ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | دی ۱۴۰۰

شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای مرتبط با امنیت فناوری اطلاعات در یک ماه گذشته پرداخته شده است.

در ماهی که گذشت، یکی از محققان امنیتی پس از بررسی اصلاحیه امنیتی نوامبر مایکروسافت و وصله آسیب‌پذیری با شناسه CVE-2021-41379، یک آسیب‌پذیری "روز-صفر" جدید و قدرتمند دیگری را شناسایی نمود که موجب "ترفیع امتیازی" می‌شود. محقق مذکور با انتشار یک نمونه اثبات‌گر از آن ضعف امنیتی در GitHub، عنوان نمود که آسیب‌پذیری فوق تحت شرایط خاصی دستیابی به سطح دسترسی SYSTEM را فراهم می‌کند.

مهم‌ترین رخداد ماه اخیر که در این ماهنامه به آن پرداخته شده کشف چند ضعف امنیتی "روز-صفر" در Log4j است که موجب انتشار سه نسخه جدید از این کتابخانه پر استفاده شد. از آنجایی که کتابخانه مذکور در بسیاری از سرویس‌ها و سرورها تعبیه شده و سوءاستفاده از این ضعف‌های امنیتی نیازی به تخصص فنی سطح بالا و احراز هویت ندارد، بخش قابل توجهی از نرم‌افزارهای سازمانی، برنامه‌های تحت وب و انواع مختلف سرورهای آپاچی در برابر سوءاستفاده از این ضعف‌های امنیتی آسیب‌پذیر هستند.

به تازگی، محققان در گزارشی به بررسی باج‌افزار Yanluowang پرداختند که در آن مهاجمان پس از دسترسی و نفوذ به شبکه موردنظر، از PowerShell برای دانلود مواردی همچون بدافزار BazarLoader جهت گسترش آلودگی در سطح شبکه استفاده می‌کردند. باج‌افزار مذکور، علاوه بر موسسات مالی، شرکت‌هایی را در بخش‌های تولید، خدمات فناوری اطلاعات، مشاوره و مهندسی مورد هدف قرار داده است. مشروح گزارش فوق در این ماهنامه قابل مطالعه است.

در سال‌های اخیر تجهیزات NAS ساخت شرکت کیونپ به کرات هدف حملات سایبری قرار گرفته‌اند. در این ماهنامه به بررسی یکی از جدیدترین نمونه از این تهدیدات پرداخته شده است. در جریان حملات مذکور، دستگاه‌های NAS ساخت شرکت کیونپ هدف حملات موسوم به Cryptojacking قرار گرفتند. مهاجمان، بدافزاری را بر روی دستگاه هک‌شده اجرا می‌کنند که امکان استخراج رمز ارز را با استفاده از منابع دستگاه برای آن‌ها فراهم می‌کند. حملات مذکور در این ماهنامه به تفصیل مورد بررسی قرار گرفته است.

در آذر ماه، محققان شرکت چیهو ۳۶۰ بر اساس بررسی‌های خود، نسبت به بزرگترین بات‌نت سال‌های اخیر، به نام Pink ، که بیش از ۱.۶ میلیون دستگاه را آلوده کرده است، هشدار دادند. مهاجمان از بات‌نت مذکور تا به امروز برای راه‌اندازی بیش از ۱۰۰ حمله منع سرویس توزیع‌شده و درج تبلیغات در ترافیک قانونی HTTP قربانیان استفاده کرده‌اند. مشروح گزارش این شرکت و نشانه‌های آلودگی در این ماهنامه قابل دریافت و مطالعه است.

در آخرین ماه از پاییز ۱۴۰۰، مایکروسافت، سیسکو، مک‌آفی‌اینترپرایز، بیت‌دیفندر، کسپرسکی، سوفوس، وی‌ام‌ور، ادوبی، گوگل، اپل، موزیلا، اس‌آپ و آپاچی اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند. جزییات این به‌روزرسانی‌ها و گزارش‌های متنوع دیگر را در این ماهنامه بخوانید.

شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی

همکاری گردانندگان باج‌افزار Yanluowang
با مهاجمان باتجربه

اخیراً حملاتی کشف شده که در آن مهاجمان باج‌افزار Yanluowang، با بکارگیری بدافزار BazarLoader در مرحله شناسایی (Reconnaissance)، سازمان‌های ایالات متحده را با تمرکز در بخش مالی مورد هدف قرار داده‌اند.

بر اساس تاکتیک‌ها، تکنیک‌ها و رویه‌های مشاهده‌شده (Tactics, Techniques, and Procedures - به اختصار TTP)، مهاجمان باج‌افزار Yanluowang از خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) استفاده می‌کنند و ممکن است با باج‌افزار Thieflock که توسط گروه Fivehands توسعه یافته، در ارتباط باشند.

به نقل از محققان سیمانتک (Symantec)، این مهاجمان حداقل از ماه آگوست به اهدافی بزرگتری در ایالات متحده حمله کرده‌اند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، چکیده‌ای از گزارش سیمانتک ارائه شده است.

در حالی که باج‌افزار Yanluowang به موسسات مالی علاقه دارد، شرکت‌هایی را در بخش‌های تولید، خدمات فناوری اطلاعات، مشاوره و مهندسی نیز مورد هدف قرار داده است.

گروه باج‌افزاری Fivehands نیز نسبتاً گروه جدیدی است و برای اولین بار در ماه آوریل در گزارشی توسط Mandiant شناخته شد که آن را به گروه UNC2447 نسبت داده بودند و سپس CISA نیز در گزارش زیر نسبت به حملات این گروه هشدار داد.

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a

در آن زمان، Mandiant عنوان نمود که UNC2447 قابلیت‌های پیشرفته‌ای برای عدم تشخیص و به حداقل رساندن شناسایی پس از نفوذ توسط محصولات و راهکارهای امنیتی دارد و گردانندگان آن، باج‌افزار RagnarLocker را نیز منتشر کرده‌اند.

سیمانتک خاطر نشان می‌کند که ارتباط بین حملات اخیر Yanluowang و حملات قدیمی‌تر باج‌افزار Thieflock غیرقطعی است، زیرا تنها به چندین TTP زیر که در حملات باج‌افزار Fivehands یافت شده، استناد شده است.

- بکارگیری ابزارهای معمول بازیابی رمزعبور و ابزارهای منبع‌باز (مانند GrabFF)
- بکارگیری ابزارهای منبع باز پویش شبکه (مانند SoftPerfect Network Scanner)
- استفاده از مرورگر S3 Browser و Cent Browser برای بارگذاری و دانلود داده‌ها

قبل از استقرار باج‌افزار بر روی دستگاه‌های مورد نظر، گردانندگان باج‌افزار، اقدامات زیر را انجام می‌دهند:

- ایجاد یک فایل txt. شامل فهرستی از ماشین‌های شناسایی شده راه‌دور جهت بررسی خط فرمان (Command Line).
- بکارگیری Windows Management Instrument - به اختصار WMI - جهت استخراج فهرستی از پروسه‌های در حال اجرا در ماشین‌های شناسایی شده راه دور که در فایل txt. ذکر شده است.
- ثبت تمام لاگ‌های (Logs) مربوط به پروسه‌ها و اسامی ماشین‌های راه دور در processes.txt

```
.rdata:004558B8 ; CHAR aNetStopMssqlMs[]
.rdata:004558B8 aNetStopMssqlMs db 'net stop MSSQL$MSFW',0
.rdata:004558B8                                         ; DATA XREF: main_module+1581↑o
.rdata:004558CC ; CHAR aNetStopSqlagen[]
.rdata:004558CC aNetStopSqlagen db 'net stop SQLAgent$ISARS',0
.rdata:004558CC                                         ; DATA XREF: main_module+1598↑o
.rdata:004558E4 ; CHAR aNetStopSqlagen_0[]
.rdata:004558E4 aNetStopSqlagen_0 db 'net stop SQLAgent$MSFW',0
.rdata:004558E4                                         ; DATA XREF: main_module+15AF↑o
.rdata:004558FB                 align 4
.rdata:004558FC ; CHAR aNetStopSqlbrow[]
.rdata:004558FC aNetStopSqlbrow db 'net stop SQLBrowser',0
.rdata:004558FC                                         ; DATA XREF: main_module+15C6↑o
.rdata:00455910 ; CHAR aNetStopReports[]
.rdata:00455910 aNetStopReports db 'net stop ReportServer$ISARS',0
.rdata:00455910                                         ; DATA XREF: main_module+15DD↑o
.rdata:0045592C ; CHAR aNetStopSqlwrit[]
.rdata:0045592C aNetStopSqlwrit db 'net stop SQLWriter',0
.rdata:0045592C                                         ; DATA XREF: main_module+15F4↑o
.rdata:0045593F                 align 10h
.rdata:00455940 ; CHAR aNetStopWindefe[]
.rdata:00455940 aNetStopWindefe db 'net stop WinDefend',0
.rdata:00455940                                         ; DATA XREF: main_module+160B↑o
.rdata:00455953                 align 4
.rdata:00455954 ; CHAR aNetStopMr2kser[]
.rdata:00455954 aNetStopMr2kser db 'net stop mr2kserv',0
.rdata:00455954                                         ; DATA XREF: main_module+1622↑o
.rdata:00455966                 align 4
.rdata:00455968 ; CHAR aNetStopMsexcha[]
.rdata:00455968 aNetStopMsexcha db 'net stop MSExchangeADTopology',0
.rdata:00455968                                         ; DATA XREF: main_module+1639↑o
.rdata:00455986                 align 4
.rdata:00455988 ; CHAR aNetStopMsexcha_0[]
.rdata:00455988 aNetStopMsexcha_0 db 'net stop MSExchangeFBA',0
.rdata:00455988                                         ; DATA XREF: main_module+1650↑o
.rdata:0045599F                 align 10h
.rdata:004559A0 ; CHAR aNetStopMsexcha_1[]
.rdata:004559A0 aNetStopMsexcha_1 db 'net stop MSExchangeIS',0
.rdata:004559A0                                         ; DATA XREF: main_module+1667↑o
.rdata:004559B6                 align 4
```

پس از استقرار، باج‌افزار Yanluowang مستقر شده، اقدامات زیر انجام می‌شود:

- تمام ماشین‌های مجازی Hypervisor را که بر روی کامپیوتر آلوده شده در حال اجرا هستند، متوقف می‌کند.
- پروسه‌های فهرست شده در txt را که شامل SQL و نرم‌افزار تهیه نسخه پشتیبان (Veeam Back up) است، خاتمه می‌دهد.
- فایل‌ها را روی کامپیوتر آلوده رمزگذاری می‌کند و به انتهای هر فایل، پسوند yanluowang. را اضافه می‌کند.
- اطلاعیه باج‌گیری (Ransome Note) به نام README.txt را روی کامپیوتر آلوده شده و سیستم‌های رمزگذاری شده قرار می‌دهد.

```
mov     [ebp+var_40], 0
push    offset aVeeam ; "veeam"
lea     ecx, [ebp+var_40]
mov     [ebp+var_30], 0
mov     [ebp+var_2C], 7
mov     word ptr [ebp+var_40], ax
call    sub_D59320
mov     [ebp+var_4], 0
lea     ecx, [ebp+var_28]
push    3
xor     eax, eax
mov     [ebp+var_28], 0
push    offset aSql ; "sql"
mov     [ebp+var_18], 0
mov     [ebp+var_14], 7
mov     word ptr [ebp+var_28], ax
call    sub_D59320
push    0 ; th32ProcessID
push    0Fh ; dwFlags
mov     [ebp+var_4], 1
call    ds:CreateToolhelp32Snapshot
mov     esi, eax
mov     [ebp+var_28C], esi
cmp     esi, 0FFFFFFFFh
jz      loc_D55646

mov     eax, ds:OpenProcess
lea     edi, [ebp+var_40]
mov     ecx, ds:Process32FirstW
mov     [ebp+openProcess], eax
mov     eax, ds:TerminateProcess
mov     [ebp+TerminateProcess], eax
mov     eax, ds:CloseHandle
mov     [ebp+CloseHandle], eax
mov     eax, ds:Process32NextW
mov     [ebp+var_278], 0
mov     [ebp+var_27C], edi
mov     [ebp+Process32FirstW], ecx
mov     [ebp+Process32NextW], eax
db      66h, 66h
```

```
push    eax             ; pnProv
call    ds:CryptAcquireContextW
lea     eax, [ebp+phKey]
push    eax             ; phKey
push    edi             ; pInfo
push    1               ; dwCertEncodingType
push    [ebp+phProv]    ; hCryptProv
call    ds:CryptImportPublicKeyInfo
mov     esi, ds:CryptEncrypt
lea     eax, [ebp+pdwDataLen]
push    20h ; ' '       ; dwBufLen
push    eax             ; pdwDataLen
push    0               ; pbData
push    0               ; dwFlags
push    1               ; Final
push    0               ; hHash
push    [ebp+phKey]     ; hKey
mov     [ebp+var_1118], 20h ; ' '
mov     [ebp+pdwDataLen], 20h ; ' '
call    esi ; CryptEncrypt
push    [ebp+pdwDataLen]
call    ??_U@YAPAXI@Z   ; operator new[](uint)
mov     ecx, [ebp+var_13B0]
add     esp, 4
mov     [ebp+pbBinary], eax
movups  xmm0, xmmword ptr [ecx]
movups  xmmword ptr [eax], xmm0
movups  xmm0, xmmword ptr [ecx+10h]
lea     ecx, [ebp+var_1118]
movups  xmmword ptr [eax+10h], xmm0
push    [ebp+pdwDataLen] ; dwBufLen
push    ecx             ; pdwDataLen
push    eax             ; pbData
push    0               ; dwFlags
push    1               ; Final
push    0               ; hHash
push    [ebp+phKey]     ; hKey
call    esi ; CryptEncrypt
lea     eax, [ebp+pbEncoded]
xor     edi, edi
push    eax             ; pcchString
push    edi             ; pszString
push    1               ; dwFlags
```

تحلیل باج‌افزار Yanluowang نشان می‌دهد که هیچ مدرکی قطعی که نشان دهد نویسندگان باج‌افزار مذکور همان نویسندگان Fivehands هستند، وجود ندارد. محققان احتمال می‌دهند که حملات باج‌افزار Yanluowang توسط شرکای سابق Thieflock در حال انجام است.

