بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره بیست و نهم

اسفندماه ۱۳۹۹

باج‌افزارها

همچنان تازنده میدان حملات سایبری

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:

مرکز تخصصی آپا دانشگاه رازی

صفحه آرایی: **سید احسان حسینی، سهیلا مرادی**

همکاران این شماره:

سهیلا مرادی

پویا شکری

سیده آرزو حسنی

آدرس:

کرمانشاه، باغ ابریشم، دانشگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

۰۸۳۳۴۳۴۳۲۵۱

apa@razi.ac.ir

@APARazi

cert.razi.ac.ir

اخبار امنیتی

هدف قرار دادن سرورهای ESXi توسط باج‌افزارهای CARBON SPIDER و SPRITE SPIDER

کمپین‌های باج‌افزاری بزرگ و هدفمند، که از آن‌ها به عنوان Big Game Hunting (BGH) نیز یاد می‌شود، در سال ۲۰۲۰ همچنان تهدید اصلی eCrime (جرایم اینترنتی) برای سازمان‌ها بودند. حجم گسترده و سرعت رشد روزافزون این کمپین‌ها باعث شده است که توجه برخی از متخصصان BGH را به خود جلب کند. به عنوان نمونه گروه SPRITE SPIDER (گروه اپراتورهای باج‌افزار Defray777، که با نام‌های RansomEXX , Defray Defray 2018, Target777,RansomX نیز شناخته می‌شوند)، گروه CARBON SPIDER و گروهی که قبلاً بر روی تسخیر دستگاه‌های POS متمرکز بودند و مسئول معرفی باج‌افزار دارک سایید بودند، از جمله‌ی این موارد هستند. در حالی‌که باج‌افزارها برای سیستم‌عامل لینوکس نیز سال‌های زیادی در دسترس بوده‌اند، مهاجمان BGH لینوکس را بسیار کمتر هدف حملات خود قرار داده‌اند (به طور خاص بسیار کمتر از ESXi hypervisor) این امر به احتمال زیاد نشان دهنده‌ی سلطه‌ی سیستم‌عامل ویندوز در کسب و کارها و سازمان‌های بزرگ است. با این حال، در نیمه دوم سال ۲۰۲۰، SPRITE SPIDER و CARBON SPIDER به ترتیب شروع به استقرار و سازمان‌دهی نسخه‌های لینوکسی Defray777 و Darkside کردند که به طور خاص برای هدف قرار دادن ESXi طراحی شده بودند.

قربانیان این حمله سازمان‌هایی هستند که از مجازی‌سازی برای میزبانی بسیاری از سیستم‌های سازمانی خود بر روی چند سرور ESXi استفاده کرده‌اند. با استقرار باج‌افزارها بر روی میزبان‌های ESXi، مهاجمان توانستند به سرعت دامنه سیستم‌های قربانی درون محیط‌های هدف را افزایش دهند که موجب اعمال فشار اضافی بر قربانیان برای پرداخت تقاضای باج شد.

ESXi چیست؟

ESXi یک هایپروایزر نوع ۱ (ملقب به هایپروایزر"bare-metal" است) که توسط VMware توسعه یافته است. هایپروایزر، نرم‌افزاری است که ماشین‌های مجازی را اجرا و مدیریت می‌کند. برخلاف برخلاف هایپروایزرهای نوع ۲ که بر روی

یک سیستم‌عامل میزبان معمولی اجرا می‌شوند، یک هایپروایزر نوع ۱ مستقیماً بر روی سخت‌افزار یک میزبان اختصاصی اجرا می‌شود. سیستم‌های ESXi معمولاً توسط vCenter که یک ابزار مدیریت سرور متمرکز جهت کنترل چندین دستگاه ESXi است، مدیریت می‌شوند و این در حالیست که ESXi یک سیستم‌عامل لینوکس نیست، بلکه می‌توان برخی از باینری‌های ELF کامپایل شده با لینوکس را در داخل پوسته فرمان ESXi اجرا کرد.

بر اساس بسیاری از برآوردها، VMware دارای اکثریت قریب به اتفاق سهم بازار ماشین مجازی در سراسر جهان و با اختلاف مناسب جلوتر از نزدیک‌ترین رقیب خود است. این بدان معنی است که مهاجمانی که به دنبال رمزگذاری زیرساخت‌های مجازی هستند، ممکن است توسعه بدافزارهایی که می‌توانند بر محیط‌های VMware تأثیر بگذارند را در اولویت قرار دهند.

SPRITE SPIDER و باج‌افزار Defray777

SPRITE SPIDER یک عامل eCrime است که کمپین‌های باج‌افزاری BGH را با استفاده از باج‌افزار Defray777 سازماندهی می‌کند. از دیگر ابزارهای مورد استفاده SPRITE SPIDER، می‌توان به Vatet loader و ابزار دسترسی از راه دور PyXie اشاره کرد. مهاجم با بهره‌برداری از کنترلرهای آسیب‌پذیر Citrix Application De-livery (به عنوان نمونه استفاده از تروجان BokBot) دسترسی اولیه ایجاد می‌کند. همچنین SPRITE SPIDER برای جلوگیری از تشخیص، اغلب بسته‌ها را بر روی سرورهای داخلی درون شبکه قربانی ارسال می‌کند و قرار دادن آن‌ها بر روی حافظه را به مراحل بعدی حمله خود موکول می‌کند.

SPRITE SPIDER از هر دو ابزار PyXie و Cobalt Strike استفاده می‌کند تا بعد از به دست آوردن دسترسی اولیه، برای حرکت‌های آینده (حملات بعدی) خود نیز راهی درون سیستم قربانی باز کند.

همانند دیگر عاملان SPRITE SPIDER، BGH نیز ابتدا تلاش می‌کند تا کنترلرهای دامنه (DCs) را به خطر بیندازد. پس از دستیابی به DC، SPRITE SPIDER داده های قربانی را جمع‌آوری می‌کند و سپس باج‌افزار Defray777 خود را مستقر می‌کند. در نوامبر ۲۰۲۰، SPRITE SPIDER یک وب‌سایت انتشار اطلاعات اختصاصی (DLS) را بر روی یک دامنه مربوط به سرویس مخفی TOR راه‌اندازی کرد تا فایل‌هایی را از قربانیان باج‌افزار منتشر کند.

انتشار داده‌های سرقت شده در واقع تلاشی برای تحت فشار قرار دادن قربانیان به پرداخت بخشی از باج در سیستم BGH است. در مقایسه با دیگر عاملان، BGH SPRITE SPIDER نسبتاً دیرتر (احتمالاً به دلیل جلوگیری از جلب توجه) این تاکتیک را اتخاذ کرد. در ماه ژوئیه سال ۲۰۲۰، SPRITE SPIDER شروع به استفاده از نسخه لینوکس باج‌افزار Defray777 خود کرد. نسخه لینوکس شامل همان منطق اسکن و رمزگذاری فایل، مشابه با نسخه ویندوز است و برای دریافت آرگومان خط فرمان با مسیری به دایرکتوری که در آن روند رمزگذاری بازگشتی خود را آغاز می‌کند، طراحی شده است. فایل‌ها با استفاده از AES در حالت ECB با یک کلید 256 بیتی رمزگذاری می‌شوند که این روند به طور منحصربه‌فرد برای هر فایل ایجاد می‌شود. سپس کلید خصوصی با استفاده از یک کلید عمومی تعبیه شده ۴۰۹۶ بیتی RSA رمزگذاری شده و به فایل رمزگذاری شده پیوست می‌شود. هر قربانی با یک Defray777 منحصربه‌فرد شامل یک کلید عمومی منحصربه‌فرد RSA هدف قرار می‌گیرد. اگر قربانی باج را پرداخت کند، ابزار رمزگشایی را که شامل کلید خصوصی RSA می‌باشد دریافت می‌کند که با کلید رمزگذاری عمومی مطابقت دارد.

نحوه‌ی دسترسی به ESXi توسط گروه SPRITE SPIDER

به منظور تسخیر دستگاه‌های ESXi، گروه SPRITE SPIDER تلاش می‌کند تا مواردی را که می‌تواند برای احراز هویت در رابط وب vCenter استفاده شود، جمع‌آوری کند. SPRITE SPIDER برای بازیابی اطلاعات حساب‌های کاربری vCenter که در مرورگرهای وب ذخیره شده‌اند، از ماژول LaZagne PyXie استفاده می‌کند و همچنین برای سرقت اطلاعات حساب‌های کاربری از حافظه میزبان، Mimikatz را اجرا می‌کند. SPRITE SPIDER پس از احراز هویت درvCenter، دسترسی مداوم به دستگاه‌های ESXi را از طریق SSH فراهم می‌سازد. در برخی موارد، مهاجم رمز ورود حساب کاربری root یا کلیدهای SSH میزبان را نیز تغییر می‌دهد.

