ماهنامه

امنیت فناوری اطلاعات

دی ماه ۱۳۹۸

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 دی ماه ۱۳۹۸ پرداخته شده است.

مدتهاست که برنامه‌نویسی و توزیع باج‌افزار به کسب‌وکاری مدرن برای مهاجمان سایبری تبدیل شده است. از ارائه سرویس‌های باج‌افزار به‌عنوان خدمت گرفته تا مشارکت با نویسندگان بدافزارهای دیگر. جای تعجب ندارد که گردانندگان باج‌افزار نیز در مناسبت‌هایی همچون کریسمس و ایام سال نوی میلادی حضوری پررنگ داشته باشند! در این ماهنامه به نمونه‌های بسیار جالبی از تخفیف‌های پرزرق‌وبرق گردانندگان باج‌افزار به مناسبت ایام سال نوی میلادی پرداخته شده است.

در دی ماه، محققان از شناسایی بدافزاری خبر دادند که گروه FIN7 از آن برای فراخوانی نسخه جدیدی از درب‌پشتی Carbanak استفاده می‌کند. این ابزار که BIOLOAD نامگذاری شده است شباهت‌های فراوانی با BOOSTWRITE، دیگر ابزار مورد استفاده گروه FIN7 دارد. همانطور که در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر خواهید خواند یکی از نکات قابل توجه در حملات اخیر مهاجمان FIN7، دست‌درازی بدافزار آنها به یکی از فرامین زمانبندی‌شده (Scheduled Task) پیش‌فرض در سیستم عامل Windows با نام FODCleanupTask با هدف اجرای خودکار فایل مخرب و ماندگار کردن آن بر روی دستگاه است.

در دهمین ماه از سال ۱۳۹۸، مرکز مدیریت راهبردی افتا از مشاهده مواردی از آلودگی به بدافزاری منسوب به گروه APT27 در برخی از دستگاه‌های کشور خبر داد. در این ماهنامه فعالیت‌های APT27 و تکنیک‌های مورد استفاده این گروه معروف مورد بررسی و کالبدشکافی دقیق قرار گرفته است.

همچنین در ماهی که گذشت، شرکت‌های سیسکو، گوگل، موزیلا، مایکروسافت، ادوبی، وی‌اِم‌وِر و اوراکل اقدام به انتشار به‌روزرسانی، اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند؛ جزییات آنها را به همراه جدیدترین اخبار مرتبط با آسیب‌پذیری‌های امنیتی 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.

هشـدارهـای امنـیـتی

BIOLOAD،
ابزار جدید گروه FIN7

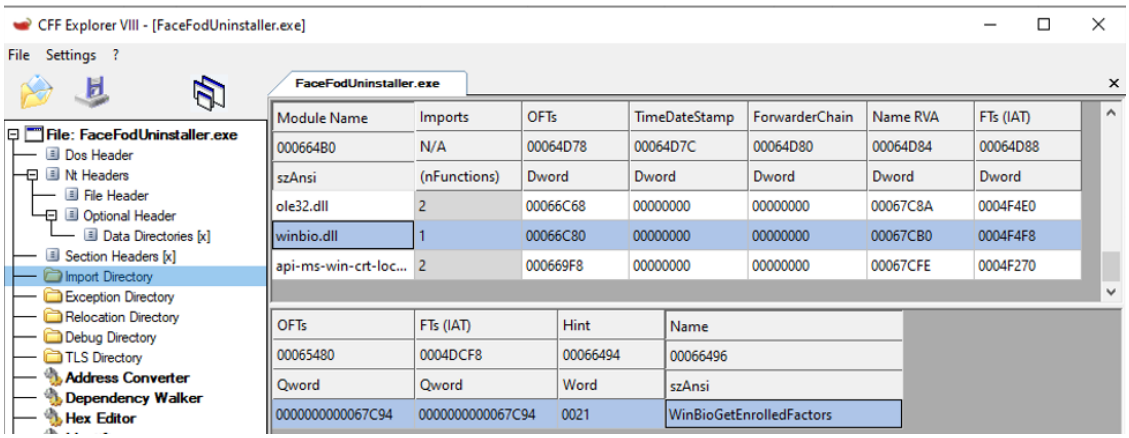
محققان شرکت فورتینت از شناسایی بدافزاری خبر داده‌اند که گروه FIN7 از آن برای فراخوانی نسخه جدیدی از درب‌پشتی Carbanak استفاده می‌کند.

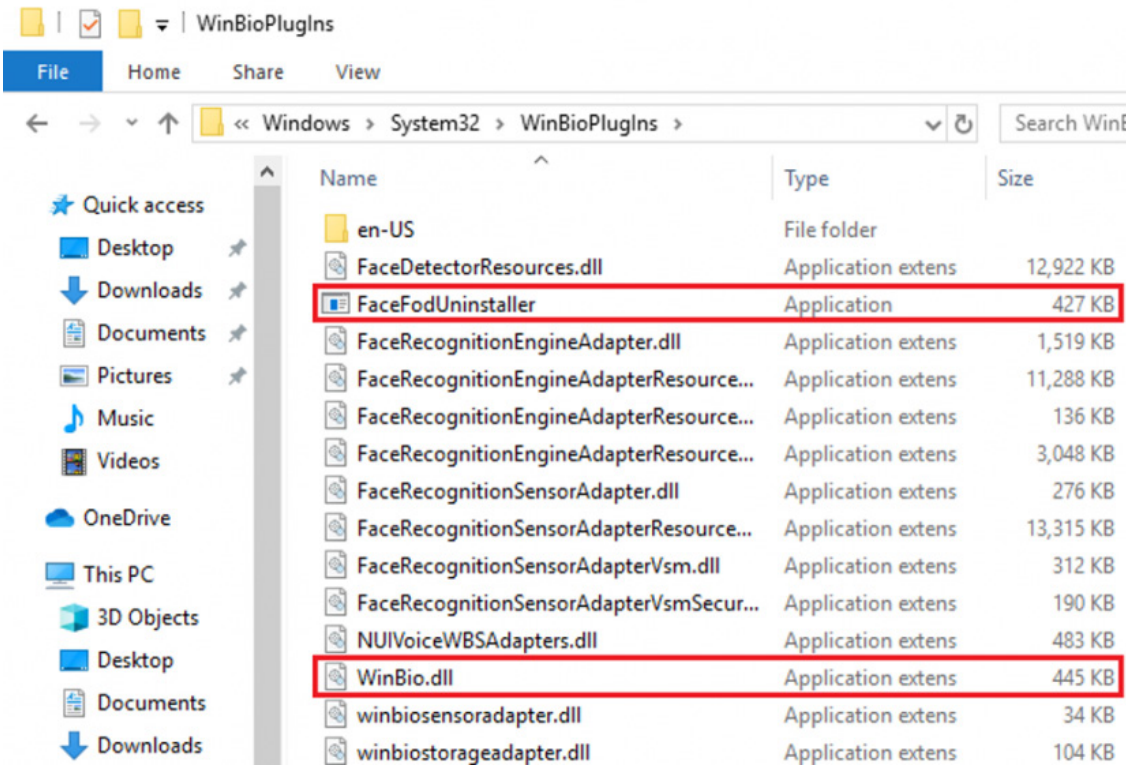
این ابزار که BIOLOAD نامگذاری شده است شباهت‌های فراوانی با BOOSTWRITE، دیگر ابزار مورد استفاده گروه FIN7 دارد.

BIOLOAD از تکنیکی موسوم به DLL Search Order Hijacking که در جریان آن از یکی از روش‌های بکار گرفته شده توسط سیستم عامل Windows در جستجوی فایل‌های DLL مورد نیاز برای اجرا شدن در یک برنامه سوءاستفاده می‌شود بهره می‌گیرد. بهره‌جویی از این طریق منجر به اجرای اموری همچون ترفیع سطح دسترسی کاربر غیرمجاز و یا ماندگاری برنامه‌ای مخرب بر روی سیستم می‌شود.

نکته قابل توجه در حملات اخیر مهاجمان FIN7، دست‌درازی بدافزار آنها به یکی از فرامین زمانبندی‌شده (Scheduled Task) پیش‌فرض در سیستم عامل Windows با نام FODCleanupTask با هدف اجرای خودکار فایل مخرب و ماندگار کردن آن بر روی دستگاه است.

به گزارش شرکت مهندسی شبکه گستر، فایل مخرب BIOLOAD با نام WinBio.dll در پوشه System32\WinBioPlugIns ذخیره می‌شود که مسیر واقعی فایل DLL معتبر winbio نیز می‌باشد.





