بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره بیست و دوم

تیر ماه ۱۳۹۹

وصله آسیب‌پذیری بحرانی ویندوز سرور پس از ۱۷ سال!

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:
مرکز تخصصـــی آپـا دانشگـاه رازی

صفحه آرایی: **سید احسان حسینی**

سردبیران:
سیده مرضیه حسینی
صبا آزرمی

با همکاری
سیده آرزو حسنی

آدرس:
کرمانشـــاه، باغ ابریشـــم، دانشـــگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

۰۸۳۳۴۳۴۳۲۵۱ apa@razi.ac.ir
@APARazi cert.razi.ac.ir

اخبار امنیتی

آلوده شدن سیستم‌های ویندوزی توسط بدافزار Try2Cry

اخیراً بخش جدیدی از باج‌افزار معروف به Try2Cry شناسایی شده است که درایوهای فلش USB و shortcutهای ویندوز (فایل‌های LNK) را آلوده کرده تا از این طریق سایر سیستم‌های ویندوزی را نیز آلوده کند.

این باج افزار توسط یک محقق به نام Karsten Hahn هنگام تجزیه و تحلیل یک بدافزار ناشناس کشف شد.

Try2Cry از الگوریتم Rijndael استفاده می‌کند و رمز عبور را به صورت هش شده رمزگذاری می‌کند. این کلید رمزگذاری شده، با محاسبه هش SHA512 رمز عبور و با استفاده از 32 بیت اول این هش ایجاد می‌شود.

باج‌افزار Try2Cry، چندین نوع فایل از جمله doc.، ppt.، jpg.، xls.، pdf.، docx.، pptx.، xls. و xlsx. را هدف قرار داده و پسوند Try2Cry. را به تمام فایل‌های رمزگذاری شده اضافه می‌کند.

فایل‌های قربانیان با استفاده از الگوریتم رمزنگاری کلید متقارن Rijndael و یک کلید رمزنگاری hardcoded، رمزگذاری می‌شوند.

این کارشناس متوجه شد که باج‌افزار Try2Cry، سیستم‌هایی را با نام‌های DESKTOP-PQ6NSM4 و IK-PC2 رمزگذاری نمی‌کند که گفته می‌شود نام دستگاه‌های توسعه‌دهنده بدافزار است و برای تست و آزمایش این بدافزار مورد استفاده قرار گرفته است.

توسعه دهنده Try2Cry همچنین یک failsafe را درون کد باج‌افزار طراحی کرده است که به منظور جستجوی رمزنگاری روی سیستم‌های آلوده با نام‌های DESKTOP-PQ6NSM4 یا IK-PC2 طراحی شده است.

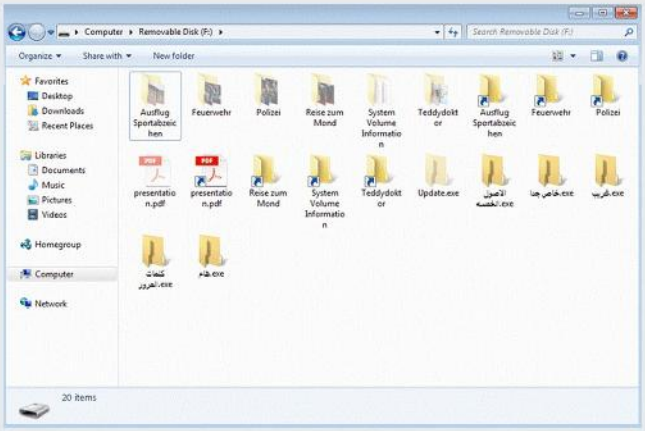
Try2Cry قادر به انتشار در سایر دستگاه‌های قربانی از طریق درایوهای فلش USB نخواهد بود.

باج‌افزار مذکور از تکنیکی استفاده می‌کند که شبیه به روشی است که توسط باج‌افزار Spora و بدافزارهای Spora، Dinihou و یا Gamaruc استفاده می‌شود. بدین صورت که درایوهای قابل جابجایی متصل به دستگاه در معرض خطر را جستجو می‌کند سپس یک نسخه از خود با نام Update.exe را در فولدر root مربوط به درایو فلش یافته شده ذخیره می‌کند.

در مرحله بعدی، باج‌افزار تمام فایل‌های موجود در این درایو را مخفی می‌کند و آنها را با shortcutهای ویندوز (فایل‌های LNK) با همان آیکون جایگزین

می‌کند. به محض کلیـــک بر روی لینک‌ها، فایل اصلی به همراه پی‌لود باج‌افزار Update.exe Try2Cry در پس زمینه باز می‌شود.

این باج‌افزار همچنین با استفاده از آیکون پیش‌فرض فولدر ویندوز و نام‌های عربی با هدف فریب قربانیان برای کلیک بر روی آنها، نسخه‌های قابل رؤیت خود را بر روی درایوهای USB ایجاد می‌کند.



خبر خوب این است که مانند سایر انواع باج‌افزارهای Stupid، قربانیان Try2Cry نیز می‌توانند فایل‌های خود را به صورت رایگان رمزگشایی کنند.

منبع خبر :

https://bit.ly/3iAYdiv

Scan Link

آلوده شـدن دسـتگاه‌های اندرویـدی به بدافزارهـای غیرقابل حذف

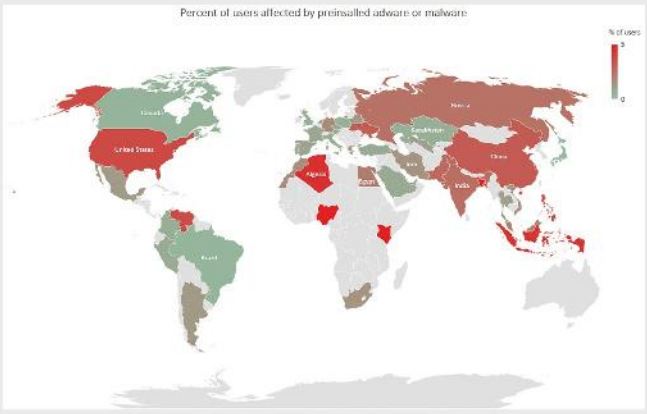
محققان مشاهده کردند که 14.8درصد از کاربران اندرویدی توسط انواع بدافزارها و یا تبلیغات[1] که هنوز در system partition دستگاه باقی مانده است، مورد حمله قرار گرفته‌اند.

بدافزارهای Lezok و Triada، رایج‌ترین بدافزارها در دستگاه‌های اندرویدی هستند؛ آن‌ها مستقیماً در کتابخانه کلیدی "libandroid_runtime" تعبیه شده‌اند و توســط هر اپلیکیشن مورد استفاده قرار می‌گیرند.

به گفته محققان، آلودگی موجود در system partition، خطر زیادی را برای کاربران دستگاه‌های آلوده ایجاد می‌کند؛ زیرا با وجود آن، راه‌حل‌های امنیتی دیگر امکان دسترسی به دایرکتوری‌های سیستم را نداشته و این بدان معناست که نمی‌توانند فایل‌های مخرب را حذف کنند. دو استراتژی اصلی این بدافزارها عبارتند از:

- این بدافزارها می‌توانند دسترسی root را بدست آورده و بدافزارهای تبلیغاتی را در system partition نصب کنند.
- گفتنی است کد نمایش تبلیغات یا loader آن، حتی پیش از آنکه به دست مصرف کننده نهایی برسد، وارد firmware دستگاه می‌شود.

عمدتاً بین 1 تا 5 درصد از کاربران اندروید از جمله کاربران ایرانی، تحت تأثیر این بدافزارها قرار گرفته‌اند که این مقدار در موارد شدید حتی به 27 درصد نیز می‌رسد.



درصد کاربران مناطق مختلف که تحت تأثیر این بدافزارها قرار گرفته‌اند

طیف گسترده‌ای از تهدیدات مشاهده شده

تروجانِ Agent در پشت رابط کاربری گرافیکی[2] یا تنظیمات سیستم پنهان شـــده و پی‌لود[3] مربوط به اجرای فایلهای دلخواه را در دستگاه مستقر می‌کند. در مرحله بعدی، تروجانِ Sivu به عنوان یک اپلیکیشن HTMLViewer خود را معرفی می‌کند که دارای دو ماژول است؛ یکی از ماژول‌ها از دسترسی root برای اعلان‌ها یا notifications استفاده می‌کند و ماژول دیگر درب پشتی[4] است که امکان کنترل از راه دور تلفن‌های هوشمند را فراهم می‌کند.

تبلیغات Plague نوع دیگری است که خود را به عنوان سرویس‌های Android معرفی کرده و اپلیکیشن‌هایی جهت نمایش اعلان‌های تبلیغاتی بر روی دستگاه قربانی نصـب می‌کند.

Trojan Agent.pa به عنوان اپلیکیشنِ CIT TEST، جهت اجرای اپلیکیشن‌ها، باز کردن URLها، دانلود و اجرای فایل‌های دلخواه DEX، نصب یا حذف اپلیکیشن‌ها، نمایش اعلان ها و شروع سرویس‌ها، با سرور C&C ارتباط برقرار می‌کند.

Penguin، Necro، Facmod، Guerrilla، Virtualinst، Secreted از دیگر بدافزارهایی هستند که غالبا در partition سیستم قرار می‌گیرند.

براساس اظهارات Kaspersky، برخی گوشی‌های هوشمند دارای ماژول‌های تبلیغاتی آلوده‌ای هستند که از پیش توسط خود تولیدکنندگان نصب شده‌اند. برخی از فروشندگان به صراحت اعتراف می‌کنند که تبلیغات را تلفن‌های هوشمند خود تعبیه کرده‌اند! برخـــی از آن‌ها این امکان را دارند که غیرفعال شوند، در حالی که برخی دیگر از آن‌ها، این امکان را ندارند.

به کاربران توصیه می‌شود که در هنگام خرید، مدل گوشی خود با دقت بیشتری انتخاب کنند و این خطر را نادیده نگیرند.

---

[1] adware
[2] GUI
[3] در امنیت سایبری payload، بسته‌ای از داده‌هاست که توسط یک بدافزار و از طریق ابزار یا شبکه‌های آسیب‌دیده، منتقل می‌شود.
[4] backdoor

منبع خبر :

https://gbhackers.com/undeletable-adware/

Scan Link

حذف 106 افزونه مخرب کروم از طرف گوگل

گوگل در پاسخ به گزارش‌هایی مبنی بر اینکه از افزونه‌ها برای سرقت اطلاعات حساس کاربران استفاده شده است، 106 افزونه‌ی مرورگر کروم را از Chrome Web Store حذف کرد. در این تحقیق، که نتایج آن اخیراً منتشر شده است، Awake Security ادعا کرد میلیون‌ها کاربر کروم توسط مهاجمان، مورد هدف قرار گرفته‌اند. مهاجمـــــان از افزونه‌های مرورگر کروم گوگل نه تنها برای سرقت داده، بلکه برای ایجاد بستری پایدار در شبکه‌های قربانیان نیز استفاده کرده‌اند. این افزونه‌های مخرب برای مرورگر رایگان بودند و برای هشدار به کاربران در مورد وب‌سایت‌های مشکوک یا فشرده‌سازی فایل‌ها طراحی شده بودند. به طور کلی، Awake Security تخمین می‌زند که این افزونه‌ها 32 میلیون بار دانلود شده‌اند.

