ماهنامه

امنیت فناوری اطلاعات

آبان 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 آبان ماه ۱۳۹۸ پرداخته شده است.

در آبان ماه، نسخه جدیدی از باج‌افزار MegaCortex منتشر شد که به رمزگذاری فایل‌های کاربر بسنده نکرده و با تغییر رمز عبور، امکان ورود به سیستم را نیز از او سلب می‌کند. این باج‌افزار که در جریان حملاتی هدفمند از طریق درب‌پشتی (Backdoor) ایجاد می‌شود، توسط بدافزارهایی همچون Emotet به دستگاه راه یافته و پس از آلوده کردن نخستین دستگاه در شبکه سازمان، خود را از طریق بسته‌های بهره‌جو (Exploit Kit) یا با بهره‌گیری از بستر Active Directory بر روی سایر سیستم‌های درون شبکه توزیع می‌کند. در این ماهنامه ضمن مرور عملکرد این باج‌افزار به بررسی باج‌افزار مخربی دیگر با عنوان Buran پرداخته شده که از ماه می سال میلادی جاری در قالب خدمات موسوم به "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) مورد استفاده مهاجمان قرار گرفته است.

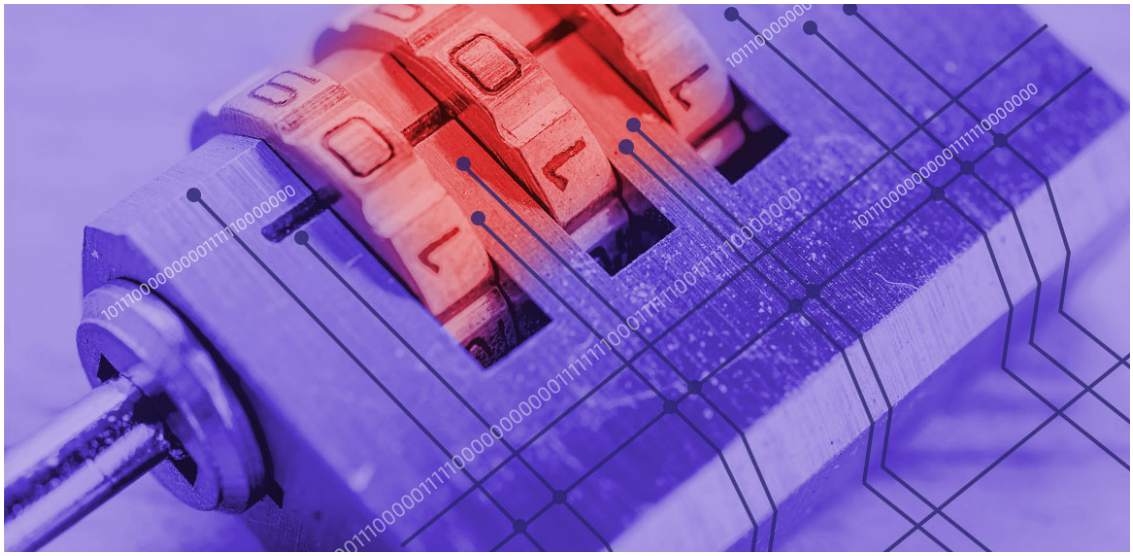
در ماهی که گذشت شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی نوامبر منتشر کرد. این اصلاحیه‌ها در مجموع، ۷۶ آسیب‌پذیری را در سیستم عامل Windows و برخی دیگر از محصولات مایکروسافت ترمیم می‌کنند. درجه اهمیت ۱۳ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical) و ۶۳ مورد "بااهمیت" (Important) اعلام شده است. علاوه بر مایکروسافت، شرکت‌های گوگل، جونیپر نت‌ورکز، موزیلا، اپل، سیسکو، ادوبی و وی‌اِم‌وِر و گروه سامبا نیز در آبان ماه اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند که جزییات آنها به همراه چند آسیب‌پذیری افشا شده دیگر در این ماهنامه قابل مطالعه است.

بر اساس نظرسنجی انجام شده توسط شرکت بیت‌دیفندر، کوتاهی و کم‌دقتی کارکنان، اصلی‌ترین دغدغه سازمان‌ها در حوزه نشت و افشای اطلاعات است. بر طبق آمار استخراج شده، در سال‌های ۲۰۱۷ و ۲۰۱۸، عامل خطا و کوتاهی انسانی به‌ترتیب در ۲۰ و ۲۱ درصد حملات منجر به نشت اطلاعات، دخیل بوده است. این آمار در سال میلادی جاری نیز ۲۰ درصد گزارش شده است. مشروح این یافته‌ها را در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر 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