> “This link begs the question of whether Yanluowang was developed by Canthroid [a.k.a. Fivehands]. However, analysis of Yanluowang and Thieflock does not provide any evidence of shared authorship. Instead, the most likely hypothesis is that these Yanluowang attacks may be carried out by a former Thieflock affiliate,” the researchers say.

پس از دسترسی و نفوذ به شبکه موردنظر، مهاجمان از PowerShell برای دانلود مواردی همچون بدافزار BazarLoader جهت گسترش آلودگی در سطح شبکه (Lateral Movement) استفاده می‌کنند.

BazarLoader توسط بات‌نت TrickBot که باج‌افزار Conti را نیز منتشر می‌کند، به اهداف مورد نظر منتقل می‌شود. اخیراً، گردانندگان TrickBot شروع به تغییر بات‌نت Emotet نیز کرده‌اند.

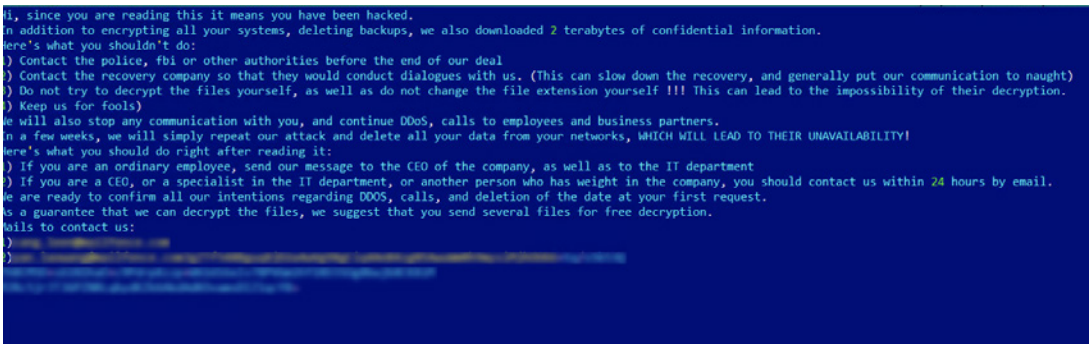
مهاجمان Yanluowang، پروتکل دسکتاپ از راه دور (Remote Desktop Service - به اختصار RDP) را از Registry فعال می‌کنند و برای دسترسی از راه دور، ابزار ConnectWise را نصب می‌کنند.

محققان اعلام نموده‌اند که وابستگان باج‌افزار مذکور، برای کشف سیستم‌های مورد نظر خود، ابزار پرس و جوی متنی مبتنی بر Active Directory (AdFind) را برای جستجو در Active Directory بکار می‌گیرند و از SoftPerfect Network Scanner برای یافتن نام سرورها و سرویس‌های شبکه استفاده می‌کنند.

همچنین آن‌ها برای سرقت اطلاعات اصالت‌سنجی از مرورگرهای Chrome، Firefox و Internet Explorer ماشین‌های آلوده، از ابزارهایی همچون GrabChrome، GrabFF و BrowserPassView استفاده می‌کنند.

نتایج تحقیقات محققان شرکت سیمانتک حاکی از آن است که مهاجمان از KeeThief برای سرقت کلید اصلی (Master Key) به منظور مدیریت رمز عبور در KeePass، ابزارهای تصویربرداری از صفحه (Screen Capture) و ابزار استخراج داده Filegrab استفاده کرده‌اند.

در اطلاعیه باج‌گیری باج‌افزار Yanluowang، مهاجمان تهدید کرده‌اند که قربانی به نهادهای قانونی مراجعه نکند یا از شرکت‌های مذاکره کننده باج‌افزار، درخواست کمک نکند. مهاجمان همچنین اعلام نموده‌اند که چنانچه قربانی، از درخواست آن‌ها اطاعت نکند، اقدام به اجرای حملات منع سرویس توزیع شده (Distributed Denial-of-Service - به اختصار DDoS)، تماس با شرکای تجاری آنان و پاک کردن داده‌ها خواهند نمود. تصویر زیر نمونه‌ای از اطلاعیه باج‌گیری این باج‌افزار را نمایش می‌دهد:



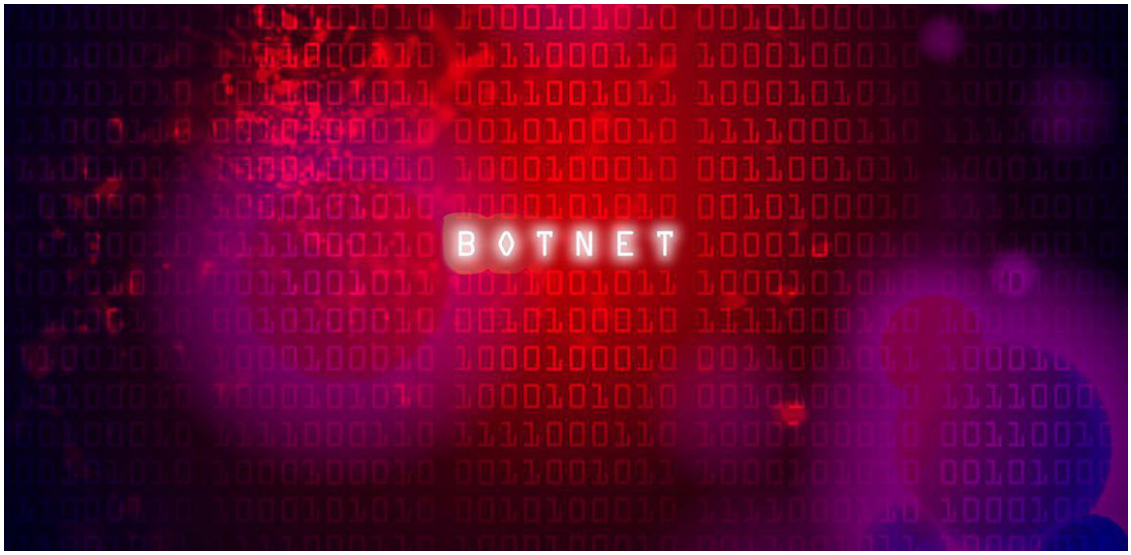
با وجود اینکه باج‌افزار Yanluowang همچنان در حال توسعه است، بسیار خطرناک بوده و یکی از بزرگترین تهدیداتی است که سازمان‌ها در سراسر جهان با آن مواجه هستند.

مشروح گزارش شرکت سیمانتک در خصوص باج‌افزار Yanluowang، نشانه‌های آلودگی (Indicators of Compromise - به اختصار IoC)، ابزارها و بدافزارهای مورد استفاده در حملات مذکور، در نشانی زیر قابل دریافت و مطالعه است:

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-ransomware-attacks-continue

Pink Botnet؛

بزرگترین بات‌نت سال‌های اخیر



محققان شرکت چیهو ۳۶۰ (Qihoo 360, Ltd)، در گزارشی در خصوص بات‌نتی به نام Pink که بیش از ۱.۶ میلیون دستگاه را آلوده کرده است، هشدار داده‌اند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، چکیده‌ای از گزارش شرکت چیهو ۳۶۰ در خصوص بات‌نت Pink ارائه شده است.

یک بات‌نت (شبکه مخرب)، شبکه‌ای از کامپیوترهای آلوده به یک بدافزار است که معمولاً برای هدفگیری چندین کامپیوتر مورد استفاده قرار می‌گیرد. بدافزار مربوطه از شبکه دستگاه‌های آلوده برای گسترش فعالیت‌های مخرب و اغلب حملات DDoS استفاده می‌کند.

از بات‌نت Pink تا به امروز برای راه‌اندازی بیش از ۱۰۰ حمله منع سرویس توزیع‌شده (Distributed Denial-of-Service - به اختصار DDoS) و درج تبلیغات در ترافیک قانونی HTTP قربانیان استفاده شده است که بیشتر آن‌ها (۹۶ درصد) در چین هستند. به گفته کارشناسان، Pink بزرگترین بات‌نتی است که آن‌ها در شش سال گذشته مشاهده کرده‌اند.

تعداد دستگاه‌های آلوده شده توسط بات‌نت Pink قابل توجه است، در ۹ آذر سال ۱۳۹۸، یک شرکت امنیتی در ایالات متحده به شرکت چیهو ۳۶۰ گزارش داد که روزانه ۱,۹۶۲,۳۰۸ نشانی IP فعال منحصر به فرد از بات‌نت Pink را مشاهده کرده که سیستم‌های آن‌ها را مورد هدف قرار داده است.

در ۱۲ دی ماه سال ۹۸، CNCERT نیز گزارش داد که تعداد نشانی‌های IP مرتبط با بات‌نت مذکور بیش از ۵ میلیون مورد است. از آنجایی که نشانی‌های IP پهنای باند خانگی به صورت پویا اختصاص داده می‌شوند، تعداد واقعی دستگاه‌های آلوده شده را نمی‌توان به طور دقیق تخمین زد و فرض بر این است که تعداد واقعی دستگاه‌های هک شده میلیون‌ها مورد است.

```
"From the data measured in multiple dimensions such as NetFlow data, active probing, a
nd real-time monitoring, the number of Bot node IP addresses associated with this botn
et exceeds 5 million. As home broadband IPs are dynamically assigned, the true size of
the infected devices behind them cannot be accurately estimated, and it is presumed th
at the actual number of infected devices is in the millions. One of the main bases of
the measurement is that the number of IPs connected to C2 in one minute was well over
one million."
```

در ۱۸ دی ماه سال ۹۸، محققان شرکت چیهو ۳۶۰ با بررسی و کاوش دریافتند که ۱.۶۵ میلیون دستگاه آلوده شده است. نشانی‌های IP آلوده بیشتر (۹۶درصد) در چین متمرکز شده‌اند و ۳۳ استان آن را دربر می‌گیرند. بات‌نت مذکور بیش از ۸۰ درصد از مشتریان اپراتور China Unicom و ۱۵ درصد از مشتریان اپراتور China Telecom را آلوده نموده است.

مهاجمان با اجرای کدها به صورت از راه دور اقدام به آلوده کردن سیستم‌ها کرده و پس از آن بر اساس دستورالعمل‌های کد، با سرور مهاجم ارتباط برقرار کرده و انواع مختلفی از فعالیت‌های مخرب را انجام می‌دهند.

معماری Pink

کارشناسان پس از تحلیل نمونه‌ای از بات‌نت مذکور پی بردند که نام Pink از اسامی تعداد زیادی تابع موجود در آن که با "Pink" شروع می‌شوند، الهام گرفته شده است. این بات‌نت از معماری پیشرفته ترکیبی مبتنی بر خدمات ثالث (Third-party services)، P2P و سرورهای کنترل و فرمان‌دهی (Command and Control - به اختصار C2) بر گرفته شده است. معماری مذکور با پشتیبانی فروشندگان دستگاه‌های آلوده جهت مقاوم‌سازی بات‌نت و جلوگیری از حذف توسط نهادهای قانونی و امنیتی اجرا شده است.

همانطور که اشاره شد، بات‌نت Pink دارای معماری ترکیبی است که از "P2P" و "C2" مرکزی برای برقراری ارتباط با بات‌های موجود در شبکه استفاده می‌کند. به طور کلی، دستوراتی که به زمان چندان حساس نیستند (همچون مدیریت پیکربندی اطلاعات)، از طریق P2P ارائه می‌شوند، در حالی که دستورات حساس به زمان (مانند راه‌اندازی حملات DDoS، درج تبلیغات در سایت‌های HTTP که توسط کاربران بازدید می‌شوند) به‌طور مرکزی از طریق C2 توزیع می‌شوند.

هر بار که فروشنده‌ای و یا ارائه‌دهندگان محصولات امنیتی تلاش می‌کنند تا بات‌نت مذکور را منهدم کنند، botmaster به‌روزرسانی‌های میان‌افزاری متعددی را در مسیریاب‌های (Routers) فیبری برای حفظ کنترل آن‌ها انجام می‌دهد.

Pink همچنین از DNS-Over-HTTPS - به اختصار DoH برای توزیع اطلاعات پیکربندی استفاده می‌کند که یا از طریق پروژه‌ای مخفی در GITHUB یا Baidu Tieba یا از طریق یک نام دامنه (Domain Name) تعبیه شده که در برخی از نمونه‌های بات‌نت مذکور جاسازی شده، اجرا می‌شود.

به گفته شرکت امنیت سایبری چینی NSFOCUS که در تحقیقات این بات‌نت مشارکت داشته است، مهاجمان از یک حمله "روز-صفر" استفاده کرده تا دستگاه‌های مدیریت پهنای باند برندهای خاصی را مورد هدف قرار دهند. دستگاه‌های آلوده شده عمدتاً در شمال و شمال شرق چین ارائه شده‌اند و بیشتر در پکن نصب شده‌اند. برخلاف سایر بات‌نت‌ها، بدافزار Pink تنها قادر است معماری MIPS مورد استفاده در دستگاه‌های فوق را مورد هدف قرار دهد.