یکی از سخنگوهای گوگل، در بیانیه‌ای اعلام کرد: "ما از افزونه‌های موجـــــود در Web Store که خط‌مشی‌های ما را نقض کرده‌اند، خبردار شده و اقدامات لازم را در این انجام داده‌ایم. همچنین از این افزونه‌ها به عنوان نمونه‌هایی آموزشی، در جهت ارتقای تحلیل خودکار و دستی خود استفاده می‌کنیم."

در حالی که گوگل مدت زمان طولانی است که Web Store کروم را برای افزونه‌های مخرب مرورگر کنترل می‌کند، آنچه که در مورد این دسته افزونه اخیر منحصر به فرد بود، این است که ادعا می‌شد بخشی از یک همکاری و "کمپین نظارت گسترده جهانی" است. محققان گوگل همچنین ادعا می‌کنند که این کمپین توسط ثبت‌کننده‌ی دامنه‌ی اینترنـــت، CommuniGal Communication Ltd. (GalComm)، پشتیبانی شده است.

به گفته محققان، ثبت‌کننده دامنه به مجرمان اجازه داده‌است تا از چند لایه‌ی امنیتی، حتی در سازمان‌های پیشرفته و با سرمایه‌گذاری‌های قابل توجه در امنیت سایبری، عبور کنند. تنها در سه ماه گذشته، 111 افزونه‌ی مخرب یا جعلی کروم که از دامنه‌های Galcomm برای زیرساخت‌های فرماندهی و کنترل مهاجم و یا به عنوان صفحات بارکننده بـرای افزونه‌ها استفاده کرده‌بودند، جمع‌آوری شده‌اند. این افزونه‌ها می‌توانند از صفحه عکس بگیرند، کلیپ‌بورد را بخوانند، توکن‌های معتبر ذخیره‌شده در کوکی‌ها یا پارامترهـــا را جمع‌آوری کنند، ضربه‌های کاربر بر صفحه‌کلید (مانند گذرواژه‌ها) را بگیرند و غیره."

بنیان‌گذار و محقق ارشد Awake Security، در تفسیر فنی این تهدید نوشت: "از میان 26079 دامنه قابل دسترسی که از طریق Galcomm ثبت شدند، تعداد 15160 دامنه مخرب یا مشکوک به میزبانی از تعداد زیادی بدافزارهای سنتی یا ابزارهای پایش بر اساس مرورگر هستند. با استفاده از روش‌های دور زدن مختلف، این دامنه‌ها از شناسایی شدن به عنوان دامنه‌های مخرب توسط بسیاری از راهکارهای امنیتی فرار کرده که این امر باعث شد این کمپین ناشناس باقی بماند. در ماه فوریه، Duo Security یک کمپین مشابه را کشف کرده است که 500 افزونه‌ی مرورگر گوگل کروم به طور مخفیانه داده‌های خصوصی کاربران را سرقت کرده و قربانیان را به وب‌سایت‌های دارای بدافزار راهنمایی می‌کردند.

منبع خبر :

https://bit.ly/392l6XO

Scan Link

اخبار کوتاه

آسیب پذیری خطرناک ویندوز سرور پس از ۱۷ سال پچ شد

محققان امنیتی به شرکت‌ها هشدار داده‌اند تا ویندوز سرور را به روز کرده و از شبکه‌های خود در برابر آسیب‌پذیری خطرناکی که 17 سال است در کدهای این سیستم‌عامل پنهان شده محافظت کنند. آسیب‌پذیری مورد بحث که با کد CVE-2020-1350 شناسایی می‌شود، در سیستم امتیازدهی آسیب‌پذیری عام (CVSS)، امتیاز 10.0 یا بسیار خطرناک را دریافت کرده و در آپدیت امنیتی جدید مایکروسافت که رفع شده است.

هکرها با سواستفاده از این حفره می‌توانند کوئری‌های مخرب DNS را در سرورهای ویندوز DNS ایجاد کرده و به طور کامل به زیرساخت شبکه نفوذ کنند. این آسیب پذیری در تمام نسخه‌های ویندوز سرور از سال 2003 تا 2019 وجود دارد. هکرها به واسطه این حفره کنترل سرور را به دست گرفته و توانایی دستکاری ایمیل‌ها و ترافیک شبکه، از دسترس خارج کردن سرویس‌ها، سرقت نام کاربری و رمز عبور کاربران و غیره را پیدا می کنند. در حال حاضر مشخص نیست وسعت سواستفاده از این آسیب‌پذیری تا چه حد است، اما به مدت 17 سال در کدهای مایکروسافت پنهان شده بوده و به گفته شرکت امنیتی Check Point احتمال دارد در این بازه از آن سواستفاده شده باشد.

آسیب پذیری

وصلـه آسـیب‌پذیری بحرانـی ویندوز سرور پـس از 17

محققان امنیتی به شرکت‌ها هشدار داده‌اند تا ویندوز سرور را به روز کرده و از شبکه‌های خود در برابر آسیب‌پذیری خطرناکی که 17 سال است در کدهای این سیستم عامل پنهان شده محافظت کنند.

این آسیب‌پذیریِ بسیار خطرناک با نام SigRed و شناسه "CVE-2020-1350" توسط محققان امنیتی شرکت Check Point کشف شده است و در سیستم امتیازدهی آسیب پذیری عام (CVSS) امتیاز 10 را دریافت کرده است.

آسیب‌پذیری مذکور که از نوع اجرای کد از راه دور در Domain Name System (DNS) ویندوز سرورها می‌باشد، زمانی به وجود می‌آید که DNS ویندوز نتواند به درستی درخواست‌ها را رسیدگی کند. مهاجمی که با موفقیت این آسیب‌پذیری را اکسپلویت نماید، می‌تواند درخواست‌های مخرب را به Windows DNS server ارسال و کد دلخواه را در Context مربوط به Local System Account اجرا کند. ویندوز سرورهایی که به عنوان DNS سرور پیکربندی شده‌اند در معرض خطر این آسیب‌پذیری خطرناک هستند.

بروزرسانی جدید مایکروسافت، با رسیدگی به درخواست DNS سرورهای ویندوز، آسیب‌پذیری مذکور را مورد بررسی قرار داده و رفع می‌کند.

مهاجمان با اکسپلویت آسیب‌پذیری SigRed می‌توانند کوئری‌های مخرب DNS را در DNS سرورهای ویندوز ایجاد کنند و به طور کامل به زیرساخت شبکه نفوذ کرده و کنترل سرور را به دست گیرند؛ همچنین این امکان برای مهاجمان فراهم می‌شود تا ایمیل‌ها و ترافیک شبکه را دستکاری کنند، نام کاربری و رمز عبور کاربران را به سرقت ببرند و سرویس‌ها را از دسترس خارج نمایند.

این آسیب‌پذیری می‌تواند کار خود را به واسطه پی‌لود HTTP از پیش گیرد که این کار را از طریق ارسال آن به DNS سرور هدف در پورت 53 انجام خواهد داد که موجب می‌شود تا Windows DNS Server پی‌لود را طوری تفسیر کند که گویی یک DNS query است.

لیست محصولات تحت تأثیر این آسیب‌پذیری در ادامه آورده شده است، همانطور که ملاحظه می‌کنید این آسیب‌پذیری در تمام نسخه‌های ویندوز سرور از سال 2003 تا 2019 وجود دارد.

گفتنی است کاربران می‌توانند جهت دانلود بروزرسانی‌های منتشر شده هر یک از این محصولات، به لینک زیر مراجعه کنند.

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1350

- Windows Server 2019
- (Server Core installation) Windows Server 2019
- (Server Core installation) Windows Server, version 1909
- (Server Core installation) Windows Server, version 1903
- (Server Core installation) Windows Server, version 2004
- Windows Server 2016
- (Server Core installation) Windows Server 2016
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2012
- (Server Core installation) Windows Server 2012
- Windows Server 2012 R2
- (Server Core installation) Windows Server 2012 R2

شایان ذکر است که شدت آسیب‌پذیری کلیه محصولات مذکور، "بحرانی" می‌باشد و در برابر حمله اجرای کد از راه دور آسیب‌پذیر هستند.

اصلاح رجیستری[1] زیر نیز به عنوان راه‌حل این آسیب‌پذیری شناسایی شده است، به توصیه محققان Check Point، حداکثر طول یک پیام DNS را بر روی 0xFF00 تنظیم کنید (بیش از TCP)، چراکه این عمل، آسیب‌پذیری را برطرف می‌سازد.

```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters"
/v "TcpReceivePacketSize" /t REG_DWORD /d 0xFF00 /f
net stop DNS && net start DNS
```

✓ در پایان، لازم است سرویس DNS مجدداً راه‌اندازی[2] شود.

این آسیب‌پذیری را اکسپلویت نماید، می‌تواند درخواست‌های مخرب را به Windows DNS server ارسال و کد دلخواه را در Context مربوط به Local System Account اجرا کند. ویندوز سرورهایی که به عنوان DNS سرور پس از اعمال وصله امنیتی منتشر شده، ادمین می‌تواند مقدار TcpReceivePacketSize و داده‌های متناظر با آن را حذف کند، به طوری که سایر موارد HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters، مانند قبل باقی بمانند.

سوالات متداول در خصوص این آسیب‌پذیری

- **باتوجه به آن که رتبه این آسیب‌پذیری 10 می‌باشد، تا چه اندازه می‌تواند مشکل‌ساز شود؟**

این آسیب‌پذیری از طرف شرکت مایکروسافت به عنوان یک آسیب‌پذیری Wormable[3] در نظر گرفته شده است، به این معنا که می‌تواند از طریق بدافزارها، بین کامپیوترهای آسیب‌پذیر و بدون رابط کاربری[4] گسترش پیدا کرده و به طور کامل شبکه را آلوده کند. DNS به عنوان یک مؤلفه شبکه، معولاً بر روی Domain Controllerها نصب می‌شود بنابراین این تهدید می‌تواند منجر به وقفه قابل توجهی در سرویس شده و حساب‌های دامنه سطح بالا را به خطر بیاندازد.

- **آیا DNS سرورهای غیر از مایکروسافت نیز تحت تأثیر این آسیب‌پذیری قرار خواهند گرفت؟**

این آسیب‌پذیری ناشی از یک نقص درDNS سرور مایکروسافت است که در سطح پروتکل نمی‌باشد، پس می‌توان نتیجه گرفت که بر روی DNS سرورهای غیر از مایکروسافت تأثیر نخواهد گذاشت.

