ماهنامه امنیت فناوری اطلاعات

تیر ۱۳۹۸

شبکه گستر
امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای امنیتی در تیر ماه ۱۳۹۸ پرداخته شده است.

در حالی که بیش از شش ماه از شناسایی نخستین نسخه از Phobos می‌گذرد این باج‌افزار مخرب همچنان سهم قابل‌توجهی از آلودگی‌ها را در کشورهای مختلف از جمله ایران به خود اختصاص داده است.

در تیر ماه، شرکت‌های مایکروسافت، ادوبی، سیسکو، گوگل، وی‌اِم‌وِر، موزیلا، جونیپر نت‌ورکز، اوراکل و اپل و بنیاد دروپل اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. در این شماره از ماهنامه ضمن مرور این اصلاحیه‌ها، در مطلبی به نزدیک شدن به تاریخ پایان پشتیبانی مایکروسافت از Windows 7 و اهمیت ارتقای این سیستم عامل به نسخه‌های جدیدتر پرداخته شده است.

بر اساس تحقیقی که یافته‌های آن در این شماره از ماهنامه قابل مطالعه است میانگین مبلغ اخاذی شده در جریان حملات باج‌افزاری در سه‌ماهه دوم سال میلادی جاری با افزایشی ۱۸۴ درصدی در مقایسه با سه‌ماهه قبل از آن به بیش از ۳۶ هزار دلار رسیده است.

همچون همیشه ویروس‌نویسان و تبهکاران سایبری از روش‌های مختلف برای فریب کاربران و آلوده‌سازی سیستم‌های آنها به بدافزار بهره گرفته‌اند که جدیدترین نمونه‌های آنها در این شماره از ماهنامه مورد بررسی قرار گرفته است.

هشدارهای امنیتی

Phobos؛

باج‌افزاری که همچنان قربانی می‌گیرد

در حالی که بیش از شش ماه از شناسایی نخستین نسخه از Phobos می‌گذرد این باج‌افزار مخرب همچنان سهم قابل‌توجهی از آلودگی‌ها را به خود اختصاص داده است.

متأسفانه ایران نیز همواره از جمله اهداف گردانندگان این باج‌افزار بوده است.

کدنویسی و عملکرد Phobos از جهات بسیاری مشابه باج‌افزار معروف Dharma است.

اتصال از راه دور مهاجمان از طریق پودمان Remote Desktop – به اختصار RDP – به دستگاه‌های با رمز عبور ضعیف و اجرای فایل مخرب باج‌افزار اصلی‌ترین روش انتشار Phobos است. هر چند که نمونه‌هایی از Phobos نیز از طریق هرزنامه‌های[۱] ناقل فایل / لینک مخرب یا با بهره‌جویی[۲] از آسیب‌پذیری‌های امنیتی منتشر شده‌اند.

محل ذخیره‌سازی فایل مخرب این باج‌افزار ٪AppData٪ یا ٪LocalAppData٪ است.

Phobos به فایل‌های رمزگذاری شده، پسوندی با قالب زیر الصاق می‌کند:

id[random numbers].[email].extension

برای مثال، در یکی از جدیدترین نمونه‌های این باج‌افزار در ایران عبارت زیر به هر فایل رمزگذاری شده چسبانده می‌شود:

id[868E1504-2239].[meachemvasili@aol.com].adage

از دیگر ایمیل‌های استفاده شده توسط مهاجمان Phobos می‌توان به موارد زیر اشاره کرد:

- Bad_boy700@aol.com
- barcelona_100@aol.com
- beltoro905073@aol.com
- Cadillac.407@aol.com
- datadecryption@countermail.com
- decryptyourdata@qq
- elizabethz7cu1jones@aol.com
- Everest_2010@aol.com
- FobosAmerika@protonmail.ch
- gabbiemciveen@aol.com
- Gomer_simpson2@aol.com
- greg.philipson@aol.com
- helpyourdata@qq.com
- Job2019@tutanota.com
- luciolussenhoff@aol.com
- ofizducwell1988@aol.com
- paper_plane1@aol.com
- Raphaeldupon@aol.com
- recover_actin@qq.com
- returnmefiles@aol.com
- simonsbarth@aol.com
- waitheisenberg@xmpp.jp
- walletwix@aol.com
- wewillhelpyou@qq.com

۱ Spam
۲ Exploiting

در هر پوشه‌ای که حداقل یکی از فایل‌های آن رمزگذاری شده است فایلی با نام info.txt یا Encrypted.txt کپی می‌شود که در آن به نحوه برقراری ارتباط با مهاجمان پرداخته شده است. ضمن اینکه پنجره‌ای مشابه شکل زیر نیز به‌صورت خودکار بر روی دستگاه اجرا می‌شود.