از جمله شباهت‌های BIOLOAD با BOOSTWRITE نحوه قرار داده شدن کد مخرب در حافظه توسط آنهاست. ضمن اینکه کد مخرب DLL مورد استفاده آنها به‌صورت رمزگذاری شده در بدافزار تزریق شده است.

BIOLOAD در ماه‌های مارس و جولای سال ۲۰۱۹ کامپایل شده است. تاریخ کامپایل BOOSTWRITE نیز به ماه می باز می‌گردد.

BIOLOAD و BOOSTWRITE تفاوت‌هایی هم با یکدیگر دارند؛ BIOLOAD توانایی پشتیبانی از چندین کد اصلی را ندارد؛ ضمن اینکه بجای الگوریتم ChaCha از XOR برای رمزگذاری استفاده می‌کند.

همچنین اتصال به سرور فرماندهی به‌منظور دریافت کلید رمزگذاری در BIOLOAD انجام نمی‌شود؛ BIOLOAD به‌طور خاص برای هر قربانی طراحی شده و کلید رمزگشایی از نام آن مشتق می‌شود.

BIOLOAD در نهایت نسخه‌ای از درب‌پشتی Carbanak را بر روی سیستم کپی می‌کند که تاریخ ایجاد آن در نمونه‌های مورد بررسی توسط محققان فورتینت در بین ماه‌های ژانویه و آوریل ۲۰۱۹ است.

این نمونه‌ها از Carbanak، قادر به شناسایی تعداد بیشتری از محصولات ضدویروس نصب شده بر روی دستگاه قربانی هستند؛ در حالی که فهرست مورد استفاده توسط نمونه‌های پیشین تنها محدود به Kaspersky،AVG و TrendMicro بود.

بر اساس شباهت‌های درون کد، تکنیک‌ها و درب‌پشتی مورد استفاده، فورتینت ساخت BIOLOAD را به گروه FIN۷ نسبت داده است.

مشروح گزارش فورتینت در اینجا قابل دریافت است.

نمونه BIOLOAD بررسی شده توسط فورتینت با نام‌های زیر قابل شناسایی است:

Bitdefender:

- GenericKD.42185659

McAfee:

- Artemis!A8BA59EEBD48

محصولاتی از مایکروسافت
که در سال ۲۰۲۰ منقضی می‌شوند

در سال میلادی جدید، پشتیبانی مایکروسافت از برخی محصولات این شرکت از جمله Office 2010، Visual Studio 2010، Windows 7، Windows Server 2008 R2 و نگارش‌هایی از Windows 10 پایان می‌یابد. با اتمام پشتیبانی، عرضه اصلاحیه‌های امنیتی برای این محصولات متوقف خواهد شد.

اگر چه مایکروسافت برای برخی از محصولات بازنشسته خود حاضر است که برای مدتی محدود خدمات پشتیبانی پولی ارائه دهد اما برای اینکه حتی مؤسسات بزرگ هم به فکر استفاده از این روش نباشند و ترجیح دهند که نسخه محصول قدیمی خود را ارتقاء دهند، این شرکت قیمت‌های قابل‌توجهی را برای این خدمات در نظر گرفته است. بطور مثال، برای دریافت خدمات پشتیبانی ویژه به ۵ هزار کامپیوتر با سیستم عامل Windows 7 Pro باید یک میلیون دلار به مایکروسافت پرداخت کرد.

سوءاستفاده از ضعف‌ها و اشکالات امنیتی در سیستم‌های عامل و نرم‌افزارهای پراستفاده از روش‌های مؤثر و بسیار مخربی است که مهاجمان حرفه‌ای از آن به‌منظور آلوده‌سازی دستگاه‌ها به بدافزار و رخنه به اهداف خود بهره می‌گیرند. به‌خصوص آنکه مسدودسازی این نوع حملات بدون نصب اصلاحیه مربوطه بسیار دشوار و در برخی موارد حتی غیرممکن است. بنابراین عدم عرضه اصلاحیه برای هر یک از این محصولات به‌معنای آسیب‌پذیری شدید سازمان‌هایی است که پس از تاریخ پایان مشتری حتی یک دستگاه با یک چنین محصولاتی در بستر شبکه آنها در حال فعالیت خواهد بود.

با توجه به اینکه بسیاری از بخش‌ها و قابلیت‌های محصولاتی همچون Windows در نسخه‌های مختلف آن یکسان هستند، با کشف یک نقطه ضعف در یکی از نسخه‌های این محصولات، این احتمال وجود دارد که نسخه‌های دیگر نیز نسبت به آن نقطه ضعف آسیب‌پذیر باشند. به گزارش شرکت مهندسی شبکه گستر، نفوذگران می‌توانند با مهندسی معکوس بر روی اصلاحیه‌های جدید، متوجه شوند که نقطه ضعف در چه بخش از محصول بوده و به چه نحوی اصلاح و ترمیم شده است. با داشتن این اطلاعات، مهاجمان قادر خواهند بود که نقطه ضعف را در نسخه‌های قدیمی و از رده خارج هم شناسایی کرده و راه سوءاستفاده از آن را به دست آورند.

باید توجه داشت که علاوه بر قطع عرضه اصلاحیه‌های امنیتی مایکروسافت برای این محصولات، بسیاری از شرکت‌های نرم‌افزاری دیگر هم به تدریج پشتیبانی از آنها را متوقف خواهند کرد.

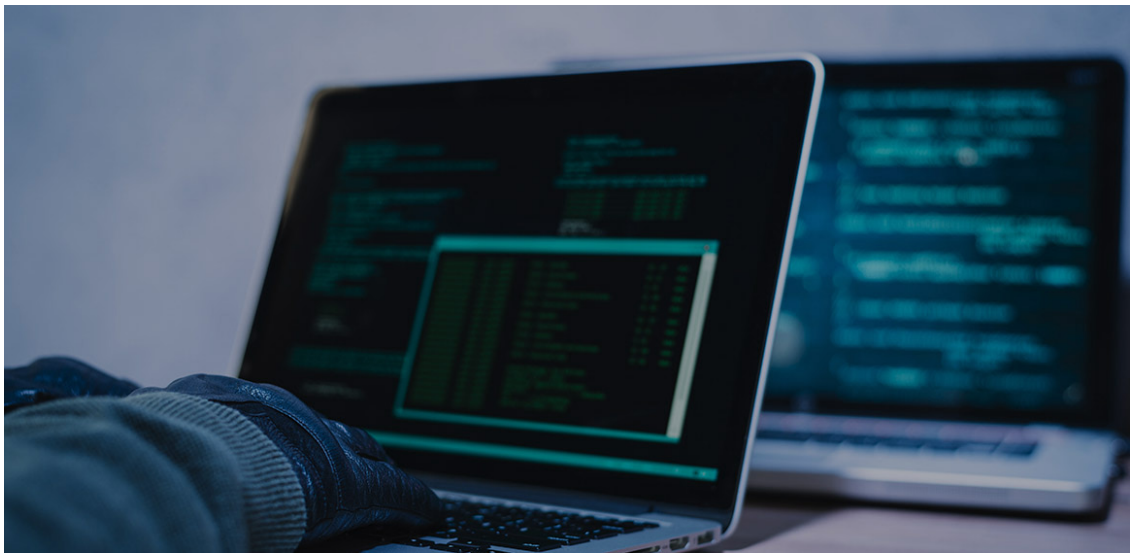
جدول صفحه بعد فهرست برخی از مهم‌ترین محصولات مایکروسافت را که در سال ۲۰۲۰ منقضی خواهند شد نمایش می‌دهد.