بات‌نت Pink از مجموعه دستورات زیر پشتیبانی می‌کند:

- دانلود فایل
- اجرای فرامین سیستمی
- حملات DDoS (حملات HTTP و حملات UDP)
- پویش (مشخصات پویش را می‌توان با فرامین تنظیم کرد)
- گزارش اطلاعات دستگاه (CPU، نوع سیستم، اطلاعات حافظه، نسخه سیستم، اطلاعات سخت‌افزار)
- خود به‌روزرسانی (نسخه جدید را در /tmp/client ذخیره نموده و سپس اجرا می‌کند)
- همگام‌سازی فهرست نودهای P2P (مجموعه‌ای از نودهای P2P را مستقیماً به بات اعمال می‌کند)
- تزریق پیام HTTP (در دستگاه قربانی، تبلیغ اسکریپت‌های js زمانی که نوع ترافیک http باشد، تزریق می‌شود)
- سرویس پراکسی Sock5 (تنظیم و راه‌اندازی سرویس پراکسی‌های Sock5 در سمت بات، تنظیم رمز عبور حساب کاربری از طریق فرامین)
- دانلود و اجرای فایل
- متوقف کردن حمله
- تنظیم مجدد ناظر

مشروح گزارش شرکت چیهو ۳۶۰ در خصوص باتنت Pink و نشانه‌های آلودگی (Indicators of Compromise - به اختصار IoC) در نشانی زیر قابل دریافت و مطالعه است:

https://blog.netlab.360.com/pink-en/

نشانه‌های آلودگی (IoC)

سرورهای C2:

cnc.pinklander[.]com

۱۴۴.۲۰۲.۱۰۹.۱۱۰:۴۰۰۸۰

۱۴۴.۲۰۲.۱۰۹.۱۱۰:۳۲۸۷۶

۲۰۷.۱۴۸.۷۰.۲۵:۱۲۳۶۸

۴۵.۳۲.۱۲۵.۱۵۰:۱۲۳۶۸

۴۵.۳۲.۱۲۵.۱۸۸:۱۲۳۶۸

۴۵.۳۲.۱۷۴.۱۰۵:۱۲۳۶۸

۵.۴۵.۷۹.۳۲:۱۲۳۶۸

نشانی‌های URL:

http[:]//1.198.50.63:1088/dlist.txt

http[:]//1.63.19.10:19010/var/sss/dlist.txt

http[:]//104.207.142.132/dlist.txt

http[:]//108.61.158.59/dlist.txt

http[:]//111.61.248.32:1088/dlist.txt

http[:]//112.26.43.199:81/dlist.txt

http[:]//113.106.175.43:19010/tmp/pinkdown/dlist.txt

http[:]//117.131.10.102:1088/d/dlist.txt

http[:]//123.13.215.89:8005/d/dlist.txt

http[:]//125.74.208.220:81/dlist.txt

http[:]//140.82.24.94/dlist.txt

http[:]//140.82.30.245/d/dlist.txt

http[:]//140.82.53.129/dlist.txt

http[:]//144.202.38.129/dlist.txt

http[:]//149.28.142.167/p/dlist.txt

http[:]//149.28.142.167/p1/dlist.txt

http[:]//155.138.140.245/dlist.txt

http[:]//167.179.110.44/dlist.txt

http[:]//173.254.204.124:81/dlist.txt

http[:]//182.139.215.4:82/dlist.txt

http[:]//207.148.4.202/dlist.txt

http[:]//218.25.236.62:1987/d/dlist.txt

http[:]//218.25.236.62:1988/d/dlist.txt

http[:]//222.216.226.29:81/dlist.txt

http[:]//45.32.26.220/dlist.txt

http[:]//45.76.104.146/dlist.txt

http[:]//45.77.165.83/p1/dlist.txt

http[:]//45.77.198.232/p1/dlist.txt

http[:]//45.88.42.38/p1/dlist.txt

http[:]//61.149.204.230:81/dlist.txt

http[:]//66.42.114.73/dlist.txt

http[:]//66.42.67.148/dlist.txt

http[:]//8.6.193.191/dlist.txt

http[:]//95.179.238.22/dlist.txt

https[:]//***.com/**/dlist.txt

https[:]//raw.githubusercontent.com/pink78day/helloworld/master/dlist.txt

درهم‌ساز MD5:

۹ec5bd857b998e60663e88a70480b828 /bin/protect

۴۵۱a3cf94191c64b5cd1be1a80be7799 /bin/tr69c

۰۶d6ad872e97e47e55f5b2777f78c1ba slient_l

۰۷cd100c7187e9f4c94b54ebc60c0965 slient_b

0f25b0d54d05e58f5900c61f219341d3 client_b

0f89e43ea433fdfd18a551f755473388 slient_l

۱۱۹۷۹۹۴۶۱۰b2ffb60edbb5ab0c125bc0 client_b

۱۶۷۳۶۴ad0d623d17332f09dbb23a980e client_b

۱۷۵b603082599838d9760b2ab264da6f slient_l

۱a6dce9916b9b6ae50c1457f5f1dfbbd slient_l

۲۲۹۵۰۳۶۸۶c854bb39efdc84f05b071b9 slient_b

۲۵a07e3ef483672b4160aa12d67f5201 client_l

۲۶۲a4e242c9ebeba79aa018d8b38d229 client_l

۲۹d0afd2a244c9941976ebf2f0f6597f client_l

۲befedd020748ff6d9470afad41bd28c slient_b

۲ca5810744173889b2440e4f25b39bd4 client_l

۳۶e48e141943a67c6fdeaa84d7af21cc client_b

۳a620ff356686b461e0e1a12535bea24 slient_l

۴۱bbe8421c0a78067bae74832c375fe8 slient_l

۴۵ee78d11db54acfdda27c19e44c3126 client_l

۴۸۳۰c3950957093dac27d4e87556721e slient_l

۴۸۴۷۶۱f281cb2e64d9db963a463efca5 client_l

۴۸a7f2799bf452f10f960159f6a405d3 client_l

۴۹۴۴۱۲۶۳۸dc8d573172c1991200e1399 client_l

۴c83ad66189a7c4d2f2afdbfb94d0e65 slient_b

۵۰۲۷۰de8d5783bb0092bf1677b93c97b slient_l

۵۴aa9e716567bd0159f4751916f7f0d1 client_l

۵ae1fec20c2f720269c2dc94732187e8 slient_b

۵b62a9bd3431c2fd55283380d81c00fa client_b

۵c322610e1845d0be9ccfc8a8b6a4c4f client_l

۵c4f8dae67dad8cac141afa00847b418 slient_b

۵d0d034845bd69179bf678104c046dc1 client_b

۶۰۶۵۸ef214c960147200d432eece3e13 slient_l

۶۰a2b1bb02a60ac49f7cc1b47abdf60c client_l

۶۱۰f0aadba3be1467125607bf2ba2aaf slient_l

۶۶a068fd860bda7950fde8673d1b5511 client_b

۶c4de9bd490841f0a6c68638f7253c65 client_b

۷۲c531a813b637af3ea56f288d65cdb7 slient_b

۷۶۰۸b24c8dcf3cd7253dbd5390df8b1f client_b

۷۶۴۵a30a92863041cf93a7d8a9bfba1a client_b

۸۵۷fc3c7630859c20d35d47899b75699 slient_b

۸۶۱af6b5a3fea01f2e95c90594c62e9d client_l

۸e86be3be36094e0f5b1a6e954dbe7c2 client_l

۸fbcd7397d451e87c60a0328efe8cd5d client_b

۹۸۷a9befb715b6346e7ad0f6ac87201f slient_b

۹eb147e3636a4bb35f0ee1540d639a1b slient_b

ae8b519504afc52ee3aceef087647d36 slient_b

b0202f1e8bded9c451c734e3e7f4e5d8 slient_b

b6f91ad027ded41e2b1f5bea375c4a42 slient_b

b9935859b3682c5023d9bcb71ee2fece slient_b

b9d1c31f59c67289928e1bb7710ec0ba client_l

bec2f560b7c771d7066da0bee5f2e001 client_b

c2efa35b34f67a932a814fd4636dd7cb slient_l

c839aff2a2680fb5676f12531fecba3b slient_b

c94504531159b8614b95c62cca6c50c9 slient_l

dfe0c9d36062dd3797de403a777577a6 client_b

e19a1106030e306cc027d56f0827f5ce slient_l

f09b45daadc872f2ac3cc6c4fe9cff90 client_b

f5381892ea8bd7f5c5b4556b31fd4b26 client_b

f55ad7afbe637efdaf03d4f96e432d10 slient_b

f62d4921e3cb32e229258b4e4790b63a client_b

f81c8227b964ddc92910890effff179b slient_b

fc5b55e9c6a9ddef54a256cc6bda3804 client_b

fe8e830229bda85921877f606d75e96d slient_l

fee6f8d44275dcd2e4d7c28189c5f5be client_l

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

به پایان عمر Sophos SSL VPN Client نزدیک می‌شویم

شرکت سوفوس، برنامه VPN Client جدید و بسیار پیشرفته Sophos Connect v2 را بیش از یک سال پیش ارائه نموده است. در نتیجه پایان عمر برنامه قدیمی‌تر Sophos SSL VPN Client را برای سیستم‌عامل Windows اعلام نموده است. این شرکت طی اطلاعیه‌ای عنوان نموده که آخرین تاریخ برای دانلود و نصب Sophos SSL VPN Client، ۱۱ بهمن ۱۴۰۰ خواهد بود.

پس از تاریخ مذکور، Sophos SSL VPN Client در شبکه‌ها و کامپیوترهایی که قبلا نصب شده است، همچنان قابل استفاده است و غیر فعال نخواهد شد، اما امکان دانلود، نصب و بروزرسانی جدید نخواهد داشت. سوفوس ضمن تشویق مشتریان به نصب و استفاده از برنامه جدیدتر و پیشرفته‌تر Sophos Connect، توصیه می‌کند که سازمان‌ها در اولین فرصت ممکن این برنامه جدید را جایگزین Sophos SSL VPN Client نمایند.

Sophos Connect v2، برنامه VPN Client جدید و بسیار پیشرفته سوفوس است که با Sophos (XG) Firewall و Sophos UTM (SG) کار می‌کند.

اطلاعات بیشتر درخصوص راه‌اندازی Sophos Connect، در نشانی‌های زیر قابل دریافت و مطالعه است:

- Sophos Connect Documentation:

https://docs.sophos.com/nsg/sophos-connect/help/en-us/nsg/scon/learningContents/InstallScon.html

- Sophos (XG) Firewall: Configuring remote access SSL VPN with Sophos Connect:

https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/learning-Content/VPNRemoteAccessSSLVPNSophosConnectClient.html

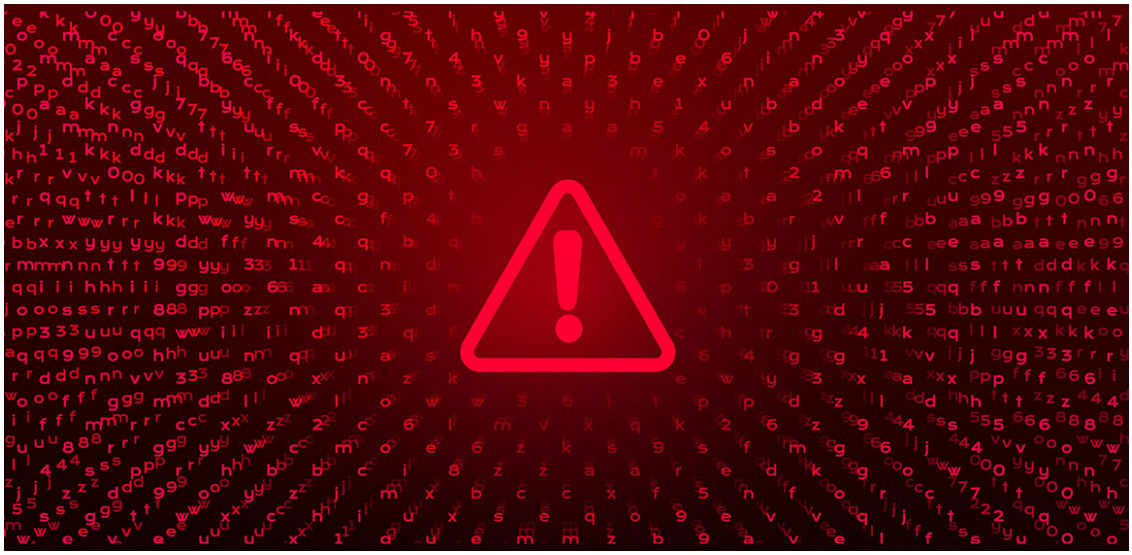
- Sophos (XG) Firewall: Bulk deployment instructions:

https://support.sophos.com/support/s/article/KB-000040793?language=en_US

- Sophos (SG) UTM: Configuring remote access SSL VPN with Sophos Connect:

https://support.sophos.com/support/s/article/KB-000043396?language=en_US

هشدار درخصوص آسیب‌پذیری امنیتی در User Portal SG UTM



اخیراً تیم تحقیقاتی شرکت سوفوس (Sophos, Ltd.)، طی یک آزمایش امنیتی داخلی، یک آسیب‌پذیری را در پورتال کاربران SG UTM، در زمان login کاربر در پورتال کشف نموده است. ضعف امنیتی مذکور که توسط این شرکت ترمیم شده است، از نوع "تزریق کد SQL" (SQL Injection) بوده و دارای شناسه CVE-2021-36807 می‌باشد.

به نقل از محققان شرکت سوفوس، تاکنون هیچ مدرکی مبنی بر سوءاستفاده از این آسیب‌پذیری شناسایی نشده و طبق اطلاعات شرکت مذکور هیچ مشتری تحت تأثیر این ضعف امنیتی قرار نگرفته است.

به عنوان یک اقدام پیشگیرانه، شرکت سوفوس به کاربران محصولات Sophos SG UTM توصیه می‌کند که ضمن غیرفعال‌سازی پورتال کاربران، اقدامات زیر را انجام دهند:

اصلاحیه مذکور در SG UTM نسخه ۷۰۸ که در ۳ آذر ۱۴۰۰ منتشر شده، گنجانده شده است.
سوفوس همیشه توصیه می‌کند که مشتریان SG UTM در اولین فرصت، محصول مذکور را به آخرین نسخه موجود ارتقاء دهند.

