن‌ها این امکان را فراهم می‌کنند که به ارائه بهترین محصولات امنیتی برای کاربران نهایی خود ادامه دهند.

جوایز Tech Innovator Awards CRN که در ماه دسامبر ارائه می‌شود، به صورت آنلاین در crn.com/techinnovators قابل مشاهده است.

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

به‌روزرسانی‌ها
و اصلاحیه‌های آبان ۱۴۰۰

مـایـکـروسـافـت

سه‌شنبه ۱۸ آبان، شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی نوامبر منتشر کرد. اصلاحیه‌های مذکور ۵۵ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند.

درجه اهمیت ۶ مورد از آسیب‌پذیری‌های ترمیم شده این ماه "حیاتی" (Critical) و ۴۹ مورد دیگر "مهم" (Important) اعلام شده است.

این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را به شرح زیر در محصولات مختلف مایکروسافت ترمیم می‌کنند:

- "ترفیع امتیازی" (Elevation of Privilege)
- "اجرای کد به صورت از راه دور" (Remote Code Execution)
- "افشای اطلاعات" (Information Disclosure)
- "جعل" (Spoofing)
- "عبور از سد امکانات امنیتی" (Security Feature Bypass)
- "منع سرویس" (Denial of Service - به اختصار DoS)

۶ مورد از آسیب‌پذیری‌های ترمیم شده این ماه، از نوع "روز-صفر" (شناسه‌های CVE-2021-42292، CVE-2021-42321، CVE-2021-38631، CVE-2021-41371، CVE-2021-43208 و CVE-2021-43209) می‌باشند. ۲ مورد از آسیب‌پذیری‌های "روز-صفر" ترمیم شده در این ماه به طور فعال مورد سوءاستفاده قرار گرفته‌اند. 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.

فهرست ۲ ضعف امنیتی "روز-صفر" این ماه که به طور فعال مورد سوءاستفاده قرار گرفته‌اند به شرح زیر است:

- CVE-2021-42292: درجه اهمیت این ضعف امنیتی از نوع "مهم" بوده و مهاجم می‌تواند از این آسیب‌پذیری در Microsoft Excel برای عبور از سد امکانات امنیتی در ماشین‌های مورد نظر سوءاستفاده کند. اکنون که فایل‌های پیوست ایمیل، عامل اصلی آلودگی سیستم‌ها می‌باشند، مهاجم می‌تواند از این آسیب‌پذیری برای افزایش کارایی حملات خود با اجتناب از نمایش اعلان امنیتی و در نتیجه کاهش مهندسی اجتماعی لازم برای آلوده کردن قربانی استفاده کند. لازم به توضیح است که به‌روزرسانی امنیتی Microsoft Office for Mac هنوز منتشر نشده است.

- CVE-2021-42321: دومین ضعف امنیتی "روز-صفر" که به طور فعال مورد سوءاستفاده قرار گرفته، بر سرور Microsoft Exchange تأثیر می‌گذارد و به دلیل اعتبار سنجی نامناسب آرگومان‌های cmdlet، می‌تواند منجر به "اجرای کد به صورت از راه دور" شود. اگرچه، مهاجمان باید احراز هویت شوند.

در سپتامبر، مایکروسافت یک ویژگی جدید به نام Microsoft Exchange Emergency Mitigation (EM) در سرورهای Exchange اضافه کرد که حفاظت خودکار را برای سرورهای آسیب‌پذیر فراهم می‌کرد. راهکار حفاظتی مذکور با اعمال خودکار کاهش موقتی اثرات مخرب ناشی از باگ‌های امنیتی پرخطر، سرورهای داخلی را در برابر حملات ورودی ایمن می‌کند و به مدیران وقت بیشتری برای اعمال به‌روزرسانی‌های امنیتی می‌دهد. با این که از این قابلیت جدید در سرورهای Exchange جهت کاهش اثر سوء ضعف‌هایی که به صورت فعال مورد بهره‌جویی قرار گرفته، استفاده می‌شود، در به‌روزرسانی‌های امنیتی ماه نوامبر مایکروسافت هیچ اشاره‌ای به استفاده از Exchange EM برای CVE-2021-42321 نشده است. لذا توصیه اکید می‌شود که راهبران امنیتی در اسرع وقت نسبت به نصب آخرین وصله در سرورهای Exchange اقدام نمایند.

۴ آسیب‌پذیری دیگر ترمیم شده در این ماه که جزییات آن به صورت عمومی افشاء شده در ادامه شرح داده شده است، هر چند تا این لحظه سوءاستفاده مهاجمان از این آسیب‌پذیری‌ها در حملات گزارش نشده است.

- CVE-2021-38631: این ضعف امنیتی از نوع "افشای اطلاعات" است و پودمان Remote Desktop Protocol - به اختصار RDP - در سیستم عامل Windows از آن تاثیر می‌پذیرد.
- CVE-2021-41371: این آسیب‌پذیری نیز از نوع "افشای اطلاعات" بوده و پودمان RDP را متأثر می‌کند. ضعف امنیتی مذکور قبل از انتشار وصله (Patch) شناخته شده بود و می‌تواند به صورت محلی جهت نشت اطلاعات مورد سوءاستفاده قرار گیرد.
- CVE-2021-43208: پنجمین ضعف امنیتی "روز-صفر" می‌تواند توسط مهاجم محلی برای اجرای "کد از راه دور" در Microsoft 3D Viewer مورد سوءاستفاده قرار بگیرد.
- CVE-2021-43209: آخرین ضعف امنیتی "روز-صفر" در 3D Viewer بوده که جزییات آن به صورت عمومی افشاء شده و مهاجم می‌تواند از آن برای "اجرای کد از راه دور" سوءاستفاده کند.

یکی از آسیب‌پذیری‌های بسیار مهم ترمیم شده در این ماه، ضعفی با شناسه CVE-2021-38666 می‌باشد، که از نوع "اجرای کد از راه دور" بوده و Remote Desktop Client از آن تاثیر می‌پذیرد. ضعف امنیتی مذکور دارای درجه اهمیت "حیاتی" است و مهاجمی که کنترل Remote Desktop Server را در اختیار دارد، می‌تواند از این آسیب‌پذیری برای اجرای کد از راه دور در ماشین Client سوءاستفاده کند. به این صورت که مهاجم قربانی را فریب می‌دهد تا به سرور تحت کنترل مهاجم، که نسخه آسیب‌پذیر Remote Desktop Client را اجرا می‌کند، متصل شود. مهاجم می‌تواند تحت شرایط خاص از این آسیب‌پذیری برای کسب امتیازات بیشتر یا گسترش آلودگی در سطح شبکه (Lateral Movement) استفاده کند.

یکی دیگر از آسیب‌پذیری‌های "اجرای کد از راه دور" با درجه اهمیت "حیاتی"، ضعفی با شناسه CVE-2021-42298 در Windows Defender است، سرویس ضدویروس رایگانی که به صورت پیش‌فرض در تمام دستگاه‌های Windows نصب شده است. یک فایل دستکاری شده خاص زمانی که توسط Windows Defender پویش می‌شود یا هنگامی که توسط کاربر باز شود، می‌تواند باعث اجرا و فعال شدن ضعف امنیتی مذکور شود. مهاجم با این روش می‌تواند سیستم راه دوری را که در آن یک فایل مخرب از طریق ایمیل یا برنامه‌های پیام رسانی فوری تحویل داده شده، آلوده کند.

دیگر ضعف امنیتی "حیاتی"، CVE-2021-26443 است که Microsoft Virtual Machine Bus از آن متاثر می‌شود و دارای درجه شدت ۹ از ۱۰ است. سوءاستفاده از این آسیب‌پذیری می‌تواند منجر به اجرای فرمان از روی ماشین مجازی میهمان (Guest VM) بر روی دستگاه میزبان (Host VM) شده و از این طریق موجب "ترفیع امتیازی" شود.

با توجه به این‌که برخی از ضعف‌های امنیتی این ماه به طور فعال مورد سوءاستفاده قرار گرفته، توصیه می‌شود کاربران در اسرع وقت نسبت به به‌روزرسانی وصله‌ها اقدام نمایند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های نوامبر 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/235046/237266/244673/

همچنین در ۲۴ آبان ماه، شرکت مایکروسافت در گزارشی اقدام به انتشار به‌روزرسانی‌های اضطراری جهت ترمیم خطاهایی که مربوط به اعطای مجوز Kerberos می‌باشند، نمود. باگ‌های مذکور پس از نصب به‌روزرسانی‌های امنیتی ماه میلادی نوامبر ۲۰۲۱ بر روی سرورهای Domain Controller که درنسخه‌های مختلف Windows Server اجرا می‌شوند، رخ داده است.

عدم اعمال این به‌روزرسانی اضطراری ممکن است باعث خطاهای احراز هویت مربوط به Kerberos Tickets که از طریق Service for User to Self - به اختصار S4U2self حاصل شده است، شود. جزییات بیشتر در گزارش زیر قابل مطالعه است:

https://newsroom.shabakeh.net/22779/microsoft-emergency-updates-fix-windows-server-auth-issues.html

سـیسـکو

شرکت سیسکو (Cisco Systems, Inc.) در آبان ماه در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها، ۴۸ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۳ مورد از آن‌ها "حیاتی"، ۱۳ مورد از آنها از نوع "بالا" (High) و ۳۲ مورد از نوع "متوسط" (Medium) گزارش شده است. آسیب‌پذیری به حملاتی همچون "منع سرویس"، "تزریق کد از طریق سایت" (Cross-Site Scripting)، "ترفیع امتیازی"، "تزریق فرمان" (Command Injection)، "افشای اطلاعات" و "سرریز حافظه" (Buffer Overflow) از جمله مهمترین اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید هستند. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌دیده سوءاستفاده کند. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

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

مـک‌آفـی اینتـرپـرایز

در آبان ۱۴۰۰، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) با انتشار توصیه‌نامه، از ترمیم دو آسیب‌پذیری با شناسه‌های CVE-2021-31848 و CVE-2021-31849 در نسخه ۱۱.۶.۴۰۰ نرم‌افزار McAfee DLP Endpoint خبر داد. این شرکت با عرضه نسخه 7.3.0 HF2 نرم‌افزار McAfee Drive Encryption، ضعفی با شناسه CVE-2021-31853 را نیز در این محصول اصلاح کرد. جزییات بیشتر در توصیه‌نامه‌های زیر قابل دریافت و مطالعه است:

https://kc.mcafee.com/corporate/index?page=content&id=SB10371

https://kc.mcafee.com/corporate/index?page=content&id=SB10374

همچنین مک‌آفی اینترپرایز، در آبان، نسخه November 2021 نرم‌افزار McAfee Endpoint Security را منتشر کرد که تغییرات لحاظ شده در این نسخه در لینک زیر قابل دسترس است:

https://docs.mcafee.com/bundle/endpoint-security-10.7.x-release-notes/page/GUID-DF4BB39D-EED2-40C6-BD54-6A62EBE68E3F.html