- **در چه شرایطی می‌توان از راه‌حل کلید رجیستری استفاده کرد؟**

مایکروسافت به تمام کاربرانی که DNS سرور را اجرا می‌کنند توصیه می‌کند که در اسرع وقت بروزرسانی امنیتی را بر روی سیستم‌های خود نصب کنند. با این حال، اگر نمی‌توانید بلافاصله وصله امنیتی را اعمال کنید، مایکروسافت توصیه می‌کند به محض دسترسی، راه‌حل اصلاح رجیستری را اعمال کرده تا از سیستم خود، پیش از نصب بروزرسانی، محافظت کنید.

- **آیا کلاینتِ DNS ویندوز تحت تأثیر این آسیب‌پذیری قرار خواهد گرفت؟**

خیر؛ این آسیب‌پذیری فقط بر روی Microsoft's Windows DNS Server تأثیر خواهد گذاشت، بنابراین کلاینت DNS ویندوزها تحت تأثیر این آسیب‌پذیری قرار نخواهد گرفت.

منبع خبر :

https://bit.ly/3j7bmQn

Scan Link

[1] registry modification
[2] restart
[3] توانایی گسترش کرمی
[4] user interaction

مجموعه آسیب‌پذیری‌های کتابخانه Treck

آزمایشگاه تحقیقاتی JSOF مجموعه‌ای از آسیب‌پذیری‌های روز صفر را در یک کتابخانه نرم‌افزاری سطح پایین TCP/IP توسعه داده شده توسط Treck Inc، که بسیار نیز مورد استفاده قرار می‌گیرد کشف کرده است. 19 آسیب‌پذیری با نام Ripple20، صدها میلیون دستگاه (یا بیشتر) را تحت تاثیر قرار داده است و شامل چندین آسیب‌پذیری اجرای کد از راه دور می‌باشد. از جمله خطرات این آسیب‌پذیری‌ها می توان به سرقت داده‌ها از یک پرینتر، اختلال در عملکرد دستگاه‌های کنترل صنعتی، حمله انکار سرویس(DoS) و افشای اطلاعات اشاره کرد. یک مهاجم می‌تواند سال‌ها کد مخرب را در دستگاه‌های جداسازی‌شده پنهان کند. یکی از این آسیب‌پذیری‌ها می‌تواند ورود به مرزهای شبکه را از خارج فعال کند.

نرم‌افزار شبکه‌ای Treck IP Stack برای انواع مختلف سیستم‌ها طراحی و ساخته شده است، این نرم‌افزار شامل چندین آسیب‌پذیری است که اکثر آن‌ها به دلیل نقص‌های موجود در مدیریت حافظه می‌باشند. گستردگی کاربرد این نرم افزار در بخش‌های مختلف که برخی از آنها در شکل زیر اشاره شده است، نگرانی‌ها را در بین فعالان امنیت سایبری بالا برده است.

حوزه‌های کاربردی که کتابخانه آسیب پذیر Treck stack در آنها به کار می‌رود

توضیحات فنی

Ripple20 مجموعه‌ای از 19 آسیب‌پذیری است که در Treck TCP/IP stack کشف شده‌اند که چهار مورد از آن‌ها دارای امتیاز CVSS بیش از 9 هستند و از طریق اجرای کد دلخواه از راه دور فعال می‌شوند. یکی از آسیب‌پذیری‌های مهم، نقص در پروتکل DNS می‌باشد که ممکن است از طریق اینترنت و توسط یک مهاجم ساختگی، خارج از مرزهای شبکه، حتی در دستگاه‌هایی که به اینترنت متصل نیستند، اکسپلویت شود.

دومین Whitepaper که به دنبال BlackHat USA2020 منتشر می‌شود، جزئیات اکسپلویت آسیب‌پذیریِ CVE-2020-11901، یعنی نقص DNS بر روی یک دستگاه Schneider Electric APC UPS را ارائه می‌دهد. 15 آسیب‌پذیری دیگر دارای CVSSهای 3.1 تا 8.2 می‌باشند که از طرق مختلف از جمله حمله انکار سرویس و اجرای کد دلخواه از راه دور، فعالیت خود را انجام می‌دهند.

بسیاری از این آسیب‌پذیری‌ها به دلیل داشتن قابلیت تغییر کد و پیکربندیStack، در اثر گذر زمان دارای چندین نوع مختلف می‌باشند؛ همچنین آسیب‌پذیری‌های Ripple20، به دلیل داشتن اثر زنجیره‌ای و آن که به مهاجمان اجازه می‌دهند NAT و فایروال‌ها را دور زده و بدون نیاز به دخالت هیچ کاربری کنترل دستگاه‌ها را به دست گیرند، در نوع خود منحصر به فرد می‌باشند.

شرح آسیب‌پذیری‌ها

در جدول زیر، اطلاعات مربوط به آسیب‌پذیری‌هایی که توسط JSOF به CERT / CC گزارش داده شد را مشاهده می‌کنید.

اطلاعات مربوط به هر یک از آسیب‌پذیری‌ها

CVE	CVSSv3	توضیحات	نسخه وصله شده
CVE-2020-11896	10	این آسیب‌پذیری کار خود را با ارسال بسته‌های ناقص IPv۴ به دستگاهی که از تونل IPv۴ پشتیبانی می‌کند، شروع کرده و بر روی هر دستگاهی که Treck را با پیکربندی خاصی اجرا می‌کند تاثیر می‌گذارد و همچنین امکان اجرای کد دلخواه از راه دور را برای مهاجم فراهم می‌آورد.	۳۰ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11897	۱۰	این آسیب‌پذیری با ارسال چندین بسته ناقص IPv۶ به یک دستگاه، شروع به کار می‌کند و با اجرای کد دلخواه از راه دور، بر روی تمامی نسخه‌های قدیمی Treck که IPv۶ را پشتیبانی می‌کنند، تأثیر می‌گذارد.	۴ژوئن ۲۰۰۹ نسخه 5.0.1.35
CVE-2020-11901	۹	این آسیب‌پذیری کار خود را پاسخ به درخواست DNS شروع می‌کند و بر هر دستگاهی که Treck را با پشتیبانی از DNS اجرا می‌کند تأثیر می‌گذارد. از این آسیب‌پذیری می‌توان جهت اجرای کد دلخواه از راه دور بر روی Schneider Electric APC UPS سوءاستفاده کرد و علیرغم انکه دارای CVSS۹,۰ است، اما از نظر ما در بین آسیب‌پذیری‌های مطرح شده، شدیدترین نوع آن‌ها به حساب می‌آید، به دلیل آنکه ممکن است درخواست‌های DNS از شبکه‌ای که دستگاه در آن قرار دارد، خارج شود و مهاجم بتواند از طریق حافظه نهان DNS و یا سایر روش‌ها جهت احاطه دستگاهی خارج از شبکه، از این آسیب‌پذیری سوءاستفاده کرده، به شبکه نفوذ کند و کنترل دستگاه را با دور زدن اقدامات امنیتی، در اختیار گیرد.	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11898	۹,۱	دستکاری نادرست پارامتر طول(CWE-130) در مؤلفه IPv4/ICMPv4 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان افشای اطلاعات حساس(CWE-200).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11900	۸,۲	امکان Double Free (CWE-۴۱۵) در مؤلفه IPv4 هنگام ارسال بسته توسط مهاجم شبکه.	۱۵ اکتبر ۲۰۱۴ نسخه 6.0.1.41
CVE-2020-11902	۷,۳	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه IPv6OverIp4 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان خواندن خارج از محدوده (CWE-125).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11904	۵,۶	امکان Overflow یا Wraparound در مؤلفه تخصیص حافظه (CWE-190) هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان نوشتن خارج از محدوده (CWE-787).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66

CVE-2020-11899	۵.۴	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه IPv6 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه، امکان خواندن خارج از محدوده (CWE-125) و امکان حمله انکار سرویس.	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11803	۵.۳	امکان خواندن خارج از محدوده (CWE-125) در مؤلفه DHCP هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان افشای اطلاعات حساس(CWE-200).	۱۰ اکتبر ۲۰۱۰ نسخه 6.0.1.28
CVE-2020-11905	۵.۳	امکان خواندن خارج از محدوده (CWE-125) در مؤلفه DHCPv6 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان افشای اطلاعات حساس(CWE-200).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11906	۵	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه Ethernet Link Layer از بسته‌ای که توسط یک کاربر غیر مجاز ارسال شده است و همچنین امکان Underflow (CWE-191)	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11907	۵	دستکاری نادرست پارامتر طول(CWE-130) در مؤلفه TCP از بسته‌ای که توسط یک کاربر غیر مجاز ارسال شده است و همچنین امکان Underflow (CWE-191)	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11909	۳.۷	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه IPv4 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان Underflow (CWE-191)	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11910	۳.۷	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه ICMPv4 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان خواندن خارج از محدوده (CWE-125).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11911	۳.۷	امکان کنترل دسترسی در مؤلفه ICMPv4 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و اختصاص مجوز درسترسی نادرست به منابع بحرانی(CWE-723).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11912	۳.۷	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه TCP هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان خواندن خارج از محدوده (CWE-125).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11913	۳.۷	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه IPv6 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان خواندن خارج از محدوده (CWE-125).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11914	۳.۱	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه ARP هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان خواندن خارج از محدوده (CWE-125).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11908	۳.۱	امکان Null Termination (CWE-۱۷۰) در مؤلفه DHCP هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان افشای اطلاعات حساس(CWE-200).	۱۱ اگوست ۲۰۰۷ نسخه 4.7.1.27

محصولات آسیب‌پذیر و تحت تأثیر

همانطور که در بخش‌های قبلی اشاره شد، این آسیب‌پذیری طیف گسترده‌ای از محصولات را شامل می‌شود. فهرستی از محصولات تحت تاثیر قرار گرفته بصورت دقیق و با تماس‌هایی که CISA ICS-CERT با تولیدکنندگان محصولات داشته است، تهیه شده است. بدیهی است این محصولات آسیب‌پذیر محدود به این لیست نمی‌باشد و ممکن است در آینده مورد بررسی مجدد قرار گیرد. جدول زیر نام شرکتهایی را نشـــان می‌دهد که وجود آسیب‌پذیری در محصولات خود را تایید کرده‌اند. در این فهرست نام شرکت‌های بزرگی چون Cisco، Intel، Caterpilar و HP به چشم می‌خورد.