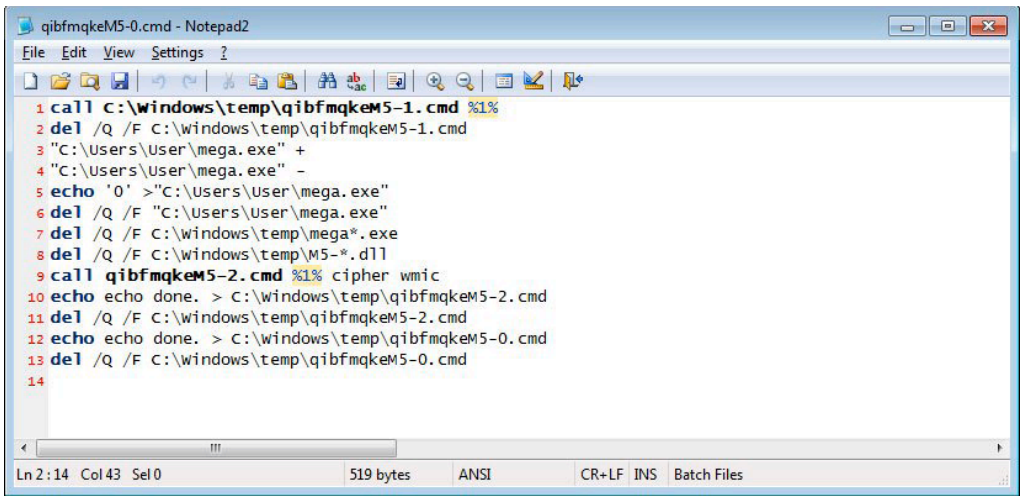
MegaCortex؛
باج‌افزاری متفاوت



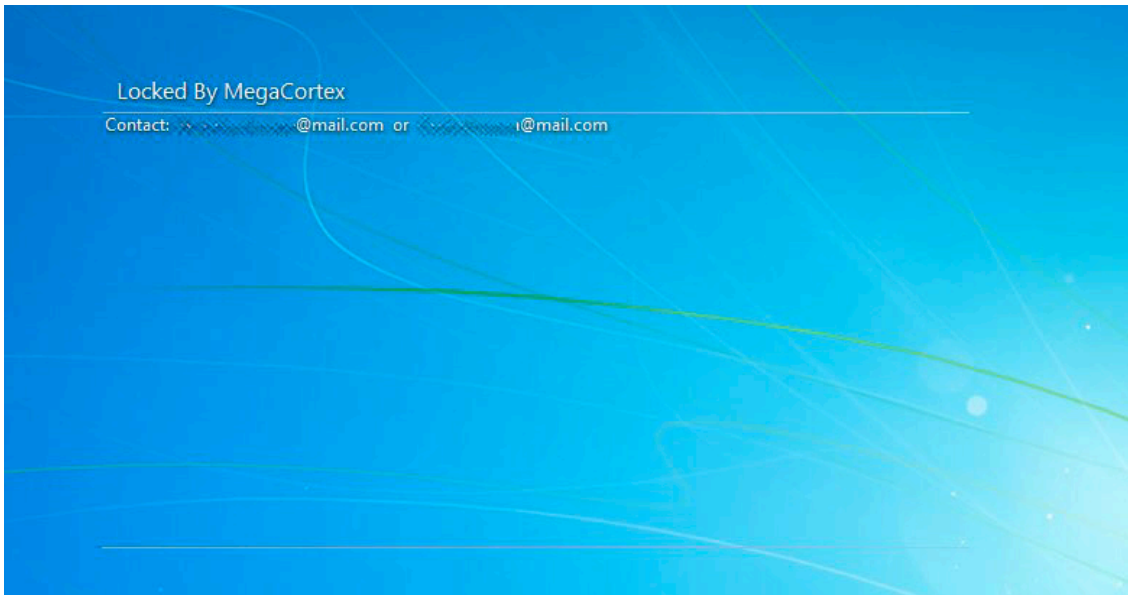
نسخه جدیدی از باج‌افزار MegaCortex در حال انتشار است که تنها به رمزگذاری فایل‌های کاربر بسنده نکرده و با تغییر رمز عبور، امکان ورود به سیستم را نیز از او سلب می‌کند.

به گزارش شرکت مهندسی شبکه گستر، MegaCortex باج‌افزاری است که در جریان حملاتی هدفمند از طریق درب‌پشتی (Backdoor) ایجاد شده، توسط بدافزارهایی همچون Emotet به دستگاه راه می‌یابد. MegaCortex پس از آلوده کردن نخستین دستگاه در شبکه سازمان، خود را از طریق بسته‌های بهره‌جو (Exploit Kit) یا با بهره‌گیری از بستر Active Directory بر روی سایر سیستم‌های درون شبکه توزیع می‌کند.

علاوه بر اجراکننده (Launcher) باج‌افزار، دو فایل DLL و چند اسکریپت CMD در اقدامات مخرب انجام شده توسط MegaCortex دخیل هستند. فایل اجراکننده با یک گواهینامه صادر شده برای شرکتی استرالیایی با نام MURSA PTY LTD امضاء شده است. از جمله وظایف اسکریپت‌های CMD مذکور نیز که نمونه‌ای از آن در تصویر زیر قابل مشاهده است حذف فایل‌های موسوم به Shadow Volume Copy و فایل‌های استفاده شده در جریان آلوده‌سازی است. فایل‌های DLL هم نه با تزریق شدن در پروسه‌های دیگر که از طریق پروسه معتبر Rundll32.exe اجرا می‌شوند.

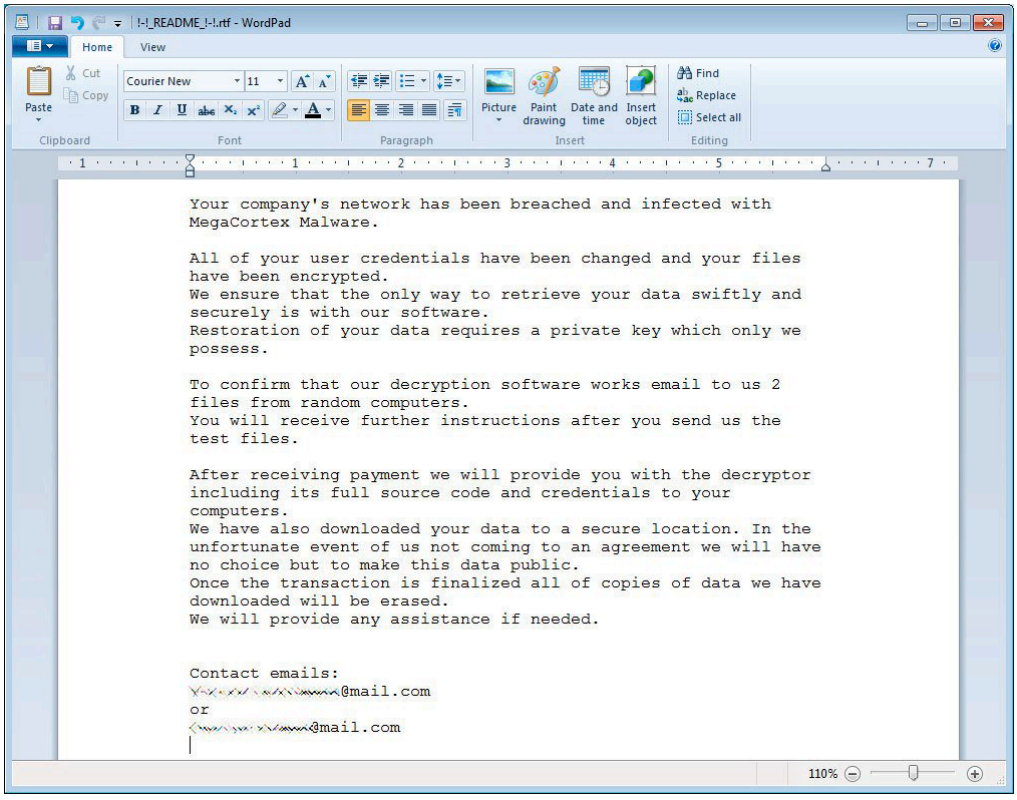


جدیدترین نسخه MegaCortex اما از جهاتی متفاوت از نسخه پیشین این باج‌افزار است. شاید بارزترین ویژگی در نسخه جدید نمایش پیامی مشابه تصویر پیش از ثبت ورود (Login) کاربر به سیستم عامل باشد.



