امنیت اطلاعات

بولتن تحلیلی ■ تیر ماه ۱۳۹۸

در این شماره می‌خوانید:

- خطر سرقت ارز دیجیتال
- ویروس چند ریختی Virut
- بسته‌های اصلاحیه نرم افزاری
- اخبار باج‌افزارها

سرقت ارز دیجیتال توسط بدافزار Siscos

بدافزار Siscos ازجمله بدافزارهای ماینینگ و از دسته تروجان‌ها می‌باشد که علاوه بر استخراج ارز دیجیتال از سیستم قربانی با نصب یک بات در قالب سرویس و دستوراتی که از سوی هکر دریافت می‌کند، کنترل سیستم را بدست می‌گیرد. با توجه به این مسئله درجه تخریب این بدافزار بر روی سیستم در درازمدت می‌تواند زیاد باشد.

این بدافزار همچنین با ایجاد یک حساب کاربری با نام mml23$ بر روی سیستم و قرار دادن آن در گروه Administrators مجوزهای خود را برای عملیات مخرب آتی بالا می‌برد و از طریق آسیب‌پذیری Eternalblue و درب پشتی ایجاد شده توسط ابزار Doublepulsar وارد سیستم قربانی شده و به‌عنوان زیرمجموعه یکی از پردازه‌های سیستمی به اجرا در می‌آید. درعین‌حال یک دانلودر نیز می‌باشد و با دانلود فایل‌های مخرب ادامه روند آلودگی را از طریق اجرای آن‌ها انجام می‌دهد.

علائم آلودگی به بدافزار Siscos:

فایل اصلی بدافزار یک dll است که از طریق آسیب‌پذیری Eternalblue و درب پشتی ایجادشده توسط ابزار Doublepulsar وارد سیستم قربانی شده و به‌عنوان زیرمجموعه یکی از پردازه‌های سیستمی (عموماً lsass.exe) به اجرا در می‌آید.

شرح عملکرد فایل اصلی بدافزار :

این dll ایجاد کننده یک حساب کاربری با مشخصات زیر می‌باشد:

User : mml23$
!Pass : bengal1
Group : Administrators

در عین حال یک دانلودر نیز می‌باشد. این dll حاوی دو تابع اکسپورت است که برای دانلود دو فایل بدافزار فراخوانی می‌شوند.

بلافاصله پس از فراخوانی تابع اول (urldown) فایلی با نام x86.exe از آدرس زیر دانلود می‌شود:

http://k.honker[.]info:8/x86.exe

این فایل با نام جعلی conhost.exe در پوشه Windows ذخیره می‌شود.

** فایل conhost.exe یک ابزار استاندارد مربوط به سیستم‌عامل ویندوز است که در حالت عادی در پوشه system32 می‌باشد.

با فراخوانی تابع دوم (urldown1) فایلی با نام madk.exe از آدرس زیر دانلود می‌شود:

http://k.honker.info:8/madk.exe

این فایل با نام جعلی smss.exe در پوشه Windows ذخیره می‌شود.

شرح عملکرد فایل x86.exe

یک dll با نام تصادفی در مسیر زیر ایجاد می‌کند و آن را به‌عنوان سرویس ثبت می‌کند.

Root]:\Program Files\NetMeeting\[Random].dll]

سپس در لیست پردازه‌های جاری پردازه 360tray.exe را جستجو می‌کند. این پردازه مربوط به یک آنتی‌ویروس چینی به نام 360safe می‌باشد. درصورتی‌که این آنتی‌ویروس در حال اجرا باشد، بدافزار کار خود را خاتمه می‌دهد. بنابراین کاملاً مشهود است که هکر چینی بوده و کشور خود را از آلودگی مستثنی کرده است. درصورتی‌که پردازه این آنتی‌ویروس در سیستم قربانی اجرا نشده باشد، سرویس بدافزار با نام lssas در رجیستری ثبت می‌شود. این سرویس یک بات است.