بـیـت‌دیـفـنـدر

در ماهی که گذشت شرکت بیت‌دیفندر (Bitdefender) با انتشار نسخ جدید، در مجموع چهار باگ امنیتی را در محصولات Bitdefender Endpoint Security Tools و Bitdefender GravityZone ترمیم و اصلاح کرد. اطلاعات بیشتر در خصوص باگ‌های مذکور در لینک‌های زیر قابل دریافت و مطالعه است:

https://www.bitdefender.com/support/security-advisories/privilege-escalation-via-seimpersonateprivilege-in-bitdefender-endpoint-security-tools-va-9848

https://www.bitdefender.com/support/security-advisories/incorrect-default-permissions-vulnerability-in-bdservicehost-exe-and-vulnerability-scan-exe-va-9848

https://www.bitdefender.com/support/security-advisories/path-traversal-vulnerability-in-bitdefender-gravitzone-update-server-in-relay-mode-va-10039

https://www.bitdefender.com/support/security-advisories/improper-link-resolution-before-file-access-in-bitdefender-endpoint-security-tools-for-windows-va-9921

کسـپرسـکی

شرکت کسپرسکی (AO Kaspersky Lab) در ۱۰ آبان از ترمیم یک ضعف امنیتی با شناسه CVE-2021-35053 و از نوع "از کاراندازی سرویس" در چندین محصول خود از جمله Kaspersky Small Office Security و Kaspersky Endpoint Security خبر داد. توضیحات این شرکت در مورد آسیب‌پذیری مذکور در لینک زیر قابل مطالعه است:

https://support.kaspersky.com/general/vulnerability.aspx?el=12430#01112021

وی‌ام‌ور

در ماهی که گذشت، شرکت وی‌ام‌ور (VMware, Inc) با انتشار توصیه‌نامه‌های امنیتی، نسبت به ترمیم محصولات زیر اقدام کرد:

- VMware Cloud Foundation
- VMware vCenter Server
- VMware Tanzu Application Service for VMs

سوءاستفاده از برخی از ضعف‌های امنیتی ترمیم شده توسط این به‌روزرسانی‌ها، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. جزییات بیشتر آن در لینک زیر قابل مطالعه است:

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

ادوبـی

در آبان ماه، شرکت ادوبی (Adobe, Inc.) اقدام به انتشار به‌روزرسانی برای محصولات زیر کرد.

- Adobe After Effects
- Adobe Animate
- Adobe Audition
- Adobe Bridge
- Adobe Campaign Standard
- Adobe Character Animator
- Adobe Creative Cloud Desktop Application
- Adobe Experience Manager
- Adobe Illustrator
- Adobe InCopy
- Adobe InDesign
- Adobe Lightroom Classic
- Adobe Media Encoder
- Adobe Photoshop
- Adobe Prelude
- Adobe Premiere Elements
- Adobe Premiere Pro
- Adobe RoboHelp Server
- Adobe XMP Toolkit SDK

اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه نوامبر ادوبی در لینک زیر قابل مطالعه است:

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

گوگل

شرکت گوگل (Google, LLC) در آبان ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۴ آبان ماه انتشار یافت، نسخه ۹۶.۰.۴۶۶۴.۴۵ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html

https://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html

اپل

در آبان ماه، شرکت اپل (Apple, Inc.) با انتشار به‌روزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله iOS، iCloud، Safari، tvOS، watchOS، iPadOS و macOS 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، به‌روزرسانی مربوطه هر چه سریع‌تر اعمال شود.

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

موزیلا

در ماهی که گذشت شرکت موزیلا (Mozilla, Corp) با ارائه به‌روزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد. اصلاحیه‌های مذکور، در مجموع ۱۵ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت ۹ مورد از آنها "بالا"، ۴ مورد "متوسط" (Moderate) و ۲ 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/

اس‌آپ

اس‌آپ (SAP SE) نیز در ۱۸ آبان ۱۴۰۰ با انتشار مجموعه اصلاحیه‌هایی، ۷ آسیب‌پذیری را در چندین محصول خود برطرف کرد. شدت یک مورد از این ضعف‌های امنیتی ۹.۶ 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=589496864

سیتریکس

در ۱۸ آبان ۱۴۰۰، شرکت سیتریکس (Citrix Systems, Inc.) نیز چند آسیب‌پذیری "منع سرویس" را در نسخه‌های مختلف محصولات زیر ترمیم کرد:

- Virtual Apps and Desktops
- Citrix Application Delivery Controller
- Citrix Gateway
- Citrix SD-WAN WANOP Edition

جزییات آنها در لینک زیر قابل دریافت است:

https://support.citrix.com/article/CTX330728

پالو آلتو نتورکس

در ۱۹ آبان ۱۴۰۰، شرکت پالو آلتو نتورکس (Palo Alto Networks, Inc.) با انتشار توصیه‌نامه‌ای، ضعفی به شناسه CVE-2021-3064 را که ضعفی از نوع "دستکاری حافظه" (Memory Corruption Vulnerability) در درگاه GlobalProtect و رابط‌های Gateway می‌باشد، رفع کرد. مهاجم با نفوذ در شبکه از طریق رابط GlobalProtect قابلیت سوءاستفاده از ضعف امنیتی مذکور را پیدا می‌کند و می‌تواند برخی پروسه‌های سیستم را مختل کند و به طور بالقوه منجر به اجرای کد دلخواه (Execution Arbitrary Code) با سطح دسترسی ممتاز می‌شود.

درجه شدت آسیب‌پذیری مذکور ۹/۸ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده است و بر پیکربندی‌های فایروال PAN-OS 8.1 در نسخه‌های قبل از ۸.۱.۱۷ تاثیر می‌گذارد. توصیه‌نامه‌های پالو آلتو نتورکس در لینک زیر قابل مطالعه است:

https://security.paloaltonetworks.com/CVE-2021-3064

دروپال

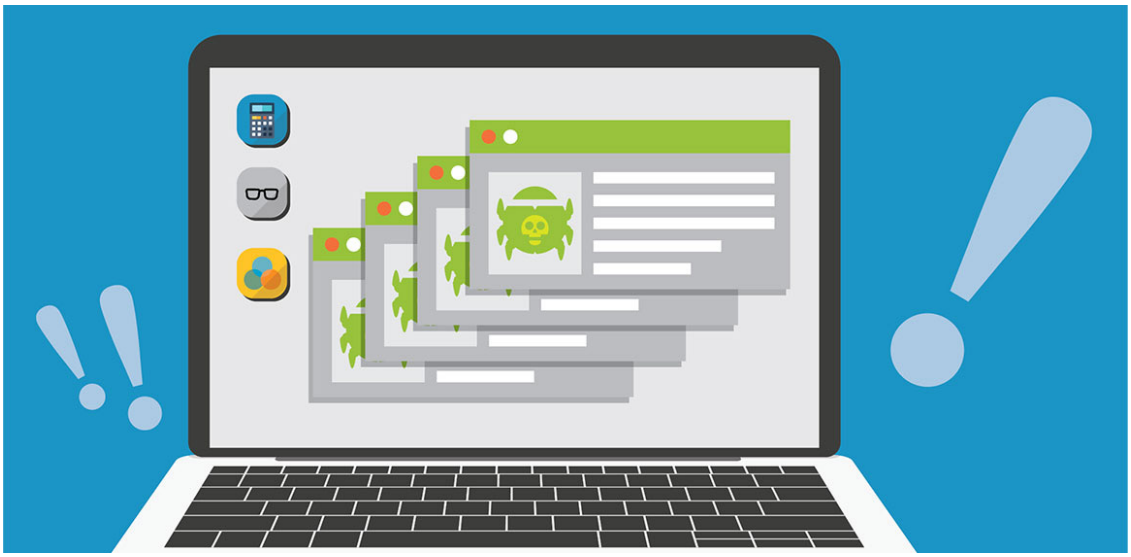
۲۷ آبان، جامعه دروپال (Drupal Community) با عرضه به‌روزرسانی‌های امنیتی، چندین ضعف امنیتی نسخ ۸.۹، ۹.۱ و ۹.۲ خود را اصلاح کرد. سوءاستفاده از بعضی از این آسیب‌پذیری‌ها مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توضیحات کامل در این خصوص در لینک زیر قابل دسترس است.

https://www.drupal.org/sa-core-2021-011

گزارش‌ها

کالبدشکافی نسخه اخیر

بدافزار BazarLoader



در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، برگردانی از گزارش محققان امنیتی شرکت پالو آلتو نتورکس در خصوص بدافزار BazarLoader ارائه شده است.

BazarLoader بدافزاری مبتنی بر Windows است که از طریق روش‌های مختلفی از جمله ایمیل منتشر می‌شود. این آلودگی‌ها برای مهاجمان دسترسی به درب پشتی (Backdoor) را فراهم می‌کنند که مهاجمان از آن برای تعیین اینکه آیا سرویس Active Directory - به اختصار AD - بر روی سرور میزبان فعال است یا خیر، استفاده می‌کنند. در صورتی که سرور میزبان بخشی از AD باشد، تبهکاران سایبری Cobalt Strike را اجرا کرده و شروع به شناسایی شبکه، ساختار و تحلیل آن می‌نمایند.

در صورتی که نتایج تحلیل شبکه نشان‌دهنده هدفی ارزشمند باشد، مهاجمان اغلب باج‌افزارهایی همچون Conti یا Ryuk را منتشر نموده و اقدام به توسعه دامنه آلودگی (Lateral Movement) می‌کنند.

این مقاله، یکی از آلودگی‌های ایجاد شده توسط BazarLoader را مورد بررسی قرار می‌دهد، این که چگونه Cobalt Strike اجرا شده و چگونه Cobalt Strike منجر به شناسایی و توسعه آلودگی در شبکه می‌شود. چنانچه راهبران امنیتی فعالیت مشابهی را در شبکه خود کشف کنند، احتمال آن وجود دارد که مورد حمله باج‌افزاری قرار گرفته باشند.

روش‌های توزیع BazarLoader

در طول تابستان ۲۰۲۱، کارزارهای مختلفی، بدافزار BazarLoader را با استفاده از ایمیل توزیع کردند. از اواخر ژوئیه تا اواسط آگوست ۲۰۲۱، اکثر نمونه‌های BazarLoader از طریق سه کارزار مختلف منتشر شدند.

یک نمونه از این بدافزار در کارزاری به نام BazarCall که جزییات آن در نشانی زیر اعلام شده، اقدام به توزیع بدافزار BazarLoader نمودند.

https://unit42.paloaltonetworks.com/bazarloader-malware/

در اوایل جولای، کارزاری با نام Copyright violation-themed campaign نیز با بکارگیری فایل‌هایی از نوع ZIP به نام Stolen Images Evidence.zip شروع به انتشار BazarLoader کرد. شرکت مایکروسافت (Microsoft Corp) جزییات این کارزار را در نشانی زیر شرح داده است.