نحوه‌ی رمزگذاری ESXi توسط باج‌افزار Defray777

SPRITE SPIDER از تکنیک استقرار در حافظه برای نسخه ویندوز Defray777 استفاده می‌کند، اما در ESXi، با استفاده از یک نام فایل که سعی دارد به عنوان یک فایلی مجاز (مانند svc-new) خود را جا بزند، نسخه‌ی لینوکس Defray777 را در پوشه /tmp/ می‌نویسد. SPRITE SPIDER، با استفاده از دستورات df ،uname و esxcli vm process list اطلاعات سیستم و پردازش‌ها را به دست می‌آورد.

قبل از اجرای Defray777، گروه SPRITE SPIDER برای اینکه به باج‌افزار امکان رمزگذاری فایل‌های مرتبط با ماشین مجازی را بدهد، VMهای در حال اجرا را خاموش می‌کند. SPRITE SPIDER همچنین می‌تواند VMware Fault Domain Manager (FDM) را با استفاده از یک اسکریپت bash به نام VMware-fdm-uninstall.sh حذف کند. FDM ابزاری است که VMها را مانیتور می‌کند و در صورت خرابی VM، آن‌ها را دوباره راه‌اندازی می‌نماید.

CARBON SPIDER و باج‌افزار Darkside

از سال ۲۰۱۶، CARBON SPIDER به طور سنتی شرکت‌های اپراتور دستگاه‌های POS را هدف قرار داده است، که با استفاده از حملات فیشینگ در ابعاد کوچک علیه این بخش‌ها، دسترسی اولیه به این دستگاه‌ها حاصل می‌شد. CARBON SPIDER از درب‌های پشتی و RATهای مختلف برای امکان دسترسی مداوم استفاده می‌کرد. ابزارهای دسترسی مداوم مورد استفاده این گروه، شامل Sekur (معروف به Anunak)، که از سال ۲۰۱۶ مورد استفاده قرار گرفته و همچنین درب پشتی Harpy (معروف به Griffon) است که از ۲۰۱۸ تا ۲۰۲۰ مورد استفاده قرار گرفته است. CARBON SPIDER به طور گسترده‌ای از Cobalt Strike و همچنین ابزارهای منبع باز مانند PowerSploit، برای حرکت‌های (حملات) آینده خود استفاده می‌کند.

در ماه آوریل ۲۰۲۰، مهاجمان این گروه، به طور ناگهانی مدل عملیاتی خود را از فعالیت‌های محدود متمرکز بر روی شرکت‌های دارای دستگاه POS، به عملیات‌هاي گسترده تغییر دادند تا تعداد زیادی از قربانیان را تقریباً در تمامي بخش‌ها مورد هدف قرار

دهند. هدف این کمپین‌ها تحمیل باج‌افزار REvil بود که CARBON SPIDER از عرضه‌کنندگان باج‌افزار به عنوان سرویس (ransomware-as-a-service)، به نام PINCHY SPIDER به دست آورده بود. مشابه SPRITE SPIDER CARBON SPIDER، نیز معمولاً سعی می‌کند قبل از استخراج داده‌ها و استقرار باج‌افزار، یک DC را به خطر بیندازد و مورد تهاجم قرار دهد.

CARBON SPIDER با معرفی باج‌افزار اختصاصی خود به نام Darkside، تعهد خود را نسبت به BGH تا سال ۲۰۲۰ افزایش داد. در آگوست سال ۲۰۲۰، CARBON SPIDER به منظور جلوگیری از تقسیم سود کمپین‌های BGH با PINCHY SPIDER (عرضه‌کننده REVIL)، شروع به استقرار Darkside کرد. در نوامبر سال ۲۰۲۰ ، با ایجاد یک برنامه متصل به RaaS برای Darkside، گام دیگری را در دنیای BGH برداشت و به سایر گروه‌ها اجازه داد تا ضمن پرداخت هزینه CARBON SPIDER، از باج‌افزارش استفاده کنند. مشابه SPRITE SPIDER، گروه CARBON SPIDER نیز از DLS برای Darkside استفاده می‌کند که از آگوست ۲۰۲۰ فعال است.

همچنین در آگوست ۲۰۲۰، CARBON SPIDER شروع به استفاده از نسخه لینوکس Darkside کرد که به طور خاص برای تأثیرگذاري بر میزبان‌های ESXi پیکربندی شده است. نسخه Darkside ESXi فایل‌های مربوط به ماشین‌های مجازی VMware را شامل می‌شود، از جمله فایل‌هایی با پسوندهاي: vmdk، vswp، log، vmxf، vmx، vmss، vmsd، nvram، vmsn، vmem.

فایل‌ها با استفاده از الگوریتم ChaCha20 با یک کلید ۳۲ بایتي و ۸ بایت nonce رمزگذاری می‌شوند و به طور منحصربه‌فرد در هر فایل ایجاد می‌شوند. سپس کلید ChaCha20 و nonce با استفاده از یک کلید عمومی ۴۰۹۶ بیتی RSA که در باج افزار تعبیه شده رمزگذاری می‌شود. همچنین Darkside برای سرعت بخشیدن به روند رمزگذاری، دارای یک اندازه رمزگذاری قابل تنظیم است که می‌تواند برای کنترل میزان رمزگذاری هر فایل استفاده شود. در نمونه‌های بازیابی شده توسط CrowdStrike Intelligence، اندازه رمزگذاری روی ۵۰ مگابایت تنظیم شده است، که میزاني کافی برای جلوگیری از بازیابی فایل‌های ماشین مجازی است. نمونه‌ای از پیکربندی Darkside، (همانطور که در فایل لاگ آن نوشته شده است) در تصویر زیر نشان داده شده است.

```
[CFG] Root Path.............. REDACTED
[CFG] Key Size.....548 Bytes
[CFG] Public Key.....VALID
[CFG] Part Size.....50mb
[CFG] Search Extension.....vmdk,vswp,vmem,vmsn,nvram,vmsd,vmss,vmx,vmxf,log
[CFG] New Extension..... REDACTED
[CFG] Thread Count.....8
[CFG] ReadMe File.....Dark-ReadMe.TXT
[CFG] ReadMe Size..... REDACTED
```

نحوه‌ی دسترسی به ESXi توسط گروه CARBON SPIDER

مشابه SPRITE SPIDER، گروه CARBON SPIDER نیز با استفاده از اطلاعات ورود معتبر به سرورهای ESXi دسترسی پیدا کرده‌اند. مهاجمان معمولاً از طریق رابط وب vCenter با استفاده از اطلاعات ورود معتبر به این سیستم‌ها دسترسی پیدا می‌کنند، اما همچنان با استفاده از قابلیت Plink برای حذف Darkside، از طریق SSH وارد سیستم می‌شوند.

نحوه‌ی رمزگذاری ESXi توسط باج‌افزار Darkside

CARBON SPIDER، Darkside را در پوشه /tmp/ بر روی میزبان‌های ESXi با یک نام عمومی می‌نویسد. در CARBON SPIDER، مهاجم معمولاً به اندازه‌ی SPRITE SPIDER میزبان را شناسایی نمی‌کند و برای خاموش کردن VMهای میهمان، از اسکریپت، های VMware Tools داخلی استفاده می‌کند تا مطمئن شود این VMها توسط Darkside رمزگذاری شده‌اند.

نتیجه

با استقرار باج‌افزار بر رویSPRITE SPIDER ، ESXi و CARBON SPIDER احتمالاً قصد دارند آسیب‌های شدیدتری را به قربانیان تحمیل کنند. رمزگذاری یک سرور ESXi، به اندازه‌ی زمانی که باج‌افزار را به صورت جداگانه در هر VM میزبانی شده در یک سرور خاص مستقر می‌کنید، موجب آسیب می‌شود. در نتیجه، هدف قرار دادن میزبان‌های ESXi می‌تواند سرعت عملیات BGH را بهبود بخشد.