در زیر لیست دستورات C&C سرویس بدافزار همراه با عملکرد آن‌ها را مشاهده می‌کنید:

عملکرد	کد کنترلی
به‌روزرسانی یا حذف سرویس بدافزار	01
خواندن اطلاعات سرویس از رجیستری سیستم قربانی	02
ارتباط با سرور بیتکوین : post.f۲pool.info	03
پاک کردن لاگ‌های موردنظر هکر مربوط به system، Application و security از بخش Eventlog سیستم	05
دانلود یک فایل مشخص	06
تغییر تنظیمات shell open command مربوط به مرورگر IE	08
اعمال تغییرات بر روی توکن‌های مربوط به ایستگاه Default\\WinSta۰	0A
جستجوی یک پردازه در لیست پردازه‌های جاری	0C
تغییر تنظیمات پراکسی	0E

از کد کنترلی شماره 0A می‌توان نتیجه گرفت که هکر برای دستکاری مجوزهای مدنظر خود در سیستم قربانی از این کد و حساب کاربری mml23$ استفاده می‌کند.

شرح عملکرد فایل madk.exe

ساخت فایلی با نام conhost.exe در مسیر زیر :
Root]:\Windows\Fonts\conhost.exe]

ساخت سرویس زیر:
Service name : MetPipAtcivator
Service path : [Root]:\windows\Fonts\svchost.exe
DisplayName : Network Location Service
Description : Provides performance library information .from Windows Management

درصورتی‌که این سرویس قبلاً بر روی سیستم قربانی وجود داشته باشد، آن‌را حذف می‌کند.

سرویس MetPipAtcivator بلافاصله اجرا شده و فایل conhost. exe را که در پوشه fonts قرار دارد را اجرا می‌کند.

ساخت سرویس زیر :
Service name : SetPipAtcivator
Service path : [Root]:\windows\Fonts\svchost.exe
DisplayName : WMI Performance Services
Description : Identify computers that are connected to the network, collect and store the properties of these networks, and notify the application when they are .changed

وظیفه این سرویس اجرای فایل rundllhost.exe ساخته شده توسط فایل conhost.exe و اجرای آن می‌باشد. rundllhost.exe فایل بیتکوین می‌باشد و با سرورهای زیر در ارتباط است:
max.csrss.website:80
l.csrss.website:14444

