امنیت اطلاعات

بولتن تحلیلی ■ اسفند ماه ۱۳۹۷

در این شماره می‌خوانید:

- حملات بی‌سابقه سایبری به شبکه‌های کشور
- انتشار بدافزار جدید از طریق ایمیل
- بسته‌های اصلاحیه نرم افزاری
- اخبار باج‌گیرها

سال نو
پادویش نو

٪۲۰ تخفیف

فروش ویژه نوروزی

تا پایان تعطیلات نوروزی

خبر اختصاصی پادویش

انتشار بدافزار ServHelper از طریق ایمیل‌های فیشینگ

بدافزار ServHelper در سیستم های ویندوزی یک در پشتی (Back-door) نصب می‌کند که از طریق آن دسترسی از راه دور به رایانه آلوده برای مهاجمین فراهم می‌شود. این خانواده از بدافزار در دو نسخه Dropper و Backdoor وجود دارد. در نسخه Backdoor با ارتباط با سرورهایی خاص اقدام به ارسال اطلاعات و دریافت دستور می‌کند. در نسخه‌ی Dropper اقدام به ایجاد بدافزار می‌کند. از دیگر اهداف این بدافزار می‌توان به سرقت اطلاعات ذخیره شده در مرورگر کاربران اشاره کرد. شیوه انتشار بدافزار ServHelper از طریق فایل‌های آلوده پیوست شده به ایمیل می‌باشد. در نمونه‌های رصد شده بوسیله آزمایشگاه تحلیل بدافزار پادویش یک فایل PDF که دارای یک لینک به ظاهر معتبر برای بروزرسانی به آخرین نسخه برنامه Adobe Reader می باشد یافت شده است.

آدرس لینک مذکور:

http://www.adobe.com/products/acrobat/readstep2.html

اما لینک بالا جعلی بوده و تنها ظاهر لینک است و در واقع کاربر را به لینک مخرب زیر هدایت می‌کند:

https://adobeupdt[dot]net/En-US/reader/download/?installer=Reader_DC_2019.009.20088_English_Windows

سه نسخه از این بدافزار در آزمایشگاه تحلیل بدافزار پادویش رصد شده‌است که علائم هر یک به شرح زیر است:

۱-نسخه اول

وجود فایل های زیر:

%USER%\appdata\local\temp\NtWrite.dat

%USER%\appdata\local\temp\tmp31.tmp

بالا بودن پردازه msra.exe (پردازه سیستمی و استاندارد remote desk-top) و تلاش برای برقراری ارتباط با این آدرس‌ها:

Checksolutions[.]pw:443

Afgdhjkrm[.]pw:443

pointsoft[.]pw:443

dedoshop[.]pw:443

۲- نسخه دوم

ایجاد یک سرویس به trust که فایل آن را با اسم winreset در مسیر زیر قرار می‌دهد:

PROGRAMFILES\Common Files\System\winreset.exe

بالا بودن پردازه دو سرویس به نام winreset.exe.

تلاش برای برقراری ارتباط با ip زیر:

46,161,27,241

۳- نسخه سوم

وجود فایل helpobj.dat , zxa.bat , sdw.vbs , 1.lnk در مسیر زیر:

%USER%\appdata\local\temp

بالا بودن دو پردازه rundll32.exe که در حال اجرا کردن فایل helpobj.dat و تلاش برای برقراری ارتباط با آدرس‌های زیر هستند:

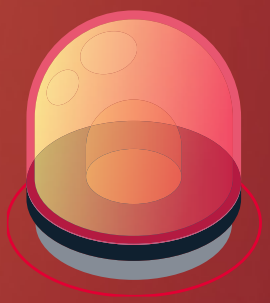
Checksolutions[.]pw:443

Afgdhjkrm[.]pw:443

pointsoft[.]pw:443

dedoshop[.]pw:443

آنتی‌ویروس پادویش این بدافزار را شناسایی کرده و از سیستم حذف می‌کند. جهت پیشگیری از ورود این دست بدافزارها به سیستم پیشنهاد می‌شود از کلیک بر روی لینک‌های مشکوک خودداری نموده و فایل‌های ضمیمه ایمیل‌ها را قبل از اجرا، حتما پویش کنید. همچنین در صورت امکان همیشه سیستم‌عامل و آنتی‌ویروس خود را به روز نگه دارید.