عنوان محصول	تاریخ پایان پشتیبانی
Windows 7	۲۴ دی ۱۳۹۸
Windows Server 2008 R2	۲۴ دی ۱۳۹۸
Windows Server 2008	۲۴ دی ۱۳۹۸
Hyper-V Server 2008	۲۴ دی ۱۳۹۸
Hyper-V Server 2008 R2	۲۴ دی ۱۳۹۸
Internet Explorer 10	۱۱ بهمن ۱۳۹۸
Azure Container Service	۱۱ بهمن ۱۳۹۸
Windows Analytics	۱۱ بهمن ۱۳۹۸
Windows 10, version 1709 (Enterprise, Education, IoT Enterprise)	۲۶ فروردین ۱۳۹۹
Windows 10, version 1809 (Home, Pro, Pro for Workstation, IoT Core)	۲۶ فروردین ۱۳۹۹
Windows Server version 1809 (Datacenter Core, Standard Core)	۲۶ فروردین ۱۳۹۹
Visual Studio Team Foundation Server 2010	۲۴ تیر ۱۳۹۹
Visual Studio 2010 (All Editions)	۲۴ تیر ۱۳۹۹
System Center Service Manager 2010	۱۸ شهریور ۱۳۹۹
Exchange Server 2010	۲۲ مهر ۱۳۹۹
Access 2010	۲۲ مهر ۱۳۹۹
Excel 2010	۲۲ مهر ۱۳۹۹
Excel Home and Student 2010	۲۲ مهر ۱۳۹۹
Office 2010 (all editions)	۲۲ مهر ۱۳۹۹
Project Server 2010	۲۲ مهر ۱۳۹۹
SharePoint Foundation 2010	۲۲ مهر ۱۳۹۹
SharePoint Server 2010	۲۲ مهر ۱۳۹۹
SharePoint Server 2010 Service Pack 2	۲۲ مهر ۱۳۹۹
System Center Data Protection Manager 2010	۲۲ مهر ۱۳۹۹
Word 2010	۲۲ مهر ۱۳۹۹
Office Home & Business 2016 for Mac	۲۲ مهر ۱۳۹۹
Office Home & Student 2016 for Mac	۲۲ مهر ۱۳۹۹
Office Standard 2016 for Mac	۲۲ مهر ۱۳۹۹
Windows 10, version 1803 (Enterprise, Education, IoT Enterprise)	۲۰ آبان ۱۳۹۹
Windows 10, version 1903 (Enterprise, Home, Pro, Pro for Workstations, IoT Enterprise)	۲۰ آبان ۱۳۹۹
Windows Server, version 1903 (Datacenter, Standard, IoT Enterprise)	۲۰ آبان ۱۳۹۹

فهرست کامل این محصولات در اینجا قابل مطالعه است.

به تمامی راهبران شبکه و کاربران توصیه می‌شود که در فرصت باقی مانده اقدام به ارتقای محصولات مذکور به نسخه‌های جدیدتر و قابل پشتیبانی کنند.

همه چیز درباره
APT27



گروه نفوذگران APT27 که با نام‌های LuckyMouse، Emissary Panda، BRONZE UNION، Threat Group 3390 و Iron Tiger نیز شناخته می‌شود حداقل از سال ۲۰۱۰ میلادی فعال بوده و صدها سازمان را در کشورهای مختلف هدف قرار می‌داده است. بسیاری از منابع، گردانندگان APT27 را نفوذگرانی با ملیت یا اصالت چینی می‌دانند.

به گزارش شرکت مهندسی شبکه گستر حملات اجرا شده توسط این گروه اهداف مختلف و متفاوتی را از سرقت اطلاعات در خصوص فناوری‌های تسلحیاتی گرفته تا جاسوسی از فعالان حقوق بشر دنبال می‌کنند.

بتازگی نیز مرکز مدیریت راهبردی افتا از مشاهده مواردی از آلودگی به بدافزاری منسوب به گروه APT27 در برخی از دستگاه‌های کشور خبر داده است. این مرکز با مشارکت یک شرکت دانش‌بنیان اقدام به عرضه ابزارهایی به‌منظور شناسای و پاکسازی بدافزار مذکور نموده که جزییات آنها در اینجا قابل دسترس است.

به گزارش شرکت مهندسی شبکه گستر منطقه خاورمیانه یکی از اصلی‌ترین اهداف در بسیاری از حملات این گروه بوده است. برای مثال، در آوریل سال ۲۰۱۹ شرکت پالوآلتو نت‌ورکز از آلودگی سازمان‌های دولتی در دو کشور در این منطقه خبر داد که در جریان آن حملات، مهاجمان با بهره‌جویی از آسیب‌پذیری CVE-2019-0604 در نرم‌افزار Microsoft SharePoint اقدام به رخنه به سرورهای حاوی این نرم‌افزار و نصب یک وب‌شل مخرب بر روی آنها می‌کردند.

حدود یک سال قبل محققان Secureworks اعلام کردند که این گروه معمولاً هر سه ماه یکبار مجدداً به شبکه قربانیان خود بازگشته و ضمن بررسی برقرار بودن دسترسی به وب‌شل‌های مخرب و اطلاعات اصالت‌سنجی (Credential) پیشین، داده‌های مورد نظر خود را مورد رصد قرار می‌دهد.

از جمله تکنیک‌های بکار گرفته شده توسط گروه APT27 می‌توان به موارد زیر اشاره کرد:

- این گروه از فرمان net user به‌منظور شناسایی نام‌های کاربری ایجاد شده بر روی دستگاه بهره می‌گیرد.
- در برخی حملات اجرا شده توسط APT27 از ابزاری به‌منظور عبور از سد User Account Control و ترفیع سطح دسترسی بهره گرفته شده است.
- در جریان برخی از حملات این گروه از درگاه‌های ۵۳، ۸۰ و ۴۴۳ استفاده شده است.
- APT27 با استفاده از gsecdump و نسخه‌ای ویرایش شده از ابزار Mimikatz (معروف به Wrapikatz) اقدام به جمع‌آوری اطلاعات اصالت‌سنجی می‌کند. همچنین این گروه سرورهای موسوم به Domain Controller را نیز به طور خاص به همین منظور هدف قرار می‌دهد.

- این گروه از ابزار RAR برای فشرده‌سازی، رمزگذاری و قرار دادن رمز عبور بر روی فایل فشرده شده پیش از ارسال آنها به سرور فرماندهی استفاده می‌کند.
- APT27 به‌صورت مرحله به مرحله و در فایل‌هایی با اندازه‌ای مشخص اطلاعات را به سرورهایی در معرض دسترس در اینترنت که پیش‌تر به بدافزار China Chopper آلوده شده‌اند ارسال می‌کند.
- این گروه از فایل appcmd.exe برای غیرفعال کردن ثبت رویدادها بر روی سرور قربانی استفاده می کند.
- از تکنیک‌های مورد استفاده این گروه، DLL Search Order Hijacking است که در جریان آن از یکی از روش‌های بکار گرفته شده توسط سیستم عامل Windows در جستجوی فایل‌های DLL مورد نیاز برای اجرا شدن در یک برنامه سوءاستفاده می‌شود. بهره‌جویی از این طریق منجر به اجرای اموری همچون ترفیع سطح دسترسی کاربر غیرمجاز و یا ماندگاری برنامه‌ای مخرب بر روی سیستم می‌شود.
- APT27 از معروف‌ترین گروه‌هایی است که به‌طور استراتژیک اقدام به هک کردن سایت‌های مورد استفاده اهداف خود و آلوده‌سازی دستگاه آنها از طریق این سایت‌ها می‌کند.
- این گروه سوءاستفاده از ضعف امنیتی CVE-2014-6324 در Windows و آسیب‌پذیری CVE-2019-0604 در نرم‌افزار Microsoft SharePoint را در کارنامه دارد.
- در برخی حملات، این مهاجمان یک ثبت‌کننده اطلاعات اصالت‌سنجی را بر روی سرورهای Microsoft Exchange نصب کرده‌اند. همچنین این گروه از ابزار ScanBox در فرایند شناسایی کلیدهای فشرده شده توسط قربانی بهره می‌گیرد.
- ابزار مورد استفاده این گروه قادر به ایجاد کلید جدید در مسیر \HKEY_CURRENT_USER\Software\Classes در محضرخانه (Registry) است.
- گروه APT27 از ابزار Hunter جهت شناسایی سرویس‌های در معرض دسترس در سطح شبکه و سیستم‌های آسیب‌پذیر بهره می‌گیرد.
- این گروه پس از سرقت اطلاعات، احتمالاً به‌منظور از بین بردن رد پا اقدام به قطع ارتباطات خود با پوشه‌های اشتراکی می‌کند.
- یکی از ابزارهای APT27 قادر به ایجاد سرویسی جدید بر روی دستگاه قربانی با هدف ماندگار کردن بدافزار خود است.
- این مهاجمان از پروسه معتبر PowerShell جهت اجرای برخی از اسکریپت‌ها و کدهای مخرب خود استفاده می‌کنند.
- یکی از ابزارهای این گروه پروسه معتبر svchost.exe را تسخیر کرده و کد مخرب را در آن تزریق می‌کند.
- در برخی حملات فایل و مسیر اجرای بدافزار در مسیر \Software\Microsoft\Windows\CurrentVersion\Run ثبت و به این ترتیب بدافزار بر روی سیستم ماندگار می‌شود.
- گروه APT27 از فرمان net view برای شناسایی سیستم‌های شبکه قربانی استفاده می‌کند.
- این مهاجمان از at در فرامین زمانبندی شده (Scheduled Task) برای اجرای فایل‌های فشرده RAR با خاصیت خوداجرایی و در ادامه نصب بدافزارهای HTTPBrowser یا PlugX بر روی دستگاه سایر قربانیان در شبکه استفاده می‌کنند.
- بدافزارهای این گروه معمولاً از پودمان HTTP برای برقراری ارتباط با سرور فرماندهی خود استفاده می‌کنند.
- گروه APT27 از ابزار nbtscan برای شناسایی سیستم‌های آسیب‌پذیر استفاده می‌کند.
- این مهاجمان از net use برای شناسایی سایر دستگاه‌ها استفاده می‌کند. همچنین گروه APT27 از quser.exe جهت شناسایی نشست‌های RDP برقرار شده بر روی یک سیستم بهره می‌گیرد.
- این گروه با بدست آوردن اطلاعات اصالت‌سنجی معتبر با استفاده از روش های مختلف در ادامه از آنها برای گسترش آلودگی استفاده می‌کند.
- در حملات گروه APT27 از وب‌شل‌های متعددی استفاده شده است.
- حداقل یکی از ابزارهای مورد استفاده این گروه قادر به اجرای فایل دودویی از طریق Windows Management Instrumentation است.
- این مهاجمان از Windows Remote Management برای فعال کردن امکان اجرای کد به‌صورت از راه دور استفاده می‌کنند.