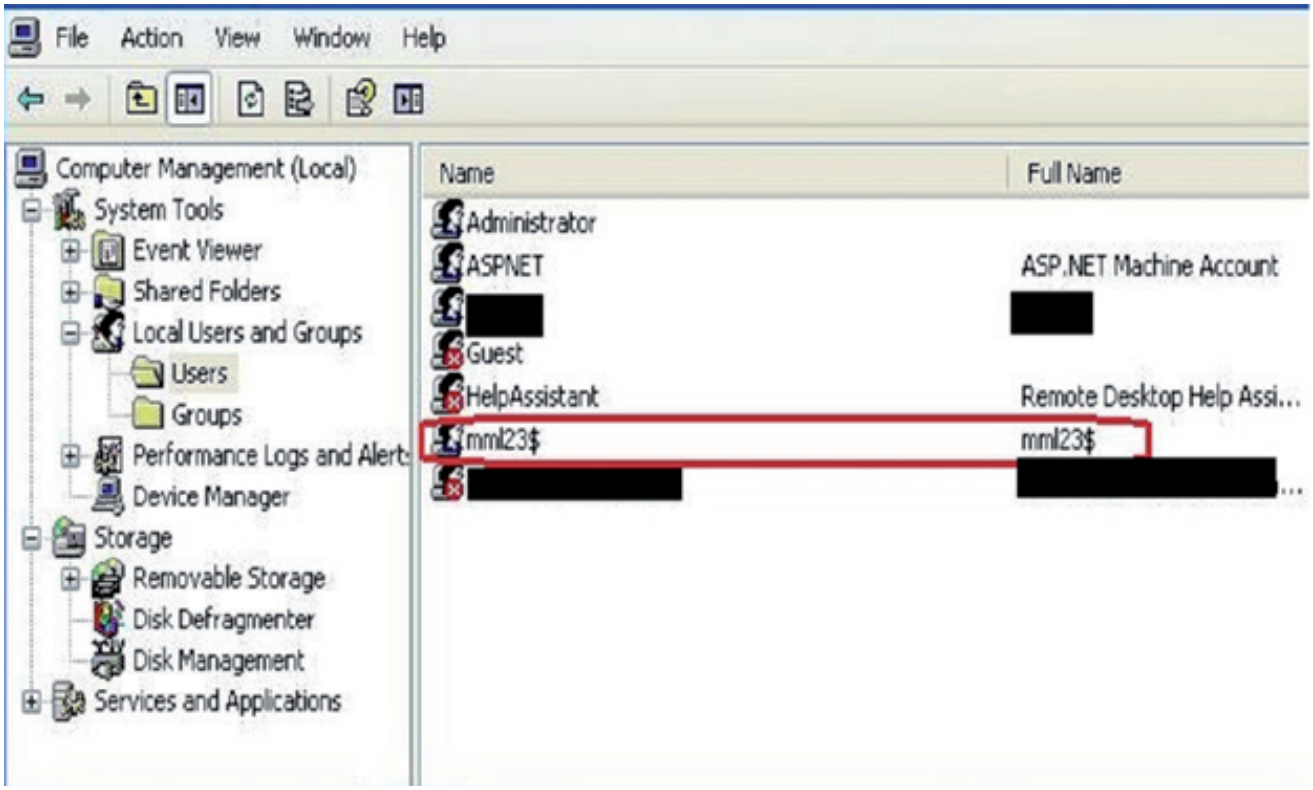
وظایف فایل conhost.exe

• ممانعت از اجرای پردازه‌های مانیتورینگ نظیر autoruns.exe، perfmon.exe، procexp.exe، ProcessHacker.exe و نیز پردازه rundll32.exe

• ایجاد فایلی با نام [Root]:\Windows\Fonts\rundllhost.exe

آنتی‌ویروس پادویش این بدافزار را شناسایی کرده و از سیستم حذف می‌کند. جهت پیشگیری از آلودگی‌های احتمالی توسط بدافزارهایی که از آسیب‌پذیری EternalBlue استفاده می‌کنند، پیشنهاد می‌شود از وصله امنیتی ارائه‌شده توسط مایکروسافت که در لینک زیر آمده استفاده کنید.
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

بخش جلوگیری از نفوذ (IPS) آنتی‌ویروس پادویش این‌گونه آسیب‌پذیری‌ها را شناسایی کرده و از ورود آن به سیستم قربانی جلوگیری می‌کند.



ویروس چندریختی Virut

بدافزار Virut در دسته ویروس‌ها قرار می‌گیرد. Virut از نوع چندریختی (Polymorph) است و با تغییر دادن برخی اجزای فایل هدف، روند اجرایی را به سمت کد خود که در بخش انتهایی فایل قرار دارد، هدایت می‌کند. ویروس فایل‌های اجرایی را آلوده می‌کند و از طریق همین فایل‌ها منتشر می‌شود. این ویروس با باز کردن یک درب پشتی و با اتصال به یک سرور IRC، دسترسی غیرمجاز به دستگاه‌های آلوده را فراهم می‌کند و به مهاجمان راه دور اجازه ورود به سیستم قربانی را می‌دهد همچنین این ویروس بستری برای دانلود برنامه‌های مخرب در سیستم قربانی را فراهم می‌آورد.