فهرست شرکت‌هایی که وجود آسیب پذیری در محصولات خود را پذیرفته‌اند

STATUS: CONFIRMED (15)

B. Braun
Baxter
Caterpillar
Cisco (through Starent)
Digi
Green Hills
HCL Tech
HP
HPE
Intel
Maxlinear (through HLFN)
Rockwell
Sandia National Labs
Schneider Electric/APC
Teradici

تجهیزات شبکه سیسکو که در کشور ما ایران نیز مورد استفاده قرار می‌گیرند تحت تاثیر این آسیب‌پذیری قرار گرفته‌اند. با توجه به اهمیت موضوع در بخش بعدی وضعیت محصولات Cisco مورد بررسی قرار گرفته است. از دیگر محصولات مهم که بصورت گسترده در کشور ایران مورد استفاده قـــرار می‌گیرد، چاپگرهـــــای HP و Samsung می‌باشند که طبق اعلام شرکت سازنده، تحت تاثیر این آسیب¬پذیری بوده و توصیه اکید می‌گردد مدیران شبکه نسبت به نصب بروزرسانی‌ها اقدام نمایند. فهرست محصولات و نحوه بروزرسانی در پیوند زیر قابل دسترسی می باشد.

https://support.hp.com/us-en/document/c06640149

وضعیت محصولات Cisco

شرکت سیسکو در حال بررسی خط تولید خود می‌باشد تا مشخص کند که کدام یک از محصولاتش ممکن است تحت تأثیر این آسیبپذیری‌ها قرار گیرند که پس از بررسی‌های صورت گرفته، به هر یک از محصولات تحت تأثیر، یک شناسه نقص[1] سیسکو اختصاص داده شد. این نقص‌ها از طریق Cisco Bug Search Tool قابل دسترسی بوده و حاوی اطلاعات تکمیلی از جمله راه‌حل‌ها[2] (در صورت وجود) و نسخه‌های وصله شده نرم‌افزار می‌باشد. شایان ذکر است هر محصول یا سرویسی که در لیست محصولاتِ تحت تأثیر یا آسیب‌پذیر ذکر نشده باشد، آسیب‌پذیر تلقی نخواهد شد، اما از آنجا که بررسی‌ها کماکان در حال انجام می‌باشد، لذا ممکن است محصولاتی که در حال حاضر آسیب‌پذیر در نظر گرفته نشده‌اند، متعاقباً در لیست محصولات آسیب‌پذیر قرار گیرند.

محصولات زیر نیز، در حال بررسی می‌باشند تا مشخص شود که آیا آن‌ها نیز تحت تأثیر این آسیب‌پذیری قرار دارند یا خیر.

- Cisco ASR 5000 Series Routers
- Cisco Home Node-B Gateway
- Cisco IP Services Gateway (IPSG)
- Cisco PDSN/HA Packet Data Serving Node and Home Agent

در جدول زیر لیستی از محصولات آسیب‌پذیر شرکت سیسکو را ملاحظه می‌کنید. گفتنی است که اگر هیچ تاریخ و یا نسخه‌ای برای مولفه تحت تأثیر ذکر نشده باشد، به این معناست که شرکت سیسکو در حال ادامه بررسی می‌باشد و در صورت دسترسی به اطلاعات تکمیلی، این اطلاعات نیز بروزرسانی خواهند شد و پس از نهایی شدن آن‌ها، مشتریان باید به بخش نقص(های) مرتبط سیسکو مراجعه نمایند.

محصولات آسیب‌پذیر شرکت سیسکو

محصول	شناسه نقص
Cisco GGSN Gateway GPRS Support Node	CSCvu60310
Cisco MME Mobility Management Entity	CSCvu60314
Cisco PGW Packet Data Network Gateway	CSCvu60313
Cisco System Architecture Evolution Gateway (SAEGW)	CSCvu60314

[1] هر نقصی دارای یک unique identifier یا همان شناسه منحصر بفرد می‌باشد.
[2] workarounds

گفتنی است فقط محصولاتی که در بخش محصولات آسیب‌پذیرِ شرکت سیسکو، یعنی Vulnerable Products لیست شده‌اند، تحت تأثیر این آسیبپذیری‌ها قرار می‌گیرند. جهت کسب اطلاعات بیشتر در خصوص محصولات وصله شده نیز باید به همین بخش مراجعه کنید.

همواره به مشتریان توصیه می‌شود که پیش از ارتقاء نسخه یک نرم‌افزار، به صفحه مشاوره‌های امنیتی سیسکو _Cisco Security Advisories_ مراجعه کرده و از نظرات آن‌ها استفاده کنند. در کلیه موارد نیز مشتریان باید اطمینان حاصل کنند که دستگاه‌ها، دارای حافظه کافی بوده و پیکربندی‌های نرم‌افزار با نسخه جدید پشتیبانی شود و اگر در این زمینه اطلاعات کافی ندارند پیشنهاد می‌شود با مرکز خدمات فنی سیسکو (TAC[1]) و یا پشتیبان‌های مربوطه تماس حاصل نمایند.

ارزیابی خطر و اقدامات پیشگیرانه

Ripple20 خطرات قابل توجهی را ایجاد می‌کند. از جمله آنها می‌توان به موارد زیر اشاره کرد:

- اگر مهاجمی خارج از شبکه باشد، در صورت دسترسی به اینترنت می‌تواند دستگاهی را در داخل شبکه کنترل کند.
- مهاجمی که قبلاً موفق به نفوذ به یک شبکه شده است می‌تواند از آسیب‌پذیری‌های این کتابخانه برای هدف قرار دادن دستگاه‌های خاص درون آن استفاده کند.
- یک مهاجم می‌تواند حمله‌ای را انتشار دهد که بتواند تمام دستگاه‌های آسیب‌دیده در شبکه را به طور همزمان در اختیار بگیرد.
- مهاجم ممکن است از دستگاه آسیب‌دیده به عنوان راهی برای پنهان ماندن در شبکه برای چندین سال استفاده کند.
- یک مهاجم در حالت پیشرفته‌تر به طور بالقوه می‌تواند خارج از مرزهای شبکه، حمله‌ای را بر روی دستگاهی در داخل شبکه انجام دهد و بنابراین پیکربندی‌های NAT را دور زند. این کار با انجام یک حمله MITM یا یک dns cache poisoning انجام می‌شود.
- در برخی از سناریوها، مهاجم ممکن است با پاسخ دادن به بسته‌هایی که مرزهای شبکه را رها می‌کنند، حملات خود را در خارج از شبکه و با دور زدن NAT انجام دهد.

در تمام سناریوهای ذکر شده، مهاجم می‌تواند بدون نیاز به تعامل کاربر، کنترل کاملی را از راه دور بر روی دستگاه مورد نظر بدست آورد.

JSOF توصیه می‌کند که اقدامات لازم را برای به حداقل رساندن یا کاهش خطر بهره برداری از دستگاه انجام دهید. گزینه‌های انتخابی جهت کاهش خطرات، به بستر موجود بستگی دارد. به طور کلی انجام مراحل زیر توصیه می‌شود:

- تمام سازمان‌ها قبل از اعمال اقدامات لازم، باید یک ارزیابی جامع از مخاطرات احتمالی را انجام دهند. ابتدا اقدامات دفاعی را در حالت غیرفعال "alert" گسترش دهید.
- اقدامات مربوط به فروشندگان دستگاه:
  - مشخص کنید که آیا از یک Treck stack آسیب‌پذیر استفاده می‌کنید یا خیر
  - ارتباط با Treck برای اطلاع از خطرات موجود
  - برزورسانی به آخرین نسخه Treck stack (6.0.1.67 و بالاتر)
  - در صورت عدم امکان بروزرسانی، در صورت امکان غیرفعال کردن featureهای آسیب‌پذیر را در نظر بگیرید
- اقدامات مربوط به اپراتورها و شبکه‌ها:
  - اولین و بهترین اقدام، بروزرسانی به نسخه‌های وصله شده است. در صورت بروزرسانی دستگاه‌ها، مراحل زیر توصیه می‌شود:
    - قرار گرفتن در معرض شبکه برای دستگاه‌های بحرانی و حساس را به حداقل رسانده مگر در موارد ضروری و اطمینان حاصل کنید که دستگاه‌ها از طریق اینترنت در دسترس نیستند مگر اینکه قطعا ضروری باشد.
    - شبکه‌ها و دستگاه‌های OT را در پشت فایروال‌ها جدا کرده و آنها را از شبکه تجاری جدا کنید.
    - تنها روش‌های امن دسترسی از راه دور را فعال کنید.
  - ترافیک غیرعادی IP را مسدود کنید
  - حملات شبکه را از طریق بررسی deep packet ها مسدود کنید تا خطرات مربوط به دستگاه‌های Treck فعال شده با TCP/IP خود را کاهش دهید.

فیلتر کردن ترافیک Pre-emptive، روش موثری است که می‌تواند متناسب با محیط شبکه شما اعمال شود. گزینه‌های فیلتر شامل موارد زیر می‌شوند:

- IP fragments ها را مسدود یا نرمال‌سازی کنید.
- در صورت لزوم، IP tunneling (IPv6-in-IPv4 یا IP-in-IP tunneling) را مسدود یا غیرفعال کنید.
- مسیریابی منبع IP و هر ویژگی کم ارزش IPv6 مانند مسیریابی هدرهای VU#267289 را مسدود کنید.
- پیام‌های استفاده نشده کنترل ICMP مانند بروزرسانی MTU و بروزرسانی Address Mask را مسدود کنید.
- DNS را از طریق یک سرور بازگشتی ایمن یا فایروال بازرسی DNS، نرمال‌سازی کنید. (بررسی کنید که سرور DNS بازگشتی شما درخواست‌ها را نرمال‌سازی می‌کند)
- امنیت DHCP/DHCPv6 را با ویژگی‌هایی مانند DHCP snooping بالا ببرید.
- در صورتیکه از قابلیت‌های multicast یا چندبخشی IPv6 در زیرساخت switching استفاده نمی‌شود، آن را غیرفعال یا مسدود کنید.
- در جایی که IPهای استاتیک قابل استفاده هستند، DHCP را غیرفعال کنید.
- IDS and IPS signatures های شبکه را بکار بگیرید.
- در صورت وجود، segmentation شبکه را انجام دهید.

جمع بندی

با توجه به اینکه در کشور ایران نمایندگی رسمی شرکت‌های تحت تاثیر این آسیب‌پذیری مشغول به فعالیت نمی‌باشند، این وظیفه مدیران و کارشناسان شبکه سازمان‌هاست که در اولین فرصت نسبت به بررسی و بروزرسانی firmware محصولات مذکور اقدام نمایند. توصیه می شود هر چه سریعتر نرم‌افزار Treck IP stack را به آخرین نسخه آن (6.0.1.67 یا بالاتر) بروزرسانی کنید. همچنین پیشنهاد می گردد حملات شبکه را از طریق deep packet inspection مسدود کنید، در برخی موارد سوییچ‌ها، روترها و

---

[1] Cisco Technical Assistance Center

فایروال‌ها بسته‌های ناقص و بدون تنظیمات تکمیلی را رها می‌کنند. توصیه می‌شود چنین ویژگی‌های امنیتی غیرفعال نباشند.