توضیح اینکه نمونه‌های بررسی شده از بدافزارهای مورد استفاده گروه APT۲۷ با نام‌های زیر توسط ضدویروس McAfee قابل شناسایی است:

- Artemis!1B2D75F9C771
- Artemis!12A522CB9670
- Artemis!1CB4B74E9D03

- Artemis!1DD30422A1CB
- Artemis!2BEC1860499A
- Artemis!37FC73C754EF
- Artemis!3EEB4A7C6925
- Artemis!4251AAF38A48
- Artemis!57E85FC30502
- Artemis!70CFF7C176C7
- Artemis!728E5700A401
- Artemis!81ED75259075
- Artemis!850DF4A726A7
- Artemis!86A05DCFFE87
- Artemis!93E40DA0BD78
- Artemis!9DD9D006D40D
- Artemis!A13772805B77
- Artemis!A9C2FF438C73
- Artemis!B333B5D541A0
- Artemis!B7F958F93E2F
- Artemis!BD9E4C82BF12
- Artemis!C69D60B82252
- Artemis!C8D83840B96F
- Artemis!F43D9C3E17E8
- ASP/Shell.h
- BackDoor-Chopper
- BackDoor-FCVY!014122D7851F
- BackDoor-FCVY!02826BB66363
- BackDoor-FCVY!0AE996B31A2C
- BackDoor-FCVY!1539B3A59212
- BackDoor-FCVY!15FD9C04D609
- BackDoor-FCVY!1606AB7A5473
- BackDoor-FCVY!1A76681986F9
- BackDoor-FCVY!20C446AD2D7D
- BackDoor-FCVY!225E10E362EE
- BackDoor-FCVY!372F5370085A
- BackDoor-FCVY!380C02B1FD93
- BackDoor-FCVY!40A9A22DA928
- BackDoor-FCVY!44CF0793E05B
- BackDoor-FCVY!46CF2F9B4A4C
- BackDoor-FCVY!5C3AB475BE11
- BackDoor-FCVY!5CD0E97A1F09
- BackDoor-FCVY!5EF719F8AEB9
- BackDoor-FCVY!692CECC94AC4
- BackDoor-FCVY!6A39A4E99334
- BackDoor-FCVY!6AAC7417EA1E
- BackDoor-FCVY!8EA5D8BB6B28
- BackDoor-FCVY!9271BCFBBA05
- BackDoor-FCVY!996843B55A7C
- BackDoor-FCVY!A554EFC88971
- BackDoor-FCVY!A631FC7C45CB
- BackDoor-FCVY!AF785B4DF71D
- BackDoor-FCVY!C66E09429AD6
- BackDoor-FCVY!C9C93C2D62A0
- BackDoor-FCVY!DDBDF0EFDF26
- BackDoor-FCVY!E3E0F3AD4FF3
- BackDoor-FCVY!E7DF18A17D8E
- BackDoor-FCVY!E7E555615A07
- BackDoor-FCVY!EA4DCAFC224F
- BackDoor-FCVY!EA8B9E0BF95F
- BackDoor-FCVY!F658BB17D699
- BackDoor-FCVY!F869A1B40F64
- BackDoor-FCVY!FAC4885324CB
- BackDoor-FDRS!40CDD3CFE86C
- DoS-FAK!19230C66AA4A
- Generic Trojan.em
- Generic Trojan.go
- Generic Trojan.gs
- Generic Trojan.gy
- Generic Trojan.hm
- Generic Trojan.i
- Generic.dx!BBFD1E703F55
- Generic.eof
- GenericR-QAF!F0044BCB4B1D
- GenericRXGO-YK!C419CDD0DECE
- GenericRXHS-MH!9F8B60567642
- GenericRXHT-WL!2BCB003D74F9
- HTML/Chopper.a
- HTool-JSPRat
- Nbtscan
- Packed-LF!313909878C72
- Packed-LF!6F5E0882316C
- PUP-XAV-HC
- RDN/Generic BackDoor
- RDN/Generic BackDoor.ml
- RDN/Generic PUP.abb
- RDN/Generic PUP.bmb
- RDN/Generic PUP.pk
- RDN/Generic PUP.z

- RDN/Generic.com
- RDN/Generic.dxw
- RDN/Generic.erp
- RDN/Generic.grp
- RDN/Generic.hra
- Trojan-FMWJ!CD5AAA37EE16
- Trojan-FPYL!62BCBFAE5276
- W97M/MacroLess.h

سیستم‌های عامل از رده خارج؛
تهدیدی جدی علیه امنیت سازمان‌ها

سالهاست که ویروس‌نویسان و نفوذگران به‌شدت به استفاده از نقاط ضعف سیستم‌های عامل - به ویژه سیستم عامل پرطرفدار Windows - روی آورده‌اند. وجود یک نقطه ضعف (Vulnerability) خطرناک در سیستم عامل می‌تواند سبب دور زدن قوی‌ترین نرم‌افزارهای ضدویروس یا دیواره‌های آتش شود!

شرکت مایکروسافت علاوه بر عرضه اصلاحیه فوری در مواقع اضطراری، در سه‌شنبه دوم هر ماه میلادی نیز اصلاحیه‌های امنیتی جدید خود را منتشر می‌کند. کمتر سه‌شنبه دوم ماه میلادی را می‌توان یافت، که مایکروسافت اصلاحیه‌ای "حیاتی" (Critical) برای سیستم عامل Windows عرضه نکرده باشد.

این در حالی است که پشتیبانی این شرکت از سیستم‌های عامل Windows 7 و Windows Server 2008/2008 R2 در ۲۴ دی ماه به پایان رسید و عملاً مایکروسافت عرضه اصلاحیه‌های امنیتی برای این سیستم‌های عامل را متوقف کرده است. بنابراین نفوذگران با اطلاع از جزئیات نقاط ضعف جدید کشف شده در سیستم‌های عامل پشتیبانی شده که توسط شرکت مایکروسافت منتشر می‌شوند می‌توانند با مهندسی معکوس این نقاط ضعف را در این سیستم‌های عامل از رده خارج نیز شناسایی نموده و از آنها سوءاستفاده کنند.

بر اساس اعلام شرکت مک‌آفی پشتیبانی محصولات این شرکت از سیستم‌های عامل Windows 7 و Windows Server 2008/2008 R2 تا ۱۰ دی ۱۴۰۰ ادامه خواهد یافت. جزییات بیشتر در این خصوص در لینک زیر قابل مطالعه است:

- https://kc.mcafee.com/corporate/index?page=content&id=KB91432

این شرکت پشتیبانی ضدبدافزار سازمانی خود را از سیستم‌های عامل XP و Server 2003 را از دی ماه ۱۳۹۴ متوقف کرده بود.