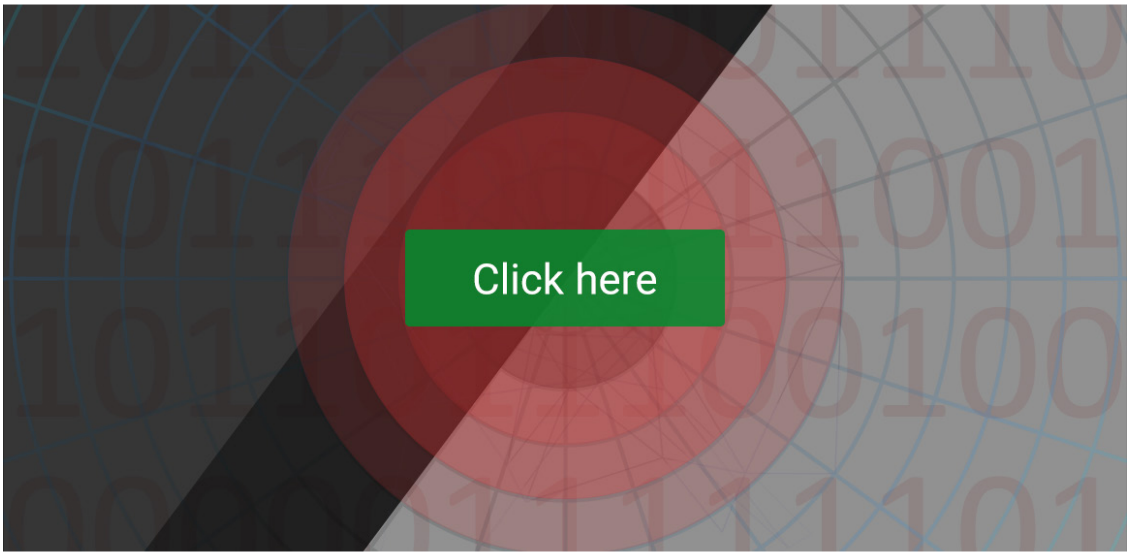
Phobos فایل‌های با هر یک از پسوندهای زیر را مورد دست‌درازی قرار می‌دهد:

- .sql
- .mp4
- .7z
- .rar
- .m4a
- .wma
- .avi
- .wmv
- .csv
- .d3dbsp
- .zip
- .sie
- .sum
- .ibank
- .t13
- .t12
- .qdf
- .gdb
- .tax
- .pkpass
- .bc6
- .bc7
- .bkp
- .qic
- .bkf
- .sidn
- .sidd
- .mddata
- .itl
- .itdb
- .icxs
- .hvpl
- .hplg
- .hkdb
- .mdbackup
- .syncdb
- .gho
- .cas
- .svg
- .map
- .wmo
- .itm
- .sb
- .fos
- .mov
- .vdf
- .ztmp
- .sis
- .sid
- .ncf
- .menu
- .layout
- .dmp
- .blob
- .esm
- .vcf
- .vtf
- .dazip
- .fpk
- .mlx
- .kf
- .iwd
- .vpk
- .tor
- .psk
- .rim
- .w3x
- .fsh
- .ntl
- .arch00
- .lvl
- .snx
- .cfr
- .ff
- .vpp_pc
- .lrf
- .m2
- .mcmeta
- .vfs0
- .mpqge
- .kdb
- .db0
- .dba
- .rofl
- .hkx
- .bar
- .upk
- .das
- .iwi
- .litemod
- .asset
- .forge
- .ltx
- .bsa
- .apk
- .re4
- .sav
- .lbf
- .slm
- .bik
- .epk
- .rgss3a
- .pak
- .big
- wallet
- .wotreplay
- .xxx
- .desc
- .py
- .m3u
- .flv
- .js
- .css
- .rb
- .png
- .jpeg
- .txt
- .p7c
- .p7b
- .p12
- .pfx
- .pem
- .crt
- .cer
- .der
- .x3f
- .srw
- .pef
- .ptx
- .r3d
- .rw2
- .rwl
- .raw
- .raf
- .orf
- .nrw
- .mrwref
- .mef
- .erf
- .kdc
- .dcr
- .cr2
- .crw
- .bay
- .sr2
- .srf
- .arw
- .3fr
- .dng
- .jpe
- .jpg
- .cdr
- .indd
- .ai
- .eps
- .pdf
- .pdd
- .psd
- .dbf
- .mdf
- .wb2
- .rtf
- .wpd
- .dxg
- .xf
- .dwg
- .pst
- .accdb
- .mdb
- .pptm
- .pptx
- .ppt
- .xlk
- .xlsb
- .xlsm
- .xlsx
- .xls
- .wps
- .docm
- .docx
- .doc
- .odb
- .odc
- .odm
- .odp
- .ods
- .odt

همچنین با اجرای فرامین زیر اقدام به غیرفعال کردن دیواره آتش می‌کند:

```
netsh.exe netsh advfirewall set currentprofile state off
netsh.exe netsh firewall set opmode mode=disable
```