منبع خبر :

https://www.jsof-tech.com/ripple20/

Scan Link

بات‌نت Lucifer و هدف قرار دادن سیستم‌های ویندوزی

به تازگی بات‌نت جدیدی به نام Lucifer مشاهده شده است که سیستم‌های ویندوزی را مورد هدف قرار می‌دهد. این بات نت پس از آلوده کردن سیستم، آن را توسط ربانی به یک کلاینت cryptomining تبدیل کرده و از این طریق می‌تواند حملات انکار سرویس (DDoS[1]) توزیع شده را آغاز کند.

نویسنده بدافزار، این ربات را Satan DDoS نام‌گذاری کرده است اما محققان Palo Alto Network's Unit 42، به آن لقب Lucifer داده‌اند زیرا بدافزار دیگری نیز با همین نام وجود دارد. (Satan Ransomware)

در 29ام ماه مه 2020، محققانِ Unit42، نوع جدیدی از بدافزار ترکیبی[2] cryptojacking را کشف کردند که آسیب‌پذیری با شناسه "CVE-2019-9081"را اکسپلویت می‌کند. بررسی‌ها نشان می‌دهد بدافزار Lucifer قادر به انجام حملات DDoS و همچنین اکسپلویت هاست‌های آسیب‌پذیر ویندوز می‌باشد.

کارشناسان هنگام بررسی مؤلفه‌های اکسپلویتِ آسیب‌پذیری با شناسه "CVE-2019-9081"، (آسیب‌پذیری بحرانی RCE که بر روی یک مؤلفه فریمورک وب Laravel تأثیر می‌گذارد) متوجه این بات‌نت شدند. اولین نمونه از ربات Lucifer، در 29 ماه مه 2020 کشف شد.

Lucifer بسیار قدرتمند است، این بات‌نت علاوه بر آن که می‌تواند XMRig را جهت cryptojacking Monero حذف کند[3]، قادر است از طریق اکسپلویت آسیب‌پذیری های مختلف، نظارت بر سرور کنترل و فرمان(C2[4]) را نیز برعهده گرفته و حملات EternalBlue, EternalRomance و DoublePulsar را علیه اهداف آسیب‌پذیر اینترانت اجرا کند. Lucifer همچنین می‌تواند ماشین‌های با پورت‌های 135 TCP (RPC) و 1433 (MSSQL) را اسکن نماید. این بات‌نت قادر به حذف XMRig Monero بوده و شامل ماژول DDoS می‌باشد و مکانیزم خود را با اکسپلویت آسیب‌پذیری‌های متعدد و اجرای حملات جدی پیاده‌سازی خواهد کرد.

در ابتدا این بدافزار به منظور آلوده کردن هاست‌های خارجی[5]، یک آدرس IP غیرخصوصی تولید کرده و سپس قربانی که به طور تصادفی انتخاب شده است را با درخواست‌های HTTP بر روی تعدادی از پورت‌ها مورد بررسی قرار می‌دهد.

آسیب‌پذیری‌های اکسپلویت شده توسط این بات‌نت

شناسه آسیب‌پذیری	وضعیت
CVE-2014-6287	HFS در پاسخ HTTP یافت می‌شود.
CVE-2018-1000861	Jetty در پاسخ HTTP یافت می‌شود.
CVE-2017-10271	Servlet در پاسخ HTTP یافت می‌شود.
ThinkPHP remote code execution (RCE) vulnerabilities CVE-2018-7600 CVE-2017-9791 CVE-2019-9081 PHPStudy Backdoor remote code execution (RCE)	هیچ کلیدواژه‌ای یافت نمی‌شود.

مهاجم می‌تواند پس از به خطر افتادن سیستم قربانی توسط این بات‌نت، دستورات دلخواه را بر روی دستگاه آلوده اجرا کند. کارشناسان دریافتند که Lucifer قادر است که هم اینترنت و هم اینترانت هاست‌های ویندوز را مورد هدف قرار دهد.

شایان ذکر است که این بدافزار می‌تواند توسط یک دیکشنری حملات بی‌رحمانه خود را آغاز کند! که در این حملات، بدافزار متکی به یک دیکشنری با 7 نام کاربریِ "mssql" "SQLDebugger" "kisadmin" "su" "SA" "sa" و "1433Chred" و صدها گذرواژه می‌باشد.

نرم‌افزارهای آسیب‌پذیر عبارتند از:

- Rejetto HTTP File Server
- Jenkins
- Oracle Weblogic
- Drupal
- Apache Struts
- Laravel framework
- Microsoft Windows

✓ توصیه امنیتی

با توجه به اهمیت این مسئله، توصیه می‌شود هر چه سریع‌تر به روزرسانی‌ها و وصله‌های امنیتی نرم‌افزارهای تحت تأثیر را اعمال کرده و همچنین جهت جلوگیری از حملاتی که از طریق دیکشنری صورت می‌پذیرند، لازم است از گذرواژه‌های قوی استفاده کنید.

جمع‌بندی

Lucifer بات‌نتی مخرب است که ترکیب جدیدی از cryptojacking و نوعی بدافزار DDoS می‌باشد که منجر به اکسپلویت آسیب‌پذیری‌های قدیمی و انجام فعالیت‌های مخرب بر روی سیستم‌عامل‌های ویندوز می‌شود، کاربران جهت حفظ امنیت سیستم خود، باید هر چه سریع‌تر اقدامات لازم را در این خصوص مبذول نمایند.

منبع خبر :

https://bit.ly/2Z8XugD

Scan Link

[1] denial-of-service
[2] hybrid
[3] dropping
[4] command and control
[5] external hosts

رفع نقص بحرانی در فایروال PAN-OS توسط شرکت Palo Alto

در پی نقص بحرانی موجود در فایروال PAN-OS با شناسه "CVE-2020-2021" که به واسطه آن مهاجمان قادرند فرآیند احراز هویت را در این فایروال دور بزنند، شرکت Palo Alto اقدام به رفع این آسیب‌پذیری کرده است.

هنگامی که احراز هویت SAML[1] فعال و قابلیت 'Validate Identity Provider Certificate' غیرفعال باشد، تأیید هویت نادرست در PAN-OS SAML، مهاجم را قادر می‌سازد تا به منابع شبکه دسترسی پیدا کند. گفتنی است که برای اکسپلویت این آسیب‌پذیری، مهاجم باید به سرور آسیب‌پذیر دسترسی داشته باشد.

آسیب‌پذیری مذکور دارای شدت بحرانی و CVSS 3.x base score of 10 بوده و کمپانی مربوطه اعلام کرده است که در صورت عدم استفاده از SAML در فرآیند احراز هویت و نیز غیر فعال بودن قابلیت Validate Identity Provider Certificate در SAML Identity Provider Server Profile، این آسیب‌پذیری اکسپلویت نخواهد شد. به گفته شرکت Palo Alto، در خصوص GlobalProtect Gateways, Prisma Access Prisma Access ,GlobalProtect Portal Clientless VPN و Prisma Access، مهاجم غیرمجاز، با دسترسی شبکه به سرورهای تحت تاثیر این آسیب‌پذیری و درصورتیکه توسط احراز هویت پیکربندی شده و سیاست‌های امنیتی، مجاز باشد می‌تواند به منابع محافظت شده شبکه دسترسی پیدا کند؛ همچنین این منابع می‌توانند از طریق احراز هویت SAML-based single sign-on (SSO)، از خطر این آسیب‌پذیری به دور باشند.

در حملات صورت گرفته علیه PAN-OS و رابط‌های وب[2] Panorama، آسیب‌پذیری مذکور می‌تواند توسط یک مهاجم غیر مجاز با دسترسی شبکه به PAN-OS و رابط‌های وب Panorama، اکسپلویت شود تا مهاجم به عنوان ادمین وارد سیستم شده و اقدامات مربوطه در حوزه اختیارات ادمین را انجام دهد که در بدترین حالت این آسیب‌پذیری دارای شدت بحرانی و CVSS 3.x base score of 10 می‌باشد، اما اگر رابط‌های وب تنها به یک شبکه منحصربفرد دسترسی داشته باشند، رتبه این آسیب‌پذیری به CVSS Base Score of 9.6 کاهش خواهد یافت.

خبر خوب این است که شبکه‌های Palo Alto از حملات ناشی از اکسپلویت این آسیب پذیری اطلاعات موثقی دریافت و منتشر نکرده‌اند.

وجود نام کاربری غیرمعمول و یا آدرس‌های IP منبع در لاگ‌ها باید به عنوان زنگ خطری مورد توجه قرار گیرد. گفتنی است این آسیب‌پذیری توسط Salman Khan از تیم Cyber Risk and Resilience ، Cameron Duck و تیم سرویس‌های Identity[3] دانشگاه Monash گزارش شده است.

به گفته یکی از محققان امنیتی، احتمالاً APTها به زودی سعی در اکسپلویت نقصِ Palo Alto Networks موجود در PAN-OS خواهند داشت.

نسخه‌های تحت تأثیر آسیب‌پذیری

آسیب‌پذیری مذکور بر روی PAN-OS 9.1 و نسخه‌های قبل از PAN-OS 9.1.3، PAN-OS 9.0 و نسخه‌های قبل از PAN-OS 9.0.9 و PAN-OS 8.1، نسخه‌های قبل از PAN-OS 8.1.15 و تمام نسخه‌های PAN-OS 8.0 (EOL) تأثیر می‌گذارد، گفتنی است که این آسیب‌پذیری بر روی PAN-OS 7.1 تأثیر نمی‌گذارد.

راهکار

در حالت کلی مشتریان می‌توانند موارد زیر را بررسی کنند تا مشخص شود که آیا تحت تاثیر آسیب‌پذیری ذکر شده قرار گرفته‌اند یا خیر:

- لاگ‌های احراز هویت
- لاگ‌های User-ID
- ACC Network Activity Source/Destination Regions (Leveraging the Global Filter feature!)
- (Monitor > Report) Custom Reports
- لاگ‌های GlobalProtect (در نسخه PAN-OS 9.1.0 و بالاتر)

اما با توجه به اهمیت این آسیب‌پذیری و نیز بالا بودن شدت آن، هرچه سریع‌تر نسبت به وصله دستگاه‌های تحت‌تأثیر این آسیب‌پذیری بخصوص اگر پروتکل SAML مورد استفاده قرار گرفته است، اقدام کنید.

منبع خبر :

https://securityaffairs.co/wordpress/105351/hacking/critical-flaw-firewall-pan-os.html

Scan Link

وصله یک آسیب‌پذیری بحرانی در دستگاه‌های BIG-IP F5

اجرای کد از راه دور در دستگاه‌های F5 BIG-IP، دولت‌ها، ارائه دهندگان فضای ابری، ISPها، بانک‌ها و بسیاری از شرکت‌های Fortune 500 را در معرض حملات احتمالی قرار می‌دهد.