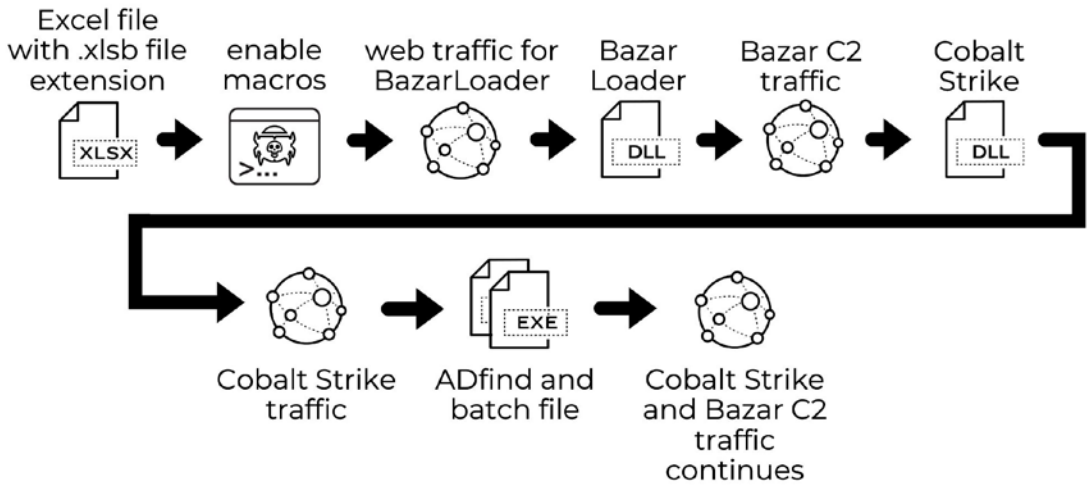
https://www.microsoft.com/security/blog/2021/04/09/investigating-a-unique-form-of-email-delivery-for-icedid-malware/

در اواخر جولای، مهاجمان در کارزاری طولانی‌مدت به نام TA۵۵۱ (Shathak) شروع به ارسال BazarLoader از طریق ایمیل‌های انگلیسی زبان کردند. جزییات این کارزار در نشانی زیر توضیح داده شده است.

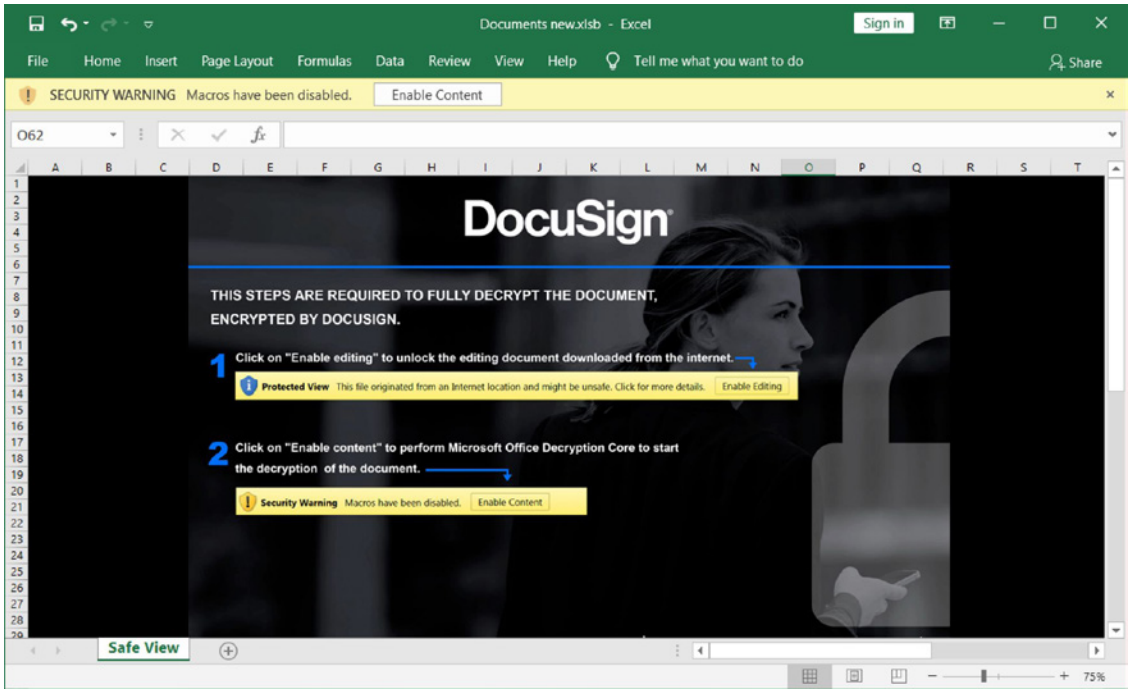
https://attack.mitre.org/groups/G0127/

محققان امنیتی پالو آلتو نتورکس (Palo Alto Networks, Inc.) در تحقیقات خود، علاوه بر سه کارزار مذکور، حداقل یک نمونه از بدافزار BazarLoader را شناسایی نمودند که از طریق یک فایل Excel با منشاء نامشخص توزیع شده است. جزییات بیشتر در لینک زیر قابل دریافت است.

https://www.malware-traffic-analysis.net/2021/08/19/index2.html

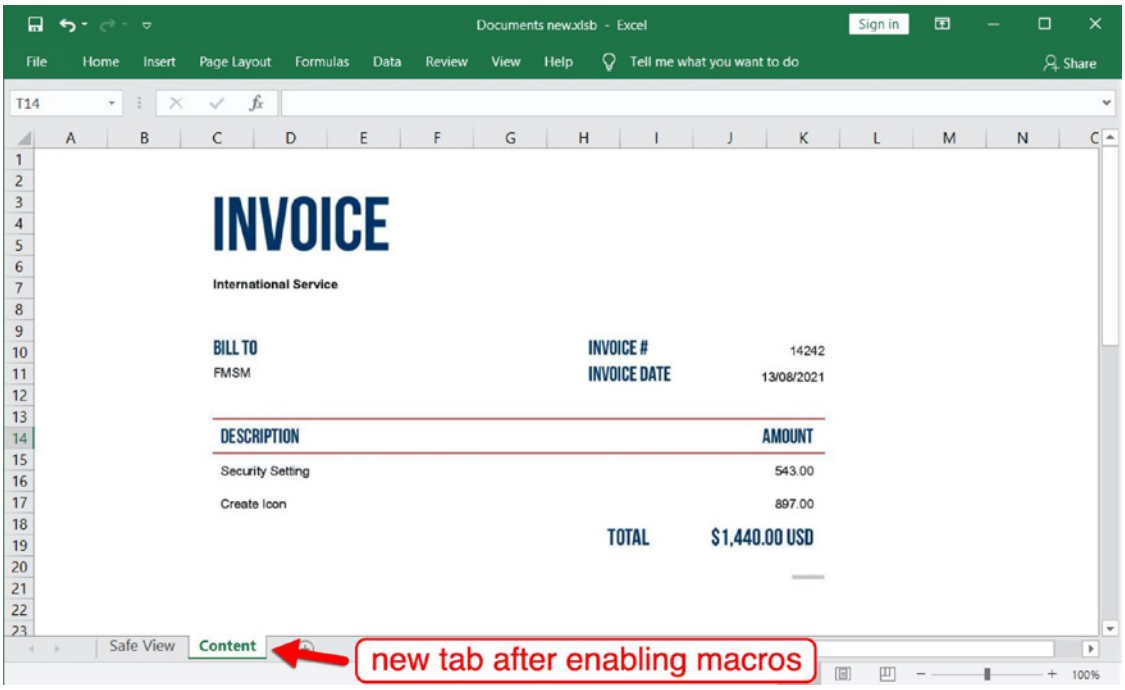


محققان امنیتی پالو آلتو نتورکس در روز چهارشنبه ۲۷ مرداد ۱۴۰۰ فایل مخربی از نوع Excel را که دارای پسوند xlsb. بود و تاریخ آخرین به‌روزرسانی آن ۲۶ مرداد بود کشف نمودند. فایل مذکور حاوی ماکروهایی بود که به منظور آلوده کردن سرورهای میزبان آسیب‌پذیر مبتنی بر Windows به بدافزار BazarLoader طراحی شده بود. شکل زیر تصویری از این فایل بدافزاری از نوع Excel را نشان می‌دهد.



اگرچه لوگوی شرکت داک‌ساین (DocuSign, Inc.) در بالای شکل و فایل نشان داده شده است، اما این فایل Excel توسط مهاجمانی ایجاد شده که سعی داشتند با سوءاستفاده از نام تجاری و تصویر شرکت داک‌ساین، اعتماد دریافت‌کننده فایل را جلب کنند. مهاجمان مختلف تقریباً روزانه از این لوگو و سایر تصاویر شرکت مذکور استفاده می‌کنند.

پس از فعال کردن ماکروهای بدافزاری در یک سرور میزبان آسیب‌پذیر مبتنی بر Windows، فایل Excel، سربرگ (Tab) جدیدی که حاوی فاکتوری جعلی تحت عنوان (Invoice Information Service) است را ارائه کرد. فاکتور مذکور در شکل زیر نشان داده شده است.

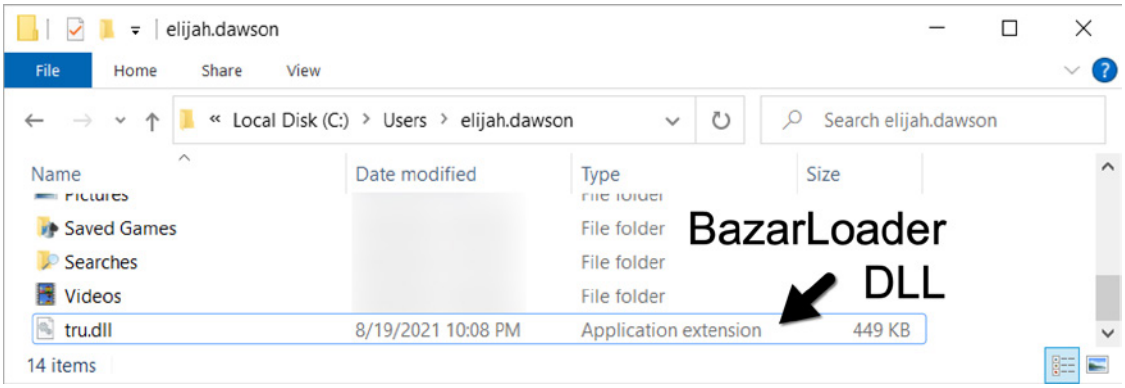


با نمایش سربرگ حاوی فاکتور جعلی، کد ماکروی جاسازی شده در فایل Excel، یک فایل بدافزاری (Malicious Binary) را برای BazarLoader فراخوانی می‌کند.