شرکت بیت‌دیفندر نیز از پایان پشتیبانی محصول Bitdefender Patch Management از Windows 7 و Windows Server 2008/2008 R2 خبر داده است. همچنین بیت‌دیفندر اعلام کرده که اگر چه ارائه به‌روزرسانی برای ضدویروس سازمانی این شرکت با عنوان Bitdefender Endpoint Security Tools بر روی دستگاه‌های با هر یک از سیستم‌های عامل مذکور همچنان ادامه خواهد یافت اما این ادامه پشتیبانی منوط به مختل نشدن قابلیت‌های بکار گرفته شده در نسخه‌های جدید این محصول در نتیجه عدم امکان به‌روزرسانی Windows 7 و Windows Server 2008/2008 R2 توسط مایکروسافت خواهد بود. جزییات بیشتر در این مورد در لینک زیر قابل دریافت است:

- https://www.bitdefender.com/support/end-of-support-for-patch-management-for-windows-7-and-windows-server-2008-2008-r2-2496.html

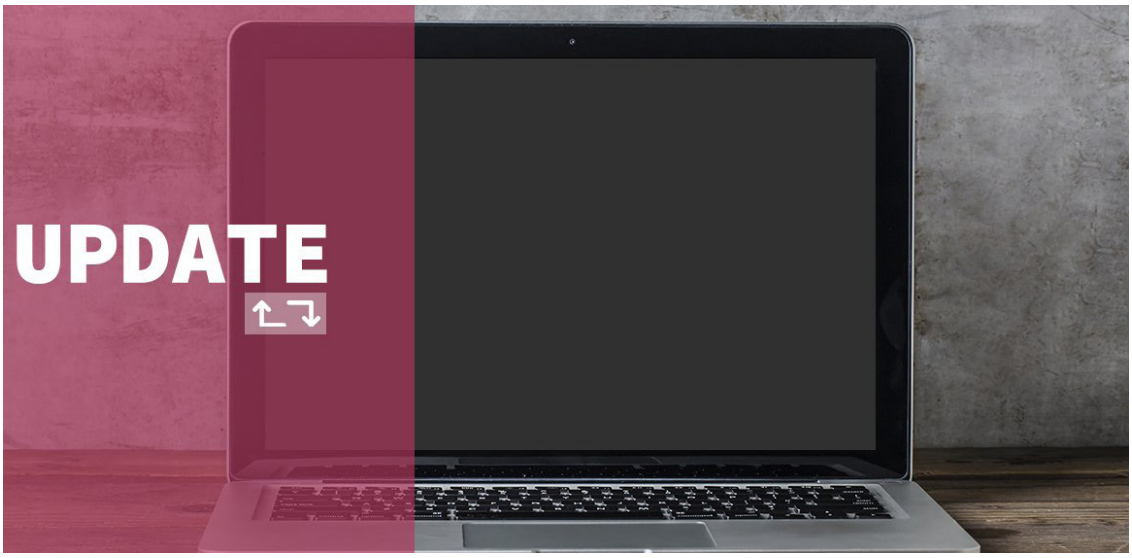
ضمن اینکه بر اساس اعلام قبلی بیت‌دیفندر، عرضه به‌روزرسانی امضای شناسایی بدافزار (Security Content Update) برای سیستم‌های عامل Windows XP و Windows Server 2003 تنها تا ۱۱ اردیبهشت ماه ۱۳۹۹ ادامه داشته و پس از آن امکان به‌روزرسانی Bitdefender Endpoint Security Tools بر روی این دو سیستم عامل ممکن نخواهد بود. از ۱۱ دی ماه سال جاری نیز ایجاد نسخه نصبی (Installation Kit) ضدویروس برای Windows XP و Windows Server 2003 در کنسول مدیریتی Bitdefender GravityZone امکان‌پذیر نبوده و مشترکین برای نصب ضدویروس بر روی سیستم‌های عامل مذکور می‌بایست از نسخه‌های نصبی قدیمی استفاده کرده یا برای دریافت آن با گروه پشتیبانی شرکت مهندسی شبکه گستر تماس حاصل کنند. توضیحات کامل در این خصوص در لینک زیر ارائه شده است:

- https://www.bitdefender.com/support/windows-xp-and-windows-server-2003-support-announcement-1670.html

ارتقای سیستم‌های عامل قدیمی و از رده خارج به نسخه‌های جدیدتر و قابل پشتیبانی در اسرع وقت توصیه اکید می‌شود.

لازم به ذکر است که محصول McAfee Application Control راهکاری مناسب برای ایمن کردن و مقاوم‌سازی این سیستم‌های عامل است.

اصلاحیه‌های عرضه شده در دی ۱۳۹۸



در دی ۱۳۹۸، شرکت‌های سیسکو، گوگل، موزیلا، مایکروسافت، ادوبی، وی‌اِم‌وِر و اوراکل اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

در دی ماه، سیسکو در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ۲۶ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۲ مورد از این آسیب‌پذیری‌ها "حیاتی" (Critical) و ۹ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "عبور از سد کنترل‌های احراز هویت" (Authentication Bypass) و "ترفیع امتیازی" (Privilege Escalation)، از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید است. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در اینجا قابل دسترس است.

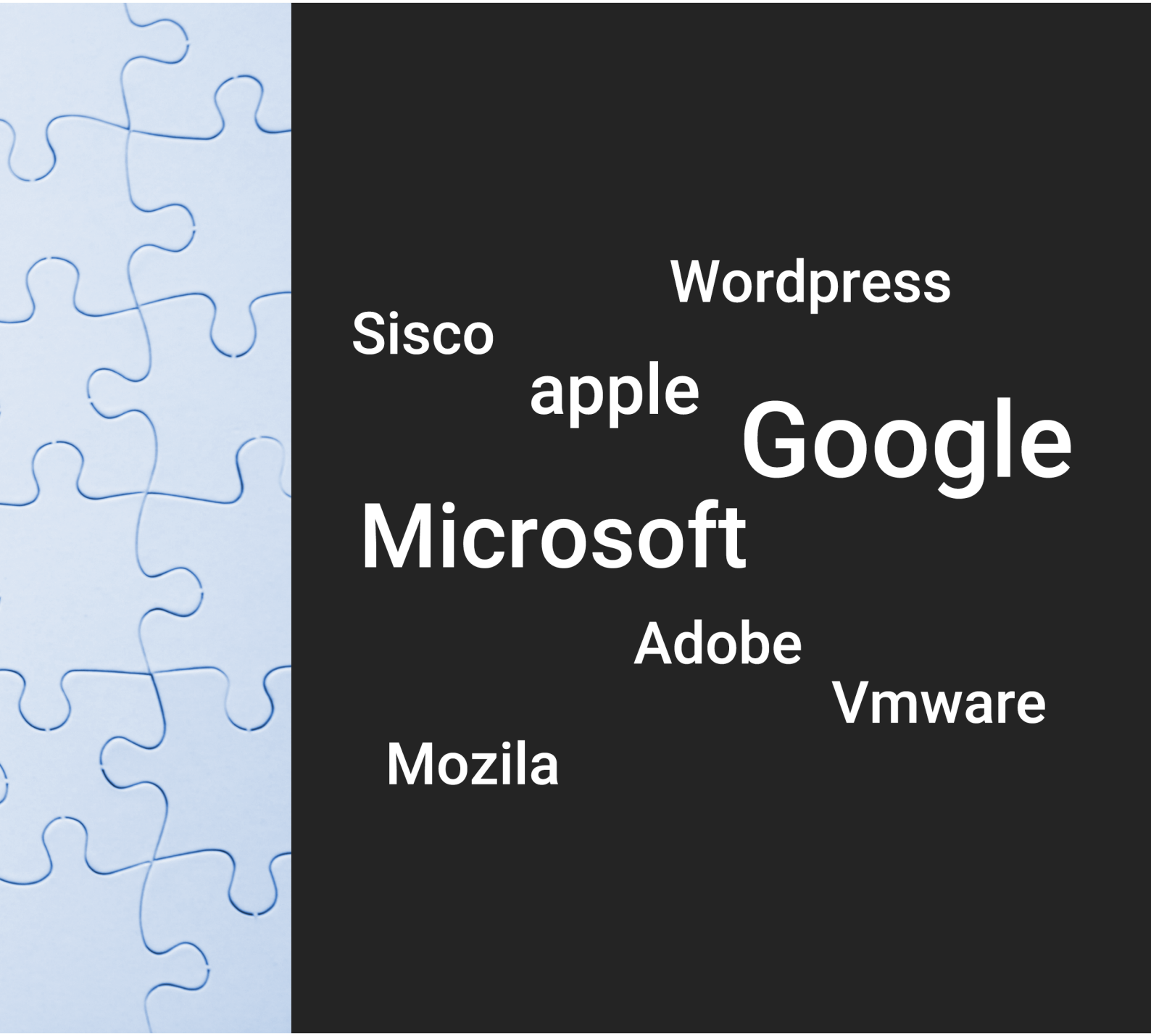
در ۱۸ دی ماه، شرکت موزیلا، با ارائه نسخه 72.0.1، یک آسیب‌پذیری "حیاتی" به شناسه CVE-2019-17026 را در مرورگر Firefox برطرف کرد.مواردی از بهره‌جویی از این آسیب‌پذیری توسط مهاجمان سایبری گزارش شده است. جزییات بیشتر در اینجا قابل مطالعه است.