هشدار حملات بی‌سابقه سایبری به شبکه‌های کشور از طریق ریموت دسکتاپ

خبر اختصاصی پادویش

به گزارش تیم رصد پادویش، در روزهای گذشته شبکه‌های شرکت‌ها و سازمان‌های سراسر کشور، شاهد حجم بسیار بالا و بی‌سابقه‌ای از حملات باج‌افزاری و تحرکات هک و نفوذ بوده‌اند. اغلب این حملات از طریق سرویس ریموت و بعضا حتی VPNها و ابزارهای ریموت انجام گرفته‌اند.
از این جهت پادویش با اعلام هشدار جدی وضعیت زرد امنیتی، توجه عموم کاربران بخصوص مدیران محترم شبکه‌ها و مسئولین فاوا را به نکات ایمنی و امنیتی زیر معطوف می‌دارد. در ادامه نکات مهم برای یادآوری بیان شده است:

۱. تهیه پشتیبان به‌روز از اطلاعات حیاتی

وجود یک پشتیبان به روز، که به صورت آفلاین نگهداری شود شرط اول موفقیت در بازگرداندن سیستم‌ها به وضعیت عادی پس از حمله است. بنابراین توصیه می‌شود که یک‌بار دیگر کل سیستم‌های حیاتی خود را مرور کرده و از اطلاعات آن‌ها پشتیبانگیری کرده و پشتیبان‌ها را به صورت آفلاین نگهداری نمایید. دقت کنید که حتماً علاوه بر گرفتن پشتیبان، امکان بازیابی پشتیبان‌ها را تست نمایید تا بعداً به مشکل برنخورید.
علاوه بر سیستم‌های اطلاعاتی و عملیاتی، گرفتن پشتیبان از تجهیزات شبکه شامل روترها، سوییچ‌ها، فایروال، و سایر سیستم‌های مهم مانند اکتیودایرکتوری نیز فراموش نشود.

۲. غیرفعال کردن فوری و سریع راه‌های ارتباطی ریموت و کاهش درجه خطر تا حد ممکن

تقریبا در تمامی حملات اخیر نفوذگران از سرویس ریموت دسکتاپ (Remote Desktop) ویندوز جهت نفوذ اولیه خود به سیستم استفاده کرده‌اند. همچنین نفوذ از طریق VPN یا ابزارهای ریموت کلاینتی (مانند AnyDesk و ابزارهای مشابه) نیز محتمل است. بنابراین بهتر است به طور موقت این راه‌ها را غیرفعال کنید یا حداقل آن‌ها را با پسوردها و پالیسی‌های سختگیرانه‌تر (مانند محدودیت آی‌پی) محدود نمایید.
همچنین ابزارهای ریموت کلاینتی مانند AnyDesk و نمونه‌های مشابه را که ممکن است روی یک سرور یا کلاینت باز مانده باشند را نیز در نظر داشته باشید.

۳. بررسی سیاست‌های شبکه و محدودسازی تا حد امکان

در وضعیت زرد لازم است که یکبار دیگر سیاست‌های امنیت شبکه را مرور نمایید و از اینکه این سیاست‌ها از اصل حداقل دسترسی پیروی می‌کنند اطمینان حاصل کنید. پورت‌های باز اضافی و غیرضروری را ببندید. تا حد امکان سرویس‌های غیرضروری را نیز غیرفعال نمایید.
در مقابله با باج‌افزار، فراموش نکنید که فولدرهای اشتراکی را ببندید یا دسترسی کاربران را به حالت فقط خواندنی محدود نمایید.

۴. فعال کردن سیستم‌های لاگبرداری و Auditing

درصورت وقوع حمله، برای بررسی منشاء حمله (جهت کشف نقاط نفوذ و جلوگیری از وقوع مجدد) و میزان تخریب و پیشروی حمله (جهت بازگرداندن سرویس‌ها و حذف درب‌های پشتی) به انواع لاگ‌های Audit نیاز خواهید داشت.
بنابراین از فعال بودن لاگ‌های Audit در تجهیزات شبکه و نیز سیستم‌عامل‌های خود اطمینان حاصل کنید. در ویندوز لازم است لاگ‌های Security و System فعال باشند. توصیه می‌کنیم لاگ Audit Process Creation را نیز روی Group Policy فعال نمایید. همچنین میزان فضای هارد دیسک را برای ذخیره این لاگ‌ها در نظر بگیرید.

۵. به‌روز کردن سیستم‌عامل و نرم‌افزارها

کمترین کاری که برای امن کردن سیستم انجام می‌شود بروزرسانی سیستم‌عامل، بروزرسانی نرم‌افزارهای سرویس‌دهنده (وب، ایمیل، اشتراک فایل ...) و نرم‌افزارهای امنیتی مانند ضدویروس و ... است. در وضعیت زرد لازم است دقت و وسواس بیشتری در این مورد داشته باشید تا از آسیب‌پذیری‌های شناخته‌شده عمومی در امان بمانید و سطح آسیب‌پذیری را کاهش دهید.