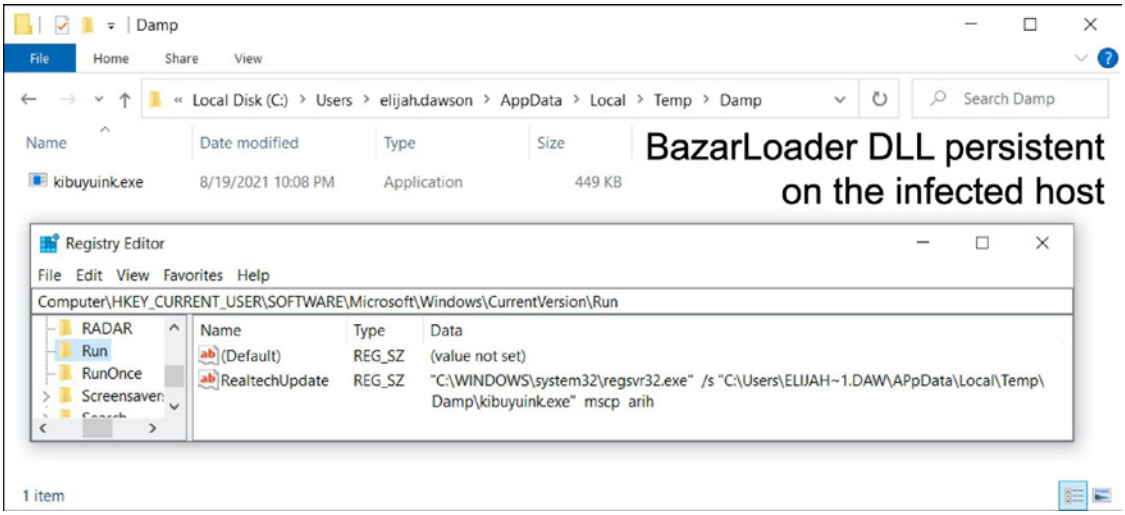
کد موجود در ماکرو فایل Excel، یک فایل بدافزاری از نوع Dynamic Link Library - به اختصار DLL - را برای BazarLoader از نشانی زیر دانلود می‌کند.

hxxps://pawevi[.]com/lch5.dll

همانطور که در شکل زیر نشان داده شده، DLL در Home Directory سیستم قربانی در نشانی C:\Users\[username]\tru.dll ذخیره شده و با استفاده از regsvr32.exe اجرا شده است.



فایل DLL مربوط به BazarLoader، همانطور که در شکل زیر نشان داده شده، بلافاصله در مکان دیگری کپی می‌شود و از طریق Windows Registry در سیستم ماندگار می‌شود.

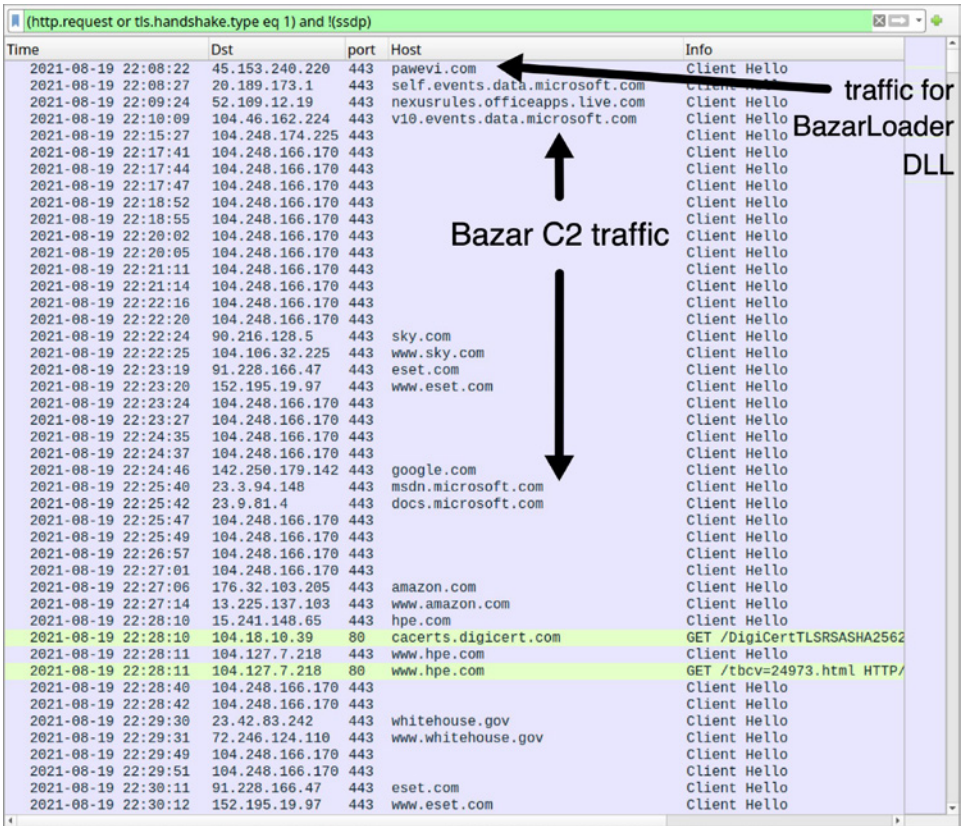


همانطور که در شکل بالا مشاهده می‌شود، نام فایل از tru.dll به kibuyuink.exe تغییر کرده، هر چند که همچنان از نوع DLL بوده و برای اجرا به regsvr32.exe نیاز دارد. تغییر پسوند نام فایل تکنیک رایجی است که در آلودگی‌های مختلف بدافزاری دیده می‌شود.

ترافیک سرور کنترل و فرمان‌دهی (C2) در Bazar

در ادامه نمونه‌ای از فعالیت سرور کنترل و فرمان‌دهی (C2) مربوط به BazarLoader، که با استفاده از ترافیک HTTPS از ۱۰۴.۲۴۸.۱۷۴[.]۲۲۵ بر روی درگاه TCP 443، درب‌پشتی با نام BazarBackdoor را بازیابی می‌کند، نمایش داده شده است.

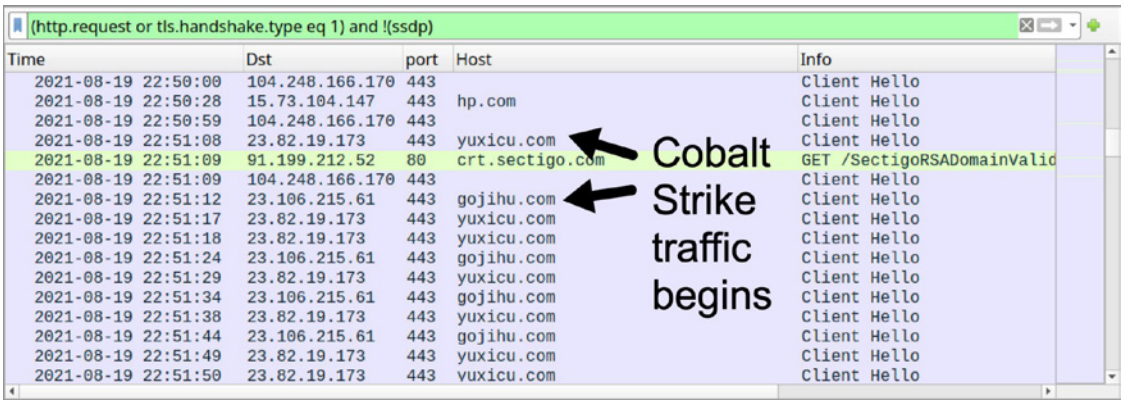
سپس درب‌پشتی مذکور (BazarBackdoor)، سرور C2 را با بکارگیری ترافیک HTTPS به ۱۰۴.۲۴۸.۱۶۶[.]۱۷۰ روی پورت TCP 443 منتقل می‌کند. در شکل زیر به این فعالیت ترکیبی C2 به عنوان ترافیک Bazar C2 اشاره شده است.



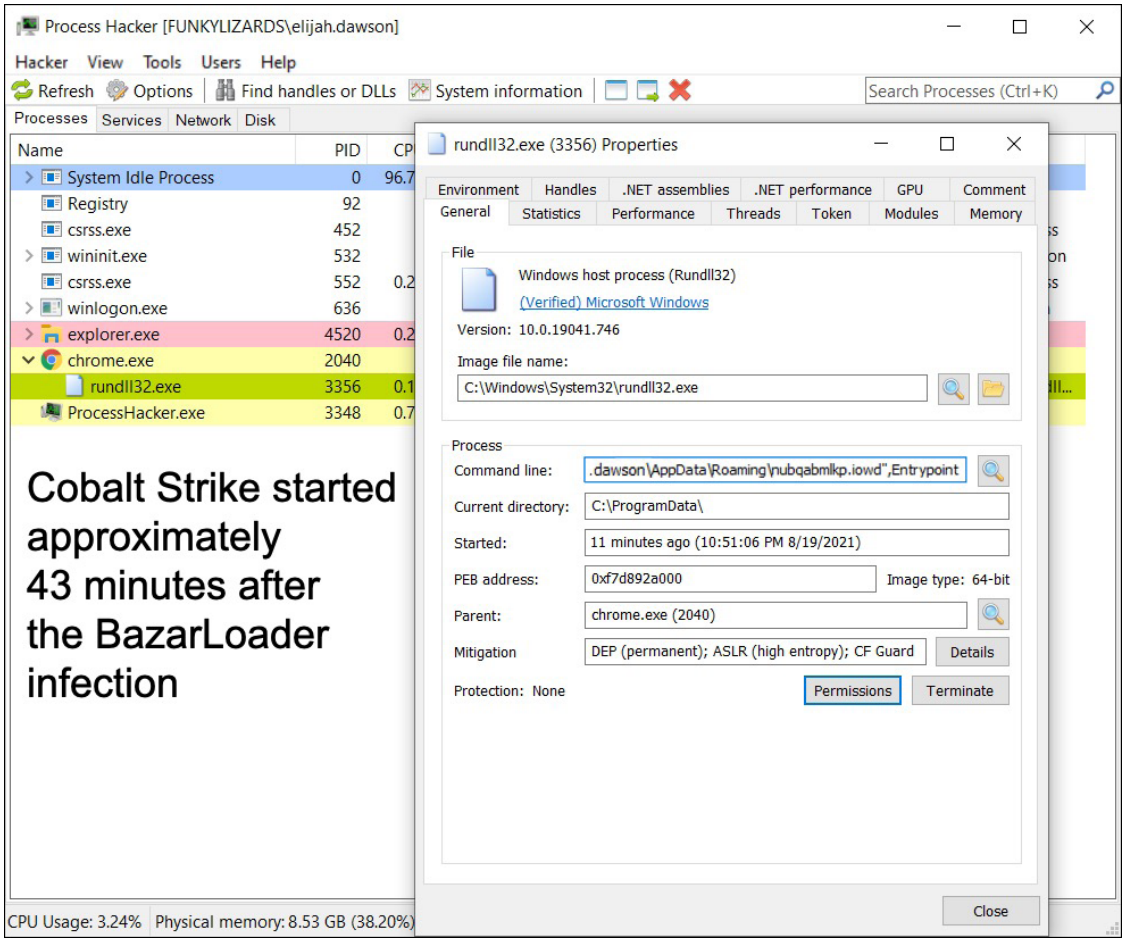
این نمونه از فعالیت Bazar C2 باعث ایجاد ترافیک در دامنه‌های (Domain) معتبر و مجاز می‌شود. این فعالیت به خودی خود ذاتاً مخرب نیست. گونه‌های‌مختلف بدافزاری ترافیک مشابهی را جهت بررسی اتصال یا اطمینان از اینکه آیا سرور میزبان آلوده مبتنی بر Windows، به اینترنت متصل است یا خیر، ایجاد می‌کنند.