به گزارش شرکت مهندسی شبکه گستر، گوگل نیز در دی ماه، در دو نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. بهره‌جویی از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. آخرین نسخه این مرورگر که در ۲۷ دی انتشار یافت 79.0.3945.130 است. فهرست اشکالات مرتفع شده در این نسخه نیز در اینجا قابل دریافت و مشاهده است.

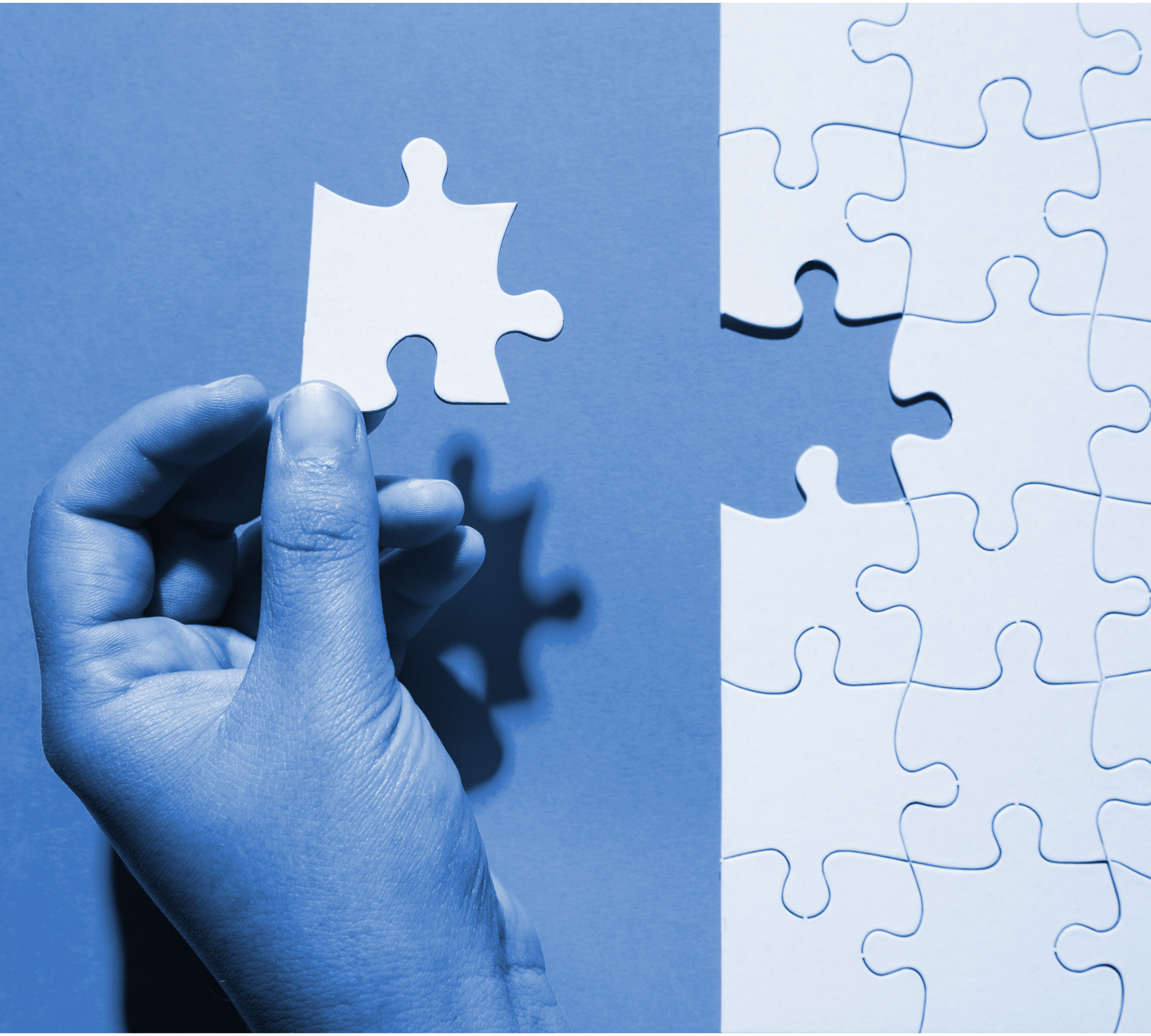
۲۴ دی، شرکت‌های مایکروسافت و ادوبی بر طبق زمانبندی معمول، اقدام به عرضه اصلاحیه‌های امنیتی ماهانه خود کردند که جزییات آنها به‌طور تفصیلی در اینجا و اینجا پوشش داده شده است. همچنین مایکروسافت در همین تاریخ اقدام به انتشار یک توصیه‌نامه با شناسه ADV20001 در خصوص نحوه مقاوم‌سازی یک آسیب‌پذیری امنیتی روز-صفر (Zero-day) در مرورگر Internet Explorer کرد که توضیحات آن در اینجا قابل مطالعه است. بر طبق مستندات مایکروسافت، این شرکت از اجرای تعداد محدودی حمله که در جریان آن از آسیب‌پذیری مذکور سوءاستفاده می‌شود آگاه شده است.

وی‌اِم‌ور دیگر شرکتی بود که در دی ۱۳۹۸ اقدام به انتشار به‌روزرسانی کرد. این شرکت در این به‌روزرسانی، ضعفی امنیتی با شناسه را در مجموعه ابزارهای VMware Tools ترمیم و اصلاح کرد. سوءاستفاده از ضعف مذکور، مهاجم را قادر به ترفیع سطح دسترسی خود بر روی ماشین مجازی با نسخه آسیب‌پذیر VMware Tools می‌کند. جزییات بیشتر در اینجا قابل مطالعه است.

و در نهایت اینکه، شرکت اوراکل طبق برنامه زمانبندی شده سه‌ماهه خود، ۲۴ دی ماه، در مجموع با انتشار ۳۳۴ به‌روزرسانی، آسیب‌پذیری‌های امنیتی ده‌ها محصول ساخت این شرکت ترمیم و اصلاح کرد. جزییات کامل در این خصوص در اینجا ارائه شده است.


Wordpress
Sisco
apple
Google
Microsoft
Adobe
Vmware
Mozila

آسیب‌پذیری‌ها
و اصلاحیه‌های امنیتی



اولین اصلاحیه‌های مایکروسافت
در سال ۲۰۲۰

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه، ۲۴ دی، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی ژانویه منتشر کرد. این اصلاحیه‌ها در مجموع، ۴۹ آسیب‌پذیری را در سیستم عامل Windows و طیف وسیعی از سرویس‌ها و نرم‌افزارهای مایکروسافت ترمیم می‌کنند. درجه اهمیت ۸ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical) و ۴۱ مورد "بااهمیت" (Important) اعلام شده است.

در درجه‌بندی شرکت مایکروسافت، نقاط ضعفی که سوءاستفاده از آنها بدون نیاز به دخالت و اقدام کاربر باشد، حیاتی تلقی شده و اصلاحیه‌هایی که این نوع نقاط ضعف را ترمیم می‌کنند، بالاترین درجه اهمیت یا "حیاتی" را دریافت می‌نمایند. نقاط ضعفی که سوءاستفاده موفق از آنها نیازمند فریب کاربر به انجام کاری باشد یا نیازمند دسترسی فیزیکی به دستگاه هدف باشد، توسط اصلاحیه‌هایی با درجه اهمیت "بااهمیت" برطرف و ترمیم می‌گردند.

آسیب‌پذیری‌های حیاتی

CVE-2020-0603، CVE-2020-0605، CVE-2020-0606 و CVE-2020-0646 چهار آسیب‌پذیری "حیاتی" از نوع "اجرای کد به‌صورت از راه دور" (Remote Code Execution) است که محصولات .NET و ASP.NET از آنها تأثیر می‌پذیرند. مهاجم قادر است تا با ارسال یا هدایت کاربر به یک فایل دستکاری شده و تشویق او به اجرا یا فراخوانی آن، کد دلخواه خود را بر روی دستگاه قربانی اجرا کند.