[1] Security Assertion Markup Language
[2] web interfaces
[3] Identity Services

F5 Networks یکی از بزرگترین شرکت‌های ارائه‌دهنده تجهیزات شبکه در سراسر جهان، این هفته یک مشاوره امنیتی را منتشر کرده است که به مشتریان خود توصیه می‌کند که یک نقص امنیتی خطرناک را که به احتمال زیاد مورد اکسپلویت قرار گرفته است، وصله نمایند.

این آسیب‌پذیری، محصول BIG-IP این شرکت را تحت تاثیر قرار می‌دهد. BIG-IP دستگاه‌های چندمنظوره شبکه هستند که می‌توانند به عنوان سیستم‌های شکل‌دهی ترافیک وب، لود بالانسرها، فایروال‌ها، دروازه‌های دسترسی (access gateways)، rate limiterها یا SSL middleware کار کنند.

BIP-IP یکی از محبوبترین محصولات شبکه است که به صورت روزانه در شبکه‌های دولتی در سراسر جهان، در شبکه‌های مربوط به ارائه‌دهندگان خدمات اینترنت، در مراکز داده محاسبات ابری و به طور گسترده در شبکه‌های سازمانی مورد استفاده قرار می‌گیرد.

این آسیب‌پذیری (باگ BIG-IP) با شناسه CVE-2020-5902، توسط فردی به نام Mikhail Klyuchnikov، از محققان امنیتی شرکت Positive Technologies، کشف شده و به صورت محرمانه به شرکت F5 گزارش داده شده است.

این باگ که "اجرای کد از راه دور" نیز نامیده می‌شود، در واقع مشکل رابط مدیریت BIG-IP است که به TMUI (Traffic Management User Interface) شهرت دارد.

مهاجمان می‌توانند این باگ را از طریق اینترنت اکسپلویت نموده و به TMUI که روی یک سرور Tomcat و دارای سیستم‌عامل مبتنی بر لینوکس در حال اجرا است دسترسی پیدا کنند.

مهاجمان برای حمله به دستگاه‌های آسیب‌پذیر به اطلاعات ورود نیاز ندارند، و یک اکسپلویت موفق می‌تواند برای مهاجمان امکان اجرای دستورات سیستمیِ دلخواه را فراهم نماید. این دستورات می‌توانند حذف فایل‌ها، غیرفعال نمودن سرویس‌ها و اجرای کدهای دلخواه به زبان جاوا باشند. حتی این امکان وجود دارد که مهاجم بتواند کنترل کامل دستگاه BIG-IP را در دست بگیرد.

آسیب‌پذیری مذکور به حدی خطرناک است که در سیستم امتیازدهی CVSSv3 امتیاز 10 از 10 به آن اختصاص یافته است. این بدان معناست که این باگ به سادگی قابل اکسپلویت بوده و از طریق اینترنت می‌تواند مورد سوءاستفاده قرار گیرد، و برای استفاده از آن نیازی به اطلاعات ورود یا مهارت‌های کدنویسی پیشرفته نیست.

به طور کاملاً تصادفی، پس از کشف آسیب‌پذیری بحرانی در دستگاه‌های فایروال و Palo Alto Networks VPN در روز دوشنبه، این دومین آسیب‌پذیری خطرناک با شدت 10 در دستگاه‌های شبکه است که در این هفته افشاء می‌شود.

فرماندهی سایبری ایالات متحده در هفته جاری هشدارهایی را به بخش‌های خصوصی و دولت صادر کرد تا نقص موجود در Palo Alto را وصله کنند زیرا همان‌طور که انتظار می‌رفت، هکرها اقدام به اکسپلویت این آسیب‌پذیری کرده‌اند.

تاکنون هیچ هشدار رسمی توسط آژانس امنیت سایبری ایالات متحده صادر نشده است؛ اما گفتنی است که نقص F5، به اندازه نقص Palo Alto خطرناک نیست.

Nate به گفته محققان،به خطر افتادن کامل یک سیستم از نظر تئوری می‌تواند به افراد اجازه دهد تا ترافیک رمزگذاری نشده داخل دستگاه را مورد جاسوسی قرار دهند.

سیستم‌عامل مدیریت این دستگاه‌ها، مبتنی بر لینوکس است و مانند اکثر ADCها[1]، در بخش‌های اصلی و پردسترس شبکه مستقر می‌شوند.

در حال حاضر بر اساس بررسی‌های Shodan، 8,400 دستگاه BIG-IP به صورت آنلاین متصل هستند. چندین شرکت و محقق امنیتی در حوزه امنیت سایبری به ZDNet خاطر نشان کردند که هیچ حمله‌ای که این دستگاه‌ها را مورد هدف قرار داده باشد، کشف نکرده‌اند؛ اما آن‌ها انتظار دارند که حملات به زودی آغاز شود، بخصوص اگر یک کد اکسپلویت proof-of-concept، به صورت آنلاین منتشر شود.

محصولات تحت تأثیر این آسیب‌پذیری

محصولات تحت تأثیر	شاخه	نسخه‌های آسیب‌پذیر	نسخه‌های وصله شده	شدت آسیب‌پذیری	CVSSv3 امتیاز	مؤلفه و ویژگی آسیب‌پذیری
BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM)	15.x	15.1.0	15.1.0.4	بحرانی	10.0	TMUI/Configuration utility
		15.0.0	-			
	14.x	14.1.0 - 14.1.2	14.1.2.6			
	13.x	13.1.0 - 13.1.3	13.1.3.4			
	12.x	12.1.0 - 12.1.5	12.1.5.2			
	11.x	11.6.1 - 11.6.5	11.6.5.2			
BIG-IQ Centralized Management	7.x	-	غیرقابل استفاده	آسیب‌پذیر نیست	-	-
	6.x	-	غیرقابل استفاده			
	5.x	-	غیرقابل استفاده			
Traffix SDC	5.x	-	غیرقابل استفاده	آسیب‌پذیر نیست	-	-

منبع خبر :

https://zd.net/2Zazudi

Scan Link

[1] application delivery controllers

آسیب‌پذیری اجرای کد از راه دور در آنتی‌ویروس Bitdefender

به تازگی یک آسیب‌پذیری در آنتی‌ویروس Bit Defender مشاهده شده است که به واسطه آن، هکرها می‌توانند کدهای مخرب خود را از راه دور اجرا کنند. این آسیب‌پذیری با شناسه "CVE-2020-8102"، نسخه بروزرسانی اخیر آنتی‌ویروس Bit Defender را تحت تاثیر قرار داده است. علاوه براین، محققان مدعی هستند که این آسیب‌پذیری اثرات خطرناک و قدرتمندی را به دنبال دارد چراکه آنتی‌ویروسی را مورد حمله قرار داده است که معمولا توسط کاربران مختلفی برای حفاظت از دستگاه‌های خود استفـــاده می‌شود.

به گفته محققان، آسیب‌پذیری مذکور به دلیل اعتبارسنجی نادرست ورودی در مرورگر Safepay است که عنصری از Bitdefender Total Security 2020 مـــی‌باشد. به سبب این آسیب‌پذیری، یک صفحه وب خارجی و ساختگی قادر است دستورات را از راه دور در فرآیند Safepay Utility اجرا کند. بر اساس ادعای محققان، آسیب‌پذیری ذکر شده نسخه‌های 24.0.20.116 آنتی‌ویروس Bitdefender Total Security 2020 را تحت تاثیر قرار داده است. این آنتی‌ویروس، اتصالات امن HTTPS را بررسی می‌کند و بنا به دلایلی ترجیح می‌دهد از نمایش صفحات خطای[1] مربوط به خود استفاده کند و با آثار مخرب کمتر، در این مورد شبیه به نحوه عملکرد آنتی‌ویروس Kaspersky می‌باشد.

این آسیب‌پذیری توسط Wladimir Palant، توسعه‌دهنده AdBlock Plus افشا شد. وی از یک وب‌سرور محلی و یک SSL معتبر استفاده کرد که در مدت کوتاهی، آن را با مقدار نامعتبری تغییر داد. Palant این رفتار را از طریق PoC نشان داد کـــه در آن یک وب‌سرور در حال اجرا داشت کـــه گواهی SSL معتبر را بر روی اولین درخواست ارائه می‌داد اما بلافاصله به یک مقدار نامعتبر تبدیل می‌شد.

جزئیات آسیب‌پذیری به شرح زیر است:

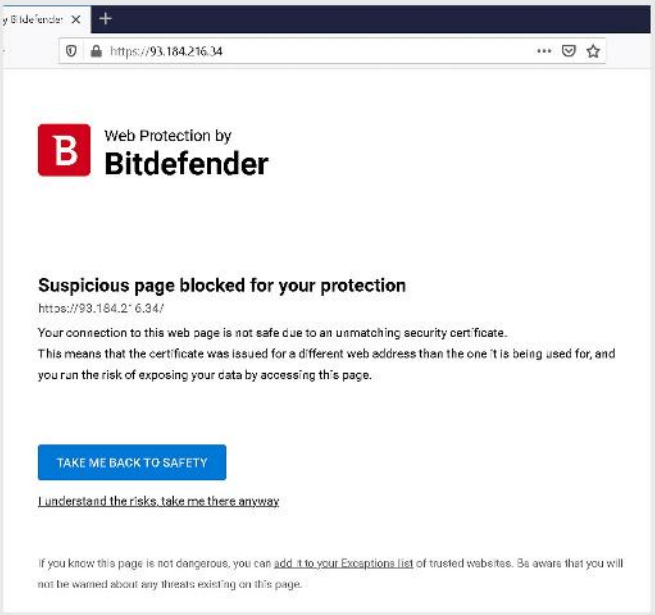
CVE ID: CVE-2020-8102

CVSS score: 8.8

Affected vendors: Bitdefender

Affected products: Bitdefender SafePay

این مورد مشخص، مربوط به آنتی‌ویروس Kaspersky با روش‌های ورودی مشابه است، اما وب‌سایت‌ها نیز می‌توانند به راحتی برخی از توکن‌های امنیتی صفحات خطا را بدست آورند.



نمایی از مرورگر Safepay

این توکن‌های امنیتی نمی‌توانند برای لغو خطاها در دیگر وب‌سایت‌ها استفاده شوند، اما می‌توان از آن‌ها جهت شروع assembly با مرورگر Safepay مبتنی بر Chromium استفاده کرد.

براساس گزارش Bitdefender Advisory، API هیچگاه جهت پذیرش داده‌های غیرقابل اعتماد درنظرگرفته نشده است و با همان آسیب‌پذیری که قبلاً کارشناسان امنیتی در Avast Secure Browser مشاهده کردند، مورد حمله قرار می‌گیرد.

در این حالت مهاجم می‌تواند به راحتی پرچم‌های خط فرمان[2] را درج کرده و باعث شود اپلیکیشنِ دلخواه، کار خود را شروع کند.