اگر این حملات باج‌افزاری به سرورهای ESXi موفقیت‌آمیز باشد، به احتمال زیاد به زودی مهاجمان بیشتری هدف قرار دادن زیرساخت‌های مجازی‌سازی را آغاز می‌کنند.

جدول زیر مروری بر تاکتیک‌ها و تکنیک‌ها و روش‌های SPRITE SPIDER و CARBON SPIDER مربوط به حملات باج‌افزاری ESXi را نشان می‌دهد.

خلاصه	CARBON SPIDER	SPRITE SPIDER	تکنیک	تاکتیک
SPRITE SPIDER و CARBON SPIDER با استفاده از اطلاعات ورود معتبر در vCenter احراز هویت می‌شوند.	بله	بله	T1078 – اطلاعات حساب‌های کاربری معتبر	دسترسی اولیه
مهاجمان از ESXi command shell برای اجرای باج‌افزار استفاده می‌کنند.	بله	بله	T1059.004 - مفسر دستورالعمل: Unix Shell	اجرا
اطلاعات ورود حمله‌ی قبلی، دسترسی مداوم را امکان‌پذیر می‌کند.	بله	بله	T1078 – حساب‌های کاربری معتبر	ماندگاری
SPRITE SPIDER کلیدهای root SSH را برای میزبان‌های ESXi تغییر داده است.		بله	T1098.004 - کلیدهای احرازهویت شده‌ی SSH	ماندگاری
هر دو با استفاده از تغییر chmod، باینری‌های باج‌افزار موردعلاقه‌ی خود را به عنوان "قابل اجرا" علامت‌گذاری می‌کنند.	بله	بله	T1222.002 - اصلاح مجوزهای فایل و دایرکتوری: اصلاح مجوزهای فایل و دایرکتوری Linux و Mac	دور زدن سیستم دفاعی
Defray777 و Darkside از نام فایل‌هایی استفاده می‌کنند که به نظر مجاز هستند.	بله	بله	T1036.005 – ظاهرسازی: تطابق دادن یا یک نام یا محل مجاز	دور زدن سیستم دفاعی
SPRITE SPIDER پس از اجرا ممکن است باینری فایل Defray777 را حذف کند.		بله	T1070.004 - حذف شاخص در سیستم میزبان: حذف فایل	دور زدن سیستم دفاعی
SPRITE SPIDER شناسایی اولیه را انجام می‌دهد (به عنوان مثال، uname، df)		بله	T1082 - کشف اطلاعات سیستم	کشف
SPRITE SPIDER شناسایی اولیه را انجام می‌دهد (به عنوان مثال، لیست فرآیند esxcli (vm		بله	T1057 - کشف پردازش	کشف
ممکن است هر دو سعی در خاتمه دادن VMهای در حال اجرا داشته باشند.	بله	بله	T1489 - توقف سرویس	اختلال در کار سیستم
Defray777 و Darkside سیستم‌های قربانی را رمزگذاری می‌کنند.	بله	بله	T1486 - رمزگذاری داده‌ها برای آسیب	اختلال در کار سیستم

منبع خبر :

Scan Link

هشدار در خصوص افزایش احتمال رخداد حملات باج‌افزاری در اثر به‌روزرسانی نرم‌افزارها از راه دور برای حل مشکل تاریخ ۱۴۰۰

بررسی‌های مرکز ماهر و گزارش مرکز آپای تخصصی دانشگاه بجنورد، نشان می‌دهد، آمار رخداد حملات باج‌افزار ی از طریق نفوذ به پروتکل‌ها و ابزارهای دسترسی از راه دور، رو به افزایش است. این افزایش به طور مشهود به دلیل آن است که شرکت‌های پشتیبان محصولات نرم‌افزاری که برای پردازش تاریخ‌های پس از ۱۴۰۰/۰۱/۰۱ نیازمند به‌روزرسانی محصولات نصب شده در محل مشتریان دولتی و خصوصی می‌باشند، عموماً این خدمت را از راه دور عرضه می‌نمایند. رخداد حمله باج افزاری با استفاده از رخنه به پروتکل‌ها و ابزارهای دسترسی از راه دور از گذشته امری معمول بوده است. این نفوذ به سه طریق ذیل اتفاق می‌افتد:

– سادگی رمز عبور، عدم تنظیم محدودیت در تعداد دفعات مجاز برای تلاش ناموفق ورود رمز و سایر کاستی‌ها در تنظیمات.

– وجود آسیب پذیری در پروتکل‌ها و ابزارهای دسترسی از راه دور.

– وجود بدافزار سرقت اطلاعات و جاسوسی بر روی کامپیوتری که با آن دسترسی راه دور برقرار می‌شود (و نه الزاما سرور قربانی).

راهکار

برای مقابله با این مخاطرات می‌توان به هشدارها و راهکارهایی که به طور مکرر مرکز ماهر و سایر متولیان امر منتشر نموده اند مراجعه نمود اما به اختصار فهرست زیر اهم موارد را ارائه می‌کند.

- عدم استفاده از دسترسی راه دور به‌ویژه بر بستر اینترنت تا جای ممکن.
- تهیه منظم نسخ پشتیبان، مخصوصاً قبل از ارائه دسترسی راه دور و توجه ویژه به این نکته که قرار دادن نسخه‌ای از اطلاعات پشتیبان بر روی رسانه‌ای که به صورت برخط در دسترس است یا عدم آزمایش صحت نسخه پشتیبان تهیه شده ابداً پشتیبان‌گیری به حساب نمی‌آید.
- به‌روزرسانی منظم پروتکل‌ها و ابزارهای دسترسی از راه دور و عدم استفاده از نسخ قدیمی سیستم‌عامل‌هایی که آسیب‌پذیری‌های شناخته شده دارند ولی پشتیبانی و به‌روزرسانی آنها متوقف شده است. همچنین دقت در به‌روز و فعال بودن آنتی ویروس.
- انجام تنظیمات امنیتی لازم برای دسترسی از راه دور بر روی سرور از جمله تنظیم عدم قبول قرار دادن رمز عبور ساده یا تکراری و همچنین اجبار به تغییر دوره ای رمز عبور در بازه های زمانی معقول، انجام دادن تنظیم محدودیت در تعداد، محدود کردن تعداد دفعات مجاز برای تلاش ناموفق ورود.
- محدود کردن ساعت دسترسی راه دور به ساعات معمول یا اداری.
- محدود کردن کاربران مجاز به دسترسی راه دور و محدود کردن دسترسی ایشان به منابع مورد نیاز و استفاده از احراز هویت دومرحله‌ای و VPN در پروتکل‌ها و ابزارهای دسترسی از راه دور.
- محدود کردن دسترسی به پورت‌های مورد استفاده برای پروتکل‌ها و ابزارهای دسترسی از راه دور به آدرس‌های مشخص از طریق لیست‌های کنترل دسترسی در فایروال‌ها و ابزارهای امنیتی.
- غیرفعال کردن امکانات، پروتکل‌ها و ابزارهای دسترسی از راه دور به محض اتمام نیاز.
- نظارت مستمر بر دسترسی راه دور مخصوصا در زمان برقراری ارتباط.
- دقت مضاعف در به روز و فعال بودن آنتی‌ویروس در سیستم مبدا دسترسی راه دور، همچنین دقت در عدم به کار گیری ماشین‌هایی با گذشته کاربرد نامعلوم (مثلا رایانه‌های دم دستی مورد استفاده برای گشت و گذار در وب یا در معرض اتصال مکرر حافظه‌های جانبی مشکوک).
- تشریح و تبیین دقیق مسئولیت و وظایف امنیتی برای کسانی که از راه دور برای ارایه خدمت متصل می‌شوند.
- کمک گرفتن از تیم های امداد سایبری در صورت مشاهده هرنوع فعالیت مشکوک.