اجرای Cobalt Strike

تقریباً ۴۱ دقیقه پس از آلودگی اولیه توسط BazarLoader، سرور میزبان آلوده مبتنی بر Windows، شروع به بکارگیری Cobalt Strike با استفاده از ترافیک HTTPS به gojihu[.]com و yuxicu[.]com می‌کند. شکل زیر اجرای Cobalt Strike را نشان می‌دهد.



در این حالت، یک فایل Cobalt Strike از نوع DLL، از طریق ترافیک Bazar C2 ارسال شده و در سرور میزبان آلوده مبتنی بر Windows در AppData\Roaming directory سیستم قربانی ذخیره می‌شود. شکل زیر نشان می‌دهد که یک فایل Cobalt Strike از نوع DLL، بر روی دستگاه آلوده شده در حال اجرا است.

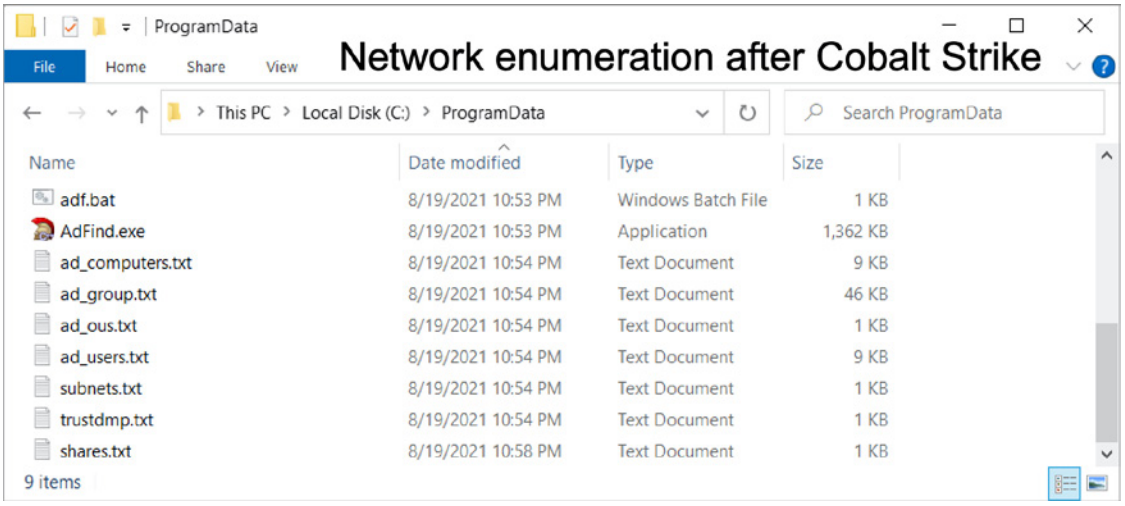


منجر به شناسایی و کشف بستر سرور میزبان آلوده می‌شود. طبق گزارش محققان شرکت پالو آلتو نتورکس در محیط‌های آزمایشگاهی، این فعالیت اکتشاف می‌تواند در عرض چند دقیقه پس از اولین ترافیک Cobalt Strike آغاز شود.

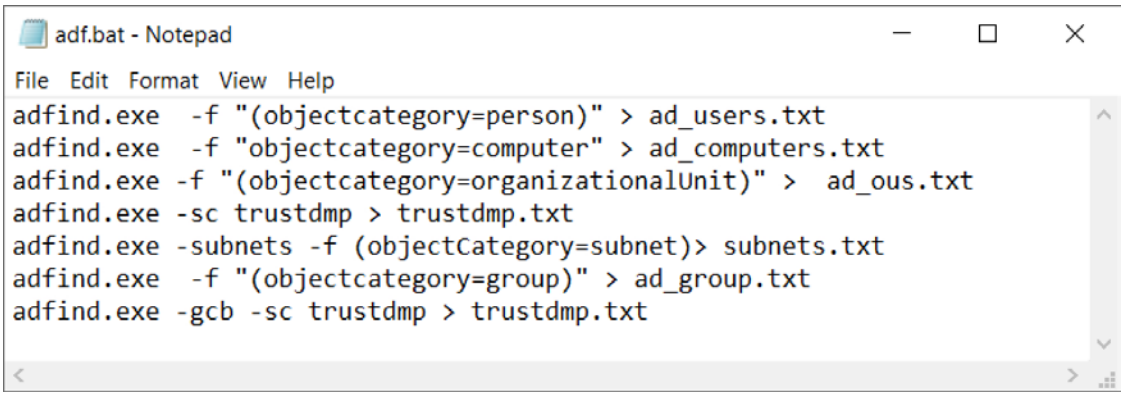
در این بررسی محققان پالو آلتو نتورکس دریافتند که مهاجمان تقریباً دو دقیقه پس از شروع فعالیت Cobalt Strike، از ابزاری به نام AdFind که در مسیر C:\ProgramData\AdFind.exe کپی شده، استفاده می‌کنند. ابزار مذکور از نوع خط فرمان (Command Line) بوده و توسط تبهکاران سایبری به منظور جمع‌آوری اطلاعات از AD بکار گرفته می‌شود. محققان در تحقیق خود از Batch File مربوطه برای اجرای ابزار مذکور استفاده نمودند. جزییات کامل ابزار AdFind در نشانی زیر قابل مطالعه است.

https://attack.mitre.org/software/S0552/

شکل زیر، مسیر Batch File، AdFind مربوطه یعنی adf.bat و نتایج جستجوی آن را که در هفت فایل متنی ذخیره شده، نشان می‌دهد.



در شکلی که در ادامه نمایش داده شده، فرامین بکار گرفته شده در فایل adf.bat که AdFind.exe را اجرا می‌کند، نشان داده شده است.



فرامین فوق، کاربران، کامپیوترها، فایل‌های به اشتراک‌گذاشته شده و سایر اطلاعات را که در بستر AD مورد هدف قرار داده شده، نشان می‌دهد.

محققان پالو آلتو نتورکس در این تحقیق و شبیه‌سازی، هدف ارزشمندی را مورد حمله قرار ندادند و محیط مذکور را طی دو یا سه ساعت پس از آلودگی اولیه پاکسازی کردند. در این مثال، هیچ باج‌افزاری پس از شناسایی ارسال نشد.

محققان پالو آلتو نتورکس در این تحقیق و شبیه‌سازی، نمونه‌ای از بدافزار BazarLoader را که به اجرای Cobalt Strike و به دنبال آن به شناسایی سیستم‌ها و فایل‌های ارزشمند منجر شده، بررسی و بازبینی کرده‌اند. هنگامی که مهاجمان از Cobalt Strike استفاده می‌کنند، توسط ابزاری با نام AdFind اطلاعاتی از AD را جمع‌آوری می‌کنند. اگر بستر AD هدفی ارزشمند برای مهاجم باشد، گام بعدی مهاجم توسعه دامنه آلودگی و دسترسی به Domain Controller و سایر سرورهای داخل شبکه است.

حقایقی درخصوص

مطالبه باج در حملات باج‌افزاری

به تازگی تیم واکنش سریع رویداد شرکت سوفوس (Sophos, Ltd.) با بازبینی حملات باج‌افزاری به بررسی روش‌هایی پرداخته‌اند که مهاجمان از طریق آن‌ها قربانیان را برای پرداخت باج تحت فشار قرار می‌دهند.

از آنجایی که نویسندگان باج‌افزارها همگام با پیشرفت‌های امنیت سایبری به سرعت تکامل یافته و خود را سازگار می‌کنند، دهه‌هاست که باج‌افزارها وجود دارند و همچنان به رشد خود ادامه می‌دهند.

برای مثال، از آنجایی که امروزه سازمان‌ها اقدام به تهیه نسخه پشتیبان از داده‌های خود می‌کنند و می‌توانند فایل‌های رمزگذاری شده را از نسخه‌های پشتیبان بازیابی کنند، مهاجمان نیز شروع به ارتقاء و تغییر رویکردهای مطالبه باج در ازای کلیدهای رمزگشایی کرده‌اند. آنها اقدامات دیگری را جهت اخاذی و افزایش فشار بر روی قربانیان جهت پرداخت باج طراحی کرده‌اند.

برخی از تاکتیک‌هایی که مهاجمان برای وادار کردن قربانیان به پرداخت باج استفاده می‌کنند، بسیار خطرناک بوده و به طور بالقوه می‌توانند بیشتر از مدتی که سامانه به علت حمله سایبری از کار افتاده، برای سازمان زیان‌بار باشند.

مهاجمان عمداً سعی می‌کنند روابط، اعتماد و شهرت قربانیان خود را تضعیف کنند. گاهی اوقات رویکردی که آنها اتخاذ می‌کنند بسیار عمومی است. برخی اوقات نیز روش آن‌ها اختصاصی‌تر است.

به عنوان مثال، محققان سوفوس، مواردی را شناسایی کرده‌اند که مهاجمان به کارکنان سازمان ایمیل ارسال کرده یا تلفن می‌زنند، کارمندان را با نام آنها مورد خطاب قرار داده و آن‌ها را تهدید به انتشار و به‌اشتراک‌گذاری اطلاعات شخصی سرقت شده همچون جزئیات هرگونه پرونده کیفری، اطلاعات مالی یا گذرنامه می‌کنند تا کارکنان ترسیده و از کارفرما درخواست کنند که باج مطالبه شده را بپردازد.

این نوع رفتار نشان می‌دهد که چگونه باج‌افزارها از یک حمله کاملاً فنی که سیستم‌ها و داده‌ها را مورد هدف قرار می‌داده به حمله‌ای تبدیل شده‌اند که افراد را نیز هدف قرار می‌دهند.

مهاجمان با چه روش‌هایی قربانیان را برای پرداخت باج تحت فشار قرار می‌دهند؟

محققان سوفوس برای کمک به سازمان‌ها جهت بهبود سیستم دفاعی خود در برابر حملات باج‌افزاری، ۱۰ روشی که مهاجمان از طریق آن قربانیان را در سال ۲۰۲۱ برای پرداخت باج تحت فشار قرار می‌دهند، گردآوری کرده‌اند:

۱- سرقت داده‌ها و تهدید به انتشار یا حراج آنلاین آن‌ها

فهرست گروه‌های باج‌افزاری که سایت «نشت‌داده» عمومی برای داده‌های استخراج‌شده دارند یا از چنین سایتی استفاده می‌کنند یا آن‌را میزبانی می‌کنند بسیار طولانی است. این رویکرد اکنون آنقدر رایج است که هر قربانی که شبکه آن تحت نفوذ قرار می‌گیرد، باید فرض کند که حمله‌های باج‌افزاری به این معنی است که آنها نشت داده را نیز تجربه خواهند کرد.