با کالبدشکافی مشخص می‌شود که نسخه جدید MegaCortex اقدام به تغییر رمز عبور کاربری می‌کند که آلوده‌سازی با حق دسترسی او انجام شده است. احتمالاً به دلیل همین ویژگی منحصربه‌فرد مهاجمان تلاش دارند تا اطلاع‌رسانی به کاربر را در قبل از ثبت ورود او به سیستم انجام دهند.

همچنین در فایلی ظکه توسط باج‌افزار بر روی Desktop ایجاد می‌شود (شکل زیر) علاوه بر تغییر رمز عبور، ادعا شده که نسخه‌ای از اطلاعات کاربر در محلی به گفته این مهاجمان امن کپی شده و اگر کارها مطابق میل آنها پیش نرود آن اطلاعات به‌صورت عمومی افشا خواهند شد. ادعایی که به نظر می‌رسد صرفاً بلفی برای وادار کردن قربانی به پرداخت باج باشد.



نسخه جدید MegaCortex که به فایل‌های رمزگذاری شده پسوند m3g4c0rtx الصاق می‌کند با نام‌های زیر قابل شناسایی است:

Bitdefender:

- Trojan.GenericKD.32683279
- Trojan.GenericKD.32684232
- Trojan.GenericKD.32684234

McAfee:

- Artemis!174B579B9577
- Artemis!3C38CFCE2026
- Artemis!68E0D3F36228

Buran؛
نواده باج‌افزار VegaLocker

شرکت امنیتی مک‌آفی، جزییات خانواده جدیدی از باج‌افزارها با نام Buran را منتشر کرده که از ماه می سال میلادی جاری در قالب خدمات موسوم به "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) مورد استفاده مهاجمان قرار گرفته است.

در RaaS، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به متقاضی و بخشی دیگر به نویسنده می‌رسد. REVil، GandCrab و Phobos نمونه‌هایی از باج‌افزارهایی هستند که با سرویس RaaS با دیگر خرابکاران به اشتراک گذاشته شده یا همچنان می‌شوند. در حالی که در RaaS سهم دریافت شده توسط سازندگان باج‌افزار از توزیع‌کنندگان معمولاً چیزی بین ۳۰ تا ۴۰ درصد مبلغ اخاذی شده است این سهم در Buran تنها ۲۵ درصد گزارش شده است. ضمن اینکه در صورت ضمانت دریافت‌کننده خدمات از انتشار گسترده آن، حتی این سهم نیز قابل مذاکره اعلام شده است!

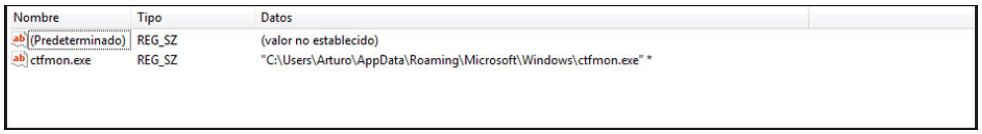
متن زیر نمونه‌ای از تبلیغ سرویس RaaS باج‌افزار Buran در یکی از تالارهای گفتگوی اینترنتی (Forum) تبهکاران سایبری است.

Buran is a stable offline cryptoclocker, with flexible functionality and support 24/7.
Functional:
Reliable cryptographic algorithm using global and session keys + random file keys;
Scan all local drives and all available network paths;
High speed: a separate stream works for each disk and network path;
Skipping Windows system directories and browser directories;
Decryptor generation based on an encrypted file;
Correct work on all OSs from Windows XP, Server 2003 to the latest;
The locker has no dependencies, does not use third-party libraries, only mathematics and vinapi;
The completion of some processes to free open files (optional, negotiated);
The ability to encrypt files without changing extensions (optional);
Removing recovery points + cleaning logs on a dedicated server (optional);
Standard options: tapping, startup, self-deletion (optional);
Installed protection against launch in the CIS segment.
Conditions:
They are negotiated individually for each advert depending on volumes and material.
Start earning with us!

گرچه در این توضیحات اشاره شده که باج‌افزار با تمامی نگارش‌ها از سیستم عامل Windows سازگار است اما بررسی‌های انجام شده توسط محققان مک‌آفی نشان می‌دهد که حداقل نسخه‌های فعلی Buran از نگارش‌های قدیمی همچون XP پشتیبانی نمی‌کنند.

همچنین در تبلیغ مذکور اشاره شده که Buran بر روی کشورهای عضو اتحادیه مشترک‌المنافع (جمهوری آذربایجان، ارمنستان، ازبکستان، بلاروس، تاجیکستان، روسیه، قرقیزستان، قزاقستان و مولداوی) اجرا نمی‌شود. اما تحقیقات صورت پذیرفته توسط مک‌آفی از آن حکایت دارد که روسیه، بلاروس و اوکراین تنها کشورهایی هستند که باج‌افزار از دست‌درازی به سیستم‌های آنها خودداری می‌کند. توانایی تشخیص این کشورها قابلیتی است که در بسیاری از باج‌افزارهای با اصالت روسی به چشم می‌خورد؛ با این هدف که گرفتار قوانین مشترک بین این کشورها نشوند.

Buran که به زبان برنامه‌نویسی Delphi نوشته شده با ایجاد کلیدی در محضرخانه (Registry) موجب اجرای خودکار خود در هر بار راه‌اندازی شدن سیستم حتی در حالت Safe Mode می‌شود.