انتشار

SG UTM Firmware Up2Date 9.708

شرکت سوفوس (Sophos, Ltd.)، به تازگی نسخه ۹.۷۰۸ SG UTM را منتشر کرده است. طبق معمول، نسخه مذکور در مراحل زیر عرضه خواهد شد:

در فاز ۱، محصول به‌روزرسانی شده از سرور به نشانی زیر قابل دانلود است.

https://download.astaro.com/

- Up2date package - 9.707 to 9.708:

https://download.astaro.com/UTM/v9/up2date/u2d-sys-9.707005-708006.tgz.gpg

- md5sum is df8266489b66c653ca83d6a148904c0e

https://download.astaro.com/UTM/v9/up2date/u2d-sys-9.707005-708006.tgz.gpg.md5

- در فاز ۲، شرکت سوفوس آن را از طریق سرورهای Up2Date برای مدل‌های محدودی از فایروال در دسترس قرار خواهد داد.
- در فاز ۳، بروزرسانی مذکور از طریق سرورهای Up2Date سوفوس برای تمام مدل‌های فایروال‌ها در دسترس قرار خواهد گرفت.

در این نسخه، آسیب‌پذیری از نوع "تزریق کد SQL" (SQL Injection) که اخیراً توسط محققان سوفوس کشف شده، ترمیم شده است. در ضعف امنیتی مذکور که دارای شناسه CVE-2021-36807 می‌باشد، تزریق کد SQL، پس از احراز هویت در پورتال کاربر صورت می‌گیرد.

جزییات بیشتر در خصوص آسیب‌پذیری مذکور در نشانی زیر قابل مطالعه است.

https://newsroom.shabakeh.net/22869/sg-utm-user-portal-vulnerability.html

سوفوس توصیه می‌کند که مشتریان در اولین فرصت، SG UTM را به آخرین نسخه موجود (۹.۷۰۸) ارتقاء دهند.

همچنین در این نسخه، OpenSSL نیز به‌روزرسانی شده است که دیگر مجموعه‌های رمزنگاری (cipher suites) را که شامل پروتکل تبادل کلید Non-EC Diffie-Hellman - به اختصار DH - می‌باشند، پشتیبانی نمی‌کند. این مجموعه‌های رمزنگاری مدتی است که ضعیف تلقی می‌شوند.

باز هم حمله

به دستگاه‌های آسیب‌پذیر NAS شرکت کیونپ

بر اساس توصیه‌نامه‌ای امنیتی که شرکت کیونپ (QNAP Systems, Inc.) در تاریخ ۱۶ آذر ۱۴۰۰ منتشر کرده، دستگاه‌های NAS (Network Attached Storage) ساخت این شرکت هدف حملات موسوم به Cryptomining قرار گرفته‌اند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده بخشی از توصیه‌نامه منتشر شده توسط شرکت کیونپ مورد بررسی قرار گرفته است.

به گزارش شرکت کیونپ در جریان حملات مذکور، مهاجمان، بدافزاری را بر روی دستگاه هک‌شده اجرا می‌کنند که امکان استخراج رمز ارز را با استفاده از منابع دستگاه برای آن‌ها فراهم می‌کند. بدافزاری از نوع Cryptominer که در این کارزار بر روی دستگاه‌های آسیب‌پذیر مستقر شده، پروسه جدیدی به نام [oom_reaper] ایجاد می‌کند که منجر به استخراج ارز دیجیتال (بیت‌کوین) می‌شود.

در حین اجرا، بدافزار مذکور می‌تواند تا ۵۰ درصد از تمام منابع CPU را اشغال کند و تظاهر می‌کند که یک پروسه هسته (با PID بالاتر از ۱۰۰۰) می‌باشد.

این شرکت در ادامه به مشتریانی که نسبت به آلودگی تجهیزات NAS خود به این استخراج‌کننده رمزارز، مشکوک هستند توصیه نموده دستگاه NAS را مجدداً راه‌اندازی کنند، چرا که ممکن است این امر منجر به حذف بدافزار شود.

همچنین شرکت کیونپ جهت درامان ماندن از این حملات، به کاربران دستگاه‌های NAS، انجام اقدامات زیر را توصیه می‌کند:

- QTS یا QuTS hero به آخرین نسخه موجود به‌روزرسانی شوند.
- Malware Remover نصب شود و یا در صورت نصب بودن، به آخرین نسخه آن به‌روزرسانی شود.
- از رمزهای عبور پیچیده و قوی‌تر برای کاربران با سطح دسترسی Admin و سایر حساب‌های کاربری استفاده شود.
- همه برنامه‌های کاربردی نصب شده به آخرین نسخه خود ارتقاء داده شوند.
- تجهیزات NAS به اینترنت متصل نشوند یا از بکارگیری درگاه‌های پیش‌فرض سیستم (درگاه‌های شماره ۴۴۳ و ۸۰۸۰) خودداری شود.

شرکت کیونپ به مشتریان تجهیزات NAS اکیداً توصیه نموده که در اسرع وقت برای محافظت از دستگاه‌های خود بر اساس توصیه‌نامه منتشر شده به نشانی زیر اقدام کنند.

https://www.qnap.com/en/security-advisory/QSA-21-56

تجهیزات NAS ساخت شرکت کیونپ، همواره هدف جذابی برای مهاجمان بوده‌اند و این اولین باری نیست که در سال جاری میلادی هدف بدافزارهای استخراج رمز ارز قرار می‌گیرند.

در ماه مارس، محققان شرکت چیهو ۳۶۰ (Qihoo 360, Ltd) گزارشی منتشر کردند که دستگاه‌های NAS ساخت شرکت کیونپ هدف حملات موسوم به Cryptojacking قرار گرفتند. در جریان حملات مذکور، یک cryptominer با نام UnityMiner اقدام به سوءاستفاده از دو آسیب‌پذیری از نوع RCE (اجرای فرمان از راه دور) به شناسه‌های CVE-2020-2506 و CVE-2020-2507 در دستگاه‌های آسیب‌پذیر و بدون وصله QNAP نمود. این در حالی بود که اصلاحیه دو آسیب‌پذیری مذکور از ماه‌ها قبل‌تر در دسترس قرار داشت.

در گزارش چیهو ۳۶۰ اشاره شده بود که مهاجمان با مخفی‌سازی پروسه و اطلاعات واقعی میزان استفاده از CPU، عملاً فعالیت‌های غیرعادی دستگاه را از دید کاربران در هنگام استفاده از رابط کاربری مخفی می‌کنند.

در ماه ژانویه نیز از کاربران تجهیزات ساخت شرکت کیونپ خواسته شد تا در برابر کارزاری بدافزاری که پس از ایجاد پروسه‌های dovecat و dedpma که تقریباً تمام منابع سیستم را مصرف نموده و دستگاه‌ها را عملاً غیرقابل استفاده می‌نمودند، با به‌روزرسانی از دستگاه‌های خود محافظت کنند.

کیونپ در ماه می ۲۰۲۱ نیز تنها دو هفته پس از هشدار به مشتریان خود در مورد انتشار باج‌افزار AgeLocker، به آن‌ها در مورد حملات باج‌افزار eCh0raix که با نام QNAPCrypt نیز شناخته می‌شود، مجدداً هشدار داد. نخستین نسخه از باج‌افزار مذکور در ژوئن سال ۲۰۱۶ منتشر شد. این باج‌افزار چندین بار در مقیاس گسترده در ژوئن ۲۰۱۹ و ژوئن ۲۰۲۰ تجهیزات NAS شرکت کیونپ را هدف حملات قرار داده است.

این گروه باج‌افزاری، از آسیب‌پذیری به شناسه CVE-2021-28799 - ضعف امنیتی که به مهاجم امکان دسترسی از طریق اطلاعات اصالت‌سنجی پیش‌فرض (Backdoor Account) را می‌دهد - برای رمزگذاری دستگاه‌های کیونپ استفاده می‌کنند. آسیب‌پذیری مذکور در حملات گسترده باج‌افزار Qlocker در آوریل نیز مورد سوءاستفاده قرار گرفته بود. مهاجمان تنها در پنج روز با قفل کردن اطلاعات قربانیان با استفاده از File Archiver منبع باز 7zip، ۲۶۰ هزار دلار به دست آوردند.

به مشتریان تجهیزات کیونپ توصیه می‌شود، با انجام اقدامات دیگری که شرکت کیونپ در نشانی زیر توصیه کرده، دستگاه‌های NAS خود را در برابر حملات، بیشتر ایمن کنند:

https://www.qnap.com/en/how-to/faq/article/what-is-the-best-practice-for-enhancing-nas-security

کابوس جدید سازمان‌ها؛

ضعف امنیتی روز-صفر در کتابخانه Log4j

اخیراً محققان یک ضعف امنیتی روز-صفر را در کتابخانه Log4j کشف کرده‌اند که به مهاجمان اجازه می‌دهد تا اسکریپت‌های مخرب را دانلود و اجرا نموده و امکان کنترل کامل و از راه دور سیستم را برای آن‌ها فراهم می‌کند.

یک نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) از ضعف امنیتی مذکور نیز که مربوط به کتابخانه مبتنی بر Java (Log4j) سرورهای آپاچی می‌باشد، در حال حاضر به صورت آنلاین منتشر و به اشتراک گذاشته شده است. آسیب‌پذیری مذکور، حملاتی از نوع RCE (اجرای کد از راه دور) را برای مهاجمان فراهم می‌کند که کاربران خانگی و سازمان‌ها را در معرض خطر قرار می‌دهد.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، این آسیب‌پذیری مورد بررسی قرار گرفته است.

Log4j توسط بنیاد نرم‌افزاری آپاچی (Apache Software Foundation) توسعه یافته است و به طور گسترده در برنامه‌های کاربردی سازمانی و سرویس‌های ابری مورد استفاده قرار گرفته است. ضعف امنیتی موجود در این کتابخانه که اخیراً منتشر شده، Log4Shell یا LogJam نامیده شده و دارای شناسه CVE-2021-44228 می‌باشد. درجه شدت آسیب‌پذیری مذکور ۱۰ از ۱۰ (بر طبق استاندارد CVSS) و با درجه اهمیت "حیاتی" (Critical) گزارش شده است.

باگ مذکور به مهاجمان اجازه می‌دهد تا اسکریپت‌ها را روی سرورهای موردنظر دانلود و اجرا نموده و امکان کنترل کامل و از راه دور سیستم را برای مهاجمان در سیستم‌های آسیب‌پذیر دارای Log4j 2.0-beta9 تا ۲/۱۴/۱ فراهم می‌کند. لازم به ذکر است که سوءاستفاده از ضعف امنیتی مذکور نیازی به احراز هویت ندارد و برای اجرای آن نیازی به تخصص فنی سطح بالا نیست.

Log4j فقط یک کتابخانه در Java نیست، همانطور که در نشانی زیر به آن اشاره شده، این کتابخانه در بسیاری از سرویس‌ها و سرورها تعبیه شده است. بخش قابل توجهی از نرم‌افزارهای سازمانی، برنامه‌های تحت وب و محصولات اپل، آمازون، کلودفلر، توییتر، استیم، انواع مختلف سرورهای آپاچی و الستیک سرچ احتمالاً در برابر سوءاستفاده از این ضعف امنیتی و حملات RCE مبتنی بر آن، آسیب‌پذیر هستند.

https://github.com/YfryTchsGD/Log4jAttackSurface

سازمان‌ها و شرکت‌های امنیتی مختلف هشدار داده‌اند که مهاجمان در حال تلاش برای پویش اینترنت، جستجوی اهداف آسیب‌پذیر و آلوده نمودن سرویس‌های مختلف وب می‌باشند. تعداد کل پویش‌ها با استفاده از Log4Shell در یک روز سه برابر افزایش یافته است. در حالی که اکثر پویش‌ها هدف خاصی ندارند، به نظر می‌رسد حدود ۲۰ درصد از تلاش‌ها برای جستجوی سرویس‌های آسیب‌پذیر Apache Solr هستند.

شرکت بیت‌دیفندر نیز در نشانی زیر با استناد به ترافیک ایجاد شده در سرویس‌های Honeypot این شرکت و به دلیل سهولت بهره‌برداری و گستردگی کاربرد کتابخانه Log4j در سرورها و نرم‌افزارها هشدار داده که مهاجمان از آسیب‌پذیری و گستردگی کتابخانه اطلاع دارند و احتمالاً شاهد شروع کارزاری بسیار طولانی هستیم.

https://www.bitdefender.com/blog/labs/bitdefender-honeypots-signal-active-log4shell-0-day-attacks-underway-patch-immediately/

با این حال تخمین اثرات مخرب ضعف امنیتی Log4Shell بسیار دشوار است زیرا با توجه به پیشینه وصله‌ها (حتی برای آسیب‌پذیری‌های با شدت بالا)، اعمال وصله در تمامی سیستم‌ها، مستلزم صرف زمان بسیار زیادی است. حتی با وجود اعمال وصله‌ها، معمولاً شاهد حملاتی هستیم که با سوءاستفاده از آسیب‌پذیری‌های وصله شده دو یا سه ساله با موفقیت اجرا می‌شوند.

> *Mass scanning activity detected from multiple hosts checking for servers using Apache Log4j (Java logging library) vulnerable to remote code execution (https://t.co/GgksMUlf94).*
>
> *Query our API for "tags=CVE-2021-44228" for source IP addresses and other IOCs. #threatintel*
>
> *— Bad Packets (@bad_packets) December 10, 2021*

در ۳ آذر ۱۴۰۰، تیم امنیتی Alibaba Cloud در نشانی زیر رسماً آسیب‌پذیری مذکور را به شرکت آپاچی گزارش نمود. از آنجایی که برخی از توابع Apache Log4j2 دارای توابع تحلیلی بازگشتی هستند، مهاجمان می‌توانند مستقیماً درخواست‌های مخرب ایجاد نموده و از آسیب‌پذیری به صورت اجرای کد از راه دور سوءاستفاده کنند. بهره‌برداری از آسیب‌پذیری مذکور نیازی به پیکربندی خاصی ندارد. شرکت آپاچی نیز تایید نمود که ضعف امنیتی CVE-2021-4428 بر پیکربندی‌های پیش‌فرض چندین بستر آپاچی از جمله Apache Struts2، Apache Solr، Apache Druid، Apache Flink و غیره تأثیر می‌گذارد.

https://www.cyberkendra.com/2021/12/worst-log4j-rce-zeroday-dropped-on.html

شرکت آپاچی نسخه Log4j 2.15.0 را برای ترمیم شدت آسیب‌پذیری CVE-2021-44228 منتشر کرده است.