اخبار کوتاه

واکسن‌های کووید اکنون بهانه‌ای برای شروع حملات فیشینگ هستند

با مشقت پس از یکسال از شناسایی ویروس کرونا به عنوان یک تهدید، اکنون چندین واکسن تولید شده که در سراسر جهان در حال استفاده هستند و زندگی‌ها را نجات می‌دهند. مجرمان اینترنتی خیلی خوب می‌دانند که مردم مشتاق دریافت واکسن هستند. آن‌ها با هدف قرار دادن تمایل افراد به زدن واکسن در حال راه‌اندازی کمپین‌های فیشینگ و دستیابی به موفقیت‌های گسترده هستند. به گفته وبروت یک شرکت امنیت سایبری از زمان دریافت دوز واکسن کووید ۱۹ توسط اولین شخص در جهان ۳۳۶ درصد دامنه فیشینگ یافت شده است. جنبه مهندسی اجتماعی شکار کردن مردم به واسطه ترس ترکیب شده وغوغایی ایجاد کرده که به نفع مجرمان سایبری است که متأسفانه بسیار هم خوب کار می کند. تجزیه و تحلیل شرکت امنیتی وبروت نشان می‌دهد که این کلاهبرداری‌های ساده ای نیستند و در مقیاس عظیم و بی نظیر انجام می‌شوند. URLهای فیشینگ شامل عباراتی مانند "COVID-19"، "Corona"، "واکسن"، "Cure COVID" و موارد دیگراست. عاملان ایجاد صفحات فیشینگ در تلاش هستند مردم را فریب دهند و تا مردم فکر کنند که آن‌ها در حال بازدید از یک وب‌سایت رسمی‌اند در حالی‌که اینطور نیست. برای افراد دفاع در برابر این نوع حملات باید شامل آموزش آگاهی از امنیت و هوشیار ماندن در بررسی دقیق انواع ایمیل های دریافتی آن‌ها باشد این امر همچنین باید توسط فناوری امنیت سایبری مانند فیلتر کردن ایمیل محافظت از آنتی ویروس و استفاده از رمز عبور قوی باشد.

آسیب پذیری

آسیب‌پذیری RCE در Microsoft Exchange Server

در تاریخ ۲ مارس، چندین آسیب‌پذیری روزصفر با شدت بحرانی و بالا دارای شناسه‌های CVE-2021-26855، CVE-2021-27078، CVE-2021-26858، CVE-2021-26412، CVE-2021-26857 و CVE-2021-27065 و CVE-2021-26854 برای Microsoft Exchange Server منتشر شد.

خطرناک‌ترین آسیب‌پذیری، SSRF است که به مهاجم اجازه می‌دهد به سرور Microsoft Exchange دسترسی گرفته و امکان سرقت و استخراج محتوای کامل Mailbox را داشته باشد.

این آسیب‌پذیری به هیچ‌گونه سطح دسترسی نیاز نداشته و تنها با داشتن آدرس IP خارجی سرور Exchange قابل انجام می‌باشد. به‌منظور بهره‌برداری از این آسیب‌پذیری، مهاجم می‌تواند با ارسال درخواست‌های HTTP دلخواه با متد POST حاوی پیلود XML SOAP به سمت API Exchange Web Services (EWS) و با استفاده از کوکی‌های خاص ساخته‌شده، احراز هویت را دور بزند و با فریب Exchange Server، دستوراتی را که هرگز مجاز به اجرای آن‌ها نیست اجرا نماید (مانند احراز هویت به‌عنوان Exchange Server و یا انجام هرگونه عملیات دلخواه بر روی صندوق پستی کاربران).

دو آسیب‌پذیری دیگر نقص نوشتن فایل پس از احراز هویت در Exchange هستند که به مهاجم اجازه می‌دهند پس از احراز هویت در Exchange server، از این نقص برای نوشتن هر نوع فایلی در هر مسیر دلخواه بر روی سرور، سوءاستفاده نماید. مهاجم با بهره‌برداری از آسیب‌پذیری CVE-2021-26855، یا تسخیر سیستم با استفاده از اطلاعات حساب کاربری ادمین، می‌تواند احراز هویت کند و از این آسیب‌پذیری بهره‌برداری نماید.

آسیب‌پذیری دیگر به دلیل deserialization ناامن در سرویس Unified Messaging به وجود می‌آید. این فرایند زمانی صورت می‌گیرد که داده‌های غیرقابل‌اعتماد و تحت کنترلِ کاربر، توسط یک برنامه deserialize شوند. بهره‌برداری از این آسیب‌پذیری منوط به اجازه مدیر و یا وجود آسیب‌پذیری دیگری در سیستم می‌باشد. بهره‌برداری موفق از این آسیب‌پذیری مهاجم را قادر می‌سازد کد دلخواه خود را با سطح

دسترسی SYSTEM در Exchange server اجرا نماید.

سه آسیب‌پذیری دیگر نیز آسیب‌پذیری‌های اجرای کد از راه دور در Microsoft Exchange Server که به مهاجم اجازه می‌دهند کدهای دلخواه خود را از راه دور بر روی سیستم اجرا نماید. درصورتی‌که مهاجم بتواند به‌عنوان یک کاربر دارای سطح دسترسی بالا (مانند Administrator) احراز هویت کند، می‌تواند از طریق دسترسی به تمام فایل‌ها و تنظیمات سیستم، کد دلخواه خود را اجرا نموده و از این آسیب‌پذیری بهره‌برداری نماید.

مهاجم همچنین با ارسال درخواست‌های ساختگی خاص می‌تواند از این آسیب‌پذیری‌ها بهره‌برداری نموده و کدهای دلخواه خود را با سطح دسترسی بالا در سیستم قربانی اجرا نماید.

Microsoft Exchange Server نسخه‌های ۲۰۱۳، ۲۰۱۶ و ۲۰۱۹ تحت تأثیر این آسیب‌پذیری‌ها قرار دارند.

توصیه امنیتی

توصیه می‌شود هر چه سریع‌تر نسبت به اعمال به‌روزرسانی‌های منتشر شده اقدام شود.

اقدامات کاهشی

ازآنجاکه این آسیب‌پذیری‌ها به‌عنوان بخشی از یک حمله‌ی زنجیره‌ای مورداستفاده قرار می‌گیرند و حمله‌ی اولیه نیازمند برقراری یک ارتباط غیرقابل‌اعتماد بر روی پورت ۴۴۳ از Exchange server است، بنابراین می‌توان با محدود نمودن ارتباطات غیرقابل اعتماد، یا استفاده از VPN به‌منظور جلوگیری از دسترسی خارج از شبکه، از آن محافظت نمود و خطرات ناشی از این آسیب‌پذیری‌ها را کاهش داد.

منبع خبر :

Scan Link

آسیب‌پذیری در محصولات شرکت VMware

سه آسیب‌پذیری با شدت بحرانی، بالا و متوسط دارای شناسه‌های CVE-2021-21974، CVE-2021-21972 و CVE-2021-21973 برای برخی از محصولات VMWare منتشر شده است.

آسیب‌پذیری CVE-2021-21972، در قابلیت vROPs از پلاگین vCenter Server وجود دارد.

پلاگین vCenter Server به منظور ارائه قابلیت‌های بیشتر در vSphere Client (HTML5) مورد استفاده قرار می‌گیرد و نقص موجود در آن، امکان اجرای کد از راه دور را برای مهاجم فراهم می‌کند. در واقع، این آسیب‌پذیری به مهاجم اجازه می‌دهد در سیستم آسیب‌پذیر فایل دلخواه خود را بارگذاری نموده و از این طریق کد موردنظر خود را از راه دور اجرا نماید. این پلاگین در تمام نصب‌های پیش‌فرض در دسترس است و امکان حملات گسترده‌ای را برای مهاجمان فراهم می‌آورد. یک مهاجم با دسترسی به پورت ۴۴۳ در شبکه می‌تواند با اجرای دستورات دلخواه، با سطح دسترسی نامحدود در سیستم‌عاملی که vCenter Server را میزبانی می‌کند، از این آسیب‌پذیری بهره‌برداری نماید. تهدید اصلی برای بهره‌برداری از این آسیب‌پذیری از جانب افرادی است که با استفاده از سایر روش‌ها _مانند مهندسی اجتماعی یا آسیب‌پذیری‌های وب_ به شبکه نفوذ کرده‌اند و یا از طریق درب‌های پشتی که قبلاً نصب کرده‌اند به شبکه‌ی داخلی دسترسی دارند.

آسیب‌پذیری CVE-2021-21974، یک نقص سرریز حافظه‌ی هیپ است و سرویس OpenSLP را در ESXi تحت تأثیر قرار می‌دهد. این نقص به مهاجم اجازه می‌دهد بتواند کد دلخواه خود را از راه دور بر روی سیستم آسیب‌پذیر اجرا نماید. مهاجمی که در همان بخش از شبکه‌ی ESXi به پورت ۴۲۷ دسترسی دارد ممکن است بتواند با ایجاد یک بسته‌ی درخواست مخرب، موجب سرریز حافظه‌ی هیپ در سرویس OpenSLP شود و امکان اجرای کد از راه دور را در سیستم آسیب‌پذیر به دست آورد.