عملیات مخرب انجام شده توسط ویروس virut

virut کد آلوده خود را به برخی پردازه‌های سیستمی مانند .winlogon exe و explorer.exe و غیره تزریق می‌کند و بر روی تابع‌های ویندوزی هوک می‌زند. این ویروس بعد از اجرا شدن، فایل‌های اجرایی را آلوده می‌کند. همچنین امضای دیجیتال فایل‌های دارای امضای دیجیتال بعد از آلوده شدن نامعتبر می‌شوند (می‌توان فایل‌های سیستمی system۳۲ را بررسی کرد)

اجرای این ویروس در سیستم موجب افزایش فعالیت‌های cpu می‌شود.

این ویروس درایوهای قابل‌حمل (فلش، هارد اکسترنال و ...) و دایرکتوری‌های Share در یک شبکه را نیز آلوده می‌کند.

پادویش با دارا بودن قابلیت UMP که جزء محافظت رفتاری آن است جلوی آلوده شدن سیستم از طریق درایو قابل‌حمل را می‌گیرد. ازاین‌رو جهت پیشگیری از آلودگی به انواع بدافزارهایی که از طریق درایو قابل‌حمل انتقال میابند ازجمله بدافزار Virut پیشنهاد می‌شود با نصب پادویش از ورود بدافزار به سیستم خود جلوگیری کنید.

چنانچه سیستم شما توسط بدافزار Virut آلوده شده است مراحل زیر را دنبال کنید:

۱. پادویش را بر روی سیستم خود نصب کنید.
۲. درایو قابل‌حمل آلوده را به سیستم وصل کنید.
۳. با استفاده از پادویش درایو قابل‌حمل خود را اسکن کنید تا درایو قابل‌حمل و سیستم آلوده شما پاکسازی شود.

توجه: درصورت پاکسازی ناموفق، پاکسازی در بوت بعدی را انتخاب کنید تا پاکسازی به طور کامل انجام شود.

هشدار

هشدار: بدافزارهایی که از اکسپلویت EternalBlue استفاده می‌کنند همچنان در سیستم کاربران ایرانی مشاهده می‌شوند.
نویسندگان بدافزار از اکسپلویت EternalBlue در بدافزارهای استخراج ارز دیجیتال همچون Vools و باج افزارها همچون WannaCry برای انتشار در سطح شبکه استفاده می‌کنند.
اکسپلویت EternalBlue توسط گروه ShadowBrokers به سرقت رفته و به طور عمومی در سال ۲۰۱۷ میلادی منتشر شد و به‌عنوان بخشی از حمله جهانی باج افزار WannaCry مورداستفاده قرار گرفت. از آن زمان، بدافزارهای زیادی برای انتشار خود از آن استفاده کرده‌اند. این اکسپلویت، آسیب‌پذیری موجود در پروتکل SMB نسخه ۱ را هدف قرار می‌دهد. بخش جلوگیری از نفوذ آنتی‌ویروس پادویش این اکسپلویت را در سطح شبکه با نام CVE.Win32.Exploit.2017.0146 به تعداد بسیار زیاد شناسایی کرده که این موضوع نشان از فراوانی بدافزارهایی دارد که از طریق این اکسپلویت در حال انتشار هستند.
نکته قابل توجه اینکه علیرغم گذشت نزدیک به دو سال از عرضه اصلاحیه MS17-010 مایکروسافت و اطلاع‌رسانی‌های گسترده در خصوص لزوم نصب آن همچنان بسیاری از سیستم‌ها فاقد اصلاحیه مذکور هستند. جهت پیشگیری از آلودگی توسط بدافزارهایی که از اکسپلویت EternalBlue استفاده می‌کنند، توصیه اکید می‌شود تا هر چه سریع‌تر سیستم‌ها ی ویندوزی توسط به‌روزرسانی امنیتی MS17-010 وصله شوند.