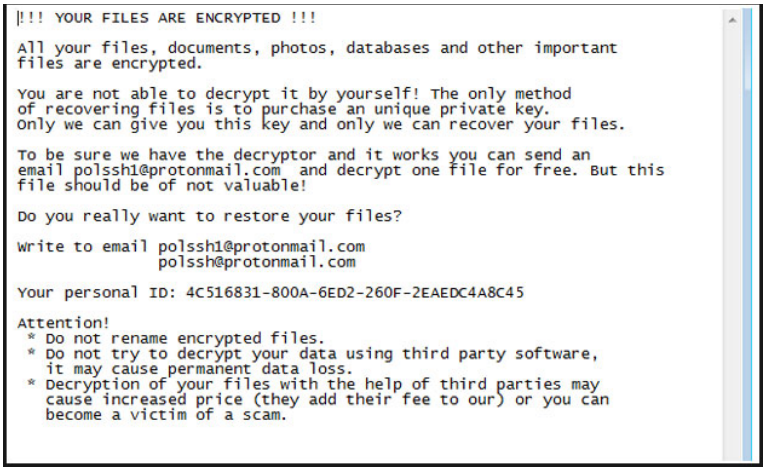
پوشه‌های نمایش داده شده در تصویر زیر از دست‌درازی‌های Buran مصون خواهند ماند:

\windows media player	**:\$windows.~bt**	**\windows nt**	**:\nvidia**
\apple computer\safari	\application data\	\windowspowershell\	\all users\
\windows photo viewer	\google\chrome\	\windows journal\	\appdata\
\windows portable devices	\mozilla firefox\	\windows sidebar\	\boot\
\windows security	\opera software\	\package cache\	\google\
\embedded lockdown manager	\tor browser\	\microsoft help\	\mozilla\
\reference assemblies	\common files\	:\recycler	\opera\
:\windows.old	\internet explorer\	:\windows\	\msbuild\
:\inetpub\logs	\windows defender\	c:\windows\	\microsoft\
:\$recycle.bin	\windows mail\	:\intel\	

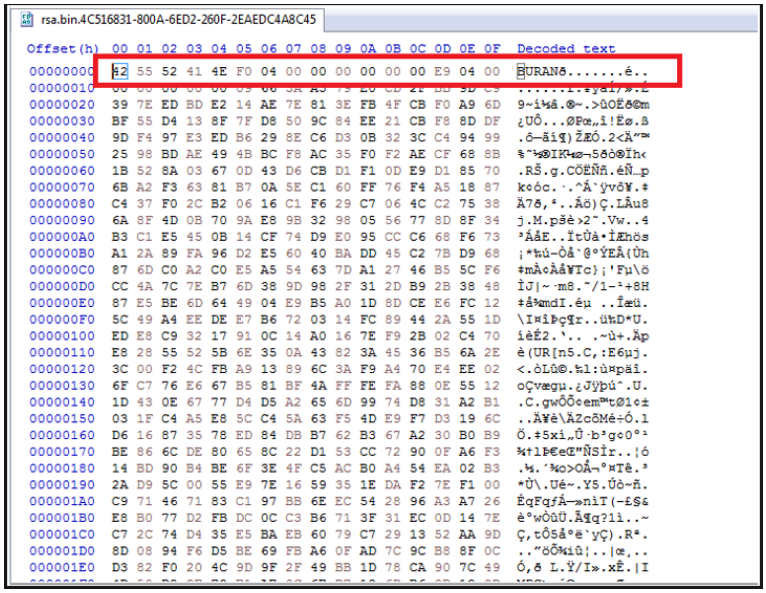
و همینطور فایل‌های زیر:

!!! your files are encrypted !!!.txt	**master.exe**
boot.ini	master.dat
bootfont.bin	ntldr
bootsect.bak	ntuser.dat
defender.exe	ntuser.ini
desktop.ini	temp.txt
iconcache.db	thumbs.db
ntdetect.com	unlock.exe
ntuser.dat.log	master.exe
unlocker.exe	master.dat

نمونه‌ای از اطلاعیه باج‌گیری (Ransomware) در تصویر زیر قابل مشاهده است.



Buran به کد هر فایل رمزگذاری شده، برچسبی که نمونه‌ای از آن در تصویر زیر نمایش داده شده را اضافه می‌کند.



بررسی‌های محققان مک‌آفی نشان می‌دهد که از زمان پیدایش Buran حداقل دو نسخه از آن ارائه شده و نسخه دوم به‌نحو چشم‌گیری در مقایسه با نسخه اول تکامل یافته است.

مک‌آفی، Buran را برگرفته شده از کد باج‌افزار Jumper که در مارس ۲۰۱۹ عرضه شد می‌داند. Jumper خود نیز مبتنی بر باج‌افزار VegaLocker است که در اوایل سال میلادی جاری شناسایی شد.