Bitdefender Safepay محصول تحت‌تأثیر این آسیب‌پذیری می‌باشد، این نرم‌افزار امنیت حریم خصوصی شما در زمان انجام عملیات بانکی و پرداخت های آنلاین را تضمین می‌کند و به صورت یک دسکتاپ ثانویه که بر پایه مرورگر گوگل کروم می‌باشد عمـــل می‌کند. هنگام استفاده از این نرم‌افزار، معاملات آنلاین شما در برابر کی‌لاگرها، صفحات فیشینگ و تروجان‌ها محافظت می‌شود و با خیال راحت می‌توانید عملیات بانکی خود را انجام دهید. این نرم‌افزار به صورت اتوماتیک تمامی نرم‌افزارهـــای دسکتاپ را غیر فعال می‌کند و حتی اجازه عکس گرفتن از دسکتاپ توسط نرم‌افزارهای جاسوســـی و حتی کیبورد را نمی‌دهد.

Bitdefender الگوهایی را ارائه می‌دهد که حاکی از چگونگی تولید کد تزریق شده در وب‌سایت بانکی می‌باشد.

```
var params = encodeURIComponent(window.location);
sid = "" + Math.random();
obj_ajax.open("POST", sid, true);
obj_ajax.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
obj_ajax.setRequestHeader("BDNDSS_B67EA559F21B487F861FDA8A44F01C50", "{%NDSECK%}");
obj_ajax.setRequestHeader("BDNDCA_BBACF84D61A04F9AA66019A14B035478", "{%NDCA%}");
obj_ajax.setRequestHeader("BDNDWB_5056E556833D49C1AF4085CB254FC242", "{%OBKCMD%}");
obj_ajax.setRequestHeader("BDNDOK_4E961A95B7B44CBCA1907D3D3643370D", "{%OBKREFERRER%}");
obj_ajax.send(params);
```

[1] error pages

[2] command-line

گفتنی است که این الگوها دیگر مورد استفاده قرار نمی‌گیرند، اما راهی برای دسترسی به وب‌سایت مخرب در مرورگر Safepay وجود دارد که در رابطه با وب‌سایت‌های بانکداری که به درستی از هم تفکیک شده‌اند، می‌تواند مورد بررسی قرار گیرد.

✓ راه‌حل

Bitdefender در حال بررسی این آسیب‌پذیری می‌باشد، آن‌ها یک بروزرسانی امنیتی را منتشر کرده‌اند که آسیب‌پذیری مذکور را در نسخه 24.0.20.116 و تمامی نسخه‌های بعدیش، رفع می‌کند، پس با توجه به اهمیت این موضوع، هر چه سریع‌تر تنظیمات بروزرسانی آنتی‌ویروس خود را بررسی کنید.

منبع خبر :

https://gbhackers.com/vulnerability-in-bitdefender-anti-virus/

Scan Link

اخبار کوتاه

فناوری جدید مایکروسافت دستکاری کـــــرنل ویندوز توسط هکرها را ناممکن می‌کند

در مبارزه دنباله‌دار مایکروسافت با هکرها، کمپانی ردموندی گام دیگری برداشته و تکنولوژی امنیتی حفاظت از داده‌های کرنل جدیدی طراحی کرده است که کار را برای هکرها و مهاجمان به شدت دشوار می‌کند. طوری که با فقط-خواندنی (Read-Olny) شدن کرنل، جلوی تکنیک‌های دست‌کاری داده‌ها گرفته خواهد شد.

سیستم حفاظت از داده‌های کرنل (KDP) بخش‌های عمده‌ای از مموری هسته رایانش را به صورت فقط-خواندنی در می‌آورد و به همین ترتیب از دست‌کاری در داده‌ها و حملات جلوگیری خواهد شد. با استفاده از این مکانیزم، کرنل ویندوز و تمام درایورها در امان می‌مانند.

تکنولوژی مورد بحث نرخ حملاتی که اخیرا باب شده را کاهش می‌دهد؛ این روزها هکرها با دست‌کاری درایورهای آسیب‌پذیر، اما ثبت شده در کرنل ویندوز، ابزار آلوده و بدافزار نصب می‌کنند و سپس به مموری هم دست خواهند یافت. اما با محافظت فقط-خواندنی، حتی درایورهای ثبت شده نمی‌توانند ساختار و تنظیمات مهم مموری را تغییر دهند. گفتنی است تمام سیستم‌های مبتنی بر ویندوز نمی‌توانند از KDP استفاده کنند، چرا کـــــــه می‌بایست آن پلتفرم حتما از لایه‌های امنیتی مجازی‌سازی محور (VBS) پشتیبانی کند. این تکنولوژی در حال حاضر در نسخه اینسایدر ویندوز 10 اعمال شده و در آینده به صورت رسمی نیز در دسترس قرار خواهد گرفت.

کلاهبرداری در پوشش فروش اکانت بازی‌های آنلاین

علاقه‌مندی تعدادی از کاربران به خصوص کودکان و نوجوانان به خرید اکانت مراحل بالاتری از یک بازی آنلاین، باعث شده است که برخي از افراد مبادرت به فروش اکانت بازی خود کنند. برخي افراد سودجو نیز با تبلیغات فریبنده از خریداران اکانت‌هاي بازي که معمولاً قشر کودك و نوجوان هستند، سوءاستفاده کرده و در نتیجه از آن‌ها کلاهبرداري مي‌کنند. پلیس فتا به کاربران یادآور شد: با توجه به اینکه شبکه‌هاي اجتماعي قابل اعتماد نیستند از خرید اکانت بازی از کاربران شبکه‌هاي اجتماعي خودداری کنند چرا که احتمال گرفتاری در دام کلاهبرداران سایبری وجود دارد.

فیشینگ با ترفند ویژه آگهی در سایت‌های واسط

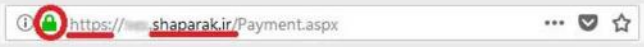
زمانی‌که فردی با پرداخت وجهی ناچیز اقدام به بارگذاری آگهی فروش کالای مدنظر خود به صورت "آگهی ویژه" در سایت دیوار، شیپور و یا دیگر سایت‌ها می‌کند، کلاهبرداران بلافاصله از طریق شماره تلفن ذکر شده در آگهی، اقدام به ارسال پیامک برای وی می‌کنند. فرد آگهی دهنده نیز چون به تازگی آگهی را بارگذاری کرده است، بدون چک کردن سرشماره پیامک ارسالی، اقدام به واریز وجه از طریق لینک ذکر شده در پیامک می کند تا آگهی به صورت ویژه و در صدر آگهی‌ها نمایش داده شود، غافل از اینکه این درگاه پرداخت یک صفحه جعلی برای فیشینگ و سرقت اطلاعات بانکی او می‌باشد که توسط فرد کلاهبردار ارسال گردیده است؛ لذا توصیه می‌شود شهروندان بسیار هشیار بوده و شماره پیامک‌های دریافتی را حتما چک کنند.

مقالات آموزشی

راهکارهای امنیتی جهت استفاده از سیستم‌های پرداخت اینترنتی

با توجه با شرایط کنونی کشور و شیوع بیماری کرونا، متعاقب آن افزایش استفاده از پرداخت‌ها وتراکنش‌های اینترنتی، پیش‌بینی می‌شود که جرائم و کلاهبرداری‌های مرتبط با «خدمات پرداخت الکترونیکی» نیز افزایش یابند. بر این مبنا ضروری است تا ضمن حفظ هوشیاری در استفاده از این خدمات، توصیه‌های امنیتی لازم مدنظر قرار داده شوند. زیرا درگاه‌های پرداخت اینترنتی از نکاتی امنیتی بهرمند هستند که کاربران با توجه به این نکات مهم می‌توانند از هر گونه کلاهبرداری فیشنگ در امان باشند و در بستری امن تراکنش انجام دهند.

1) هنگام انجام خرید اینترنتی، پیش از وارد کردن اطلاعات کارت، از اینکه به «درگاه پرداخت اینترنتی» معتبر هدایت شده‌اید، اطمینان حاصل کنید. هنگام خرید از فروشگاه‌های اینترنتی از معتبر بودن آدرس نمایش داده شده در مرورگر با درج عبارت https در ابتدای آن و وجود علامت تأیید سرویس دهنده (معمولاً به صورت قفل سبز رنگ) مطابق شکل زیر، اطمینان پیدا کنید. آدرس معتبر درگاه‌های پرداخت اینترنتی باید زیردامنه‌هایی از دامنه Shaparak.ir باشند. هرگونه ترکیب دیگری از کلمه Shaparak و هر پسوند دامنه دیگری به غیر از .ir غیرمجاز است. به عنوان مثال ترکیب‌هایی نظیر Shapaarak یا Shaparack نامعتبر هستند. برای اطلاع از آدرس اینترنتی درگاه‌های پرداخت اینترنتی معتبر، به پورتال کاشف به آدرس www.kashef.ir مراجعه نمایید. اکیداً توصیه می‌شود از صفحه کلید مجازی برای ورود اطلاعات کارت خود استفاده کنید.



2) برنامه‌های همراه فراهم‌کننده خدمات پرداخت را فقط از طریق مراجع معتبر بارگیری، نصب و استفاده کنید. مراجع معتبر به معنای پورتال رسمی بانک / موسسه اعتباری مجاز یا فراهم‌کننده مجاز خدمات پرداخت (PSP) است. جهت مشاهده آدرس پورتال بانک‌ها و مؤسسات اعتباری و همچنین شرکت‌های ارائه‌دهنده خدمات پرداخت که فراهم‌کننده برنامک‌های همراه معتبر هستند، به پورتال کاشف به آدرس www.kashef.ir مراجعه کنید.

3) خریدهای اینترنتی خود را از فروشگاه‌های مطمئن انجام دهید. در خریدهای اینترنتی به وجود «نماد اعتماد الکترونیک» دقت کنید و از اعتبار آن اطمینان حاصل کنید. با کلیک روی نماد به سایت enamad.ir هدایت خواهید شد، مسیر و اطلاعات ارائه شده باید با مشخصات فروشگاه اینترنتی منطبق باشد .از انجام خرید در سایت‌های اینترنتی، کانال‌های تلگرامی یا صفحات اینستاگرامی که خلاف موازین جمهوری اسلامی ایران فعالیت می‌کنند یا تخفیف‌ها و شرایط فروش غیرمتعارف و جذاب پیشنهاد می‌دهند، خودداری کنید.

[1] error pages

4) از امنیت رمزهای خود اطمینان حاصل نمایید. توصیه می‌شود رمز اول و دوم کارت را به صورت دوره‌ای تغییر دهید. از فرآیندهای تغییر رمز و مسدودسازی کارت که توسط بانک شما ارائه شده است مطلع باشید، تا بتوانید در مواقع ضروری رمز خود را در سریع‌ترین زمان ممکن تغییر یا کارت خود را مسدود کنید. در انتخاب رمز کارت از به‌کارگیری اعداد مرتبط با داده‌های شخصی (مانند سال تولد، شماره شناسنامه و غیره) که قابل حدس هستند، اجتناب کنید. از یادداشت کردن اطلاعات کارت از جمله رمز اول یا دوم در مکان‌های ناامن خودداری کنید.