سرقت ارز رمز؛
تحت نام افراد سرشناس

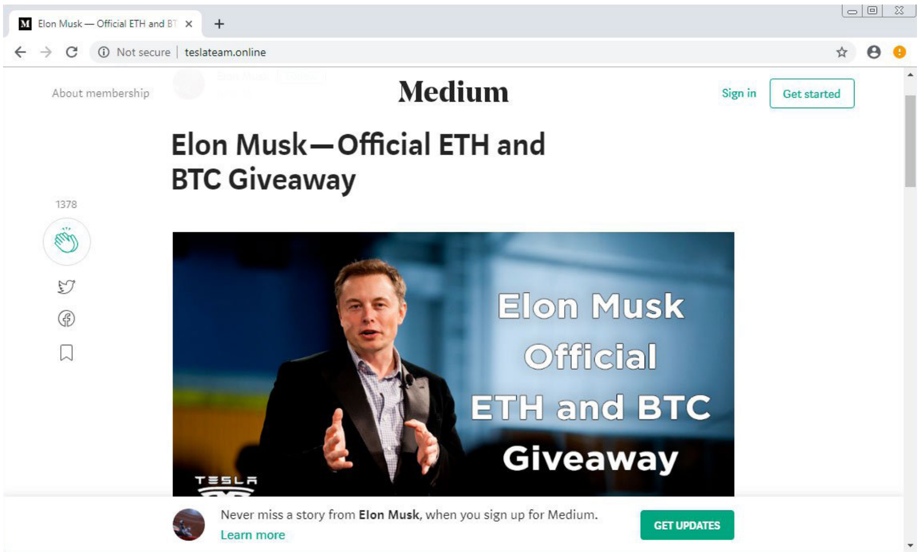


در هفته‌های اخیر، همزمان با روند صعودی ارزش ارز رمزهایی نظیر بیت‌کوین، گروهی از مهاجمان در بستر شبکه اجتماعی توییتر در حال اجرای حملات کلاهبرداری علیه کاربران ناآگاه هستند.

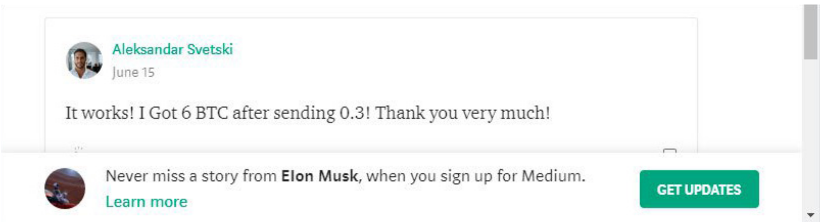
این تبهکاران برای فریب کاربر و هدایت او به سایت‌های مخرب تحت کنترل خود از معروفیت افرادی که ارتباط آنها با محصولات برتر و منحصربه‌فرد سبب شهرت جهانی آنها شده است بهره گرفته‌اند. بدین‌منظور مهاجمان با ساخت حساب‌هایی جعلی در توییتر اینطور القا می‌کنند که مالک حساب، شخصیت‌هایی نظیر ایلان ماسک و جان مک‌آفی است. در ادامه تلاش می‌شود تا با انتشار مطالب و دیدگاه‌هایی با محتوای فریبنده، تحت نام حساب‌های مذکور، خواننده متقاعد به کلیک بر روی لینک درج شده در این پیام‌ها شود.

در صورت موفقیت در فریب کاربر، صفحه‌ای در مرورگر باز شده و در آن با استفاده از تکنیک‌های مهندسی اجتماعی و ادعای اجرای برنامه اهدای ارز رمز از سوی یکی از افراد سرشناس اشاره شده در ابتدای این خبر، کاربر به سایتی دیگر هدایت می‌شود.