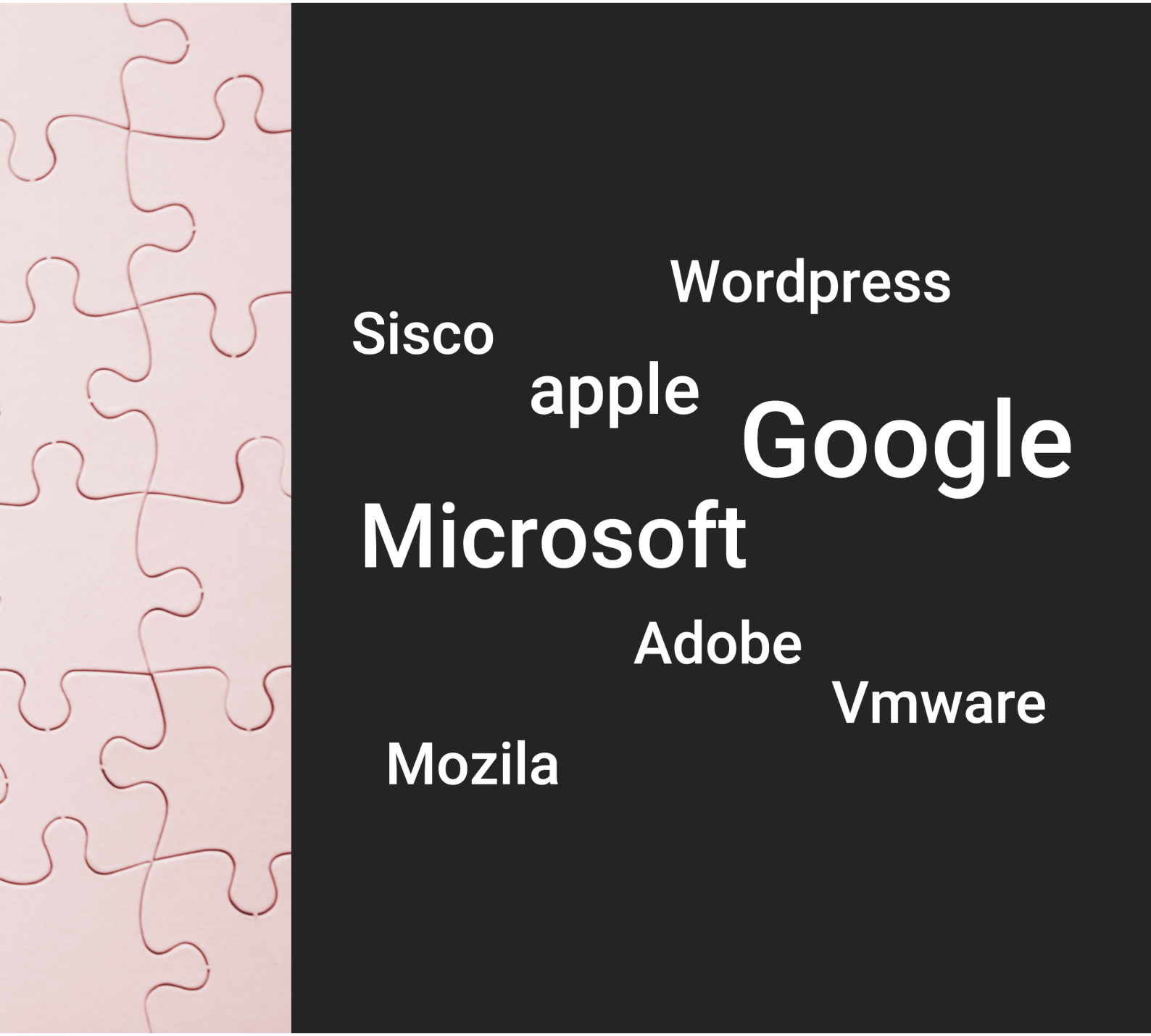
Year	Malware family
February – 2019	VegaLocker
March – 2019	Jumper
May – 2019	Buran

لازم به ذکر است حداقل برخی نمونه‌ها از Buran از طریق بسته بهره‌جوی Rig منتشر شده‌اند. این بسته بهره‌جو از آسیب‌پذیری‌هایی همچون CVE-2018-15982 در نرم‌افزار Flash Player و CVE-2018-8174 در مرورگر Internet Explorer سوءاستفاده می‌کند.

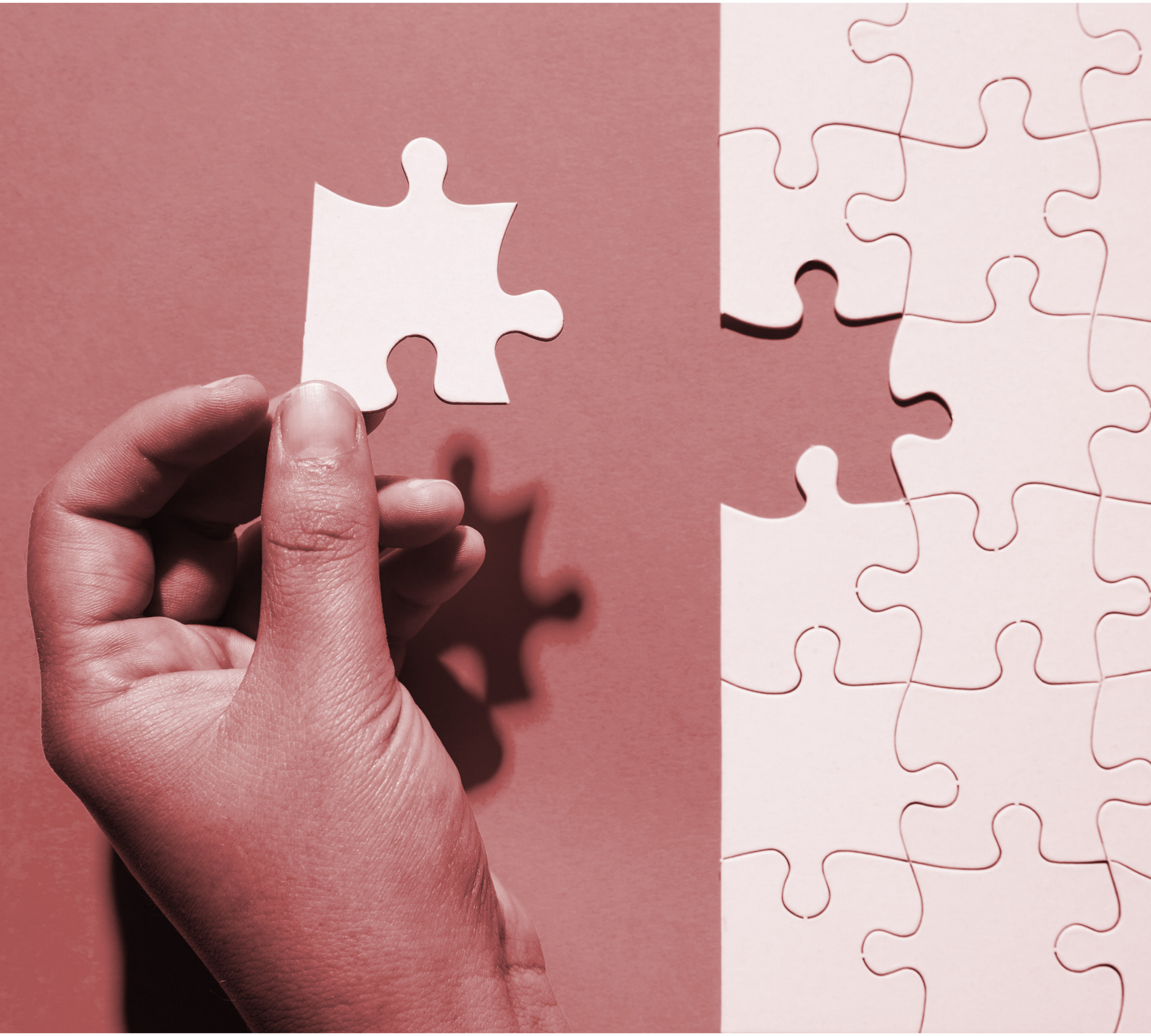
نسخه‌های بررسی شده در گزارش McAfee با نام‌های زیر قابل شناسایی می‌باشند:

- RDN/Ransom
- Ransomware-GOS!E60E767E33AC
- Ransom
- RDN/Ransom
- RDN/Generic.cf
- Ransom-Buran!