CVE-2020-0609 و CVE-2020-0610 دیگر آسیب‌پذیری‌های "حیاتی" وصله شده در این ماه هستند. بخش Remote Desktop Gateway - به اختصار RD Gateway - در سیستم عامل Windows از هر دوی این آسیب‌پذیری‌ها تأثیر می‌پذیرد. سوءاستفاده از CVE-2020-0609 و CVE-2020-0610 مهاجم را قادر به اجرای کد به‌صورت از راه دور بر روی دستگاه بدون نیاز به هر گونه دخالت قربانی می‌کند.

CVE-2020-0611 نیز ضعفی از نوع "از کارانداری سرویس" (Denial of Service) است که بهره‌جویی از آن موجب از کار افتادن خدمات‌دهی Remote Desktop Protocol - به اختصار RDP - می‌شود.

CVE-2020-0640 آخرین آسیب‌پذیری "حیاتی" ترمیم شده در این ماه است که مرورگر Internet Explorer از آن تأثیر می‌پذیرد. مهاجم با سوءاستفاده از این باگ و هدایت کاربر به یک صفحه اینترنتی حاوی بهره‌جوی آن، قادر به اجرای کد مورد نظر خود خواهد بود.

آسیب‌پذیری‌های بااهمیت

یکی از آسیب‌پذیری‌های "بااهمیت" ترمیم شده توسط اصلاحیه‌های ماه ژانویه ضعفی با شناسه CVE-2020-0601 است که توسط NSA (آژانس امنیت ملی آمریکا) کشف شده است. ضعف مذکور از نحوه مدیریت گواهینامه‌های Elliptic Curve Cryptography - به اختصار ECC - توسط بخش Windows CryptoAPI (در فایل Crypt32.dll) ناشی می‌شود. با بهره‌جویی از این آسیب‌پذیری می‌توان فایل مخرب بدافزار را در قالب یک کد امضا شده توسط شرکت‌های معتبر ارائه کرده، حملات موسوم به "مرد میانی" (Man-in-the-Middle) را اجرا نموده و اطلاعات رمزگذاری شده در بستر ارتباطات شبکه را رمزگشایی کرد. گرچه موردی از بهره‌جویی از این آسیب‌پذیری گزارش نشده اما با توجه به عمومی شدن جزییات آن نصب اصلاحیه در اولین فرصت توصیه می‌شود.

CVE-2020-0616 دیگر ضعف امنیتی "بااهمیت" برطرف شده در سیستم عامل Windows است که سوءاستفاده از آن منجر به رونویسی فایل‌های سیستمی و به‌صورت بالقوه از کارافتادن سرویس‌دهی محصول می‌شود.

سایر آسیب‌پذیری‌های "بااهمیت" این ماه به‌شرح زیر است:

CVE-2020-0654	CVE-2020-0602	CVE-2020-0607
CVE-2020-0608	CVE-2020-0612	CVE-2020-0613
CVE-2020-0614	CVE-2020-0615	CVE-2020-0617
CVE-2020-0620	CVE-2020-0621	CVE-2020-0622
CVE-2020-0623	CVE-2020-0624	CVE-2020-0625
CVE-2020-0626	CVE-2020-0627	CVE-2020-0628
CVE-2020-0629	CVE-2020-0630	CVE-2020-0631
CVE-2020-0632	CVE-2020-0633	CVE-2020-0634
CVE-2020-0635	CVE-2020-0636	CVE-2020-0637
CVE-2020-0638	CVE-2020-0639	CVE-2020-0641
CVE-2020-0642	CVE-2020-0643	CVE-2020-0644
CVE-2020-0647	CVE-2020-0650	CVE-2020-0651
CVE-2020-0652	CVE-2020-0653	CVE-2020-0656

لازم به ذکر است که با عرضه اصلاحیه‌های ماه ژانویه، پشتیبانی مایکروسافت از سیستم‌های عامل Windows 7 و Windows Server 2008/2008 R2 و عرضه عمومی اصلاحیه‌های امنیتی برای آنها توسط این شرکت پایان یافته است. لذا به تمامی راهبران شبکه توصیه می‌شود که در اسرع وقت اقدام به ارتقای دستگاه‌های با Windows 7 و Windows Server 2008 R2 خود به نسخه‌های جدیدتر و قابل پشتیبانی کنند.

اصلاحیه‌های امنیتی ادوبی
برای ماه میلادی ژانویه

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه، ۲۴ دی، شرکت ادوبی مجموعه اصلاحیه‌های امنیتی ماه میلادی ژانویه خود را منتشر کرد.

اصلاحیه‌های مذکور، در مجموع، ۹ ضعف امنیتی را در محصولات زیر ترمیم می‌کنند:

- Adobe Experience Manager
- Adobe Illustrator CC

ازمیان ۹ آسیب‌پذیری وصله شده، ٤ مورد که درجه اهمیت تمامی آنها "بااهیمت" (Important) اعلام شده، نرم‌افزار Experience Manager را تحت تأثیر قرار می‌دهند. بهره‌جویی از این ٤ آسیب‌پذیری، موجب نشت اطلاعات بالقوه حساس می‌شود.

همچنین نرم‌افزار Illustrator CC از ۵ ضعف امنیتی ترمیم شده توسط مجموعه اصلاحیه‌های ماه ژانویه تأثیر می‌پذیرد. بهره‌جویی از این آسیب‌پذیری‌ها که درجه اهمیت همه آنها "حیاتی" (Critical) گزارش شده، مهاجم را قادر به اجرای کد به‌صورت از راه دور بر روی دستگاه قربانی می‌کند.

نکته جالب اینکه در روالی غیرمعمول، این ماه اصلاحیه‌ای برای Flash Player و مجموعه نرم‌افزارهای Acrobat / Reader ارائه نشده است.

اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه ژانویه سال 2020 ادوبی در لینک‌های زیر قابل مطالعه است:

- https://helpx.adobe.com/security/products/experience-manager/apsb20-01.html
- https://helpx.adobe.com/security/products/illustrator/apsb20-03.html

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

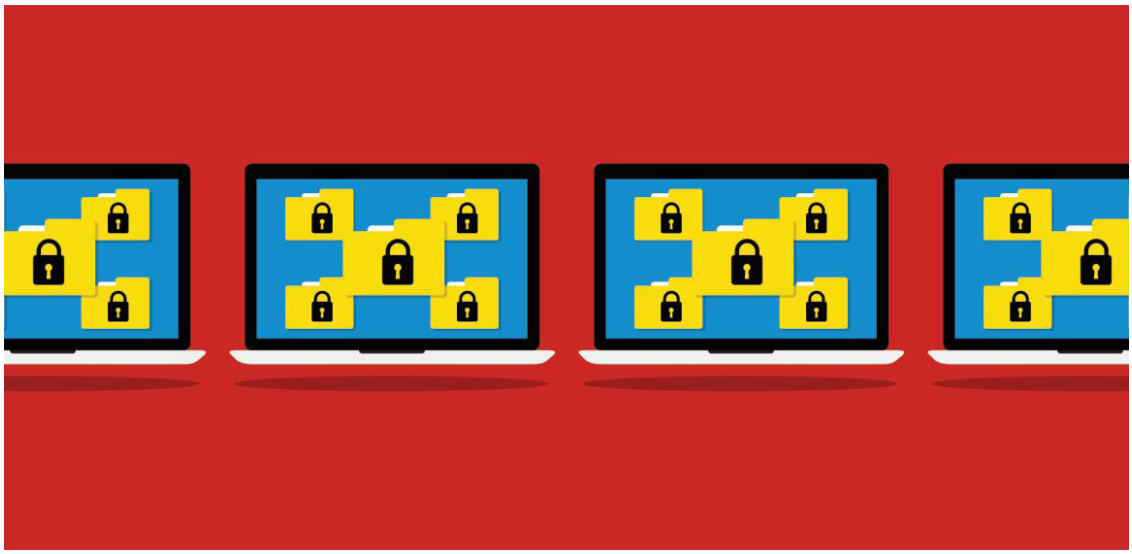
شرکت گوگل نیز با عرضه نسخه 79.0.3945.79 مرورگر Chrome اقدام به ترمیم ۳۷ آسیب‌پذیری امنیتی در این مرورگر کرد. جزییات بیشتر در خصوص آسیب‌پذیری‌های ترمیم شده در اینجا قابل دریافت است. همچنین این شرکت در ۲۷ آذر ماه نسخه 79.0.3945.86 را که در آن قابلیت‌های جدیدی به این مرورگر افزوده شده است منتشر کرد.