مراقب آسیب پذیری ریموت دسکتاپ ها باشید

بهره‌جویی از آسیب پذیری با شناسه CVE-2019-0708 در بخش Services Desktop Remote سیستم عامل ویندوز، امکان اجرای کد را به صورت از راه دور بر روی دستگاه آسیب پذیر برای مهاجم فراهم می کند. خطر این آسیب پذیری به حدی زیاد است که از آن به عنوان Eternalblue دوم که باعث فاجعه‌هایی مثل Wannacry بود، یاد می کنند. این آسیب پذیری با اینکه بسیار خطرناک است در حدی که مایکروسافت حتی برای سیستم هایی که دیگر از آنها پشتیبانی نمی کند بروزرسانی های امنیتی مربوطه را ارائه کرد، ولی روال کارش بسیار ساده است. در پروتکل RDP برای اینکه امکانات و توانایی هایی که در اختیار شخص ریموت زننده قرار می گیرد بیشتر شود (توانایی هایی مانند انتقال صدا، کنترل سخت افزار و...) از مفهومی به اسم Channel Virtual استفاده می‌شود که تا قبل از Windows8 این کانال های ارتباطی از نوع static بودند SVC ولی پس از آن از نوع dynamic شدند DVC. از عمده تفاوت های این دو نوع کانال می توان به این موارد اشاره کرد که تعداد کانال ها در Static به ۳۲ محدود است ولی در dynamic این چنین نیست و همچنین در static کانال در شروع ارتباط ایجاد شده و تا پایان ارتباط وجود دارد ولی در dynamic کانالها از نوع on demand هستند. در کانال های static کانال مجازی MS_T120 که شماره‌ی منتصب به آن همیشه باید ۳۲ باشد، کانالی است که برای استفاده های داخلی رزرو شده است و کسی نباید درخواست ساخت کانالی با این نام را بدهد، و تنها کار این آسیب پذیری این است که درخواست ساخت کانالی با همین نام را می دهد. در درایور مربوط به RDP بررسی می شود که اگر کانالی پیش از این با نام درخواستی وجود نداشته باشد، کانال جدید ساخته شود (که در این حالت اجازه ساخت کانال با نام MS_T120 داده نمی‌شود(، ولی از آنجایی که کانال MS_T120 وجود دارد فقط اقدام به Bind کردن ارتباطRDP برقرار شده با این کانال منتها با ID غیر از ۳۲ می‌کند و در نتیجه مهاجم می‌تواند اقدام به اجرای دستور از راه دور کند. همچنین چون یک اشاره گر جدید به کانال MS_T120 ایجاد می کند، وقتی کارش تمام می‌شود طبق روال عادی SVCها درایور RDP اقدام به حذف کانال MS_T120 می کند و اگر در ادامه خود سیستم بخواهد اشاره گر به این کانال را ببندد، چون کانالی وجود ندارد با صفحه مرگ آبی مواجه می شود. به تمامی کاربران توصیه میشود هر چه سریعتر نسبت به نصب اصلاحیه جدید اقدام کنند:

https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

اصلاحیه‌های امنیتی تیر ماه

شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی «ژوئیه » منتشر کرد.
این اصلاحیه‌ها درمجموع، ۷۷ آسیب‌پذیری را در سیستم‌عامل ویندوز و برخی دیگر از محصولات مایکروسافت ترمیم می‌کنند. درجه اهمیت ۱۵ مورد از آسیب‌پذیری‌های ترمیم‌شده توسط اصلاحیه‌های مذکور (Critical) و ۶۲ مورد از آن‌ها (Important) اعلام شده است.
برای جزئیات بیشتر به لینک زیر مراجعه شود.
https://portal.msrc.microsoft.com/en-us/security-guidance

شرکت ادوبی اصلاحیه‌های امنیتی ماه میلادی «ژوئیه » را منتشر کرد.
جزییات بیشتر در لینک‌های زیر قابل مطالعه است:
https://helpx.adobe.com/security/products/bridge/apsb19-37.html
https://helpx.adobe.com/security/products/experience-manager/apsb19-38.html
https://helpx.adobe.com/security/products/dreamweaver/apsb19-40.html