مشروح گزارش McAfee در اینجا قابل دریافت و مطالعه است.


Wordpress
Sisco
apple
Google
Microsoft
Adobe
Vmware
Mozila

آسیب‌پذیری‌ها
و اصلاحیه‌های امنیتی



اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی نوامبر

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه ۲۱ آبان، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی نوامبر منتشر کرد. این اصلاحیه‌ها در مجموع، ۷۶ آسیب‌پذیری را در سیستم عامل Windows و برخی دیگر از محصولات مایکروسافت ترمیم می‌کنند. درجه اهمیت ۱۳ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical) و ۶۳ 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 ترمیم‌شده

از جمله آسیب‌پذیری‌های حیاتی ترمیم شده در این ماه، ضعفی با شناسه CVE-2019-1429 در مرورگر Internet Explorer است که از مدتی پیش حداقل توسط یک گروه از مهاجمان مورد بهره‌جویی قرار گرفته است. سوءاستفاده از این آسیب‌پذیری مهاجم را قادر به اجرای کد بر روی دستگاه قربانی به‌صورت از راه دور و بدون نیاز به دخالت کاربر می‌کند. هدایت قربانی به صفحه اینترنتی حاوی بهره‌جوی (Exploit) آسیب‌پذیری مذکور و در ادامه آلوده شدن دستگاه به‌محض فراخوانی صفحه در Internet Explorer از جمله سناریوهای احتمالی بکارگیری CVE-2019-1429 برای آلوده‌سازی دستگاه‌ها به بدافزار بدون نیاز به هر گونه دخالت کاربر است. ضمن اینکه این امکان فراهم است که با تزریق یک افزونه ActiveX در یک سند تحت مجموعه نرم‌افزاری Office و ارسال آن به کاربر و تشویق او به اجرای آن، کاربر به سایتی مخرب هدایت و از آنجا بهره‌جویی انجام شود. با توجه به مورد بهره‌جویی قرار گرفتن این آسیب‌پذیری، نصب اصلاحیه آن در اولین فرصت به تمامی کاربران و راهبران شبکه توصیه می گردد.

CVE-2019-0721، CVE-2019-1389، CVE-2019-1397 و CVE-2019-1398 دیگر آسیب‌پذیری‌های حیاتی این ماه هستند که بستر مجازی‌سازی Hyper-V از آنها تأثیر می‌پذیرد. سوءاستفاده از ضعف‌های مذکور نیز مهاجم را قادر به اجرای کد به‌صورت از راه دور بر روی ماشین میزبانی شده در بستر مجازی می‌کند.

سایر اصلاحیه‌های حیاتی این ماه عبارتند از:

CVE-2019-1373 CVE-2019-1419 CVE-2019-1426 CVE-2019-1427 CVE-2019-1428 CVE-2019-1430

CVE-2019-1441 CVE-2019-1390

آسیب‌پذیری‌های بااهمیت وصله‌شده

در میان آسیب‌پذیری‌های "بااهمیت" ترمیم شده در این ماه، CVE-2019-1020 بیش از سایر موارد جلب توجه می‌کند. بهره‌جویی از این آسیب‌پذیری مهاجم را قادر به عبور از سد پروسه موسوم به Secure Boot در سیستم عامل Windows می‌کند.

همچنین در این ماه، یک آسیب‌پذیری با شناسه CVE-2019-1457 در مجموعه نرم‌افزاری Microsoft Office for Mac ترمیم شده است. جزییات وجود این ضعف امنیتی پیش‌تر به‌صورت عمومی افشا شده بود. بهره‌جویی از این آسیب‌پذیری سبب می‌شود که در شرایطی خاص حتی در صورت فعال بودن گزینه Disable all macros without notification، ماکروی بالقوه مخرب بدون هر گونه اعلان به کاربر بر روی دستگاه به اجرا درآید.