همچنین می‌توان شدت ضعف امنیتی مذکور را در نسخه‌های قبلی (۲.۱۰ به بعد) با تنظیم ویژگی سیستم "log4j2.formatMsgNoLookups" به گزینه "true" یا حذف کلاس JndiLookup از classpath کاهش داد.

شرکت آپاچی نیز از آنجایی که مهاجمان در حال جستجوی اهداف آسیب‌پذیر هستند، به راهبران امنیتی سازمان‌ها توصیه می‌کند که در اسرع وقت با مراجعه به نشانی زیر توصیه‌نامه مربوطه را مطالعه و کتابخانه مذکور را به آخرین نسخه ارتقاء دهند.

https://logging.apache.org/log4j/2.x/security.html

https://logging.apache.org/log4j/2.x/download.html

بروزرسانی نسخه MR2.18.5

فایروال‌های XG سوفوس

شرکت سوفوس (Sophos Ltd.)، اخیراً بروزرسانی Firewall OS v18.5 MR2 (Build 380) را ارائه نموده است که شامل تعدادی ویژگی ارزشمند است. در Sophos Firewall OS v18.5 MR2 بهینه‌سازی‌هایی جهت افزایش امنیت و کارایی صورت گرفته و اشکالات گزارش شده در نسخه‌های قبلی نیز اصلاح شده است.

شرکت سوفوس به تمامی مشتریان توصیه می‌کند که فایروال خود را به آخرین نسخه میان‌افزار ارتقاء دهند تا از ویژگی‌های جدید ارائه شده در فایروال مذکور بهره‌مند شوند. بکارگیری Sophos Firewall OS v18.5 MR2 ضمن تضمین عملکرد بهینه فایروال به دلیل بهره‌مندی از جدیدترین فناوری‌ها و بهینه‌سازی‌های امنیتی، به بهترین شکل از سازمان شما در برابر تهدیدات محافظت می‌کند.

قابلیت‌های جدید در Sophos Firewall OS v18.5 MR2 (Build 380)

- گواهی سطح یک استاندارد FIPS 140-2
    - فایروال سوفوس نسخه MR2 ۵، بر اساس آخرین ماژول رمزنگاری (Cryptographic Module) موفق به اخذ جایزه Federal Information Processing Standards Publications - به اختصار FIPS 140-2 در سخت‌افزار و ماشین‌های مجازی سری XGS، سوفوس شده است.
- بهینه‌سازی IPsec VPN
    - بهبود عملکرد و کارایی IPSec-VPN با قابلیت پشتیبانی از GCM و استانداردهای امنیتی Suite-B Ciphers
    - بهبود مدت زمان موسوم به Idle Time-Out برای حفظ طولانی‌تر اتصالات VPN
    - بهینه‌سازی مسیریابی با استفاده از نشانی IP تونل برای پشتیبانی از masquerading (MASQ) در IPsec-VPN
- ارائه قابلیت جدید موسوم به Sophos Assistant
    - این ابزار جدید که بطور مستقیم در نسخه MR2 ۵ در دسترس است، به صورت یک راهنماهای تعاملی در گردش‌های کاری مهم عمل می‌کند. قابلیت مذکور ضمن راهنمایی در فرایند یادگیری و سهولت انجام وظایف رایج، در پیکربندی و اجرای وظایف پیچیده نیز راهنمایی‌هایی را به کاربر ارائه می‌دهد. جزئیات بیشتر در خصوص Sophos Assistant را می‌توانید در نشانی زیر دریافت و مطالعه کنید:

https://community.sophos.com/product-documentation/b/blog/posts/introducing-sophos-assistant-in-sophos-firewall

- قابلیت ثبت‌نام بدون اصالت‌سنجی در Sophos Central
    - این قابلیت، ثبت فایروال‌های جدید را در Sophos Central بسیار آسان‌تر می‌کند.
- بهینه‌سازی احراز هویت
    - احراز هویت چندعاملی (Multi-Factor Authentication - به اختصار MFA) برای حساب‌های کاربری با دسترسی Admin به همراه قابلیت هشدار بهبود داده شده و فرایند تنظیم و راه‌اندازی آسان‌تر.
    - پشتیبانی از عضویت در چندین گروه Active Directory و نمایش تمام گروه‌هایی که یک کاربر در آن‌ها عضو می‌باشد.
- ارتقاء در بخش گواهی‌های دیجیتال (Certificates)
    - در این نسخه جدید، اطلاعات مفید و جدیدی در مورد CA ها، شناسایی آسان گواهی‌نامه‌های محلی که از کلیدهای خصوصی استفاده می‌کنند و دانلود آسان بخش عمومی هر گواهی‌نامه افزوده شده است.
- بهینه‌سازی ویژگی‌های کاربردی و افزودن ویژگی‌های مضاعف
    - افزودن دامنه‌های جدید جهت استثنا در TLS و بهینه‌سازی عملکرد TLS و بهبود تجربه کاربران نهایی
    - پشتیبانی از Cloudflare به عنوان یک ارائه‌دهنده خدمات DDNS
    - افزودن یک سوئیچ اصلی برای فعال یا غیرفعال کردن موتور IPS
    - بهبود برنامه راهنمای تنظیمات (installation wizard) که به طور پیش‌فرض فقط دو پورت شبکه را bridge می‌کند.
    - ارتقای نسخه JQuery به x.5.
- بهبود لاگ و گزارش‌ها
    - بهبود مدیریت لاگ‌ها و تولید گزارش‌های مختلف در پس زمینه
- سایر موارد
    - بیش از ۱۰۰ مشکل جزئی ترمیم شده است.

توصیه‌نامه امنیتی سوفوس

در خصوص ضعف امنیتی Log4Shell

آذر ۱۴۰۰، یک آسیب‌پذیری با درجه اهمیت حیاتی (Critical) که از نوع RCE (اجرای کد از راه دور) می‌باشد در کتابخانه Log4j کشف شد.

ضعف امنیتی مذکور Log4Shell یا LogJam نامیده می‌شود و دارای شناسه CVE-2021-44228 می‌باشد.

از آنجایی که Log4j، کتابخانه‌ای منبع‌باز (Open source) و بسیار پرکاربرد است، در بسیاری از برنامه‌ها و نرم‌افزارهای سازمانی از جمله بسترهای ابری، برنامه‌های کاربردی تحت وب و سرویس‌های پست الکترونیک استفاده می‌شود. بنابراین طیف گسترده‌ای از نرم‌افزارها در سطح اینترنت وجود دارند که می‌تواند در معرض خطر سوءاستفاده از آسیب‌پذیری مذکور باشند.

از طرفی تقریباً هر یک از برنامه‌های تحت وب و اکثر سرورها به نوعی پروسه ورود به سیستم (Logging) را اجرا می‌کنند و همگی از کتابخانه محبوب Log4j که مبتنی بر زبان برنامه‌نویسی Java پیاده‌سازی شده استفاده می‌کنند لذا این آسیب‌پذیری طیف گسترده‌ای از سرویس‌ها و برنامه‌های کاربردی روی سرورها را تحت تأثیر قرار می‌دهد و آن را به شدت خطرناک می‌کند. از این رو اعمال آخرین به‌روزرسانی‌ها برای تمامی برنامه‌های کاربردی و سرورها بسیار ضروری است.

در همین حال محققان شرکت سوفوس (Sophos, Ltd)، هشدار داده‌اند که صدها هزار تلاش برای اجرای کد از راه دور با استفاده از آسیب‌پذیری Log4Shell تنها در همین روزهای پس از افشای عمومی آن، شناسایی کرده‌اند. آن‌ها اعلام نموده‌اند که مهاجمان در حال حاضر تلاش می‌کنند تا اینترنت را برای نمونه‌های آسیب‌پذیر Log4j پویش کنند.

در حال حاضر نمونه‌های فعالی از مهاجمانی شناسایی شده که به دنبال سوءاستفاده از آسیب‌پذیری Log4j جهت نصب بدافزار استخراج رمز ارز هستند. گزارش‌هایی نیز از چندین بات‌نت، از جمله Mirai، Tsunami و Kinsing وجود دارد که تلاش می‌کنند از ضعف امنیتی مذکور سوءاستفاده کنند.

شرکت سوفوس نیز تحقیقاتی را برای تعیین اینکه آیا راهکارهای امنیتی این شرکت تحت تأثیر آسیب‌پذیری مذکور قرار گرفته‌اند انجام داده است. نتیجه تحقیقات نشان میدهد که امکان Log4j در فایروال‌های سوفوس بطور کلی استفاده نشده است و بنابراین فایروال‌های سوفوس در مقابل این آسیب‌پذیری مصون هستند. توصیه‌نامه امنیتی سوفوس و جزئیات بیشتر در این خصوص در نشانی زیر قابل دریافت و مطالعه است.

https://www.sophos.com/en-us/security-advisories/sophos-sa-20211210-log4j-rce

با وجود اینکه خود فایروال‌های سوفوس در برابر این آسیب‌پذیری مصون هستند، SophosLabs در راستای حفاظت کامل از سرورهای وب مشتریان خود که ممکن است آسیب‌پذیر باشند، تعدادی IPS Signature را در محصولات Sophos Endpoint، Sophos Firewall و Sophos SG UTM پیاده‌سازی کرده که هر گونه ترافیک را که سعی در سوءاستفاده از آسیب‌پذیری مذکور دارد، شناسایی و مسدود می‌کند.

تیم Sophos Managed Threat Response - به اختصار MTR - شرکت سوفوس نیز، همواره به طور فعال حساب‌های مشتریان MTR را برای فعالیت‌های پسابهره‌جویی زیر نظر دارد.

همچنین مشتریان Sophos XDR می‌توانند از یک Query به نشانی زیر برای کمک به شناسایی اجزای آسیب‌پذیر Log4j در محیط سازمان خود استفاده کنند.

https://community.sophos.com/intercept-x-endpoint/i/compliance/identify-vulnerable-log4j-apache-components?cmp=136634

Query مذکور نشان می‌دهد که آیا Log4j توسط راهبران و مدیران فناوری اطلاعات نصب شده است. در صورت شناسایی کتابخانه مذکور، بایستی فوراً با مراجعه به نشانی‌های زیر به‌روزرسانی‌های لازم انجام شده و تمامی پروسه‌های ورود به سیستم (Log) به منظور هرگونه نشانه‌ای از سوءاستفاده و آلودگی بررسی شود.

https://logging.apache.org/log4j/2.x/security.html

https://logging.apache.org/log4j/2.x/download.html

سوفوس با توجه به شدت و ماهیت گسترده این آسیب‌پذیری، به مشتریان توصیه می‌کند استفاده از Log4j را در همه برنامه‌ها، سیستم‌ها و سرویس‌ها در سراسر محیط خود بررسی کنند. در این راستا شرکت مذکور توصیه می‌کند که راهبران امنیتی ابتدا بر روی سرویس‌های منتشر شده در اینترنت تمرکز کنند و دستورالعمل‌های به روزرسانی شرکت‌های مختلف را در خصوص این کتابخانه در اولین فرصت اعمال کنند.

جهت کسب اطلاعات بیشتر در خصوص ضعف امنیتی Log4j مطالعه مقالات زیر توصیه می‌شود.

https://newsroom.shabakeh.net/22888/new-zero-day-exploit-log4j-java-library-enterprise-nightmare.html

https://nakedsecurity.sophos.com/2021/12/10/log4shell-java-vulnerability-how-to-safeguard-your-servers/

https://nakedsecurity.sophos.com/2021/12/13/log4shell-explained-how-it-works-why-you-need-to-know-and-how-to-fix-it/

https://news.sophos.com/en-us/2021/12/12/log4shell-hell-anatomy-of-an-exploit-outbreak/

به‌روزرسانی‌ها و اصلاحیه‌های

آذر ۱۴۰۰

در آذر ۱۴۰۰، مایکروسافت، سیسکو، مک‌آفی‌اینترپرایز، بیت‌دیفندر، کسپرسکی، سوفوس، وی‌ام‌ور، ادوبی، گوگل، اپل، موزیلا، اس‌آپ و آپاچی اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به برخی از بااهمیت‌ترین اصلاحیه‌های آذر ماه پرداخته شده است.

مایکروسافت

شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی دسامبر منتشر کرد. اصلاحیه‌های مذکور بیش از ۶۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند.

درجه اهمیت ۷ مورد از آسیب‌پذیری‌های ترمیم شده ماه دسامبر ۲۰۲۱، "حیاتی" (Critical) و دیگر موارد "مهم" (Important) اعلام شده است.

این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را به شرح زیر در محصولات مختلف مایکروسافت ترمیم می‌کنند:

- "ترفیع امتیازی" (Elevation of Privilege)
- "اجرای کد به صورت از راه دور" (Remote Code Execution)
- "افشای اطلاعات" (Information Disclosure)
- "جعل" (Spoofing)
- "منع سرویس" (Denial of Service - به اختصار DoS)

مجموعه اصلاحیه‌های امنیتی ماه دسامبر ۲۰۲۱ شامل ترمیم آسیب‌پذیری مربوط به Windows Installer است که به طور فعال مورد سوءاستفاده قرار گرفته و در کارزارهای توزیع بدافزار استفاده می‌شود.

۶ مورد از آسیب‌پذیری‌های ترمیم شده ماه دسامبر، از نوع "روز-صفر" (شناسه‌های CVE-2021-43890، CVE-2021-41333، CVE-2021-43880، CVE-2021-43893، CVE-2021-43240، CVE-2021-43883) می‌باشند، اگرچه تنها یک مورد از آسیب‌پذیری‌های "روز-صفر" ترمیم شده در ماه دسامبر به طور فعال مورد سوءاستفاده قرار گرفته است.