مهاجمان داده‌های سرقت شده را در سایت‌های نشت داده منتشر می‌کنند تا رقبا، مشتریان، شرکا، رسانه‌ها و دیگران ببینند. این سایت‌ها اغلب دارای ربات‌های رسانه‌های اجتماعی هستند که به طور خودکار پست‌های جدید را به صورت عمومی منتشر می‌کنند، بنابراین احتمال کمی برای مخفی نگه داشتن یک حمله وجود دارد. گاهی اوقات نیز مهاجمان داده‌ها را در وب تاریک یا در میان شبکه‌های مجرمان سایبری به حراج می‌گذارند.

با این حال، بزرگترین نگرانی برای قربانیان نوع داده‌هایی است که توسط مهاجمان سرقت می‌شود. داده‌های سرقت شده ممکن است طرح‌های فنی محصول یا دستور العمل‌های سرّی باشد. مهاجمان معمولاً به دنبال اطلاعاتی همچون جزئیات بانکی سازمان‌ها و اشخاص، فاکتورها، اطلاعات حقوق و دستمزد، جزئیات پرونده‌های کیفری، گذرنامه‌ها، گواهینامه‌های رانندگی، شماره تامین اجتماعی، کد ملی و دیگر اطلاعات متعلق به کارمندان هستند.

به عنوان مثال، محققان سوفوس یکی از حمله‌های باج‌افزار Conti که در آن یک تامین‌کننده لجستیک حمل و نقل را مورد هدف قرار داده بودند، بررسی کردند. مهاجمان جزئیات یکی از تصادف‌های آن‌هارا که شامل نام رانندگان درگیر، تلفات و سایر اطلاعات مرتبط بود، کشف کرده بودند. این واقعیت که قرار بود چنین اطلاعاتی در اختیار عموم قرار گیرد، استرس قابل توجهی را به وضعیت فوق اضافه کرده بود.

سرقت یا انتشار عمومی اطلاعات شخصی، سازمان‌های قربانی را در معرض خطر نقض قوانین حفاظت از داده‌ها قرار می‌دهد، مانند قانون حفظ حریم خصوصی مصرف کنندگان کالیفرنیا (California Customer Privacy Act - به اختصار CCPA) یا GDPR اروپا.

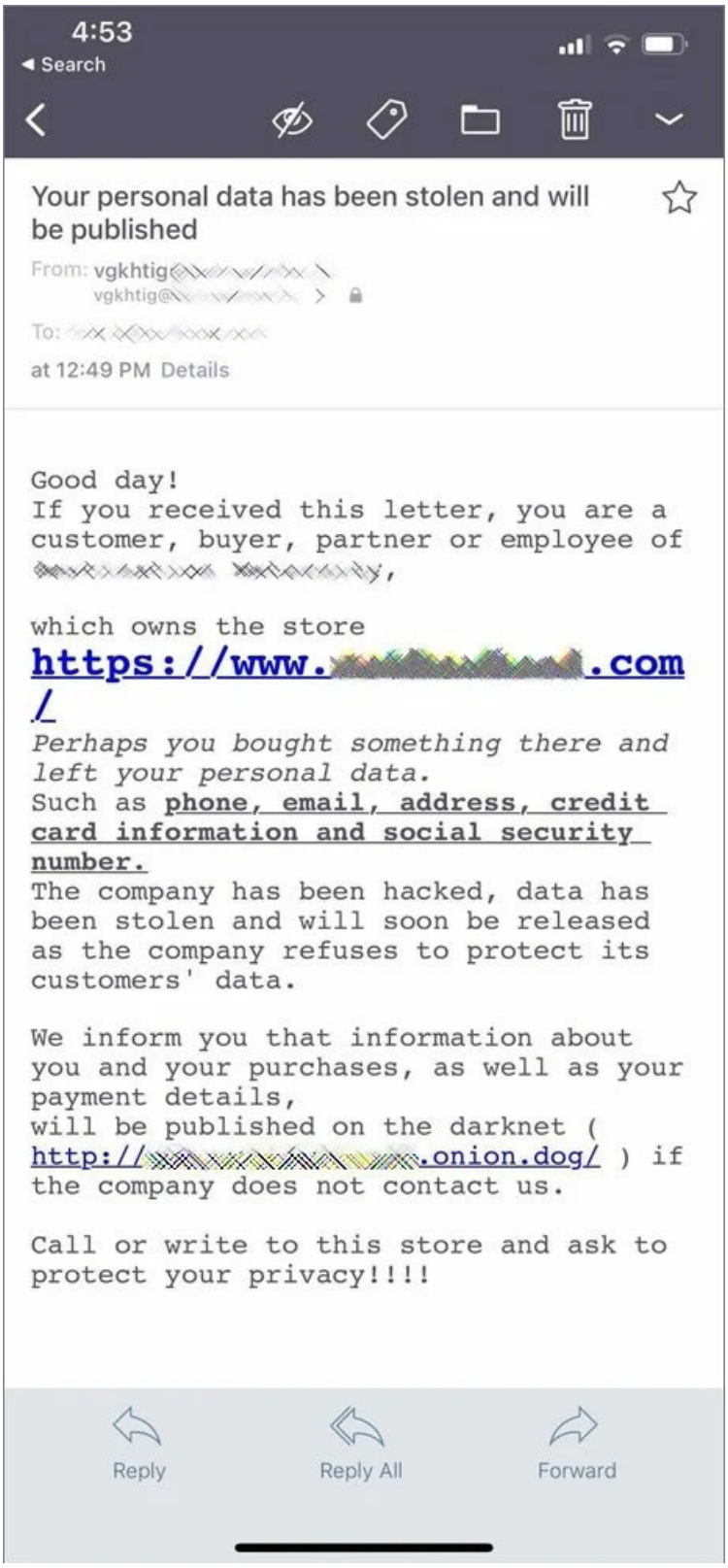
۲- ارسال ایمیل و تماس با کارکنان از جمله مدیران ارشد و تهدید به افشای اطلاعات شخصی آنها

SunCrypt، Maze، Conti، REvil و دیگر انواع باج‌افزارها از ارسال ایمیل و تماس مستقیم با کارکنان جهت ایجاد رعب و وحشت استفاده کرده‌اند. این امر می‌تواند برای دریافت‌کنندگان پیام بسیار ناراحت‌کننده باشد.

مشاهده شده که مهاجمان وابسته به باج‌افزار SunCrypt با کارمندان سازمان تماس تلفنی برقرار کرده‌اند، اپراتورهای باج‌افزار REvil نیز در یکی از حملات بررسی شده توسط تیم سوفوس، با رسانه‌ها و شرکای تجاری قربانیان تماس گرفتند و ضمن ارائه جزئیات حمله، از آن‌ها خواستند که سازمان هک شده را وادار به پرداخت باج کنند. آنها همچنین ادعا کردند که یک سرویس رایگان راه‌اندازی کرده‌اند که تماس‌های صوتی VOIP را برای مشتریان همکار خود ارائه می‌دهد.

۳- اطلاع‌رسانی یا تهدید به اطلاع‌رسانی شرکای تجاری، مشتریان، رسانه‌ها و موارد دیگر در خصوص نشت داده‌ها

مهاجمان در این روش به افراد یا سازمان‌هایی است که اطلاعات تماسشان را در فایل‌های سرقت شده پیدا کرده‌اند، ایمیل یا پیامی ارسال و به آن‌ها می‌گویند که به منظور محافظت از حریم خصوصی‌شان، از سازمان هک شده درخواست کنند که باج مطالبه شده را بپردازند. Clop، REvil و دیگر خانواده‌های باج‌افزار، همانطور که در تصویر زیر مشاهده می‌کنید، از این رویکرد استفاده می‌کنند.



٤- ساکت کردن قربانیان

Conti و RagnarLocker اخیراً با ارسال پیام‌هایی مبنی بر اینکه قربانیان نباید با مجریان قانون تماس بگیرد یا جزئیات مذاکرات باج را به اشتراک بگذارد، آن‌ها را تهدید کرده‌اند. این منجر می‌شود که قربانیان کمکی از ارائه‌دهندگان پشتیبانی ثالث (Third-party support) جهت پرداخت‌نکردن باج دریافت نکنند. همچنین نشان می‌دهد که مهاجمان باج‌افزاری بیشتر نگران شناسایی فعالیت‌های خود توسط نهادهای قانونی هستند.

٥- جذب و استخدام افراد داخلی و اشخاص دارای اطلاعات محرمانه

یکی دیگر از تاکتیک‌های اخیر و غیرعادی که مهاجمان باج‌افزاری از آن استفاده می‌کنند، تلاش برای استخدام افراد داخلی سازمان جهت فعال کردن یک حمله باج‌افزاری در ازای دریافت سهمی از باج مطالبه شده است.

در یکی از نمونه‌هایی که به طور گسترده گزارش شده، اپراتورهای پشت حمله LockBit 2.0 آگهی استخدامی را برای جذب افراد داخلی هر سازمان جهت کمک در نفوذ و رمزگذاری شبکه سازمان مذکور در ازای پرداخت مبلغ قابل توجهی از باج دریافت شده، منتشر کردند. اعلامیه زیر که پس از رمزگذاری بر روی کامپیوترهای قربانی ارسال شده بود، نشان می‌دهد که مهاجمان در تلاش هستند تا افراد داخل سازمان‌ها را استخدام کرده تا به آنها کمک کنند تا شرکای ثالث یا تأمین‌کنندگان را مورد نفوذ قرار دهند که این می‌تواند دلیلی دیگر برای نگرانی قربانی و شرکای آن باشد.

٦- تغییر رمزهای عبور

پس از نفوذ به شبکه، بسیاری از مهاجمان باج‌افزاری، یک حساب کاربری با سطح دسترسی Domain Admin جدید ایجاد کرده و سپس رمز عبور سایر حساب‌های کاربری با سطح دسترسی Domain Admin را تغییر می‌دهند. این بدان معنی است که راهبران ارشد نمی‌توانند برای تعمیر سیستم وارد شبکه شوند. در عوض، آنها باید قبل از تلاش برای بازیابی نسخه‌های پشتیبان، دامنه جدیدی را راه‌اندازی کنند.

٧- حملات فیشینگ از طریق حساب‌های ایمیل قربانیان

محققان سوفوس، در رویدادی که توسط باج‌افزار Lorenz مورد حمله قرار گرفته بود، مشاهده نمودند که مهاجمان، کارکنان را با ایمیل‌های فیشینگ مورد هدف قرار داده‌اند و آن‌ها را ترغیب به نصب برنامه‌ای کرده که دسترسی کامل به ایمیل کارمندان را حتی پس از تغییر رمزهای عبور برای مهاجمان فراهم می‌کرد.

مهاجمان سپس با بکارگیری حساب‌های ایمیل هک شده، اقدام به ارسال ایمیل‌هایی به تیم‌های فناوری اطلاعات، تیم‌های حقوقی و بیمه سایبری که با سازمان مورد نظر همکاری می‌کردند، نمودند تا در صورت عدم پرداخت، آن‌ها را به حملات بیشتری تهدید کنند.