CVE-2018-12207 CVE-2019-0712 CVE-2019-11135 CVE-2019-1234 CVE-2019-1309 CVE-2019-1310

CVE-2019-1324 CVE-2019-1370 CVE-2019-1374 CVE-2019-1379 CVE-2019-1380 CVE-2019-1381

CVE-2019-1382 CVE-2019-1383 CVE-2019-1384 CVE-2019-1385 CVE-2019-1388 CVE-2019-1391

CVE-2019-1392 CVE-2019-1393 CVE-2019-1394 CVE-2019-1395 CVE-2019-1396 CVE-2019-1399

CVE-2019-1402 CVE-2019-1405 CVE-2019-1406 CVE-2019-1407 CVE-2019-1408 CVE-2019-1409

CVE-2019-1411 CVE-2019-1412 CVE-2019-1413 CVE-2019-1415 CVE-2019-1416 CVE-2019-1417

CVE-2019-1418 CVE-2019-1420 CVE-2019-1422 CVE-2019-1423 CVE-2019-1424 CVE-2019-1425

CVE-2019-1432 CVE-2019-1433 CVE-2019-1434 CVE-2019-1435 CVE-2019-1436 CVE-2019-1437

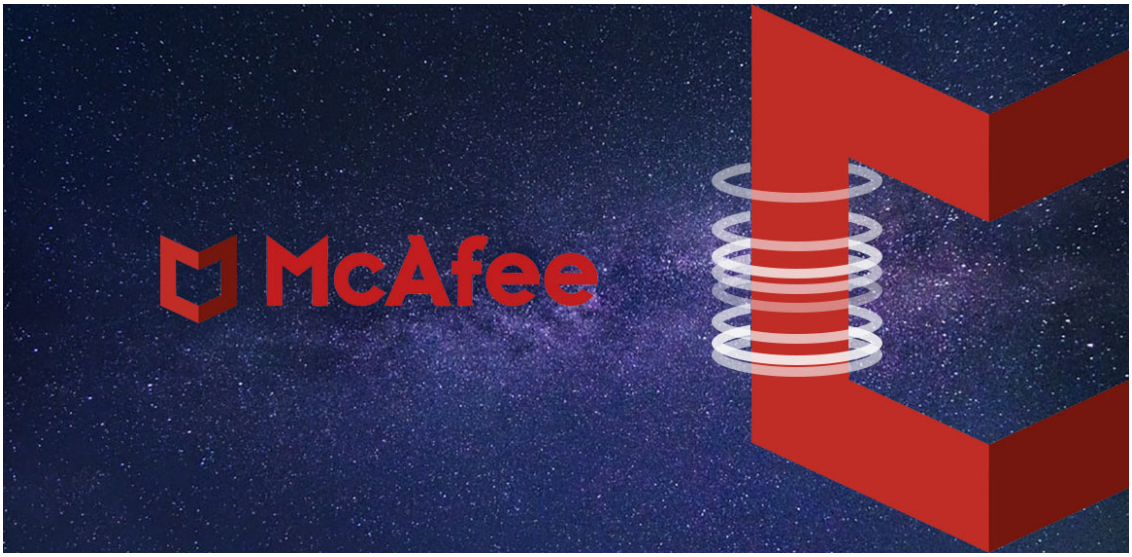
CVE-2019-1438 CVE-2019-1439 CVE-2019-1440 CVE-2019-1442 CVE-2019-1443 CVE-2019-1445

CVE-2019-1446 CVE-2019-1447 CVE-2019-1448 CVE-2019-1449 CVE-2019-1456 CVE-2019-0721

CVE-2019-1373

یادآوری می‌شود شرکت مایکروسافت پشتیبانی از این دو سیستم عامل را کمتر از سه ماه دیگر پایان خواهد داد و از ۲۵ دی به بعد، هیچ اصلاحیه امنیتی و پشتیبانی فنی برای سیستم‌های عامل Windows 7 و Windows Server 2008 R2 ارائه نخواهد شد. لذا به تمامی راهبران شبکه توصیه می‌شود که در فرصت باقی مانده اقدام به ارتقای دستگاه‌های با Windows 7 و Windows Server 2008 R2 خود به نسخه‌های جدیدتر و قابل پشتیبانی کنند.

آسیب‌پذیری CVE-2019-3648
و محصولات مک‌آفی



شرکت مک‌آفی یک آسیب‌پذیری امنیتی با درجه اهمیت "متوسط" (Medium)، به شناسه CVE-2019-3648 را ترمیم کرد. این آسیب‌پذیری که ضعفی از نوع "ترفیع امتیازی" (Privilege Escalation) است و از بخش Microsoft Windows Client مورد استفاده در برخی از محصولات مک‌آفی ناشی می‌شود مهاجم با سطح دسترسی Administrator را در شرایطی خاص قادر به اجرای کد با سطح دسترسی SYSTEM می‌کند.

نرم‌افزارهای زیر از آسیب‌پذیری مذکور تأثیر می‌پذیرند:

- McAfee Total Protection (MTP)
- McAfee Anti-Virus Plus (AVP)
- McAfee Internet Security (MIS)

لازم به ذکر است که این نرم‌افزارها همگی در دسته محصولات خانگی مک‌آفی قرار داشته و وجود آسیب‌پذیری مذکور در هیچ یک از محصولات سازمانی این شرکت گزارش نشده است.

بر طبق اعلام شرکت مک‌آفی، آسیب‌پذیری CVE-2019-3648 در آخرین نسخه این محصولات برطرف شده و کاربران آن‌ها می‌توانند با ارتقای محصولات مورد استفاده از ایمن بودن در برابر این آسیب‌پذیری اطمینان حاصل کنند.

توضیحات بیشتر در مورد این آسیب پذیری در اینجا قابل دریافت است.

اصلاحیه‌های عرضه شده
در آبان ۱۳۹۸

در آبان ماه علاوه بر مایکروسافت، شرکت‌های گوگل، جونیپر نت‌ورکز، موزیلا، اپل، سیسکو، ادوبی و وی‌اِم‌وِر و گروه سامبا اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

در اولین روز از آبان ماه ۱۳۹۸، شرکت موزیلا، با ارائه به‌روزرسانی، چندین آسیب‌پذیری را در مرورگر Firefox و نرم‌افزار مدیریت ایمیل Thunderbird برطرف کرد. سوءاستفاده از برخی از ضعف‌های مذکور به مهاجم امکان می‌دهد تا به‌صورت از راه دور اقدام به اجرای کد مخرب بر روی دستگاه آسیب‌پذیر کند. جزییات بیشتر در اینجا، اینجا و اینجا قابل مطالعه است.

جونیپر نت‌ورکز دیگر شرکتی بود که در همین تاریخ با ارائه به‌روزرسانی یک ضعف امنیتی را در تجهیزات ساخت این شرکت ترمیم کرد. سوءاستفاده از ضعف مذکور مهاجم را قادر به ارتقای سطح دسترسی خود بر روی دستگاه آسیب‌پذیر می‌کند. جزییات بیشتر در اینجا قابل دریافت است.

به گزارش شرکت مهندسی شبکه گستر، ۶ آبان، گروه سامبا با عرضه به‌روزرسانی امنیتی، ضعفی را در نرم‌افزار کدباز Samba برطرف کرد. سوءاستفاده از ضعف ترمیم شده مهاجم را قادر به دست یافتن به داده‌های بالقوه حساس می‌کند. توضیحات بیشتر در خصوص این به‌روزرسانی در اینجا، اینجا و اینجا قابل دسترس است.

در ماهی که گذشت، شرکت اپل نیز با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در سیستم‌های عامل macOS، WatchOS، iOS و tvOS و مرورگر Safari ترمیم و اصلاح کرد. سوءاستفاده از برخی از این ضعف‌ها که جزییات آنها در لینک‌های زیر قابل دریافت است امکان در اختیار گرفتن کنترل سیستم را برای مهاجم فراهم می‌کند:

- https://support.apple.com/en-us/HT210722
- https://support.apple.com/en-us/HT210724
- https://support.apple.com/en-us/HT201222
- https://support.apple.com/en-us/HT210725
- https://support.apple.com/en-us/HT210721
- https://support.apple.com/en-us/HT201222
- https://support.apple.com/en-us/HT210723

در آبان ماه، سیسکو در چندین نوبت اقدام به انتشار به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ۴۳ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۱ مورد از این آسیب‌پذیری‌ها "حیاتی" و ۱۵ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون اجرای کد به‌صورت از راه دور و عبور از سد تنظیمات امنیتی، از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید است. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در اینجا قابل دسترس است.