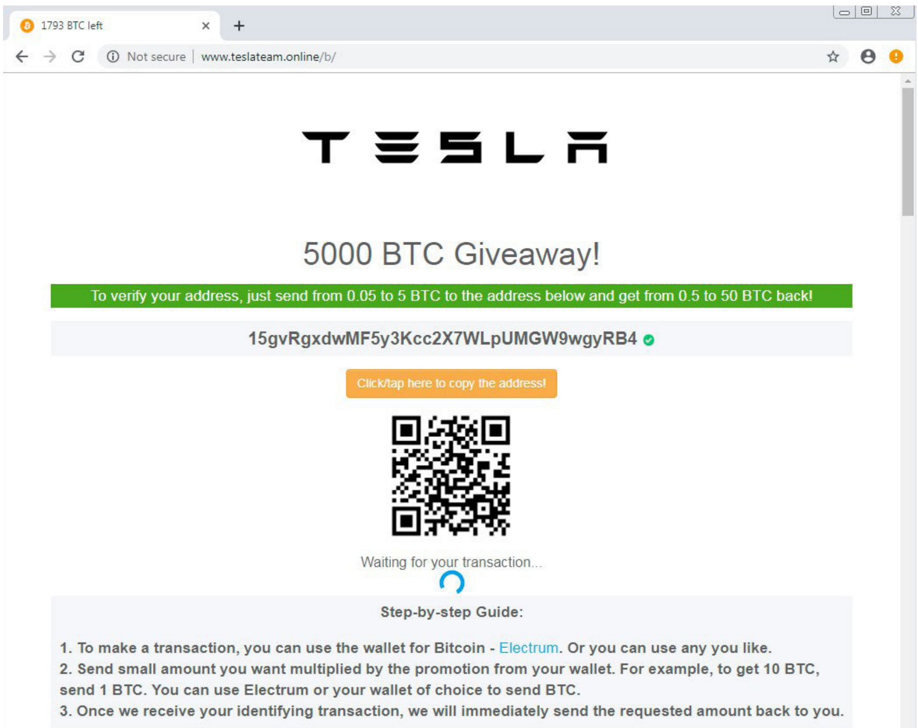
۱ Scam



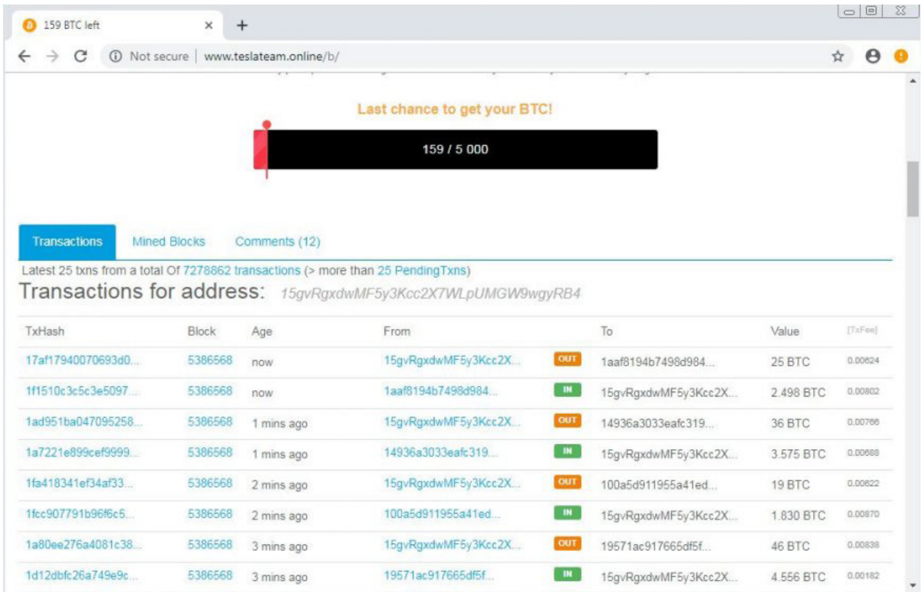
در صفحه مذکور دیدگاه‌هایی جعلی نیز درج شده تا شانس در دام افتادن کاربر افزایش پیدا کند.



در سایت جدید گفته می‌شود که در صورت ارسال ۰٫۰۵ تا ۵ بیت‌کوین یا اِتیریِم به شماره کیفی که در سایت به آن اشاره شده، به کاربر تا ۱۰ برابر مبلغ واریز شده پاداش اعطا خواهد شد.



بخشی از این صفحات به‌صورت در ظاهر زنده – اما دروغین – تبادلات صورت پذیرفته در شماره کیف ارز رمز مذکور را نشان می‌دهد. با این هدف که در ذهن کاربر شرکت گسترده مردم در این برنامه تداعی شود.


159 BTC left

Not secure | www.teslateam.online/b/

Last chance to get your BTC!

159 / 5 000

Transactions | Mined Blocks | Comments (12)

Latest 25 txns from a total Of 7278862 transactions (> more than 25 PendingTxns)

Transactions for address: 15gvRgxdwMF5y3Kcc2X7WLpUMGW9wgyRB4

TxHash	Block	Age	From		To	Value	[TxFee]
17af17940070693d0...	5386568	now	15gvRgxdwMF5y3Kcc2X...	OUT	1aaf8194b7498d984...	25 BTC	0.00624
1f1510c3c5c3e5097...	5386568	now	1aaf8194b7498d984...	IN	15gvRgxdwMF5y3Kcc2X...	2.498 BTC	0.00802
1ad951ba047095258...	5386568	1 mins ago	15gvRgxdwMF5y3Kcc2X...	OUT	14936a3033eafc319...	36 BTC	0.00766
1a7221e899cef9999...	5386568	1 mins ago	14936a3033eafc319...	IN	15gvRgxdwMF5y3Kcc2X...	3.575 BTC	0.00688
1fa418341ef34af33...	5386568	2 mins ago	15gvRgxdwMF5y3Kcc2X...	OUT	100a5d911955a41ed...	19 BTC	0.00622
1fcc907791b96f6c5...	5386568	2 mins ago	100a5d911955a41ed...	IN	15gvRgxdwMF5y3Kcc2X...	1.830 BTC	0.00870
1a80ee276a4081c38...	5386568	3 mins ago	15gvRgxdwMF5y3Kcc2X...	OUT	19571ac917665df5f...	46 BTC	0.00838
1d12dbfc26a749e9c...	5386568	3 mins ago	19571ac917665df5f...	IN	15gvRgxdwMF5y3Kcc2X...	4.556 BTC	0.00182