5) از ابزارهای شخصی امن برای انجام تراکنش‌های بانکی استفاده کنید. مطمئن شوید که ابزارهای شخصی (تلفن همراه، تبلت، رایانه شخصی و غیره) مورداستفاده در تراکنش‌های بانکی از امنیت کافی برخوردار باشند. در این خصوص:

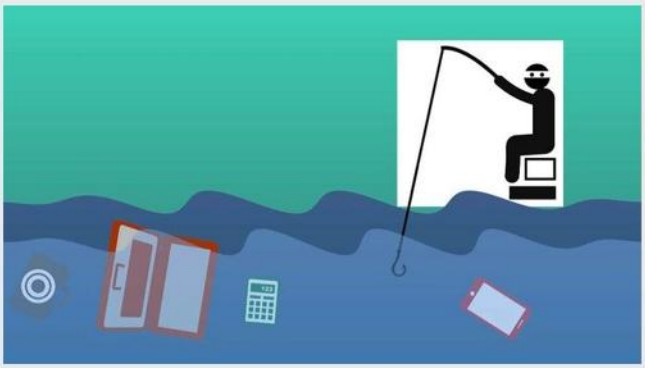
1) از نصب آنتی‌ویروس به‌روز بر روی ابزار خود مطمئن شوید

2) از نصب برنامه‌های غیرضروری روی ابزار خودداری کنید

3) در استفاده از شبکه‌های اجتماعی و وب سایت‌ها از دریافت فایل یا کلیک روی لینک‌های نامطمئن که عموماً شامل پیشنهاداتی نظیر شارژ رایگان، جوایز و سایر پیشنهادات جذاب هستند، اکیداً خودداری کنید

4) علاوه بر برنامه‌های مورد استفاده برای انجام خدمات پرداخت، دیگر برنامه‌های نصب‌شده روی ابزارهای مورد اشاره نیز باید سازندگان معتبری داشته باشند.

6) درصورتی‌که از اینترنت WiFi اماکن عمومی مانند رستوران‌ها، فروشگاه‌ها، مراکز خرید و غیره استفاده می‌کنید، تا حد امکان از تراکنش مالی یا خرید اینترنتی خودداری نمایید و با استفاده از آن به برنامه‌های همراه بانک و اینترنت بانک خود متصل نشوید.



اخبار کوتاه

مسئولیت قانونی اکانت‌های شبکه های اجتماعی بر عهده صاحب اکانت است

کلاهبرداران پس از دسترسی به حساب کاربری افراد در شبکه‌های اجتماعی، با ارسال پیامی مبنی بر درخواست کمک مالی و قرار گرفتن در شرایط حاد به مخاطبان اکانت هک شده، از دوستان و آشنایان مبالغی را تحت عنوان وجه قرضی مطالبه می‌کنند. به کاربران توصیه می‌شود کاربران از اطلاعات حساب‌های کاربری خود در شبکه‌های اجتماعی گوناگون محافظت کنند تا نه تنها خود آن‌ها مورد تهدید و آسیب قرار نگیرند، بلکه دوستان و آشنایان آن‌ها نیز قربانی برنامه‌های مجرمانه تحت نام وی نشوند.

شبکه‌های اجتماعی خارجی بستری مناسب برای انجام فعالیت‌های مجرمانه

کاربران پیام‌رسان‌های موبایل باید در نظر داشته باشند عدم توجه به سطح دسترسی‌هایی که هنگام نصب نرم‌افزار با دستان خود در اختیار سرویس‌دهندگان این قبیل از نرم‌افزارها قرار می‌دهند، می‌تواند زمینه نقض حریم خصوصی برای سرویس‌دهندگان پیام‌رسان‌های موبایلی نسخه خارجی را به‌راحتی فراهم کند. معمولاً در شبکه‌های اجتماعی، جزئی‌ترین اطلاعات کاربران قابل دریافت و انتشار است، و هرلحظه امکان سوءاستفاده از آن‌ها وجود دارد لذا در صورت عدم رعایت نکات ایمنی و امنیتی حریم خصوصی افراد به مخاطره می‌افتد بنابراین توصیه می‌شود کاربران فضای مجازی هشدارهای پلیس فتا را جدی بگیرند.

اپلیکیشن‌های بانکی از طریق سایت‌های رسمی بانک، نصب شود

برخی کلاهبرداران با روش‌هایی متقلبانه از قبیل ارسال پیامک، طراحی نرم‌افزارهایی مشابه و غیره سعی در فریب و سوءاستفاده از حساب مشتریان بانک‌ها را دارند. مجرمان سایبری ابتدا آن‌ها را به درگاه جعلی هدایت و در مدت زمان تعیین شده برای رمزهای یک بار مصرف اقدام به دریافت رمز کاربران و از آن طریق اقدام به برداشت وجه از حساب آن ها می‌کنند. لذا توصیه می‌شود نصب هرگونه اپلیکیشن‌های بانکی صرفاً از طریق سایت های رسمی بانک ارائه دهنده خدمات صورت پذیرد و توجه گردد برای دریافت پیامک رمز یک‌بار مصرف فقط از قسمت تعیین شده در ابزار مورد استفاده مشتریان هر بانک استفاده شود.

برگزاری وبینار رایگان Netwrok Automation

یکی از بزرگترین موضوعات برای مدیران شبکه، رشد و هزینه‌های فناوری اطلاعات برای فعالیت‌های شبکه است. در سازمان‌ها و شرکت‌ها رشد داده‌ها و تجهیزات در حال پیشی گرفتن از قابلیت‌های فناوری اطلاعات بوده و پیکربندی تجهیزات به صورت دستی بسیار دشوار و زمان بر است. اما با این وجود ۹۵ درصد تغییرات شبکه بصورت دستـــی انجام می‌پذیرد و در نتیجه هزینههای عملیاتی ۲ تا ۳ برابر بیشتر از هزینه شبکه می‌باشد. افزایش اتوماسیون فناوری اطلاعات، به صورت متمرکز و از راه دور، برای مشاغل ضروری است. که مدیریت این امر با به کارگیری و پیادهسازی مکانیزم Network Automation برای مدیران راحت‌تر صورت می‌گیرد. در همین راستا به منظور آشنایی علاقمندان این حوزه در مورخ ۵ تیر ماه ۱۳۹۹ وبینار رایگان Network Automation بـــا استقبال پرسنل سازمان‌ها، شرکت‌های خصوصی، دانشجویان و علاقمندان توسط مرکز آپا برگزار گردید.

برگزاری اولین جلسه مجازی مسابقات فتح پرچم غرب کشور

روز پنج‌شنبه مورخ ۱۹ تیر ماه ۱۳۹۹، جلسه‌ای با محوریت همکاری و همفکری به منظور برگزاری سومین دوره مسابقات فتح پرچم غرب کشور به صورت ویدئو کنفرانس با مشارکت مسئولین و نمایندگان سازمان‌ها، بخش خصوصی و دانشگاه‌های سطح استان به میزبانی مرکز تخصصی آپا دانشگاه رازی برگزار گردید.

دکتر منکرسی مدیر مرکز تخصصی آپا ضمن معرفی فعالیت‌های مرکز، گزارشی از نحوه برگزاری و نتایج دومین دوره مسابقات فتح پرچم (CTF) که سال گذشته در دانشگاه رازی برگزار شد ارائه نمودند. ایشان هدف از برگزاری این جلسه را گسترش همکاری و ارتباط با فعالان حوزه فناوری اطلاعات استان به منظور برگزاری هرچه بهتر این مسابقه مطرح کردند.

در ادامه این جلسه چالش‌های مرکز داده و زیر ساخت و اهمیت آن در سازمان‌های استان توسط دکتر مکی، هیات علمی گروه برق دانشگاه رازی مطرح گردید.

با توجه به ضرورت و اهمیت امنیت در سازمان‌ها به منظور کاهش چالش‌های موجود، مسابقه شکارچیان تهدیدات امنیتی توسط دکتر منکرسی مطرح شد. ایشان خاطر نشان نمودند که هدف از برگزاری چنین رویدادهایی ترغیب و تبادل تجربیات بین مدیران و کارشناسان IT در جهت افزایش امنیت سایبری درسطح استان می‌باشد، که به افراد برگزیده در این مسابقه جوایز نفیسی اهداء می‌گردد.

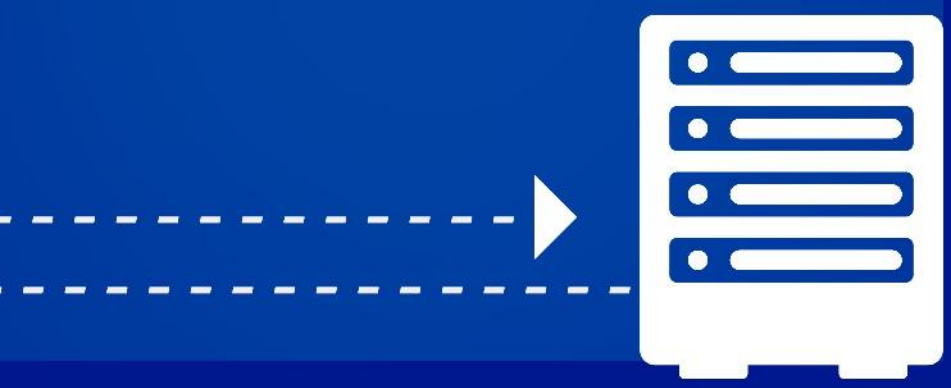
در ادامه شرکت کنندگان حاضر در مورد مسائلی همچون تعیین اعضاء کمیته‌های علمی، فنی، کمپ‌های پیش از مسابقه، تبلیغات، کانال‌های اطلاع‌رسانی و حامیان مسابقه به بحث و تبادل نظر پرداختند.

در پایان، جمع حاضر در این ویدئو کنفرانس با برگزاری سومین دوره مسابقه فتح پرچم غرب کشور در آبان ماه و به صورت آنلاین به توافق رسیدند. همچنین مقرر شد تصمیم گیری در خصوص جزییات برگزاری در جلسات آتی در کمیته های تخصصی انجام پذیرد.

کارآموزی در مرکز تخصصی آپا دانشگاه رازی، تابستان ۹۹

علاقمندان در هر یک از حوزه‌های ذکر شده که تمایل به گذراندن دوره کارآموزی در مرکز تخصصی آپا دانشگاه رازی دارند می توانند رزومه خود را به آدرس ایمیل edu.apa@razi.ac.ir ارسال نمایید.

مهلت ارسال: ۳ مرداد ۱۳۹۹



DNS

مرکز تخصصی آپا دانشگاه رازی