۶. اطمینان از عملکرد سیستم‌های امنیتی، مانیتورینگ و هشداردهی آنها

آخرین توصیه: لاگ‌های سیستم‌های خود را مرور کنید و گوش به زنگ رویدادهای نامتعارف (ریموت‌های خارج ساعت کاری یا از کشورهای خارجی و ...) باشید.
طبعا لازم است مجددا از عملکرد سنسورهای امنیتی مانند IDS, WAF و ضدویروس‌ها و نیز نرم‌افزارهای مانیتورینگ اطمینان حاصل کنید تا به محض رخداد اتفاق امنیتی از آن مطلع شوید. بد نیست سیستم هشدار این نرم‌افزارها را نیز تست کنید تا از عملکرد صحیح آن‌ها مطمئن شوید.

اصلاحیه‌های امنیتی اسفند ماه

شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی مارس منتشر کرد.

درجه اهمیت ۱۷ مورد از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها "Critical" و ۴۵ 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 مارس را منتشر کرد.

دو آسیب‌پذیری حیاتی در محصولات این شرکت ترمیم و اصلاح شده است. جزییات بیشتر در خصوص اصلاحیه‌های عرضه شده در لینک‌های زیر قابل مطالعه است:
https://helpx.adobe.com/security/products/photoshop/apsb19-15.html
https//helpx.adobe.com/security/products/Digital-Editions/apsb19-16.html

به روزرسانی‌های امنیتی سیسکو

سیسکو به روزرسانی‌هایی را برای رفع چندین آسیب‌پذیری در برخی محصولات خود ارائه کرده است.
اطلاعات بیشتر در خصوص به روزرسانی‌ها در لینک زیر قابل مطالعه است.
https://tools.cisco.com/security/center/publicationListing.x

اگر از مرورگر کروم استفاده می کنید، هرچه سریع تر آخرین بروزرسانی این نرم افزار را نصب کنید

محققان یک آسیب پذیری بحرانی در مرورگر کروم کشف و گزارش کرده اند که به هکرها اجازه می دهد با اجرای کدهای مخرب، کنترل رایانه قربانی را در اختیار بگیرند. این موضوع به شدت وضعیت امنیت و حریم خصوصی کاربرانی که از این مرورگر استفاده می کنند را به خطر انداخته و تهدید می کند.
این آسیب پذیری با شناسه CVE-2019-5786 شناخته می شود.
گوگل، پچ امنیتی شماره ۷۲,۰,۳۶۲۶,۱۲۱ را برای سیستم عامل های ویندوز، مک و لینوکس منتشر کرده و کاربران امکان دانلود و نصب آن را دارند.

اخبار باج افزارها

باج‌افزار Neptune

باج افزار Neptune اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند Neptune را اضافه می‌کند.

باج‌افزار Scarab

باج افزار Scarab در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند dy8wud را اضافه می‌کند و در انتها پیغام باج خواهی خود را در فایل HOW TO RECOVER ENCRYPTED FILES.TXT نمایش می دهد.

باج‌افزار Dharma

باج افزار Dharma در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند korea را اضافه می‌کند.

باج‌افزار Phobos

باج افزار Phobos در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند Frendi را اضافه می‌کند.

باج‌افزار GarrantyDecrypt

باج افزار GarrantyDecrypt اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند cammora را اضافه می‌کند.

باج‌افزار DelphiMorix

باج افزار DelphiMorix در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند you__demonslay335 cannot_decrypt_me! و malwarehunterteam را اضافه می‌کند.

باج‌افزار Snatch

باج افزار Snatch در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند jupstb را اضافه می‌کند.

چگونه از آلودگی به باج‌افزار از طریق هک جلوگیری کنیم؟

نفوذ به شبکه یا هک شدن یکی از بزرگترین خطراتی است که همه سازمان ها 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 آنتی‌ویروس پادویش
- اطمینان از نصب آخرین وصله‌های امنیتی ویندوز و نرم‌افزارهای کاربردی
- داشتن فرآیند منظم پشتیبان‌گیری دوره‌ای و اطمینان از صحت پشتیبان‌ها
- استفاده از Tape برای تهیه نسخه پشتیبانی
- اطمینان از فعال بودن داده‌بان 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