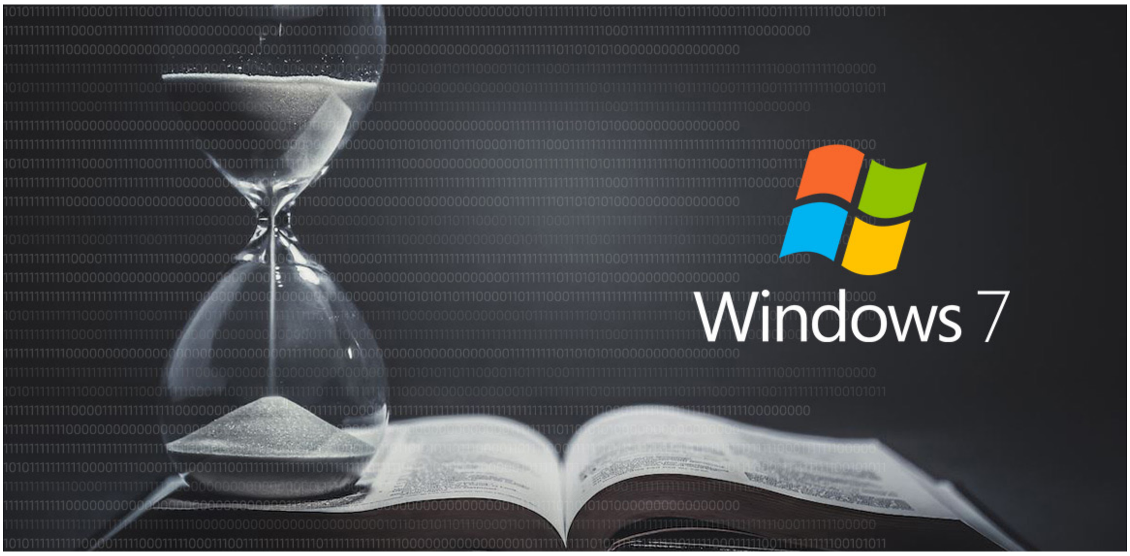
متأسفانه بررسی تبادلات واقعی انجام شده در شماره کیف‌های بکار گرفته شده در این حملات از قربانی شدن برخی کاربران حکایت دارد.

با توجه به افزایش ارزش ارز رمزها، انتظار می‌رود که روند این کلاهبرداری‌ها نیز سیری صعودی به خود بگیرد.

در اتاق خبر شبکه گستر بخوانید...

رویـدادهـای امنـیـتی

Windows 7؛
سیستم عاملی در شرف بازنشستگی



بر طبق اعلام مایکروسافت این شرکت پشتیبانی از سیستم عامل Windows 7 را کمتر از شش ماه دیگر پایان خواهد داد و از ۲۵ دی به بعد، هیچ اصلاحیه امنیتی و پشتیبانی فنی برای این محصول ارائه نخواهد شد. بدین ترتیب Windows 7 پس از حدود ۱۰ سال بازنشسته خواهد شد.

البته مایکروسافت حاضر است بعد از پایان تاریخ مذکور به مدت سه سال خدمات پشتیبانی پولی برای نگارش‌های Pro و Enterprise این نسخه از Windows ارائه دهد. ولی برای اینکه حتی مؤسسات بزرگ هم به فکر استفاده از این روش نباشند و ترجیح دهند که سیستم عامل قدیمی خود را ارتقاء دهند، این شرکت قیمت‌های قابل توجهی را برای این خدمات در نظر گرفته است. بطور مثال، برای دریافت خدمات پشتیبانی ویژه به ۵ هزار کامپیوتر با سیستم عامل Windows 7 Pro باید یک میلیون دلار به مایکروسافت پرداخت کرد.

Windows 7 یکی از موفق‌ترین و صدالبته از پرطرفدارترین سیستم‌های عامل مایکروسافت بوده است. به‌نحوی که همچنان بیش از ۳۸ درصد از بازار سیستم‌های عامل را به خود اختصاص داده است.