مایکروسافت آن دسته از آسیب‌پذیری‌هایی را از نوع روز-صفر می‌داند که پیش‌تر اصلاحیه رسمی برای ترمیم آن‌ها ارائه نشده، جزییات آن‌ها به‌طور عمومی منتشر شده یا در مواقعی مورد سوءاستفاده مهاجمان قرار گرفته است.

فهرست ۶ ضعف امنیتی "روز-صفر" ترمیم شده آخرین ماه از سال میلادی ۲۰۲۱، به شرح زیر است:

- CVE-2021-43890: این آسیب‌پذیری از نوع "جعل" بوده و Windows AppX Installer از آن تاثیر می‌پذیرد. درجه شدت آسیب‌پذیری مذکور که به طور فعال مورد سوءاستفاده قرار گرفته، ۱ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده و دارای درجه اهمیت "مهم" می‌باشد. مایکروسافت اعلام نموده که از تلاش مهاجمان در بکارگیری بسته‌های دستکاری شده جهت سوءاستفاده از این ضعف امنیتی آگاه است و این باگ برای انتشار بدافزارهای Emotet، Trickbot و Bazaloader در کارزارهای مختلف مورد سوءاستفاده قرار گرفته است.
- CVE-2021-41333: برای دومین ضعف امنیتی "روز-صفر"، درجه شدت ۸ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده و از نوع "ترفیع امتیازی" است. آسیب‌پذیری مذکور بر Windows Print Spooler تأثیر می‌گذارد، نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) آن به صورت عمومی منتشر شده و پیچیدگی بسیار پایینی در حملات دارد.
- CVE-2021-43880: این آسیب‌پذیری از نوع "ترفیع امتیازی" می‌باشد. مهاجمان محلی می‌توانند از این ضعف امنیتی در Windows Mobile Device Management برای حذف فایل‌های مورد نظر در یک سیستم سوءاستفاده کنند.
- CVE-2021-43893: درجه شدت این ضعف امنیتی "روز-صفر" که از نوع "ترفیع امتیازی" است، ۵ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده و Windows Encrypting File System از آن تاثیر می‌پذیرد.
- CVE-2021-43240: درجه شدت این آسیب‌پذیری ۸ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده است. مایکروسافت اعلام کرده که این ضعف امنیتی موجب "ترفیع امتیاز" در NTFS Set Short Name شده و نمونه اثبات‌گر آن به صورت عمومی منتشر شده است.
- CVE-2021-43883: آخرین ضعف امنیتی "روز-صفر"، منجر به ترفیع امتیازی غیرمجاز بر Windows Installer شده و درجه شدت آن ۸ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده است.

در ادامه به بررسی ۷ آسیب‌پذیری ترمیم شده "حیاتی" ماه دسامبر می‌پردازیم:

اولین ضعف امنیتی حیاتی دارای شناسه CVE-2021-43233 است که مهاجم را قادر به سوءاستفاده از پودمان RDP (Remote Desktop Protocol) نموده و بر روی Windows Remote Desktop Client تاثیر می‌گذارد.

آسیب‌پذیری حیاتی دیگر، CVE-2021-43217 نیز ناشی از باگی در Windows Encrypted File System - به اختصار EFS - است. این ضعف امنیتی می‌تواند بدون توجه به استفاده یا عدم استفاده از EFS در سیستم مورد نظر فعال شده و مورد سوءاستفاده قرار بگیرد. سوءاستفاده مهاجم از این آسیب‌پذیری و بکارگیری یک فایل دستکاری شده می‌تواند منجر به خطای موسوم به سرریز حافظه (Buffer Overflow Write) و در نتیجه اجرای کد احراز هویت نشده با راه‌اندازی EFS شود. نمونه اثبات‌گر این ضعف امنیتی به طور عمومی منتشر شده و ضروری است هر چه سریع‌تر نسبت به وصله آن اقدام شود.

سومین ضعف امنیتی حیاتی آخرین ماه میلادی ۲۰۲۱، دارای شناسه CVE-2021-43215 است و Windows 7 را در سرورهای کمتر فراگیر Internet Storage Name Service Server - به اختصار iSNS - متاثر می‌کند؛ مولفه‌ای نرم‌افزاری که اتصالات را از طریق iSCSI در Storage Area Network مدیریت می‌کند. مهاجم با سوءاستفاده از آسیب‌پذیری مذکور و ارسال بسته‌های دستکاری شده می‌تواند در ماشینی که به SAN متصل است، منجر به اجرای کد از راه دور شود.

دو آسیب‌پذیری حیاتی دیگر محصولاتی غیر از Windows را متاثر می‌کند. CVE-2021-43905 که با سوءاستفاده از Microsoft Office App در Windows Store سیستم را مورد هدف قرار می‌دهد و CVE-2021-43907 که Visual Studio Code را با سوءاستفاده از افزونه Windows Subsystem for Linux - به اختصار WSL - متاثر می‌کند.

ششمین ضعف امنیتی حیاتی در یکی از جدیدترین محصولات مایکروسافت به نام Defender for IOT بوده و دارای شناسه CVE-2021-42310 می‌باشد. این نرم‌افزار متصل به Azure، داده‌های دستگاه‌های IoT را برای شناسایی آسیب‌پذیری‌های احتمالی و مسائل امنیتی ثبت می‌کند. اما یک آسیب‌پذیری در نسخه ۱۰.۵.۲ و بالاتر Defender for IOT این امکان را برای مهاجم فراهم می‌کند تا داده‌هایی را به کنسول مستقر ارسال نموده و منجر به اجرای کد از راه دور شود. (هفت آسیب‌پذیری دیگر نیز از نوع "اجرای کد از راه دور" و یک آسیب‌پذیری از نوع "افشای اطلاعات" در Defender for IOT وجود دارد.)

آخرین آسیب‌پذیری حیاتی ماه دسامبر با سوءاستفاده از ضعفی در Microsoft's 4K Wireless Display Adapter، "اجرای کد از راه دور" را بر روی سیستم قربانی برای مهاجم فراهم می‌کند. این یک آسیب‌پذیری در سطح میان‌افزار (Firmware-level) بوده و نیاز به دانلود یک برنامه به‌روزرسانی شده دارد. مهاجم احراز هویت نشده می‌تواند با ارسال بسته‌های دستکاری شده در دستگاه‌های آسیب‌پذیر wireless display adapter، کد دلخواه را اجرا نماید.

با توجه به این‌که نمونه اثبات‌گر برخی از ضعف‌های امنیتی ماه دسامبر منتشر شده و بعضی از آن‌ها به طور فعال مورد سوءاستفاده قرار گرفته‌اند، توصیه می‌شود کاربران در اسرع وقت نسبت به به‌روزرسانی وصله‌ها اقدام نمایند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های دسامبر ۲۰۲۱ مایکروسافت در گزارش زیر که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده قابل مطالعه است:

https://afta.gov.ir/portal/home/?news/235046/237266/244794/

سـیسـکو

شرکت سیسکو (Cisco Systems, Inc.) در آذر ماه در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها، ۸ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۲ مورد از آن‌ها "حیاتی"، ۴ مورد از آن‌ها از نوع "بالا" (High) و ۲ مورد از نوع "متوسط" (Medium) گزارش شده است. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

https://tools.cisco.com/security/center/publicationListing.x

مـک‌آفـی اینتـرپـرایز

در آذر ماه، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) اقدام به انتشار نسخ جدید زیر کرد:

- Application and Change Control for Linux 6.4.18
- Command Line Scanner 7.0.1
- Endpoint Security for Linux 10.7.8
- File and Removable Media Protection 5.4.2
- Management of Native Encryption 5.2.1
- McAfee Client Proxy 4.3.0
- MVISION DLP 2112
- MVISION Private Access for macOS
- Endpoint Security Storage Protection 2.1

همچنین این شرکت با انتشار ePolicy Orchestrator 5.10.0 Update 11 Hotfix 2 مجموعه آسیب‌پذیری‌های معروف به Log4J را نیز در این محصول ترمیم و برطرف کرد. جزییات بیشتر در این خصوص در لینک زیر قابل دریافت است:

https://kc.mcafee.com/corporate/index?page=content&id=KB95109

بـیـت‌دیـفـنـدر

در ماهی که گذشت شرکت بیت‌دیفندر (Bitdefender) نسخ زیر را منتشر کرد:

- GravityZone Control Center 6.27.1-1
- Bitdefender Endpoint Security Tools for Windows 7.4.2.130
- Bitdefender Endpoint Security Tools for Linux 7.0.3.1922
- Bitdefender Endpoint Security for Mac 7.4.8.200007

- Bitdefender Security Server Multi-Platform 6.2.5.11201
- Bitdefender Security Server (VMware NSX-T) 1.1.4.11199
- Bitdefender Security Server (VMware NSX-V) 6.2.3.11022

اطلاعات کامل در خصوص تغییرات و بهبودهای لحاظ شده در نسخ مذکور در لینک زیر قابل مطالعه است:

https://www.bitdefender.com/business/support/en/77212-48453-release-notes.html

کسـپرسـکی

شرکت کسپرسکی (AO Kaspersky Lab) در ۱ آذر با انتشار نسخ جدید، در مجموع، ۳ آسیب‌پذیری را در محصولات زیر ترمیم کرد:

- Kaspersky VPN Secure Connection
- Kaspersky Anti-Virus
- Kaspersky Internet Security
- Kaspersky Total Security
- Kaspersky Small Office Security
- Kaspersky Security Cloud
- Kaspersky Password Manager

توضیحات این شرکت در مورد آسیب‌پذیری‌های مذکور در لینک زیر قابل مطالعه است:

https://support.kaspersky.com/general/vulnerability.aspx?el=12430#221121

سوفوس

شرکت سوفوس (Sophos, Ltd.) در اوایل آذرماه طی اطلاعیه‌ای عنوان نموده که پس از ۱۱ بهمن ۱۴۰۰، Sophos SSL VPN Client دیگر قابلیت دانلود، نصب جدید و به‌روزرسانی نخواهد داشت. سوفوس مشتریان را به نصب، استفاده از برنامه جدیدتر و پیشرفته‌تر Sophos Connect v2، تشویق می‌کند. برنامه VPN Client جدید و بسیار پیشرفته سوفوس با Sophos (XG) Firewall و Sophos (SG) UTM کار می‌کند. اطلاعات بیشتر درخصوص راه‌اندازی Sophos Connect، در نشانی‌های زیر قابل دریافت و مطالعه است:

- Sophos Connect Documentation:

https://docs.sophos.com/nsg/sophos-connect/help/en-us/nsg/scon/learningContents/InstallScon.html

- Sophos (XG) Firewall: Configuring remote access SSL VPN with Sophos Connect:

https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/index.html

- Sophos (XG) Firewall: Bulk deployment instructions:

https://support.sophos.com/support/s/article/KB-000040793?language=en_US

- Sophos (SG) UTM: Configuring remote access SSL VPN with Sophos Connect:

https://support.sophos.com/support/s/article/KB-000043396?language=en_US

در اواسط آذر ماه، شرکت مذکور، یک آسیب‌پذیری را در پورتال کاربران SG UTM، در زمان login کاربر در پورتال کشف نمود. ضعف امنیتی مذکور که توسط این شرکت ترمیم شده، از نوع "تزریق کد SQL" (SQL Injection) بوده و دارای شناسه CVE-2021-36807 می‌باشد.

شرکت سوفوس به کاربران محصولات Sophos SG UTM توصیه می‌کند که ضمن غیرفعال‌سازی پورتال کاربران، در اولین فرصت محصول مذکور را به آخرین نسخه موجود (نسخه SG UTM ۹.۷۰۸) ارتقاء دهند.

همچنین در این نسخه، OpenSSL نیز به‌روزرسانی شده است که دیگر مجموعه‌های رمزنگاری (cipher suites) را که شامل پروتکل تبادل کلید Non-EC Diffie-Hellman - به اختصار DH - می‌باشند، پشتیبانی نمی‌کند. این مجموعه‌های رمزنگاری مدتی است که ضعیف تلقی می‌شوند. جزییات بیشتر در خصوص آسیب‌پذیری مذکور در نشانی زیر قابل مطالعه است.

https://newsroom.shabakeh.net/22874/sg-utm-up2date-9-708-released.html

در ماهی که گذشت، سوفوس، به‌روزرسانی Firewall OS v18.5 MR2 (Build 380) را نیز ارائه نمود که شامل بهینه‌سازی‌هایی جهت افزایش امنیت و کارایی صورت گرفته و اصلاح اشکالات گزارش شده در نسخه‌های قبلی است. شرکت سوفوس به تمامی مشتریان توصیه می‌کند که فایروال خود را به آخرین نسخه میان‌افزار ارتقاء دهند تا از ویژگی‌های جدید ارائه شده در فایروال مذکور بهره‌مند شوند. بکارگیری Sophos Firewall OS v18.5 MR2 ضمن تضمین عملکرد بهینه فایروال به دلیل بهره‌مندی از جدیدترین فناوری‌ها و بهینه‌سازی‌های امنیتی، به بهترین شکل از سازمان شما در برابر تهدیدات محافظت می‌کند.

پس از کشف یک آسیب‌پذیری در کتابخانه Log4l در تاریخ ۱۸ آذر ۱۴۰۰، که دارای درجه اهمیت "حیاتی" بوده و از نوع RCE (اجرای کد از راه دور) می‌باشد، توصیه‌نامه امنیتی سوفوس و جزئیات بیشتر در این خصوص در نشانی زیر قابل دریافت و مطالعه است.

https://www.sophos.com/en-us/security-advisories/sophos-sa-20211210-log4j-rce

SophosLabs در راستای حفاظت کامل از سرورهای وب مشتریان خود که ممکن است آسیب‌پذیر باشند، تعدادی IPS Signature را در محصولات Sophos Endpoint، Sophos Firewall و Sophos SG UTM پیاده‌سازی کرده که هر گونه ترافیکی را که سعی در سوءاستفاده از آسیب‌پذیری مذکور دارد، شناسایی و مسدود می‌کند.