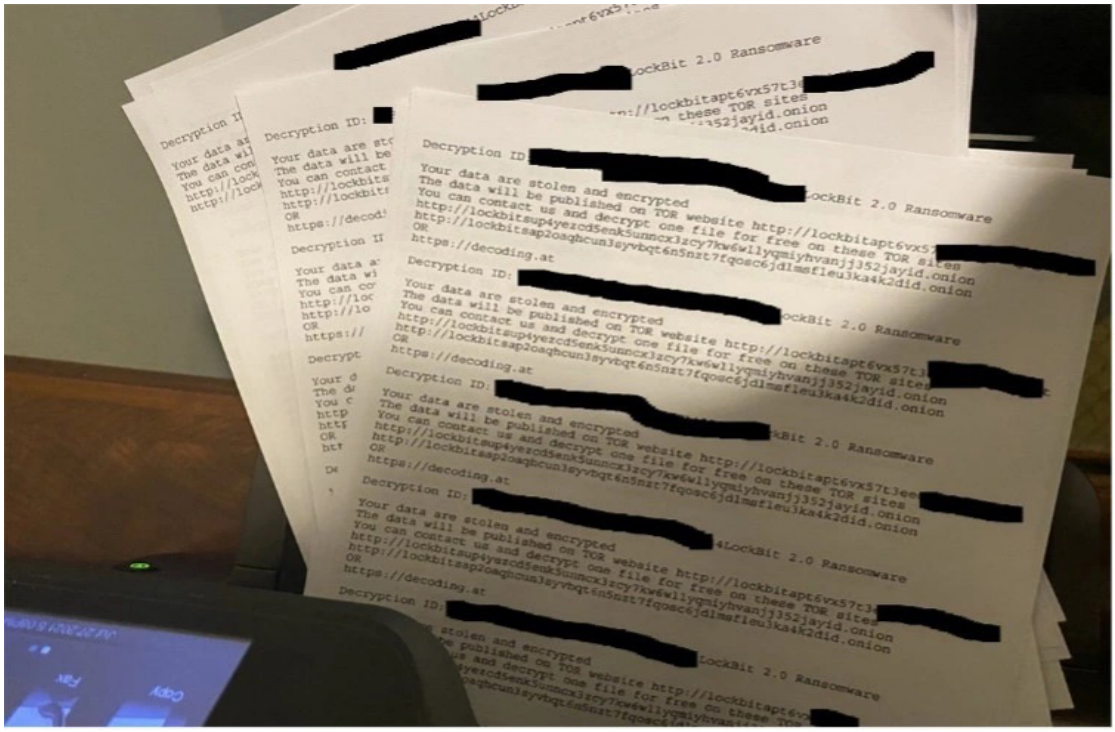
۸-حذف نسخه‌های پشتیبان آنلاین و نسخه‌های رونوشت سرّی

اکثر مهاجمان باج‌افزاری در طول شناسایی شبکه قربانی، به دنبال نسخه‌های پشتیبان آنلاین و متصل به شبکه یا اینترنت می‌گردند و آن‌ها را حذف می‌کنند تا قربانی نتواند برای بازیابی فایل‌های رمزگذاری شده از آن‌ها استفاده کند. این می‌تواند شامل حذف نرم‌افزار پشتیبان‌گیری و تنظیم مجدد رونوشت‌های مجازی باشد.

در یکی از نمونه‌ها، تیم پاسخ به رویداد سوفوس مشاهده کردند که مهاجمان باج‌افزار DarkSide، نسخه‌های پشتیبان محلی قربانی را حذف کرده و سپس از یک حساب کاربری هک شده برای تماس با شرکتی که نسخه‌های پشتیبان ابری خارج از سایت قربانی را میزبانی می‌کرد، استفاده کردند و از آن‌ها خواستند نسخه‌های پشتیبان خارج از سایت را حذف کنند. شرکت مذکور نیز از آنجایی که درخواست حذف نسخه‌های پشتیبان از یک حساب مجاز ارسال شده بود، با درخواست حذف موافقت کرد. خوشبختانه، فروشنده توانست پس از اطلاع از رخنه، نسخه‌های پشتیبان را بازیابی کند.

۹-چاپ نسخه‌های فیزیکی مطالبه باج بر روی تمام دستگاه‌های متصل، از جمله پایانه‌های فروش

سیلی از تهدیدهای چاپی نه تنها از منظر بکارگیری کاغذ زیاد، آزاردهنده است، بلکه برای افراد حاضر در سازمان نیز احساس ناخوشایندی ایجاد می‌کند. مهاجمان باج افزاری از جمله Egregor و LockBit از این تاکتیک استفاده کرده‌اند.



۱۰- اجرای حملات منع سرویس توزیع شده (Distributed Denial-of-Service - به اختصار DDoS) علیه سایت سازمان

RagnarLocker، DarkSide، Avaddon و SunCrypt بعد از متوقف شدن مذاکرات باج‌گیری، از حملات منع سرویس توزیع شده برای بازگرداندن قربانیان به میز مذاکره استفاده کرده‌اند. مهاجمان همچنین از حملات DDoS برای سرقت اطلاعات به صورت مستقل یا عاملی جهت حواس‌پرتی استفاده کرده تا سازمان را مجبور به تمرکز به حمله DDos کنند، در حالی که فعالیت اصلی حمله باج‌افزاری در جای دیگری از شبکه در حال انجام است.

چه اقداماتی توسط راهبران امنیتی قابل انجام است؟

این واقعیت که مهاجمان باج‌افزاری، دیگر حملات خود را تنها به رمزگذاری فایل‌هایی که از طریق نسخه‌های پشتیبان توسط قربانیان قابل بازیابی است، محدود نمی‌کنند، نشان می‌دهد که چقدر برای راهبران و مدیران امنیتی ضرورت دارد که رویکرد دفاعی عمیق در امنیت سازمان خود داشته باشند. این رویکرد عمیق باید امنیت و حفاظت پیشرفته را با آموزش و آگاهی کارکنان نیز ترکیب کند.

مراحل زیر به سازمان‌ها کمک می‌کند تا با رفتارهای مهاجمان مقابله کنند:

- اجرای یک برنامه جهت آگاهی و آموزش کارکنان که شامل نمایش نمونه ایمیل‌ها و تماس‌هایی است که مهاجمان از طریق آن درخواست‌های خود را اعلام می‌کنند.
- یک مرکز تماس ۲۴ ساعته در هر ۷ روز هفته (۲۴/۷) برای کارمندان سازمان خود ایجاد کنید تا بتوانند هر آنچه را که ادعا می‌شود از سوی مهاجمان است گزارش دهند و هر گونه پشتیبانی مورد نیاز را دریافت کنند.
- معیارهایی را جهت شناسایی فعالیت‌های بالقوه و مخرب افراد داخل سازمان، مانند تلاش کارکنان برای دسترسی به حساب‌ها یا محتوای غیرمجاز تعریف نموده و اقدامات لازم را در این خصوص انجام دهید.

همچنین توصیه می‌شود به منظور افزایش امنیت فناوری اطلاعات در سازمان در برابر طیف وسیعی از تهدیدات سایبری از جمله باج‌افزارها، اقدامات زیر را اعمال و بازبینی کنید:

- امنیت شبکه را به صورت ۲۴ ساعته رصد کنید و از پنج شاخص اولیه که نشانه حضور مهاجم قبل از راه‌اندازی باج‌افزار در شبکه است، آگاه باشید تا بتوانید در سریع‌ترین زمان ممکن حملات باج‌افزاری را متوقف کنید. پنج شاخص اولیه که نشانه حضور مهاجم قبل از راه‌اندازی باج‌افزار در شبکه است، را می‌توانید در بدبیاری‌های مهاجمان باج‌افزاری مطالعه کنید.
- برای جلوگیری از دسترسی مجرمان سایبری به شبکه‌ها، پروتکل دسکتاپ از راه دور (Remote Desktop Protocol - به اختصار RDP) را خاموش کنید. اگر کاربران نیاز به دسترسی به RDP دارند، این پروتکل را فقط باید از طریق یک اتصال VPN امن همراه با احراز هویت چندعاملی (Multi-Factor Authentication - به اختصار MFA) جهت اتصال از راه دور به شبکه سازمان اجرا کنند. به منظور کسب اطلاعات بیشتر در این خصوص، مطالعه مقاله مسدود کردن پروتکل ریموت دسکتاپ (RDP) پیشنهاد می‌شود.
- به کارکنان سازمان آموزش دهید تا مراقب حملاتی همچون فیشینگ و یا نشانه‌های هرزنامه‌های مخرب باشند و سیاست‌های امنیتی قوی را اجرا کنید.
- به صورت منظم از مهم‌ترین داده‌های فعلی و حیاتی سازمان با پیروی از قاعده ۱-۲-۳ نسخه پشتیبان تهیه کنید. بر طبق این قاعده، به طور دوره‌ای از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه به عنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود.
- از دسترسی مهاجمان به امکانات امنیتی و حفاظتی جهت غیرفعال کردن این امکانات جلوگیری کنید. راهکار امنیتی سازمان خود را از طریق یک کنسول مدیریتی مبتنی بر ابر با فعال نمودن احراز هویت چندعاملی و مدیریت نقش-محور (Role Based Administration) جهت محدود کردن حقوق دسترسی کاربران انتخاب کنید.
- به یاد داشته باشید که هیچ راهکار واحدی برای محافظت سامانه‌ها وجود ندارد و بکارگیری یک مدل امنیتی لایه‌ای و دفاعی عمیق ضرورت دارد. راهکارهای مذکور را در تمام نقاط پایانی و سرورها گسترش دهید و اطمینان حاصل کنید که آن‌ها می‌توانند داده‌های مرتبط با امنیت را به اشتراک بگذارند.
- یک طرح واکنش موثر و سریع به رویداد داشته باشید و در صورت نیاز آن را به‌روزرسانی کنید. برای رصد تهدیدات یا پاسخگویی فوری به رویدادهای اضطراری، در صورت نیاز برای کمک بیشتر به کارشناسان امنیتی در خارج از سازمان مراجعه کنید.

مشروح گزارش محققان سوفوس در نشانی زیر قابل مطالعه است:

https://news.sophos.com/en-us/۲۸/۱۰/۲۰۲۱/the-top-۱۰-ways-ransomware-operators-ramp-up-the-pressure-to-pay/

بیت‌دیفندر،

۲۰ سال پیشرو در حوزه امنیت سایبری

مشتری گرامی؛

نوامبر ۲۰۲۱، نقطه عطف بزرگی برای شرکت بیت‌دیفندر (Bitdefender) است چرا که ما بیستمین سالگرد تاسیس خود را جشن می‌گیریم. از زمان تأسیس بیت‌دیفندر در سال ۲۰۰۱، سفری هیجان‌انگیز و مسیری طولانی طی شده تا به یکی از قابل اعتمادترین پیشگامان امنیت سایبری در جهان تبدیل شویم و از داده‌های میلیون‌ها مشتری و هزاران کسب‌وکار در ۱۷۰ کشور محافظت کنیم. این کار بدون همراهی و همکاری شما میسر نمی‌شد.