مایکروسافت، سه‌شنبه ۲۱ آبان اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی نوامبر منتشر کرد که پیش‌تر در این خبر به تفصیل به آنها پرداخته شد.

در همین تاریخ، ادوبی نیز اقدام به عرضه به‌روزرسانی‌های امنیتی برای محصولات Animate، Illustrator، Media Encoder و Bridge کرد که جزییات آنها در لینک‌های زیر قابل مطالعه است:

- https://helpx.adobe.com/security/products/animate/apsb19-34.html
- https://helpx.adobe.com/security/products/illustrator/apsb19-36.html
- https://helpx.adobe.com/security/products/media-encoder/apsb19-52.html
- https://helpx.adobe.com/security/products/bridge/apsb19-53.html

در آبان ماه شرکت گوگل در سه 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 آبان انتشار یافت 78.0.3904.108 است. فهرست اشکالات مرتفع شده در این نسخه نیز در اینجا قابل دریافت و مشاهده است.

وی‌اِم‌وِر دیگر شرکتی بود که در آبان ۱۳۹۸ اقدام به انتشار به‌روزرسانی برای محصولات خود کرد. محصولات ESXi، Workstation و Fusion از آسیب‌پذیری‌های ترمیم شده توسط این به‌روزرسانی‌ها تأثیر می‌پذیرند. اطلاعات بیشتر در مورد به‌روزرسانی‌های عرضه شده در لینک‌های زیر قابل مطالعه است:

- https://www.vmware.com/security/advisories/VMSA-2019-0020.html
- https://www.vmware.com/security/advisories/VMSA-2019-0021.html

مدیران سایت‌های مبتنی بر WordPress
مراقب باشند

به مدیران و صاحبان سایت‌های مبتنی بر WordPress توصیه می‌شود که در صورت استفاده از افزونه Jetpack، در اسرع وقت نسبت به نصب به‌روزرسانی حیاتی این افزونه اقدام کنند.

به گزارش شرکت مهندسی شبکه گستر، Jetpack، افزونه‌ای پرطرفدار است که قابلیت‌هایی همچون تهیه نسخه پشتیبان، ثبت ورود امن، پویش بدافزار و حفاظت در برابر حملات سعی و خطا (Brute-force) را به رایگان برای مدیران سایت‌های مبتنی بر WordPress فراهم می‌آورد.

گفته می‌شود که این افزونه بیش از ۵ میلیون نصب فعال دارد.

بر اساس اعلام عمومی Automattic، شرکت توسعه‌دهنده Jetpack، تمامی نسخه‌های این افزونه که بعد از جولای ۲۰۱۷ عرضه شده‌اند به ضعفی با درجه اهمیت حیاتی (Critical) آسیب‌پذیر هستند. ضعف مذکور که از نحوه پردازش بخشی از کدهای مورد استفاده در این افزونه ناشی می‌شود در نسخه 7.9.1 ترمیم و اصلاح شده است.

گرچه بهره‌جویی از این آسیب‌پذیری تا کنون گزارش نشده اما با توجه به اعلام عمومی آن، احتمال می‌رود که به‌زودی مهاجمان برای سوءاستفاده از آن و رخنه به سایت‌های مجهز به Jetpack دست به کار شوند.

ضمن فراهم بودن قابلیت به‌روزرسانی Jetpack از طریق پیشخوان سامانه WordPress، نصب دستی نسخه جدید 7.9.1 امکان‌پذیر است.

جزییات بیشتر در خصوص آسیب‌پذیری Jetpack و به‌روزرسانی‌های مربوطه در اینجا قابل دریافت و مطالعه است.

گـزارش‌هـا

قصور کارکنان،
اصلی‌ترین تهدید در نشت اطلاعات

بر اساس نظرسنجی انجام شده توسط شرکت بیت‌دیفندر، کوتاهی و کم‌دقتی کارکنان، اصلی‌ترین دغدغه سازمان‌ها در حوزه نشت و افشای اطلاعات است. بر طبق آمار استخراج شده، در سال‌های ۲۰۱۷ و ۲۰۱۸، عامل خطا و کوتاهی انسانی به‌ترتیب در ۲۰ و ۲۱ درصد حملات منجر به نشت اطلاعات، دخیل بوده است. این آمار در سال میلادی جاری نیز ۲۰ درصد گزارش شده است.

به گزارش شرکت مهندسی شبکه گستر، "کوتاهی کارکنان" یا Employee Negligence که در نظرسنجی بیت‌دیفندر به آن اشاره شده، روش‌های مختلف اجرای حمله از جمله حملات مبتنی بر فیشینگ و اجرای بدافزار با دخالت کاربر (با بهره‌گیری از تکنیک‌های مهندسی اجتماعی) را شامل می شود. صرف‌نظر از تکنیک مورد استفاده مهاجم، آموزش کاربران و آگاهی‌رسانی به آنها در خصوص تهدیدات سایبری مؤثرترین راهکار در خنثی کردن و مقابله با این گونه حملات است.

بدافزارها با ۱۷ درصد دومین عامل تأثیرگذار در نشت اطلاعات در سال ۲۰۱۹ گزارش شده است.

همچنین نتایج این نظرسنجی نشان می‌دهد مکانیزم مطلع شدن از ۱۵ درصد از نشت‌های اطلاعات در سال ۲۰۱۹، تحلیل ترافیک مشکوک شبکه‌ای بوده است. کشف اقدامات مشکوک بر اساس رویدادهای ثبت شده توسط محصولات دیواره آتش، خرابی سیستم‌های داده، اختلال در زیرساخت کسب‌وکار و ممیزی امنیتی توسط ارزیابان خارج سازمانی، دیگر عامل مؤثر در اطلاع سازمان از درز شدن اطلاعات سازمان عنوان شده است.

در این نظرسنجی که نتایج با عنوان The Hacked Off در اینجا قابل دریافت و مطالعه است بیش از ٦ هزار متخصص و فعال امنیت اطلاعات از کشورهای انگلیس، آمریکا، استرالیا، نیوزلند، آلمان، فرانسه، ایتالیا و اسپانیا شرکت داشته‌اند.

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