آسیب‌پذیری CVE-2021-21973، نقص SSRF در vSphere Client (HTML5) است، که به دلیل اعتبارسنجی نامناسب URLها در پلاگین vCenter Server وجود دارد و می‌تواند منجر به افشای اطلاعات حساس شود.

محصولات زیر تحت تأثیر این آسیب‌پذیری‌ها قرار دارند:

- vCenter Server 6.5, 6.7, 7.0
- Cloud Foundation (vCenter Server) 3x, 4x
- ESXi 6.5, 6.7, 7.0
- Cloud Foundation (ESXi) 3x, 4x
- vCenter Server 6.5, 6.7, 7.0
- Cloud Foundation (vCenter Server) 3.x, 4.x

توصیه امنیتی

توصیه می‌شود هر چه سریع‌تر نسبت به اعمال به‌روزرسانی‌های منتشر شده اقدام شود.

منبع خبر :

Scan Link

آسیب‌پذیری در پلاگین Ninja Forms وردپرس که سایت را در معرض خطر هک قرار می‌دهد

این پلاگین محبوب با بیش از یک میلیون نصب فعال در سایت‌های وردپرسی، حاوی ۴ آسیب‌پذیری بحرانی است که سایت را در معرض خطر حملات جدی قرار می‌دهد، نمـــونه‌ای از این حمـــلات در دست گرفتن کنترل کامل سایت توسط هـــکر و email hijacking می‌باشد.

Ninja Forms یک پلاگین محبوب برای وردپرس است که به طراحان سایت اجازه می‌دهد بدون داشتن مهارت برنامه‌نویسی فرم‌هایی با قابلیت drag-and-drop ایجاد کنند.

این ۴ آسیب‌پذیری برای کاربری با سطح دسترسی پایین (حتی یک کاربر ساده که فقط در سایت ثبت‌نام کرده باشد) امکان انجام فعالیت‌های مخربی را فراهم می‌آورد. این فعالیت‌های مخرب می‌توانند شنود ایمیل‌های سایت، در دست گرفتن حساب‌های کاربری ادمین، نصب پلاگین‌های دلخواه در سایت مورد هدف و هدایت مالکان سایت به مقصدهای مخرب باشند.

سه مورد از آسیب‌پذیری‌ها برای بهره‌برداری موفقیت‌آمیز، به مهندسی اجتماعی نیاز دارند.

- **آسیب‌پذیری اول:** ربودن ایمیل‌های معتبر و در دست گرفتن حساب‌های کاربری با پلاگین SendWP

به گفته‌ی محققان، این نقص به مهاجمان دارای سطح دسترسی اعضا یا بالاتر اجازه می‌دهد تا از SendWP برای دریافت ترافیک ایمیل، شامل پیوندهای بازیابی رمز عبور برای حساب‌های کاربری ادمین سوءاستفاده کنند. SendWP یک سرویس تحویلِ ایمیل و ورود به سیستم است که به منظور ساده‌سازی مدیریت ایمیل‌ها در وردپرس طراحی شده است.

مهاجمان با سطح دسترسی اعضا یا بالاتر به سایت وردپرسیِ آسیب‌پذیر می‌توانند با برقراری یک ارتباط SendWP[1] با حساب کاربری SendWP خویش، تمام ایمیل‌های ارسال شده به سایت وردپرسی را به حساب کاربری SendWP خود که با آن وارد شده‌اند هدایت کنند. به گفته‌ی Wordfence، بهره‌برداری موفق از این آسیب‌پذیری می‌تواند منجر به اجرای کد از راه دور و در دست گرفتن کنترل کامل سایت با استفاده از حساب کاربری ادمین شود. مهاجم می‌تواند از حساب کاربری ادمین برای ویرایش قالب/فایل‌های پلاگین یا بارگذاری یک قالب/ پلاگین مخرب استفاده کند. گفته می‌شود این آسیب‌پذیری دارای شدت ۹.۹ از ۱۰ می‌باشد (هنوز شناسه‌ای برای نقص‌ها در نظر گرفته نشده است).

محققان هشدار دادند: "هنگام برقراری ارتباط SendWP توسط مهاجمان، آن‌ها می‌توانند تمام داده‌های ایمیل شده را که از طریق فرم ثبت اطلاعات قابل شناسایی افراد (PII[2]) _که به منظور گزارش‌گیری در سایت در نظر گرفته شده‌اند_ به دست می‌آیند، مانیتور کنند." به علاوه، اگر مهاجم بتواند نام کاربری یک حساب ادمین را به دست آورد، آنگاه قادر خواهد بود رمزعبور را برای آن حساب کاربری بازنشانی کند." به گفته‌ی Wordfence، دستیابی به این مسئله چندان دشوار نیست.

محققان تشریح کردند: "به منظور ارائه‌ی این عملکرد، پلاگین، کُنش AJAX مربوط به wp_ajax_ninja_forms_sendwp_remote_install را ثبت می‌کند." این کُنش AJAX به تابع wp_ajax_ninja_forms_sendwp_remote_install_handler متصل است که بررسی می‌کند پلاگین SendWP نصب و فعال شده باشد. اگر پلاگین در حال حاضر نصب نشده باشد، نصب و فعال‌سازی پلاگین را انجام می‌دهد.

به محض اینکه پلاگین با موفقیت نصب شود، تابع، url ثبت‌نام را به همراه register_url، client_secret، client_name و client_url باز می‌گرداند. این برای نشان دادن صفحه‌ی ثبت‌نام به کاربران و اتصال آسان نمونه سایت وردپرسی با SendWP می‌باشد.

تجزیه و تحلیل‌ها نشان می‌دهد متأسفانه این کُنشAJAX قابلیت بررسی پلاگین SendWP و هیچگونه محافظتی برnonce ندارد، بنابراین، نصب و فعال‌سازی آن این امکان را می‌دهد که کاربران سطح پایین، مانند اعضای عادی سایت بتوانند این پلاگین را نصب و فعال کنند و کلید client_secret را که برای ایجاد ارتباط SendWP مورد نیاز است بازیابی نمایند.

البته محققان خاطرنشان کردند که خوشبختانه پلاگین SendWP یک پلاگین غیررایگان است _ماهیانه ۹ دلار برای هر سایت_ و این را می‌توان یک راه کاهش خطر بالقوه برای نقص مذکور در نظر گرفت.

- **آسیب‌پذیری دوم:** افشای کلید اتصال پروتکل احراز هویت OAuth

برای این آسیب‌پذیری شدت ۷.۷ از ۱۰ برآورد شده است و در سرویس "Add-on Manager" از پلاگین Ninja Forms وجود دارد. این سرویس یک داشبورد متمرکز است که به کاربران امکان می‌دهد از راه دور تمام افزونه‌های خریداری شده Ninja Forms را مدیریت کنند.

به گفته‌ی Wordfence، مهاجمان می‌توانند با حساب کاربری خود یک ارتباط OAuth برای سایت وردپرسی آسیب‌پذیر برقرار کنند و هرگونه پلاگینِ افزونه‌ایِ خریداری شده را در سایت مورد نظر خود نصب کنند.

به منظور تکمیل این ارتباط مخرب، مهاجمان باید مدیران سایت را برای کلیک بر روی یک لینک خاص فریب دهند تا پارامتر client_id در پایگاه داده سایت با یک action AJAX تغییر یافته آپدیت شود.

طبق این تجزیه و تحلیل، پلاگین نامبرده، کُنش AJAX مربوط به wp_ajax_nf_oauth- را ثبت می‌کند که برای بازیابی connection_url که حاوی اطلاعات مهمی است _مانند client_secret برای برقراری ارتباط OAuth با پورتال Ninja Forms Add-On Management _ مورد استفاده قرار می‌گیرد و متأسفانه قابلیت بررسی این تابع وجود ندارد. و این بدان معناست که کاربران سطح پایین، مانند اعضای عادی سایت

---

[1] SendWP connection
[2] personally identifiable information

می‌توانند action را فعال کرده و URL مورد نیاز برای برقراری ارتباط با داشبورد را بازیابی کنند. مهاجمان همچین می‌توانند client_id را برای ارتباطِ فعلیِ OAuth بازیابی کنند.