مشتریان Sophos XDR می‌توانند از یک Query به نشانی زیر برای کمک به شناسایی اجزای آسیب‌پذیر Log4j در محیط سازمان خود استفاده کنند.

https://community.sophos.com/intercept-x-endpoint/i/compliance/identify-vulnerable-log4j-apache-components?cmp=136634

Query مذکور نشان می‌دهد که آیا Log4j توسط راهبران و مدیران فناوری اطلاعات نصب شده است. در صورت شناسایی کتابخانه مذکور، بایستی فوراً با مراجعه به نشانی‌های زیر به‌روزرسانی‌های لازم انجام شده و تمامی پروسه‌های ورود به سیستم (Log) به منظور هرگونه نشانه‌ای از سوءاستفاده و آلودگی بررسی شود.

https://logging.apache.org/log4j/2.x/security.html

https://logging.apache.org/log4j/2.x/download.html

سوفوس با توجه به شدت و ماهیت گسترده این آسیب‌پذیری، به مشتریان توصیه می‌کند که استفاده از Log4j را در همه برنامه‌ها، سیستم‌ها و سرویس‌های خود بررسی کنند. در این راستا شرکت مذکور توصیه می‌کند که راهبران امنیتی ابتدا بر روی سرویس‌های منتشر شده در اینترنت تمرکز کنند و دستورالعمل‌های به روزرسانی شرکت‌های مختلف را در خصوص این کتابخانه در اولین فرصت اعمال کنند. جهت کسب اطلاعات بیشتر در خصوص ضعف امنیتی Log4j مطالعه مقالات زیر توصیه می‌شود.

https://newsroom.shabakeh.net/22919/apache-log4j-vulnerability.html

وی‌ام‌ور

در ماهی که گذشت، شرکت وی‌ام‌ور (VMware, Inc) با انتشار توصیه‌نامه‌های امنیتی، نسبت به ترمیم محصولات زیر اقدام کرد:

- VMware Workspace ONE Access (Access)
- VMware Identity Manager (vIDM)
- VMware vRealize Automation (vRA)
- VMware Cloud Foundation (Cloud Foundation)
- vRealize Suite Lifecycle Manager
- VMware Workspace ONE UEM console
- VMware Horizon
- VMware vCenter Server (vCenter Server)
- VMware HCX
- VMware NSX-T Data Center
- VMware Unified Access Gateway
- VMware WorkspaceOne Access
- VMware vRealize Operations
- VMware vRealize Operations Cloud Proxy
- VMware vRealize Automation
- VMware vRealize Lifecycle Manager
- VMware Site Recovery Manager, vSphere Replication
- VMware Carbon Black Cloud Workload Appliance
- VMware Carbon Black EDR Server
- VMware Tanzu GemFire
- VMware Tanzu GemFire for VMs
- VMware Tanzu Greenplum
- VMware Tanzu Operations Manager
- VMware Tanzu Application Service for VMs
- VMware Tanzu Kubernetes Grid Integrated Edition
- VMware Tanzu Observability by Wavefront Nozzle
- Healthwatch for Tanzu Application Service
- Spring Cloud Services for VMware Tanzu
- Spring Cloud Gateway for VMware Tanzu
- Spring Cloud Gateway for Kubernetes
- API Portal for VMware Tanzu
- Single Sign-On for VMware Tanzu Application Service
- App Metrics
- VMware vCenter Cloud Gateway
- VMware vRealize Orchestrator
- VMware Workspace ONE Access Connector
- VMware Horizon DaaS
- VMware Horizon Cloud Connector
- VMware NSX Data Center for vSphere
- VMware AppDefense Appliance

- VMware Cloud Director Object Storage Extension
- VMware Telco Cloud Operations
- VMware vRealize Log Insight
- VMware Tanzu Scheduler
- VMware Smart Assurance NCM
- VMware Smart Assurance SAM [Service Assurance Manager]
- VMware Integrated OpenStack
- VMware vRealize Business for Cloud
- VMware vRealize Network Insight
- VMware Cloud Provider Lifecycle Manager
- VMware SD-WAN VCO
- VMware NSX-T Intelligence Appliance
- VMware Horizon Agents Installer
- VMware Tanzu Observability Proxy

سوءاستفاده از ضعف‌های امنیتی ترمیم شده توسط این به‌روزرسانی‌ها، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر و دستیابی به اطلاعات حساس می‌کند. جزییات بیشتر آن در لینک زیر قابل مطالعه است:

https://www.vmware.com/security/advisories.html

ادوبـی

در آذر ماه، شرکت ادوبی (Adobe, Inc.) مجموعه اصلاحیه‌های امنیتی ماه دسامبر را منتشر کرد. اصلاحیه‌های مذکور، در مجموع ۶۰ آسیب‌پذیری را در ۱۱ محصول زیر ترمیم می‌کنند:

- Adobe Premiere Rush
- Adobe Experience Manager
- Adobe Connect
- Adobe Photoshop
- Adobe Prelude
- Adobe After Effects
- Adobe Dimension
- Adobe Premiere Pro
- Adobe Media Encoder
- Adobe Lightroom
- Adobe Audition

ادوبی در مجموعه اصلاحیه ماه دسامبر، یک آسیب‌پذیری با شناسه CVE-2021-43014 را در Adobe Connect ترمیم نموده که نسخه ۱۱.۴ و قبل‌تر این نرم‌افزار از آن تاثیر می‌پذیرند. درجه اهمیت ضعف امنیتی مذکور "مهم" (Important) بوده و سوءاستفاده مهاجم از این آسیب‌پذیری منجر به باگی موسوم به Arbitrary File System Write می‌شود. اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه دسامبر ۲۰۲۱ در لینک زیر قابل مطالعه است:

https://helpx.adobe.com/security/security-bulletin.html

گوگل

شرکت گوگل (Google, LLC) در آذر ماه، اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۲ آذر ماه انتشار یافت، نسخه ۹۶.۰.۴۶۶۴.۱۱۰ است. فهرست اشکالات مرتفع شده در لینک زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop_13.html

اپل

در آذر ماه، شرکت اپل (Apple, Inc.) با انتشار به‌روزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله iOS، iPadOS، watchOS، tvOS، Safari، Security Update Catalina و macOS ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. توصیه می‌شود با مراجعه به نشانی زیر، به‌روزرسانی مربوطه هر چه سریع‌تر اعمال شود.

https://support.apple.com/en-us/HT201222

موزیلا

در ماهی که گذشت شرکت موزیلا (Mozilla, Corp) با ارائه به‌روزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار Thunderbird و NSS برطرف کرد. اصلاحیه‌های مذکور، در مجموع ۱۷ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت ۱ مورد از آن‌ها "حیاتی"، ۶ مورد از آن‌ها "بالا"، ۷ مورد "متوسط" (Moderate) و ۳ مورد "پایین" (Low) گزارش شده است. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. توضیحات بیشتر در لینک زیر قابل مطالعه است:

https://www.mozilla.org/en-US/security/advisories/

اس‌آپ

اس‌آپ (SAP SE) نیز در ۲۴ آذر ۱۴۰۰ با انتشار مجموعه‌اصلاحیه‌هایی، ۲۷ آسیب‌پذیری را در چندین محصول خود برطرف کرد. شدت یک مورد از این ضعف‌های امنیتی ۱۰ از ۱۰، سه مورد ۹.۹ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده است. بهره‌جویی از بعضی از آسیب‌پذیری‌های ترمیم شده مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+December+2021

آپاچی

در ماهی که گذشت، بنیاد نرم‌افزار آپاچی (Apache Software Foundation)، یک توصیه‌نامه امنیتی برای رفع یک ضعف امنیتی که مربوط به کتابخانه مبتنی بر Java (Log4j) سرورهای آپاچی می‌باشد، منتشر کرد. آسیب‌پذیری مذکور، حملاتی از نوع RCE (اجرای کد از راه دور) را برای مهاجمان فراهم می‌کند که کاربران خانگی و سازمان‌ها را در معرض خطر قرار می‌دهد.

Log4j توسط بنیاد نرم‌افزاری آپاچی توسعه یافته و به طور گسترده در برنامه‌های کاربردی سازمانی و سرویس‌های ابری مورد استفاده قرار گرفته است. ضعف امنیتی موجود در این کتابخانه که Log4Shell یا LogJam نامیده می‌شود، دارای شناسه CVE-2021-44228 می‌باشد. درجه شدت آسیب‌پذیری مذکور ۱۰ از ۱۰ (بر طبق استاندارد CVSS) و با درجه اهمیت "حیاتی" گزارش شده است.

ضعف امنیتی "روز-صفر" مذکور به مهاجمان اجازه می‌دهد تا اسکریپت‌های مخرب را دانلود و اجرا نموده و امکان کنترل کامل و از راه دور سیستم را برای آن‌ها فراهم می‌کند. باگ مذکور به مهاجمان اجازه می‌دهد تا اسکریپت‌ها را روی سرورهای موردنظر دانلود و اجرا نموده و امکان کنترل کامل و از راه دور سیستم آسیب‌پذیر را برای مهاجمان در سیستم‌های آسیب‌پذیر دارای Log4j 2.0-beta9 تا ۲/۱۴/۱ فراهم می‌کند. لازم به ذکر است که سوءاستفاده از ضعف امنیتی مذکور نیازی به احراز هویت ندارد و برای اجرای آن نیازی به تخصص فنی سطح بالا نیست.

شرکت آپاچی نسخه Log4j 2.15.0 را برای ترمیم آسیب‌پذیری CVE-2021-44228 منتشر کرده است.

پس از گذشت چند روز از کشف نخستین ضعف امنیتی در کتابخانه Log4j، دومین آسیب‌پذیری موجود در کتابخانه مذکور به شناسه CVE-2021-45046 کشف شد که بر نسخه ۲.۱۵.۰ که برای ترمیم Log4Shell ارائه شده بود، تأثیر می‌گذاشت.

سومین آسیب‌پذیری که به تازگی کشف شده نیز دارای شناسه CVE-2021-45105 بوده، از نوع "Infinite Recursion" است و بر همه نسخه‌های Log4j از 2.0-alpha1 تا ۲.۱۶.۰ تأثیر می‌گذارد. برای این ضعف امنیتی، شدت ۷.۵ از ۱۰ (بر طبق استاندارد CVSS) و درجه اهمیت "بالا" (High) گزارش شده است.

شرکت آپاچی نیز از آنجایی که مهاجمان در حال جستجوی اهداف آسیب‌پذیر هستند، به راهبران امنیتی سازمان‌ها توصیه می‌کند که در اسرع وقت با مراجعه به نشانی زیر توصیه‌نامه مربوطه را مطالعه و کتابخانه مذکور را به آخرین نسخه ارتقاء دهند.

https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

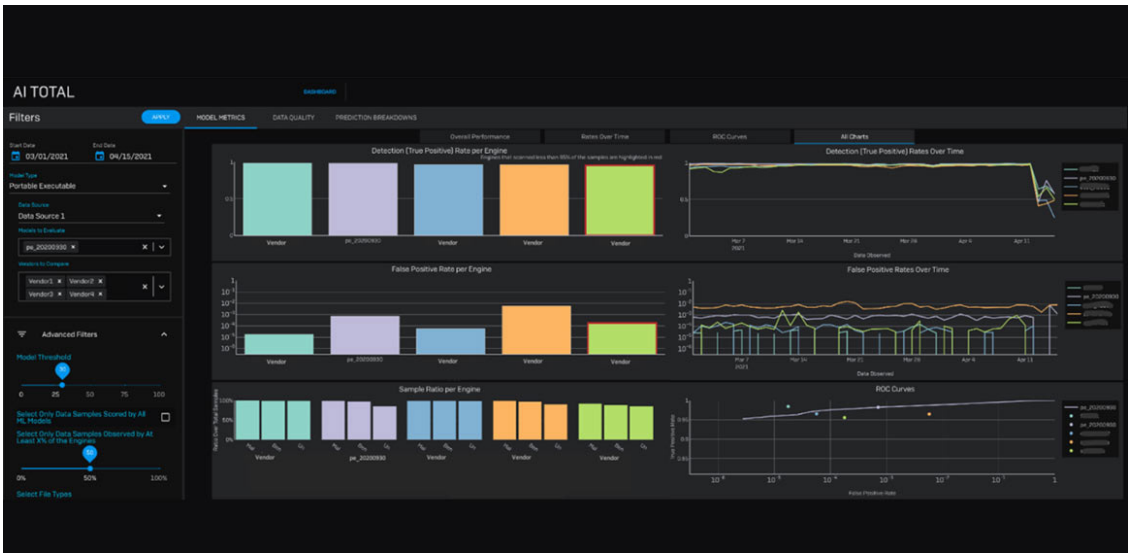
https://logging.apache.org/log4j/2.x/security.html

https://logging.apache.org/log4j/2.x/download.html

گزارش‌ها

تحلیل مدل‌های یادگیری ماشینی سوفوس

در زمینه امنیت شبکه



تیم هوش مصنوعی شرکت سوفوس (Sophos, Ltd) مدل‌های یادگیری ماشینی متعددی را توسعه می‌دهد که مستقیماً با محصولات سوفوس ادغام می‌شوند.

در حال حاضر سوفوس بیش از ۳۰ مدل یادگیری ماشینی تولید شده دارد که در محصولات سوفوس بکارگرفته شده و فایل‌های بدافزاری، آدرس‌های URL و ایمیل‌های مخرب را شناسایی می‌کنند.

هنگام توسعه مدل‌های یادگیری ماشینی جدید، معمولاً مدل‌ها با استفاده از مجموعه داده‌های ثابت که به‌صورت دستی انتخاب شده‌اند، آموزش داده شده و سپس ارزیابی می‌شوند. ارزیابی مدل موجب می‌شود عملکرد نهایی مدل بررسی شده و پیشرفت تحقیقات به‌طور دقیقی رصد شود.