به‌روزرسانی‌های امنیتی سیسکو
سیسکو به‌روزرسانی‌هایی را برای رفع چندین آسیب‌پذیری در برخی محصولات خود ارائه کرده است.
توصیه می‌شود نسبت به به‌روزرسانی اقدام شود.
جزئیات آسیب‌پذیری‌ها در جدول زیر ارائه شده است.
https://tools.cisco.com/security/center/publicationListing.x

اخبار باج افزارها

باج‌افزار Phobos

این باج‌افزار همچنان سهم قابل‌توجهی از آلودگی‌ها را به خود اختصاص داده است که در کشورمان نیز شیوع دارد و به فایل‌های آلوده پسوندهای actin, actor را اضافه می‌کند.

باج افزار STOP

باج افزار STOP در این ماه بسیار فعال بوده و با رمزگذاری اطلاعات قربانی پسوندهای، berosuce, godes, dalle, trvke را به فایل‌های آلوده اضافه می‌کند.

باج‌افزار Maoloa

باج افزار Maoloa اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند Persephone۶۶۶ را اضافه می‌کند.

باج‌افزار Dharma

باج افزار Dharma در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند ۱bct را اضافه می‌کند. در برخی نسخه‌ها نیز بعد از رمزگذاری پسوند saveday یا cap یا ۰ را اضافه می‌کند.

باج‌افزار Nemesis

باج افزار Nemesis اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند YOUR_LAST_CHANCE را اضافه می‌کند.

باج‌افزار Craftul

باج افزار Craftul اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند craftul را اضافه می‌کند.

باج‌افزار GarrantyDecrypt

باج افزار GarrantyDecrypt اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند popoticus را اضافه می‌کند.

آلودگی به باج‌افزار از طریق هک و اقدامات لازم جهت جلوگیری از آن

نفوذ به شبکه یا هک شدن یکی از بزرگترین خطراتی است که همه سازمان‌ها را تهدید می‌کند. فعالیت هکرها این روزها بیشتر به چشم می‌خورد و سازمان هایی که رویکرد پیشگیرانه ای نسبت به تهدیدات ندارند، با عواقب جدی مواجه خواهند شد.

به گزارش پادویش در روزهای اخیر نفوذ هکرها به شبکه و اجرای باج‌افزار توسط آنها، بارها مشاهده شده است. لذا توصیه می‌شود جهت پیشگیری، اقدامات زیر صورت گیرد:

- بستن پورت ریموت و غیرفعال کردن سرویس ریموت دسکتاپ از طریق اینترنت (روی تمام سرورها و نیز سیستمهای دیگر)
- اطمینان از عدم باز بودن پورت ۱۴۳۳ برای سرورهای SQL از سمت اینترنت
- تغییر نام کاربر Administrator در تمام شبکه و سرورها به نامی که قابل حدس زدن نباشد
- اعمال پسوردهای دارای پیچیدگی لازم در تمام اکانتهای ادمین دامین و لوکال سرورها و سایر سیستم ها
- اعمال پسوردهای دارای پیچیدگی لازم برای آنتی ویروس پادویش
- اطمینان از نصب آخرین وصله‌های امنیتی ویندوز و نرم افزارهای کاربردی
- داشتن فرآیند منظم بکاپ‌گیری دوره‌ای و اطمینان از صحت بکاپ‌ها
- استفاده از Tape برای تهیه نسخه پشتیبانی
- اطمینان از فعال بودن داده بان پادویش
- اطمینان از به روز بودن پادویش
- انجام کامل فرآیند امن‌سازی مبتنی بر استانداردهای موجود مانند ISMS و اخذ مشاوره امنیت شبکه

WWW.PADVISH.COM