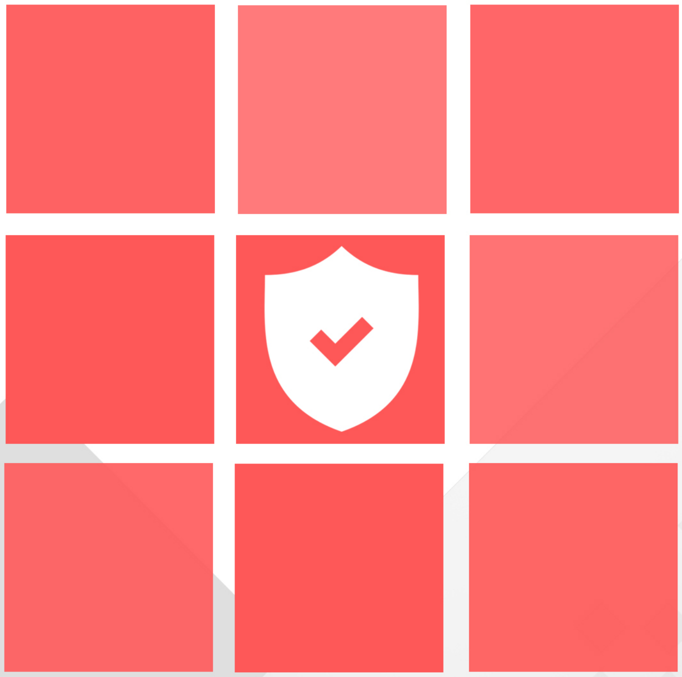
با توجه به اینکه بسیاری از بخش‌ها و قابلیت‌های Windows در نسخه‌های مختلف آن یکسان هستند، با کشف یک نقطه ضعف در یکی از نسخه‌های این سیستم عامل، این احتمال وجود دارد که نسخه‌های دیگر نیز نسبت به آن نقطه ضعف آسیب‌پذیر باشند. از بهمن ماه سال جاری، یک چنین نقاط ضعف مشترک در Windows، در نسخه‌های جدید توسط اصلاحیه‌های امنیتی ماهانه مایکروسافت ترمیم خواهند شد ولی اصلاحیه‌ای برای Windows 7 ارائه نخواهد گردید. نفوذگران می‌توانند با مهندسی معکوس بر روی اصلاحیه‌های مایکروسافت، متوجه شوند که نقطه ضعف در چه بخش از سیستم عامل Windows است و به چه نحوی اصلاح و ترمیم شده است. با داشتن این اطلاعات، مهاجمان قادر خواهند بود که نقطه ضعف را در Windows 7 هم شناسایی کرده و راه سوءاستفاده از آن را به دست آورند.

باید توجه داشت که علاوه بر قطع عرضه اصلاحیه‌های امنیتی مایکروسافت برای این نسخه از Windows، بسیاری از شرکت‌های نرم‌افزاری دیگر هم به تدریج پشتیبانی از Windows 7 را متوقف خواهند کرد.

پشتیبانی از Windows 7 توسط شرکت‌های مک‌آفی و بیت‌دیفندر پس از ۲۵ دی ماه تا تاریخی که متعاقبا اعلام خواهد شد ادامه خواهد یافت. با این توضیح که این ادامه پشتیبانی منوط به مختل نشدن قابلیت‌های بکار گرفته شده در نسخه‌های جدید محصولات این دو شرکت در نتیجه عدم به‌روزرسانی Windows ۷ خواهد بود.

به تمامی راهبران شبکه توصیه می‌شود که در فرصت باقی مانده اقدام به ارتقای دستگاه‌های با Windows ۷ خود به نسخه‌های جدیدتر و قابل پشتیبانی کنند.

آسیب‌پذیری‌ها
و اصلاحیه‌های امنیتی



اصـلاحیه‌های امـنیتی مایکروسـافت
بـرای مـاه مـیلادی ژوئـیـه

سه‌شنبه ۱۸ تیر، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی ژوئیه منتشر کرد. این اصلاحیه‌ها در مجموع، ۷۷ آسیب‌پذیری را در سیستم عامل Windows و برخی دیگر از محصولات مایکروسافت ترمیم می‌کنند. درجه اهمیت ۱۵ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی"[1] و ۶۲ مورد از آنها "بااهمیت"[2] 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 اهمیت 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 اهمیت "بااهمیت" برطرف و ترمیم می‌گردند.

از ۱۵ آسـیب‌پذیری حـیـاتی این ماه، ۱۱ مورد آنها مـرتبط با بخش Scripting Engine مـرورگرهای[3] شرکت مایکروسـافت هستند. چهار مـورد دیگر نیز هر کـدام یکی از محصـولات DHCP Server، GDI+، Dot Net Framework و Azure DevOps Server/Team Foundation Server را تحت تأثیر قرار می‌دهند.

دو مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های ماه ژوئـیـه، از قبل از این توسـط مهاجمان مورد بـهره‌جویی مهاجمان قرار گرفته است. هر دوی این ضـعف‌های امـنیتی – با شناسـه‌های CVE-2019-1132 و CVE-2019-0880 – مهاجـم را قادر به ارتقای دسـترسی خود بر روی سـیستم قربانی می‌کنند. سوءاسـتفاده از آسـیب‌پذیری‌های مذکور مسـتلزم فراهـم بودن امکان دسترسی فیزیـکی مهاجم به سـیستم یا بهره‌جویی از آسـیب‌پذیری دیگر برای دسـترسی یافتن از راه دور به دسـتگاه قربانی است و به همین خاطر درجـه "بااهمیت" – و نه "حـیـاتی" – به آنها اختصـاص داده شده است. اما با توجه به مورد بـهره‌جـویی قرار گرفتن آنها نـصب اصلاحیه‌های مربوطه با اولـویت بالا توصـیه می‌شود.