آسیب‌پذیری سوم: حمله‌ی CSRF برای قطع ارتباط سرویس OAuth

آسیب‌پذیری سوم نیز در قابلیت مدیریت افزونه‌های Ninja Forms وجود دارد که به راحتی یک ارتباط OAuth را با چند کلیک ساده قطع می‌کند. برای این آسیب‌پذیری شدت متوسط با مقدار ۶.۱ در نظر گرفته شده است.

مهاجمان می‌توانند با ارسال یک درخواست، ارتباط فعلیِ OAuth را قطع کنند. Wordfence خاطرنشان کرد که: "این می‌تواند یک تجربه‌ی گیج‌کننده برای مالک سایت باشد." برای انجام این کار، مهاجمان باید یک درخواست معتبر بسازند، آن را در خارج از سایت مورد هدف میزبانی کنند و مدیر سایت هدف را مجاب کنند تا بر روی یک لینک یا فایل پیوست کلیک کند.

به گفته‌ی Wordfence، "به منظور ارائه این عملکرد، پلاگین، کُنش AJAX مربوط به wp_ajax_nf_oauth_disconnect را که متصل به تابع ()disconnect می‌باشد ثبت می‌کند. تابع ()disconnect به سادگی یک ارتباط را با حذف موارد مربوط به تنظیمات ارتباط در پایگاه داده، قطع می‌کند."

آسیب‌پذیری چهارم: نقص Administrator Open Redirect

آخرین نقص، در فرایند پردازش ارتباط OAuth وجود دارد. شدت این آسیب‌پذیری متوسط و مقدار آن ۴.۸ از ۱۰ می‌باشد.

به منظور بهره‌برداری از این آسیب‌پذیری، مهاجم باید یک URL خاص با پارامتر تغییر مسیر بسازد که برای هدایت به سایت دلخواهی تنظیم شود، سپس با مهندسی اجتماعی ادمین را وادار به کلیک بر روی یک لینک نماید. اگر این فرایند موفقیت‌آمیز باشد، ادمین به یک سایت خارجی مخرب هدایت می‌شود که می‌تواند سیستم وی را با بدافزار آلوده کند.

تجزیه و تحلیل‌ها نشان می‌دهد، این پلاگین، کُنش AJAX مربوط به wp_ajax_nf_oauth_connect را ثبت می‌کند که متصل به تابع ()connect می‌باشد. این تابع برای هدایت مالک سایت و بازگشت وی به سرویس Ninja Forms وردپرس پس از اتمام فرایند برقراری ارتباط OAuth می‌باشد. این تابع به طور پیش‌فرض برای هدایت مالک سایت و بازگشت به صفحه‌ی admin.php?page=nin-ja-forms#services از wp_safe_redirect استفاده می‌کند.اکنون مسئله این است که پارامتر 'redirect' می‌تواند با مقادیر مختلفی جایگزین شود تا ادمین سایت را به URL دلخواهی که در این پارامتر آمده است هدایت کند. محققان تشریح کردند: "هیچ‌گونه محافظتی جهت اعتبارسنجی مقصدی که در URL هدایت مسیر می‌آید وجود ندارد و همچین برای جلوگیری از استفاده از این تابع توسط مهاجمان که ادمین را به مقاصد مخرب هدایت نکنند راهی وجود ندارد." البته پیش از این، تابع ()wp_verify_nonce مورد استفاده قرار می‌گرفت اما پس از ارائه توضیحاتی، منسوخ و غیرقابل استفاده شد.

آسیب‌پذیری‌های مذکور در نسخه‌ی ۳.۴.۳۴.۱ پلاگین Ninja Forms برطرف شده‌اند.

منبع خبر :

Scan Link

آسیب‌پذیری‌های بحرانی در محصولات F5

شرکت F5 برای چند آسیب‌پذیری بحرانی موجود در محصولات BIG-IP به‌روزرسانی‌هایی را منتشر کرده است؛ این آسیب‌پذیری‌های بحرانی در نسخه‌های ۱۱.۶.۵.۳، ۱۲.۱.۵.۳، ۱۳.۱.۳.۶، ۱۴.۱.۴، ۱۵.۱.۲.۱ و ۱۶.۰.۱.۱ محصول BIG-IP و در نسخه‌های ۸.۰.۰، ۷.۱.۰.۳ و ۷.۰.۰.۲ محصول BIG-IQ برطرف شده است. راهکارهای موقت کاهش مخاطرات ناشی بهره‌برداری از این آسیب‌پذیری های بحرانی برای هر آسیب‌پذیری (در صورت وجود) به شرح زیر است:

- **آسیب‌پذیری CVE-2021-22992:** برای کاهش مخاطرات بهره‌برداری از این آسیب‌پذیری می‌توانید از iRule ارائه شده توسط F5 در پیوند زیر برای سرورهای مجازی آسیب‌پذیر، استفاده کنید. این iRule پاسخ دریافتی از سرور را بررسی کرده و برای پاسخ‌های آسیب‌پذیر خطای ۵۰۲ برمی‌گرداند.

https://support.f5.com/csp/article/K52510511

- **آسیب‌پذیری CVE-2021-22987:** از آنجایی که بهره‌برداری از این آسیب‌پذیری فقط توسط کاربران احراز هویت شده و مجاز امکان‌پذیر است، به جز قطع دسترسی کاربران غیر قابل اعتماد به برنامه‌ی پیکربندی، هیچ راهکار موقت مطمئنی برای کاهش مخاطرات این آسیب‌پذیری وجود ندارد. اطلاعات بیشتر در پیوند زیر موجود است:

https://support.f5.com/csp/article/K18132488

- **آسیب‌پذیری CVE-2021-22986:** محدودسازی iControl REST به شبکه‌ها و تجهیزات قابل اعتماد. اطلاعات بیشتر در خصوص نحوه‌ی مسدود کردن دسترسی به iControl REST در پیوند زیر موجود است:

https://support.f5.com/csp/article/K03009991

جزییات آسیب‌پذیری‌ها

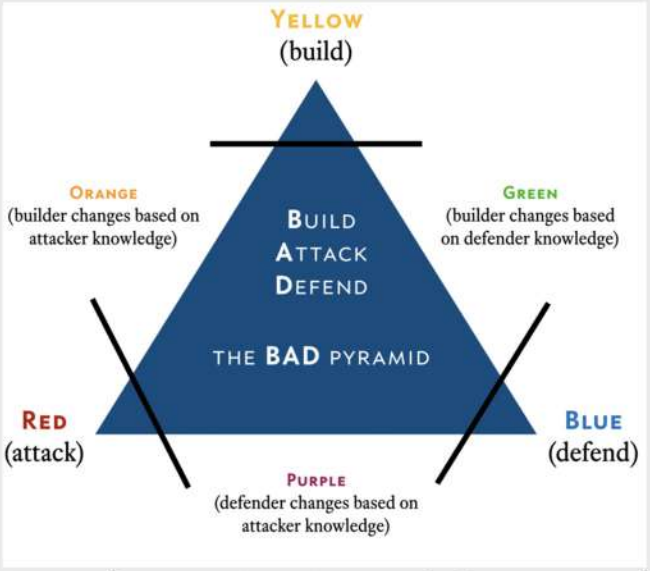
مهم‌ترین آسیب‌پذیری‌های این به‌روزرسانی، آسیب‌پذیری‌های بحرانی CVE-2021-22987 و CVE-2021-22986 با شدت ۹.۹ و ۹.۸ است. آسیب‌پذیری CVE-2021-22986 برای مهاجم احراز هویت نشده که از طریق شبکه به رابط iControl REST دسترسی دارد، امکان اجرای دستورات دلخواه سیستمی، ایجاد یا حذف فایل‌ها و غیرفعال‌سازی سرویس‌ها را فراهم می‌کند. سیستم‌های BIG-IP در حالت Appliance نیز آسیب‌پذیر هستند.

منبع خبر :

Scan Link

مقالات آموزشی

معرفی تیم‌های امنیت سایبری زرد، نارنجی و سبز (بخش دوم)



آپریل رایت در برنامه Blackhat علاوه بر مفاهیم تیم‌های معروف قرمز، آبی و بنفش، با شجاعت چند مدل تیم امنیت سایبری دیگر را نیز معرفی می‌کند و به عقیده وی، تیم نارنجی همان تیم بنفش جدید است.