داستان ما بیش از ۳۰ سال پیش شروع شد، درست پس از تجزیه شوروی سابق در دهه ۱۹۹۰، زمانی که من به همراه همسرم یکی از اولین شرکت‌های توسعه نرم‌افزار خصوصی رومانی را تأسیس کردیم. یک حادثه ناگوار مربوط به یک ویروس کامپیوتری، یک فلاپی دیسک و یک مشتری بسیار ناراحت و ناراضی، در نهایت به لحظه‌ای تعیین کننده تبدیل شد.

پس از کشف ویروسی که شناسایی نشده بود و از طریق یک فلاپی دیسک به سیستم مشتری منتقل شد، ما با تیم مهندسی به دنبال راه حل بهتری بودیم تا چنین اتفاقی دیگر رخ ندهد. در این زمان بود که ایده بیت‌دیفندر متولد شد و متوجه شدیم آنچه توسعه داده‌ایم می‌تواند به افراد بی‌شماری بسیار بهتر از آنچه در بازار موجود است، کمک کند.

از آغاز ساده در یک دفتر کوچک در بخارست (پایتخت رومانی) تا اکنون با نزدیک به ۱۸۰۰ کارمند در سراسر جهان، از جمله تیم نخبه‌ای از محققان، مهندسان و ریاضیدانان، رشد و موفقیت مستمر بیت‌دیفندر همچنان بر یک ماموریت واحد یعنی مبارزه با جرایم سایبری متمرکز است.

تعهد ما در مبارزه با تهدیدات سایبری طی چندین دهه دستاوردهای مهمی را به همراه داشته است، از موارد متعددی ثبت اختراع و نوآوری‌های فناوری در زمینه تشخیص تهدیدات، یادگیری ماشین و هوش مصنوعی گرفته تا اکتشافات مهم بدافزارهای جدید، کارزارهای نهادهای دولتی و تاکتیک‌های مهاجمان. نوآوری‌های بیت‌دیفندر نه تنها امنیت سایبری مشتریان خود را ارتقاء داده، بلکه به طور قابل توجهی تمامی جوامع را در برابر تهدیدات سایبری محافظت می‌کند.

یکی از زمینه‌هایی که ما به آن افتخار می‌کنیم، ابزار رمزگشای بیت‌دیفندر است که حملات باج‌افزاری را بی‌اثر می‌کند. تا به امروز، بیت‌دیفندر ۲۰ رمزگشای رایگان را برای عموم منتشر کرده که میلیون‌ها دلار در بازیابی فایل‌ها و عدم پرداخت باج مطالبه شده برای سازمان‌ها و کاربران صرفه‌جویی کرده است.

بیت‌دیفندر در زمینه پیشگیری از تهدیدات، تشخیص و پاسخ در نقاط پایانی و ارائه خدمات امنیتی مدیریت شده، توسط شرکت‌های ارزیابی همچون IDC، Gartner و Forrester به عنوان شرکتی پیشرو شناخته شده است. بیت‌دیفندر افتخارات متعددی را از AV-Comparatives، AV-TEST، MITRE و دیگر آزمایشگاه‌های ارزیابی برتر و مستقل جهت امکانات بی‌نظیر خود در شناسایی تهدیدات در هر محیطی از جمله موبایل و بسترهای ابری دریافت کرده است.

بدون کار گروهی، فداکاری و همکاری، موفقیت‌ها و دستاوردهای بیت‌دیفندر ممکن نمی‌شد. مخصوصاً در این ایام سخت که همه‌گیری کرونا همکاران بیت‌دیفندر را از هم دور نگه داشته است. به زبان ساده، موفقیت بیت‌دیفندر به خاطر سخت‌کوشی اعضای آن است، از تیم‌های مهندسی، فروش، امور مالی، منابع انسانی، بازاریابی، تحقیق و توسعه، فناوری اطلاعات و پشتیبانی گرفته تا آزمایشگاه‌ها، تحلیلگران سرویس پاسخ‌دهی و تشخیص مدیریت شده بیت‌دیفندر (Managed Detection and Response Services - به اختصار MDR). هر یک به تنهایی نقش ویژه‌ای در انجام ماموریت بیت‌دیفندر جهت محافظت و پیشگیری مداوم ایفا می‌کنند.

ما با هم متحد شده‌ایم تا چشم‌اندازی را محقق کنیم که در آن هر کسب‌وکاری قادر به حفظ محرمانگی، یکپارچگی و در دسترس بودن سیستم‌ها و داده‌ها باشد. بیت‌دیفندر با پیشگیری از وقوع حملات سایبری، شناسایی و پاسخ سریع به رویدادها جهت به حداقل رساندن اثرات سوء آن‌ها، مأموریت خود را به عنوان یکی از سرسخت‌ترین پیشگامان امنیت سایبری تعریف کرده است. بررسی کارنامه عملکرد بیت‌دیفندر، نشان می‌دهد که موفق شده‌ایم و این موفقیت به خاطر همراهی شماست.

هر روزه مشتریان، الهام‌بخش بیت‌دیفندر هستند. آنها برای محافظت از ارزشمندترین دارایی‌های دیجیتال خود به ما اعتماد دارند، خدمت و سرویس‌دهی به آنها برای ما سعادت و افتخاری بزرگ است. ما مشتاقانه منتظر سال‌های پیش رو هستیم تا با ارائه راهکارها و محصولات تخصصی بیت‌دیفندر در زمینه امنیت سایبری، مشتریان خود را جهت نیل به اهدافشان یاری نماییم.

بیت‌دیفندر همواره این فرصت را داشته است که با بهترین عرضه‌کنندگان محصولات در زمینه فناوری، ارائه‌دهندگان خدمات و شرکای آن‌ها همکاری کند. هر کدام از این‌ها، بخشی از پروسه توسعه تیم بیت‌دیفندر بوده و نقش مهمی در کمک به ارائه محصولات باکیفیت، پشتیبانی و بهبود مستمر بیت‌دیفندر دارند زیرا همکاری با بخش‌های مذکور، تقاضا برای ارائه راهکارهای پیشرفته امنیت سایبری در سراسر جهان را افزایش می‌دهد.

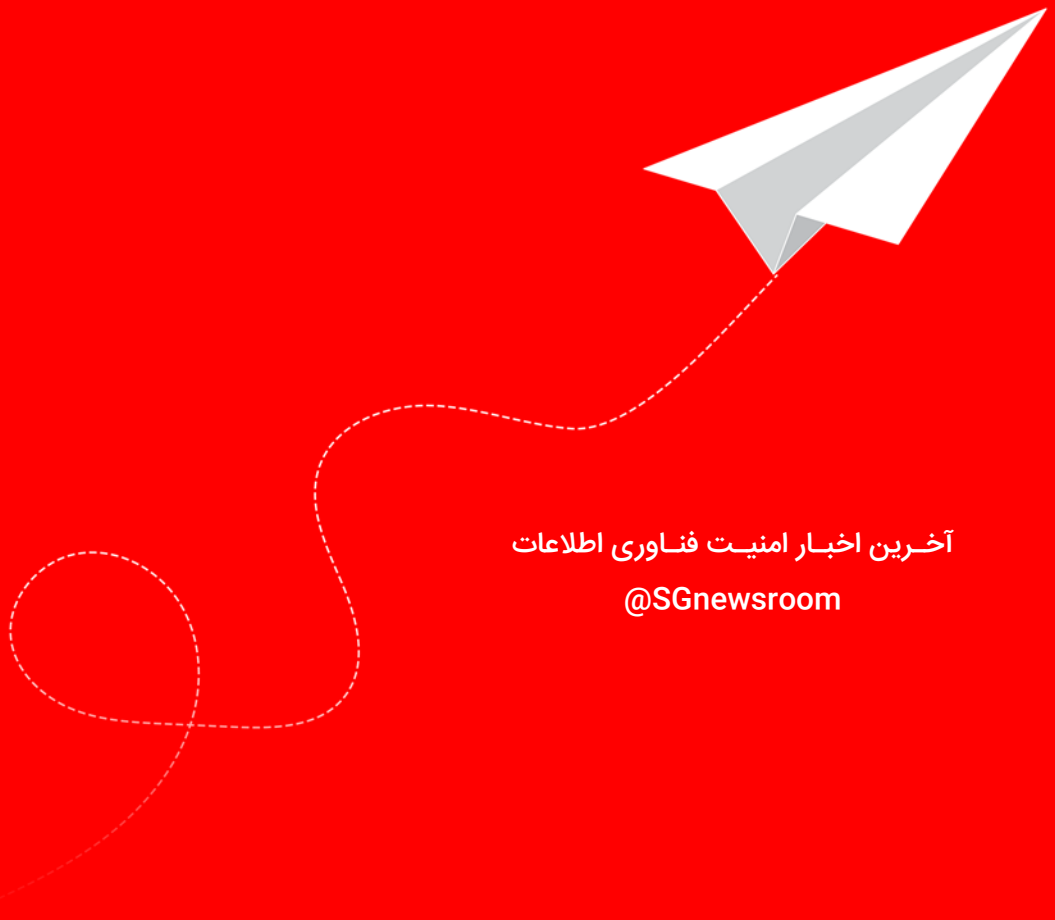
ما این سالگرد تاسیس بیت‌دیفندر را نمونه‌ای قدرتمند از پایداری مستمر در طول این ۲۰ سال دانسته و همچنین با ادامه همه‌گیری COVID-19، نشانه‌ای از امید می‌دانیم. سالگردهایی همانند این که در حال مبارزه با این همه‌گیری هستیم، مثبت‌اندیشی، اتحاد و احساس غرور را به ارمغان می‌آورند. این نشان‌دهنده همدلی و احساس مسئولیت اجتماعی است که تضمین می‌کند که با هم از این مشکل عبور می‌کنیم.

پیش‌بینی دقیق چگونگی تکامل دنیای دیجیتال در ۲۰ سال آینده دشوار است. با این حال، آنچه مسلم است این است که امنیت سایبری همیشه برای کاربرانی که خواهان حفاظت از اطلاعات، هویت و حریم خصوصی آنلاین خود هستند، سازمان‌هایی که نگران سرقت مالکیت معنوی و حملات باج‌افزاری هستند و دولت‌هایی که نگران امنیت شهروندان خود هستند، همچنان بسیار مهم باقی خواهد ماند. هر چالش جدیدی که پیش روی ما باشد، مطمئن باشید که بیت‌دیفندر با آن روبرو خواهد شد.

ما بیستمین سالگرد بیت‌دیفندر را جشن می‌گیریم و همه کسانی را که نقش مهمی در این سال‌ها ایفا کرده‌اند، تحسین می‌کنیم. ما در مورد آنچه هنوز در راه است هیجان‌زده‌تر هستیم زیرا دستاوردهای خود را برای کمک به شکل‌دهی راهکارهای آینده ایجاد می‌کنیم. ما عمیقاً به پیشینه، شرکتی که ساخته‌ایم و به اعضای تیم جهانی بیت‌دیفندر که با جرایم سایبری مبارزه می‌کنند تا جهان را به مکانی امن‌تر تبدیل کنند، افتخار می‌کنیم.

با احترام

Florin Talpes، مدیرعامل شرکت بیت‌دیفندر



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