جزییات پنج آسـیب‌پذیری نیز پیش‌تر به‌صورت عمومی منتشـر شده بود؛ گر چه خوشبختانه هیچ مورد بـهره‌جویی تا قبل از عرضه اصـلاحیه آنها در ۱۸ تیر گزارش نشده است. این آسـیب‌پذیری‌ها عبارتند از:

- CVE-2019-0865 – ضعفی که بهره‌جویی از آن موجب از کاراندازی سرویس[4] در بخش SymCrypt سیستم عامل می‌شود.

[1] Critical
[2] Important
[3] Browser
[4] Denial of Service

- CVE-2018-15664 – اشکالی از نوع ترفیع امتیازی[۱] که مهاجم با بهره‌جویی از آن در نسخه آسیب‌پذیر Docker قادر به ارتقای دسترسی خود خواهد بود.
- CVE-2019-0962 – ضعفی در Azure Automation که سوءاستفاده از آن مهاجم را قادر به ترفیع دسترسی خود بر روی سیستم آسیب‌پذیر می‌کند.
- CVE-2019-1068 – اشکالی در SQL Server که امکان اجرای کد بالقوه مخرب را به‌صورت از راه دور[۲] برای مهاجم فراهم می‌کند.
- CVE-2019-1129 – ضعفی در سیستم عامل Windows که به مهاجم امکان می‌دهد تا دسترسی خود را ارتقا دهد.

درجه همه موارد مذکور "بااهیمت" گزارش شده است.

جزییات بیشتر در خصوص اصلاحیه‌های امنیتی عرضه شده مایکروسافت در ماه میلادی ژوئیه در اتاق خبر شرکت مهندسی شبکه گستر قابل دریافت و مطالعه است.

۱ Elevation of Privilege
۲ Remote Code Execution

اصلاحیه‌های امنیتی ادوبی
برای ماه میلادی ژوئیه

سه‌شنبه ۱۸ تیر، شرکت ادوبی مجموعه اصلاحیه‌های امنیتی ماه میلادی ژوئیه خود را منتشر کرد.

اصلاحیه‌های مذکور، در مجموع، ۵ ضعف امنیتی را در محصولات زیر ترمیم می‌کنند:

- Bridge CC
- Experience Manager
- Dreamweaver

درجه اهمیت چهار مورد از این آسیب‌پذیری‌ها "بااهمیت" و یک مورد از آنها "متوسط"[۱] اعلام شده است.

بر خلاف معمول، این ماه هیچ اصلاحیه‌ای برای محصول پراستفاده Flash Player ارائه نشده است.

اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه ژوئیه ادوبی در لینک‌های زیر قابل مطالعه است:

- https://helpx.adobe.com/security/products/bridge/apsb19-37.html
- https://helpx.adobe.com/security/products/experience-manager/apsb19-38.html
- https://helpx.adobe.com/security/products/dreamweaver/apsb19-40.html

۱ Moderate

اصلاحیه‌های عرضه شده

در تیر ۱۳۹۸

در تیر ماه، علاوه بر شرکت‌های مایکروسافت و ادوبی، شرکت‌های سیسکو، گوگل، وی‌اِم‌وِر، موزیلا، جونیپر نت‌ورکز، اوراکل و اپل و بنیاد دروپل اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

در این ماه، سیسکو در چندین نوبت اقدام به انتشار به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ٤٤ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت چهار مورد از این آسیب‌پذیری‌ها "حیاتی" و ۲۰ مورد از آنها "بالا"[۱] گزارش شده است. مهاجم با بهره‌جویی از برخی از آسیب‌پذیری‌های مذکور، قادر به در اختیار گرفتن کنترل سیستم خواهد بود. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در اینجا قابل دسترس است.

در هفته سوم تیر ماه، شرکت موزیلا، با ارائه به‌روزرسانی، چندین آسیب‌پذیری را در مرورگر Firefox و نرم‌افزار مدیریت ایمیل Thunderbird برطرف کرد. سوءاستفاده از برخی از ضعف‌های مذکور به مهاجم امکان می‌دهد تا به‌صورت از راه دور اقدام به اجرای کد مخرب بر روی دستگاه آسیب‌پذیر کند. جزییات بیشتر در اینجا، اینجا و اینجا قابل مطالعه است.

شرکت گوگل نیز با عرضه نسخه ۷۵/۰/۳۷۷۰/۱٤۲ مرورگر Chrome دو آسیب‌پذیری امنیتی را در این مرورگر ترمیم کرده که جزییات آنها در اینجا قابل دریافت است.

وی‌اِم‌وِر دیگر شرکتی بود که در تیر ماه ۱۳۹۸ اقدام به انتشار به‌روزرسانی برای ترمیم دو آسیب‌پذیری امنیتی در محصولات خود کرد. سوءاستفاده از این ضعف‌های امنیتی موجب از کاراندازی سرویس‌دهی محصول آسیب‌پذیر می‌شود. توضیحات کامل در این خصوص در اینجا قابل مطالعه است.