رایت در این برنامه، از مفهوم تیم نارنجی سخن می‌گوید که اعضای آن، سازندگان[1] هستند و سپس آن را با تیم‌های امنیت آبی و قرمز ترکیب می‌کند تا رنگ‌های دیگر را ایجاد کند. این کار بسیار هوشمندانه است، اما نسبت به برخی از خصوصیات این ترکیب‌ها، نقدهایی وجود دارد. تفسیر منحصربه‌فردی از این تعاملات ترکیبی در بالا نشان داده شده که اقتباسی از مدل آپریل است.

همچنین باور دیگری وجود دارد که لزومی به گذاشتن عنوان «تیم» بر این رنگ‌ها نیست، چرا که در بیشتر موارد، این رنگ‌ها در واقع بیانگر ذهنیت یا نقش هستند و کمتر به گروه‌هایی اختصاصی از افراد اشاره دارند. به عنوان مثال، تیم زرد، خود عنوان دیگری دارد و اعضای این تیم در واقع همان Developers یا توسعه‌دهندگان هستند. در حقیقت باید به جای عناوین سبز، نارنجی و بنفش از همان Developers یا رفتارهای تیم آبی استفاده شود.

خلاصه‌ای از نقش و عملکرد امنیتی رنگ‌ها

- زرد: Builder یا سازنده
- قرمز: Attacker یا مهاجم
- آبی: Defender یا مدافع
- سبز: سازنده‌ای که از مدافع می‌آموزد
- بنفش: مدافعی که از مهاجم می‌آموزد
- نارنجی: سازنده‌ای که از مهاجم می‌آموزد

[1] Builders

مشکلات رایج در تعاملات تیم‌های امنیت قرمز و آبی

در حالت ایده‌آل، تیم‌های امنیت قرمز و آبی با بیشترین حد هماهنگی با هم در تعامل هستند، همان طور که دو دست با یکدیگر توانایی دست زدن را ایجاد می‌کنند.

تاکتیک‌ها و رفتارهای تیم‌های امنیت قرمز و آبی، مانند Yin و Yang یا حمله و دفاع، در تضاد کامل با یکدیگر هستند اما دقیقاً همین تفاوت‌ها آن‌ها را به صورت بخشی از یک مجوعه سالم و تاثیرگذار مبدل می‌کند. تیم قرمز حمله و تیم آبی دفاع می‌کند، اما در هدف اصلی مشترک هستند: هردو می‌خواهند وضعیت امنیت سازمان را بهبود بخشند.

برخی از مشکلات برخاسته از تعامل و همکاری تیم‌های قرمز و آبی در زیر آورده شده است:

- تیم قرمز خود را برتر از آن می‌بیند که بخواهد اطلاعات را با تیم آبی به اشتراک بگذارد.
- تیم قرمز به سازمان نفوذ کرده و قرنطینه، محدود و تضعیف می‌گردد و در نتیجه اساساً تاثیرگذاری آن به صورت کامل کاهش می‌یابد.
- تیم قرمز و آبی در واقع به گونه‌ای طراحی نشده‌اند که به طور مداوم با یکدیگر در تعامل باشند، در نتیجه، دروس آموخته شده در هر طرف تا حد قابل توجهی از دست خواهد رفت.
- مدیریت امنیت اطلاعات اقدامات تیم قرمز و آبی را به صورت تلاشی واحد در نظر نمی‌گیرد و هیچ گونه اطلاعات، مدیریت و کنترل یا معیار سنجشی بین آن‌ها مشترک نیست.
- سازمان‌هایی که یک یا دو مورد از این مشکلات را دارند، به احتمال زیاد به فکر به کارگیری یک تیم بنفش برای حل آن می‌افتند. اما لازم است که «بنفش» به جای یک تیم اضافه همیشگی، به عنوان یک نقش یا مفهوم در نظر گرفته شود و این به معنای همکاری و منافع مشترک برای رسیدن به هدفی مشترک است.

بنابراین، شاید زمانی که شخص ثالثی چگونگی کارکرد مشترک تیم‌های امنیت قرمز و آبی سازمان را تحلیل می‌کند و اصلاحاتی را پیشنهاد می‌دهد، تیم بنفشی دخیل شود. شاید هم زمانی که شخصی بصورت Real-Time هر دو تیم را مانیتور می‌کند تا چگونگی کارکرد آن‌ها را ببیند، عملکرد تیم بنفش وارد کار شود. ممکن است زمانی که دو تیم به یکدیگر می‌پیوندند، تجربیاتشان را به اشتراک می‌گذارند و درباره حملات و دفاع‌های مختلف صحبت می‌کنند، جلسه تیم بنفش مطرح شود.

آنچه باعث یکپارچه شدن تیم‌های امنیت قرمز و آبی می‌شود، واداشتن آن‌ها به توافق بر سر هدف مشترکشان، یعنی بهبود سازمان است، نه این که موجودیت دیگری معرفی و با این دو تیم تلفیق شود.

تیم بنفش را می‌توان به عنوان یک مشاور روابط دوستی در نظر گرفت. اشکالی ندارد شخص دیگری وارد شود و نقشی در اصلاح رابطه ایفا کند، اما تحت هیچ شرایطی نباید این طور اندیشید که تنها از طریق روش جدید دخالت دادن یک میانجی می‌توان برای همیشه رابطه تیم‌های قرمز و آبی را بهبود بخشید.

چکیده‌ای از عملکرد تیم‌های امنیت سایبری

۱. تیم قرمز از مهاجمان الگوبرداری می‌کند تا ببیند امنیت سازمانی که برایش کار می‌کند با چه کم و کاستی‌هایی روبه‌رو است.

۲. تیم آبی در برابر مهاجمان دفاع می‌کند و تلاش می‌کند تا وضعیت امنیت سازمان خود را به طور مداوم بهبود بخشد.

۳. برای پیاده‌سازی عملکرد صحیح تیم قرمز / آبی باید به طور مرتب دانش را بین این دو تیم به اشتراک گذاشت تا هر دو به طور مداوم بهبود یافته و اصلاح شوند.

۴. اغلب، تیم‌های بنفش برای تلفیق مداوم این دو گروه مورد استفاده قرار می‌گیرند که در این حالت به مشکل اصلی تیم‌های امنیت قرمز و آبی، که عدم اشتراک اطلاعات است، پرداخته نمی‌شود.

۵. مفهوم تیم بنفش باید عملکرد ترکیبی یا نقطه تعامل باشد و نباید آن را جداگانه به صورت ایده‌آل، موجودیتی مازاد در نظر گرفت.

۶. در یک سازمان تکامل‌یافته، کل هدف تیم قرمز، بهبود تاثیرگذاری تیم آبی است، بنابراین خدمتی که تیم بنفش ارائه می‌کند، باید بخشی از تعامل طبیعی آن‌ها باشد و نباید از جانب این تیم به عنوان موجودیتی دیگر، فشاری وارد شود.

۷. می‌توان از ترکیب تیم زرد (سازندگان) با تیم‌های امنیت قرمز و آبی، به نقش‌های دیگری مانند سبز و نارنجی رسید. این کار باعث می‌شود ذهنیت و طرز فکر مهاجم و مدافع به دیگر بخش‌های سازمان نیز برسد.

لازم است بدانید:

۱. همه این اصطلاحات را می‌توان برای هر نوع عملکرد امنیتی به کار برد، اما این مفاهیم به خصوص برای امنیت اطلاعات تعریف شده‌اند.

۲. تیم Tiger شبیه به تیم قرمز است اما کاملاً با آن یکسان نیست. یکی از مقالاتی که در سال ۱۹۶۴نوشته شد، چنین تعریفی از این اصطلاح ارائه داد: «تیمی متشکل از متخصصان فنی طبیعی و بی‌پروا که بابت تجربه، انرژی و قدرت تخیلشان برگزیده و گماشته می‌شوند تا به صورت بی‌وقفه هر نوع منشأ محتمل خرابی را در یکی از سیستم‌های فرعی فضاپیمایی ردیابی کنند.» این اصطلاح امروزه به صورت مترادفی برای تیم قرمز به کار می‌رود، اما مفهوم کلی آن، گروه سرآمدی از افراد است که به حل مسئله فنی ویژه‌ای گماشته شده‌اند.