۲۲ آذر، بنیاد وردپرس نسخه 5.3 سامانه مدیریت محتوای WordPress را عرضه کرد. در نسخه مذکور ضعف‌هایی ترمیم شده که سوءاستفاده از برخی آنها به مهاجم امکان می‌دهد تا کنترل سایت تحت مدیریت این سامانه را به دست بگیرد. اطلاعات بیشتر در این مورد در اینجا قابل مطالعه است.

۲۸ آذر نیز بنیاد دروپل، باگ‌هایی را در برخی از نسخه‌های Drupal اصلاح کرد که بهره‌جویی از آنها، مهاجم را قادر به در اختیار گرفتن کنترل سیستم با نسخه آسیب‌پذیر این محصول می‌کند. توضیحات کامل در این خصوص در اینجا، اینجا، اینجا و اینجا قابل دسترس است.

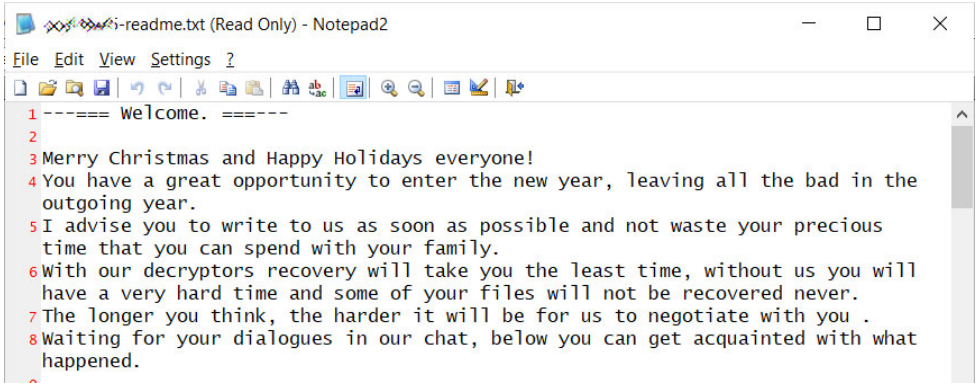
گـزارش‌هـا

تخفیف‌های پرزرق‌وبرق
گردانندگان باج‌افزار



مدتهاست که برنامه‌نویسی و توزیع باج‌افزار به کسب‌وکاری مدرن برای مهاجمان سایبری تبدیل شده است. از ارائه سرویس‌های باج‌افزار به‌عنوان خدمت گرفته تا مشارکت با نویسندگان بدافزارهای دیگر. جای تعجب ندارد که گردانندگان باج‌افزار نیز در مناسبت‌هایی همچون کریسمس و ایام سال نوی میلادی حضوری پررنگ داشته باشند!

برای مثال، نویسندگان باج‌افزار Sodinokibi - که با نام REvil نیز شناخته می‌شود - عبارت "کریسمس مبارک و تعطیلات، خوش" را در ابتدای اطلاعیه باج‌گیری (Ransom Note) خود درج کرده‌اند. در ادامه آن نیز به قربانی توصیه کرده‌اند که بجای داشتن استرس و نگرانی در تعطیلات، با پرداخت مبلغ اخاذی‌شده، پایان‌بخش اتفاقات بد در سال ۲۰۱۹ و آغازگر خوبی و شادی در سال میلادی جدید باشد!



به گزارش شرکت مهندسی شبکه گستر، در نمونه‌ای دیگر گردانندگان باج‌افزار Maze از تخفیف ۲۵ درصدی برای قربانیانی که در فاصله ۲۵ تا ۳۱ دسامبر اقدام به پرداخت باج می‌کردند خبر داده بودند.

Maze از جمله باج‌افزارهایی است که ضمن رمزگذاری فایل‌ها، اقدام به سرقت اطلاعات حساس از روی دستگاه می‌کند. در سال گذشته میلادی، مهاجمان Maze در حمله‌ای باج‌افزاری به شرکت Allied Universal، باجی ۲٫۳ میلیون دلاری را از آن شرکت طلب کردند. مدتی بعد و با تحقق نیافتن این خواسته مهاجمان، ۷۰۰ مگابایت از داده‌های Allied Universal در تالارهای گفتگوی اینترنتی نفوذگران منتشر و در دسترس قرار گرفته شد.

این افراد همچنین اعلام کرده‌اند که به مناسبت آغاز سال نوی میلادی ۵۰۰ هزار دلار به شهرداری پنساکولا تخفیف داده و از ادامه به‌اشتراک‌گذاری اسناد خصوصی آنها نیز صرف‌نظر می‌کنند. در اواخر سال میلادی گذشته دستگاه‌های شهرداری پنساکولا به نحوی بسیار گسترده آلوده به باج‌افزار Maze شد. مهاجمان Maze نیز در ازای آنچه که بازگردانی فایل‌های رمزگذاری شده توسط این باج‌افزار می‌خوانند ۱ میلیون دلار درخواست باج کردند. در پی برآورده نشدن این درخواست، ۲ گیگابایت فایل - که گفته می‌شود ٦ درصد از کل اطلاعات سرقت‌شده است - به‌صورت عمومی منتشر شد. با این حال علیرغم این تخفیف ۵۰ درصدی به نظر نمی‌رسد که مسئولان شهر پنساکولا حاضر به پرداخت باج باشند.

میزان مبلغ اخاذی شده توسط گردانندگان باج‌افزار نرخ مشخصی ندارد. شاید به همین خاطر است که در چند سال اخیر، عده‌ای در کسب‌وکاری جدید اقدام به میانجیگری و واسطه‌گری میان نویسندگان باج‌افزار و قربانیان این نوع بدافزارها می‌کنند.

آنچه مشخص است حملات باج‌افزاری، حداقل به این زودی‌ها پایانی ندارد. لذا، همچون همیشه بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها و مقاوم سازی پودمان RDP برای ایمن ماندن از گزند باج‌افزارها توصیه می‌شود.

برگزاری سمینار "باج‌افزارها؛ دیروز، امروز و فردا"
در دانشگاه تهران

شرکت مهندسی شبکه گستر و مرکز فناوری اطلاعات و فضای مجازی دانشگاه تهران، سمینار "باج‌افزارها؛ دیروز، امروز و فردا" را برگزار کردند.

روز یکشنبه، ۲۹ دی ماه در حالی این سمینار در سالن آمفی‌تئاتر دانشکده برق و کامپیوتر دانشگاه تهران برگزار شد که ارائه خدمات تأمین امنیت نقاط پایانی بزرگترین مرکز آموزش عالی کشور توسط شرکت مهندسی شبکه گستر در آستانه ورود به دهمین سال پیاپی خود قرار دارد.

در ابتدای سیمنار، ریاست محترم مرکز فناوری اطلاعات و فضای مجازی دانشگاه تهران، جناب آقای دکتر سید امید فاطمی به ارائه توضیحاتی در خصوص برنامه‌های آتی این مرکز در دانشگاه پرداختند.

در ادامه، کارشناسان شرکت مهندسی شبکه گستر، علاوه بر اشاره به اهمیت حفاظت از سیستم‌ها در برابر بدافزارها، انواع باج‌افزارها، روش‌های رمزنگاری و رمزگشایی فایل‌ها، راه‌های دریافت باج و نحوه انتشار جدیدترین باج‌افزارها را تحلیل و بررسی کردند و در نهایت روش ها و راهکارهای پیشگیری و مقابله با این نوع بدافزارها را مرور نمودند. همچنین در جریان این سمینار، چند نمونه از باج‌افزارهای مطرح مورد کالبدشکافی دقیق قرار گرفتند.

در پایان نیز، جلسه پرسش‌وپاسخ میان شرکت‌کنندگان و ارائه‌دهندگان برگزار شد و طی آن به سئوالات و ابهامات مطرح شده پاسخ داده شد.

در سال‌های اخیر تعداد باج‌افزارها رشد فزاینده‌ای داشته است. بر اساس آخرین گزارش منتشر شده توسط شرکت ضدویروس McAfee، تنها در سه‌ماهه اول سال ۲۰۱۹، بیش از ۷۰۰،۰۰۰ نمونه باج‌افزار منحصربه‌فرد جدید منتشر شده است. متأسفانه، تعداد قابل‌توجهی از سیستم‌های سازمان‌ها و شرکت‌های ایرانی نیز به دلیل عدم رعایت موارد امنیتی، هر روز به این نوع از بدافزارهای مخرب آلوده می‌شوند.

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.

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

شرکت مهندسی شبکه گستر

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

تلفن/دورنگار ۰۲۱-۴۲۰۵۲

رایانامه info@shabakeh.net

تارنمای شرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net