هنگامی که مدل در محصولات امنیتی تولید شده، پیاده‌سازی می‌شود، این‌بار به‌جای ارزیابی عملکرد آن توسط مجموعه‌داده‌های ایستا، ارزیابی خودکار بر روی داده‌های جدید درحال ورود انجام می‌شود. به عبارت دیگر، بعد از انتخاب مدل، یک Data Pipeline برای آموزش مدل ایجاد می‌شود، یعنی جریانی پیوسته و کارامد از داده‌ها ایجاد می‌شود تا مدل به صورت مناسبی آموزش ببیند. این کار عمدتاً ساده به نظر می‌رسد، اما در عمل اینطور نیست. اساساً به این دلیل که در یک Pipeline کاملاً خودکار، درک این‌که آیا خطاها و کاهش عملکرد، ناشی از کارایی مدل، Data Pipeline و یا مجموعه‌داده‌های نامتوازن (سوگیری توزیع داده‌های در حال ورود) یا ترکیبی از موارد فوق است، بسیار دشوار می‌باشد.

در تیم هوش‌مصنوعی سوفوس (SophosAI)، تیم‌های زیرساخت‌داده، علم داده و محققان بدافزار با یکدیگر جهت توسعه، ارائه و بهبود مستمر مدل‌های تولیدی همکاری می‌کنند. آن‌ها باید به منبع مشترکی از اطلاعات دسترسی داشته باشند به صورتی که در آن همه تیم‌ها بتوانند درک یکسانی از مدل‌های تولیدی داشته باشند. با در نظر گرفتن همه این موارد، تیم هوش مصنوعی سوفوس، یک داشبورد مصورسازی بلادرنگ (Real-time Visualization Dashboard) به نام AI Total ساخته‌اند که اهداف زیر را محقق می‌سازد:

- رصد منظم عملکرد مدل‌های پیاده‌سازی شده، مشاهده روندهای زمانی (Time Trends) و تشخیص رفتار غیر نرمال (Anomaly Detection)
- شناسایی خطاها از طریق ارزیابی مجموعه‌داده‌ها، مدل‌ها یا داده‌های برچسب‌گذاری شده
- یافتن و بررسی علت رخداد خطاها

این داشبورد مصورسازی بلادرنگ مبتنی بر وب سوفوس (AI Total)، به کاربران اجازه می‌دهد تا به سرعت نتایج عددی عملکرد مدل را مشاهده نموده و در عین حال از صحت مجموعه‌داده بکار گرفته شده در مرحله آموزش (Train) اطمینان داشته باشند. همچنین به کاربران این امکان را می‌دهد که وقتی خطایی پیش می‌آید، فوراً علت اصلی آن را مشاهده کنند.

سوفوس به‌تازگی روش جدیدی را به‌منظور تحلیل کارایی و مشکلات مربوط به مجموعه‌داده‌ها با استفاده از روش Data Coverage Equalizer، ارائه داده و مقاله‌ای نیز در این خصوص در ۲۱ مهر ۱۴۰۰ ارائه کرده است.

بررسی مقاله مذکور نشان می‌دهد که چگونه قابلیت مصورسازی بلادرنگ، نیازهای عملیاتی تیم تحقیقاتی سوفوس در حوزه صنعت را جهت شناسایی و حل مشکلات رایج در مدل‌های امنیتی تولید شده برآورده می‌کند.

پنل مصورسازی از سه سربرگ (Tab) تشکیل شده که هر کدام از آن‌ها جهت دستیابی به اهداف زیر طراحی شده است:

- پارامترهای ارزیابی مدل (Model Metrics): اولین سربرگ، کارایی کلی مدل را با ارزیابی پارامترها (Metrics) نشان می‌دهد. این سربرگ پارامترهایی همچون TPR، Scanned Data Ratio Plot، FPR، TPR و FPR در طول زمان و منحنی ROC مدل را نشان می‌دهد. تشخیص درست بدافزارها (TPR) و کاهش نرخ مثبت کاذب (FPR) از شاخص‌های بسیار کلیدی عملکرد در حوزه امنیت هستند، بنابراین عملکرد یک مدل امنیتی در ابتدا با دو پارامتر مذکور ارزیابی می‌شود.

- کیفیت داده (Data Quality): در فاز پیاده‌سازی، ممکن است یکی از دلایل شکست و عدم کارایی مدل، مربوط به مجموعه‌داده‌های مورد استفاده باشد. دومین سربرگ، حجم و نرخ داده‌ها را جهت رصد آسان مسائل مربوط به مجموعه‌داده‌ها که بر عملکرد مدل‌های یادگیری ماشینی تأثیر می‌گذارند، نشان می‌دهد. این اطلاعات اساساً توسط دانشمندان داده، مهندسان، توسعه‌دهندگان و مهندسان زیرساخت مورد استفاده قرار می‌گیرند. در واقع، هدف این سربرگ، نظارت بر داده‌ها، سازگاری آن‌ها و تشخیص رفتار غیر نرمال در منابع ورودی و برچسب‌گذاری داده‌ها می‌باشد. در اینجا داده‌های بکارگرفته شده، داده‌های گم شده، داده‌های بدون برچسب و داده‌های فاقد نوع نیز نمایش داده می‌شوند.

مشاهده حجم بالای داده‌های فاقد برچسب نشان می‌دهد که سیستم برچسب‌گذاری عملکرد پایینی دارد و قابل اعتماد نیست و داده‌های برچسب‌گذاری شده کافی جهت آموزش مدل نداریم. نمودارهایی نیز در این سربرگ وجود دارند که حجم نمونه‌های بدافزاری، غیربدافزاری و بدون برچسبی را که پویش شده‌اند، نشان می‌دهند.

- پیش‌بینی (Prediction Breakdown): این سربرگ تحلیلی از عملکرد مدل را بر اساس چندین دسته مرتبط، حجم داده‌های مربوطه و چند آمار تجمعی جهت بررسی بیشتر مسائل نشان می‌دهد. در سربرگ مذکور، دو جدول نیز ارائه می‌شود که یکی مجموعه‌داده‌ها را بر اساس نوع بدافزار و دیگری بر اساس نوع فایل نشان می‌دهد. این اطلاعات اغلب توسط دانشمندان داده مورد استفاده قرار می‌گیرند.

مقاله روش ابداعی سوفوس تحت عنوان AI Total: Analyzing Security ML Models with Perfect Data in Production به IEEE Symposium on Visualization for Cyber Security, 2021، ارسال شده است. مقاله مذکور در پایگاه‌علمی arXiv نیز منتشر شده و در نشانی زیر قابل دریافت و مطالعه می‌باشد:

https://arxiv.org/abs/2110.07028

گزارش فصلی مک‌آفی
منتشر شد

شماره جدید گزارش McAfee Enterprise Advanced Threat Research منتشر شد. در این گزارش میزان فراوانی تهدیدات سایبری و اهداف آن‌ها در ماه‌های اخیر مورد بررسی قرار گرفته است.

در حالی به ماه‌های پایانی سال ۲۰۲۱ نزدیک می‌شویم که مهاجمان با تهدیدات و تاکتیک‌های جدید و دائما در حال تکامل خود صنایع مختلف را هدف قرار می‌دهند.

حملات باج‌افزاری همچنان در حال گسترش هستند و کسب‌وکار آن‌ها با میلیون‌ها دلار اخاذی از شرکت‌های بزرگ تا کوچک هر روز پررونق‌تر از قبل می‌شود.

در اواسط سال ۲۰۲۱ که DarkSide و REvil پس از حملاتی پرسروصدا فعالیت خود را متوقف کردند، BlackMatter خیلی زود توانست جای خالی آن‌ها را پر کند. بر اساس شواهد موجود برخی منابع معتقدند که BlackMatter نسخه جدیدی از DarkSide است؛ اگر چه این موضوع از سوی گردانندگان BlackMatter رد شده است.

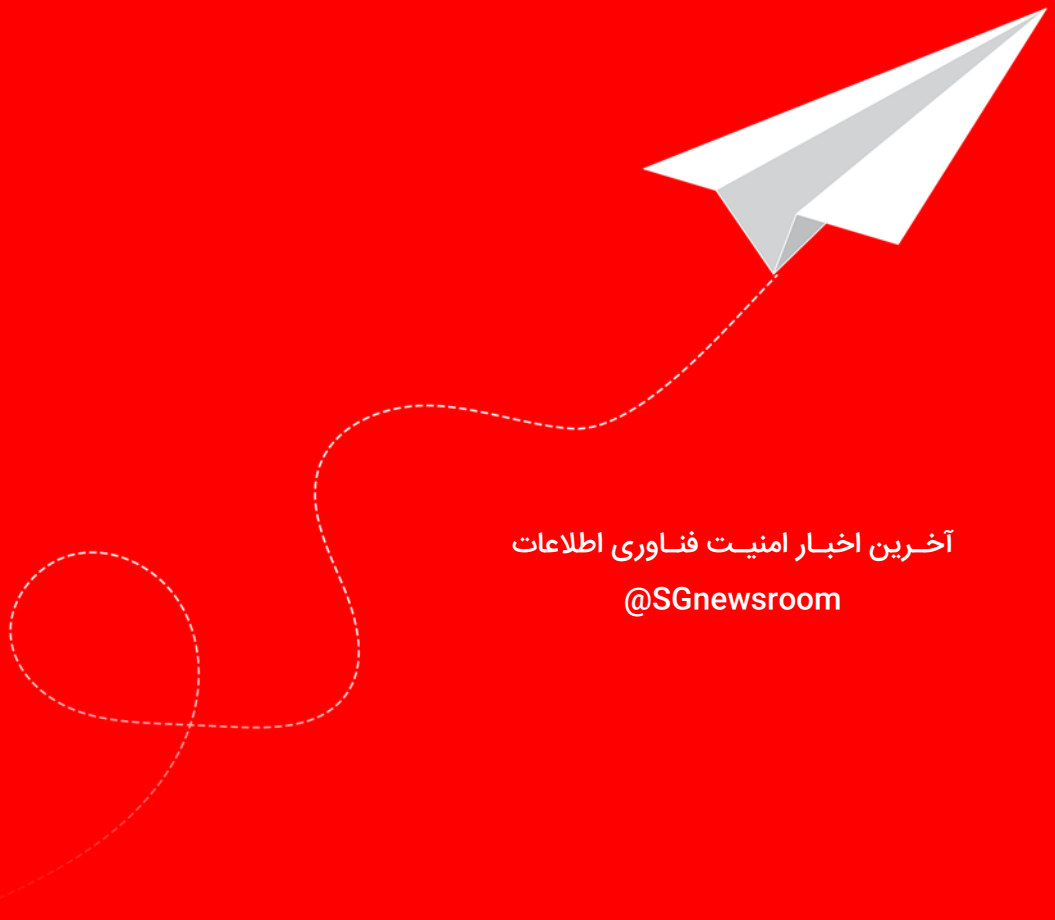
باج‌افزار قدیمی دیگر که نگارش متفاوتی از آن در ماه‌های اخیر منتشر شد LockBit 2.0 است. LockBit 2.0 نگارشی به‌روز شده از نسخه ۲۰۲۰ باج‌افزار LockBit است که با قابلیت‌های جدید قادر به اجرا امور مخربی از جمله رمزگذاری دستگاه‌ها در سطح دامنه و سرقت داده‌ها است.

سه‌ماهه دوم ۲۰۲۱ دوره‌ای پرتلاطم برای حملات باج‌افزاری به برخی سازمان‌ها و شرکت‌های مطرح بود. در پی اختلالات و بحران‌های ناشی از حمله گردانندگان باج‌افزار DarkSide به خط لوله شرکت کولونیال، تأثیرات مخرب و بالقوه فاجعه‌بار حملات باج‌افزاری بیش از هر زمانی روشن شد. فشارهای سیاسی پس از آن و تلاش‌های نهادهای امنیتی، موجب توقف فعالیت DarkSide شد. چندین گروه دیگر از گردانندگان تهدیدات سایبری نیز اعلام کردند تا برای در امان ماندن از چنین فشارهایی، از حمله به برخی حوزه‌های خاص خودداری خواهند کرد. اندکی بعد، دو تالار گفتگوی اینترنتی معروف هکرها به نام‌های XSS و Exploit، تبلیغات باج‌افزاری را در سایت خود ممنوع کردند. برای سالها این تالارها، بهشتی امن برای تبهکاران سایبری و گردانندگان باج‌افزاری برای فروش خدمات RaaS، تبادل اطلاعات سرقت‌شده و بسیاری امور مخرب دیگر بود. به نظر می‌رسد که این اقدام مدیران XSS و Exploit تلاشی برای بقای این تالارهای گفتگو در برابر فشارهای دولتی و نهادهای قانونی بوده که بر اثر حملات گسترده باج‌افزاری ماه‌های گذشته تشدید شده است. با این حال همان‌طور که در این گزارش خواهید خواند همچنان تالارهای متعددی هستند که گردانندگان باج‌افزار بی‌محابا در آن‌ها جولان می‌دهند.

در بخشی از این گزارش، متداول‌ترین تاکتیک‌ها و تکنیک‌های MITRE ATT&CK که در سه‌ماهه دوم سال ۲۰۲۱ توسط گروه‌های مختلف از مهاجمان استفاده شدند نیز به تفصیل مورد بررسی قرار گرفته است.

این گزارش، منبعی باارزش در مطالعات و تحقیقات در حوزه تهدیدات سایبری است. آمار و اطلاعات ارائه شده در این گزارش، بر پایه شبکه جهانی McAfee Enterprise متشکل از بیش از یک میلیارد حسگر (Sensor)، بررسی‌ها و رصدهای مستمر متخصصان این شرکت است.

برای دریافت گزارش فصلی مک‌آفی بر روی تصویر زیر کلیک کنید.



آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

شـرکـت مـهـنـدسـی شـبـکـه گـسـتـر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظـفـر)، شـماره ۲۷۳

تلفـن / دورنـگار ۰۲۱ - ۴۲۰۵۲

رایانامـه info@shabakeh.net

تارنمای شـرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکـز آمـوزش events.shabakeh.net

اتـاق خبـر newsroom.shabakeh.net