۳. مهم است که تیم‌های قرمز به اندازه مشخصی از سازمانی که در حال سنجیدن آن هستند، جدا بمانند، چرا که این کار مجال کافی و دورنمای مناسب را در اختیار آن‌ها قرار داده تا به الگوبرداری از مهاجمان ادامه دهند. سازمان‌هایی که تیم‌های قرمز را وارد تیم امنیتی خود می‌کنند، می‌خواهند به آرامی قدرت، مجال و آزادی کلی تیم قرمز در عمل کردن مانند یک مهاجم واقعی را از میان ببرند. تیم‌های قرمز در طول زمان، معمولا فقط طی چند ماه، سرآمدی و تاثیرگذاری خود را از دست می‌دهند و محدود، یکنواخت و اساساً عاجز می‌گردند.

۴. تیم‌های بنفش، علاوه بر آن که به عنوان پلی برای برنامه‌های ناقص‌تر در سازمان عمل می‌کنند، می‌توانند به سازمان‌ها در وفق دادن مدیریت خود به مفهوم الگوبرداری از مهاجم کمک کنند این موضوع برای بسیاری از سازمان‌ها ممکن است به مفهوم مبارزه باشد.

۵. جنبه دیگری که به تضعیف تاثیرگذاری تیم‌های قرمز داخلی می‌انجامد، این است که

اعضای ارشد تیم‌های قرمز به ندرت با فرهنگ داخلی شرکت‌هایی که برایشان کار می‌کنند، سازگار می‌شوند. به بیان دیگر، شرکتی که می‌تواند هزینه یک تیم قرمز واقعی را بپردازد، احتمالاً تابع آدابی است که پذیرش آن برای اعضای تیم‌های قرمز ، سخت یا ناممکن است. این مسئله اغلب منجر به تضعیف تدریجی اعضای تیم قرمزی می‌گردد که باید با این فرهنگ‌های داخلی سازگار شوند.

۶. از نظر فنی، تاثیرگذاری تیم قرمز داخلی شدنی است، اما احتمال بسیار کمی می‌رود که اعضای آن در دوره‌های طولانی به بهترین نحو محافظت و حمایت شوند. این امر احتمالا منجر به زوال، ناکامی و تضعیف تدریجی آن‌ها خواهد شد.

۷. یکی از تله‌هایی که تیم قرمز مرتباً در آن می‌افتد، کاهش قدرت و مجال اوست، تا جایی که اثر آن از بین می‌رود. در این زمان مدیریت شرکت مشاورانی را می‌آورد که بسیار تحت حمایت هستند و یافته‌های فراوانی را به شرکت بازمی‌گردانند. سپس مدیریت به تیم داخلی نگاه می‌کند و می‌گوید: «این یافته‌ها فوق‌العاده هستند! شما چرا نمی‌توانید این کار را بکنید؟»

۸. از تشابهات دیگر با تیم قرمزی که همکاری نمی‌کند می‌توان به فوتبالیست‌های حرفه‌ای که به توپ لگد می‌زنند اما آن را پاس نمی‌دهند، مشوقان حرفه‌ای که فقط از دست راستشان استفاده می‌کنند، حسابرسان حرفه‌ای که گزارش نمی‌نویسند، معلمان حرفه‌ای که با دانش‌آموزان وارد تعامل نمی‌شوند، و مواردی از این قبیل اشاره کرد.

اخبار داخلی

وبینار رایگان مدل امنیتی لایه ای شبکه با ضریب اعتماد صفر Zero Trust Network

Zero Trust Network، یک مدل امنیتی لایه‌ای با ضریب اعتماد صفر است که در سازمان‌های فناوری محور استفاده می‌شود. در این مدل امنیتی به صورت پیش فرض به هیچ ماشین، سرویس و یا شخصی اعتماد نمی شود و در تمام مراحل و از هر جایی (داخل شبکه سازمانی، DMZ، بیرون شبکه سازمانی) کاربران و دستگاه ها باید احراز و تأیید هویت شوند و دسترسی آن‌ها به صورت "حداقل سطح دسترسی" به منابع مورد نیاز تعریف می‌شود. در همین راستا و به منظور آشنایی با نحوه عملکرد این مکانیسم، در مورخ ۶ اسفندماه ۱۳۹۹ وبینار رایگان Zero Trust Network با استقبال پرسنل سازمان‌ها، شرکت‌های خصوصی، دانشجویان و علاقمندان توسط مرکز آپا برگزار گردید.

اخبار کوتاه

استفاده هکرها از نرم‌افزار Exchange Server برای انتشار باج‌افزار DearCry

در حال حاضر، بیش از ۸۰،۰۰۰ سرور در معرض باج‌افزار DearCry قرار دارند، مایکروسافت از مشتریان خواسته است تا وصله‌های صادر شده در هفته گذشته را نصب کنند.

هفته گذشته مایکروسافت فاش کرد که سرور Exchange Email خود توسط هکرهای چینی هدف قرار گرفته است و پس از آن ۳۰۰۰۰ سازمان در سراسر جهان در معرض خطر قرار دارند. این شامل سازمان بانکی اروپا (EBA) است که قبلاً اعلام کرده است که هکرها در سیستم ایمیل آن بوده‌اند نیز می‌شود.

اکنون، مایکروسافت عاملان تهدیدی را شناسایی کرده است که باج‌افزار DearCry را بر روی سیستم‌هایی که به جدیدترین نسخه به‌روز نمی‌شوند، ارسال می‌کنند.

هشدارهای مایکروسافت درباره DearCry Ransomware Strain

مایکروسافت هشدار داده است تا به مشتریان Exchange در مورد فشار جدید باج‌افزار با نام DearCry هشدار دهد. طبق توئیتی از طرف Microsoft Security Security Team ، هکرها برای استقرار باج افزار DearCry ، سرورهای Exchange وصله نشده موجود در داخل را هدف قرار داده‌اند.

به گفته مایکروسافت، هکرها به طور خاص سرورهایی را هدف قرار می‌دهند که هنوز در معرض چهار آسیب‌پذیری هستند که هکرهای حمایت شده از دولت چین از آنها سوء استفاده کرده‌اند.

ESET گزارش داد که حداقل ده گروه هک تحت حمایت دولت در تلاشند تا از نقایص وصله نشده سرور Exchange استفاده کنند.

کاربرانِ سرورِ Exchange وصله‌ها را اعمال کنند

مایکروسافت همچنین با ارسال توییت از مشتریان خواست تا وصله‌های اضطراری را که هفته گذشته منتشر کرده اعمال کنند و این امر بر سرورهای ایمیل Exchange داخلی آن تأثیر می‌گذارد.

فیلیپ میسنر، محقق مایکروسافت در توئیتر خود نوشت که مجرمان اینترنتی در تلاشند تا از نقایص سرور ProxyLogon Exchange Server که به شدت مورد سوء استفاده قرار گرفته است برای نصب باج‌افزار DearCry استفاده کنند.

این شرکت توییت کرد که مشتریان Microsoft Defender که به‌روزرسانی خودکار را فعال کرده‌اند نیازی به اقدامی ندارند، اما مشتریان Exchange Server در محل باید بلافاصله به‌روزرسانی‌های امنیتی را نصب کنند.

حدود ۸۰،۰۰۰ سرور هنوز پچ نشده‌اند.

ثبت‌نام دوره‌های
مرکز آپا دانشگاه رازی

همراه با ارائه گواهی معتبر دارای اعتبار افتا

با اساتیدی مجرب دارای مدرک بین المللی

آنلاین ◀ دوره امنیت شبکه سیسکو CCNA Security

۴۰ ساعت

یکشنبه‌ها
ساعت ۱۷ الی ۲۰

مهندس شهاب ارکان

CISCO CERTIFIED CCNA SECURITY

حضوری ◀ دوره حرفه‌ای شبکه CCNP Enterprise (New)

۶۰ ساعت

شنبه‌ها
ساعت ۱۷ الی ۲۰

مهندس سعید زنگنه

CISCO CERTIFIED CCNP ENTERPRISE

حضوری ◀ دوره پیکربندی و مدیریت ویندوز سرور ۲۰۱۹

۶۰ ساعت

سه‌شنبه‌ها
ساعت ۱۷ الی ۲۰

مهندس محمد عزیزی

MICROSOFT CERTIFIED PROFESSIONAL Microsoft MCSA Windows Server 2016

ظرفیت دوره‌ها محدود می‌باشد.

★ با همکاری انجمن علمی مهندسی کامپیوتر

cert.razi.ac.ir | APA_Razi | APARazi | ۰۸۳۳۴۳۴۳۲۵۱

جهت ثبت‌نام به آدرس evand.com/events/aparazi-99 مراجعه نمایید.


مرکز تخصصی آپا دانشگاه رازی