۲٦ تیر ماه نیز، بنیاد دروپل، یک ضعف امنیتی را در نرم‌افزار مدیریت محتوای Drupal ترمیم و اصلاح کرد. بهره‌جویی از ضعف مذکور، مهاجم را قادر به عبور از سد تنظیمات کنترلی این محصول می‌کند. توضیحات بیشتر در اینجا قابل مطالعه است.

[۱] High

در آخرین روز تیر ماه، شرکت اپل نیز با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در محصولات و سیستم‌های عامل زیر ترمیم و اصلاح کرد:

- iOS
- tvOS
- Safari
- macOS
- watchOS

سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. توضیحات بیشتر در خصوص به‌روزرسانی‌های منتشر شده در لینک‌های زیر قابل دریافت است:

- https://support.apple.com/en-us/HT210346
- https://support.apple.com/en-us/HT210351
- https://support.apple.com/en-us/HT210355
- https://support.apple.com/en-us/HT210348
- https://support.apple.com/en-us/HT210353

همچنین بتازگی شرکت نت‌فلیکس از شناسایی سه آسیب‌پذیری امنیتی در پودمان TCP در هسته‌های FreeBSD و Linux خبر داده است. آسیب‌پذیری‌های مذکور از نحوه مدیریت Selective Acknowledgement در پودمان TCP و قابلیت MSS آن ناشی می‌شود. در میان این سه آسیب‌پذیری، ضعف موسوم به TCP SACK Panic با شناسه CVE-2019-11477 با درجه Important بالاترین سطح حساسیت را به خود اختصاص داده است. مهاجم با بهره‌جویی از TCP SACK Panic قادر به از کاراندازی سیستم به‌صورت از راه دور خواهد بود. درجه اهمیت دو ضعف دیگر – با شناسه‌های CVE-2019-11478 و CVE-2019-11479 –، "متوسط" گزارش شده است. در پی اعلام نت‌فلیکس در خصوص شناسایی این آسیب‌پذیری‌ها، شرکت امنیتی سوفوس نیز بلافاصله محصولات خود را از لحاظ تأثیر پذیرفتن از این اشکالت مورد بررسی قرار داده که نتایج آن در اینجا قابل دریافت است.

و در آخر اینکه مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) در اطلاعیه‌ای نسبت به خطر عدم ترمیم یک آسیب‌پذیری "حیاتی" با شناسه CVE-2019-9670 در Zimbra که به گفته این مرکز یکی از سرویس‌دهنده‌های ایمیل پرکاربرد در کشور تلقی می‌شود هشدار داده است. مشروح اطلاعیه ماهر در اینجا قابل مطالعه است.

از رسانه‌های دیگر

مـرکـز مـاهـر
و دو هشـدار امـنیتـی

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) در مطلبی که مشروح آن در اینجا قابل دریافت است به بررسی یک برنامک جعلی با عنوان Updates for Samsung پرداخته است. این برنامک برای مدتی بر روی انباره رسمی شرکت گوگل (Play Store) به اشتراک گذاشته شده بود.

برنامک مذکور با عملکردی مخرب هیچ گونه ارتباطی با شرکت سامسونگ ندارد.

به گفته ماهر این برنامک ۱۰ میلیون دستگاه با سیستم عامل Android را به خود آلوده کرده که از این تعداد ۳۰ هـزار مورد آن متعلق به کاربران ایرانی است.

همچنین این مرکـز در مطلبی دیگر نسـبت به شـدت گرفتن سوءاسـتفاده مهاجمان از آسـیب‌پـذیری پودمـان CLDAP (درگـاه UDP/۳۸۹) جهت اجـرای حملات DDoS از نوع بـازتـابی/تـقـویتـی[۱] در ایران هشـدار داده است.

به گفته ماهر این موضوع در گزارش‌های واصله مراکز CERT سایر کشـورها نیز مشاهده شده است.

این مـرکـز، مسدودسازی دسـترسی اینترنتی به سـرویس‌های LDAP و CLDAP را توصیه کرده است.

ماهـر تصـریح کرده که ضعف امـنیتـی مذکور در کشـور، در سـرویس‌دهنده‌های Active Directory سـیستم عامـل Windows رواج بیشتری دارد.

[۱] Amplification/Reflection

گزارش‌ها

مجموعه گزارش‌های پلیدهای ابدی؛
بررسی بدافزارهای مخرب قدیمی اما همچنان ماندگار

شرکت مهندسی شبکه گستر در حال انتشار مجموعه گزارش‌هایی تحت عنوان "پلیدهای ابدی" است که در هر یک از آنها یکی از بدافزارهای مخرب قدیمی اما همچنان ماندگار مورد بررسی قرار گرفته است.

در اولین شماره از این مجموعه گزارش‌ها به تحلیل بدافزار Conficker پرداخته شده است.

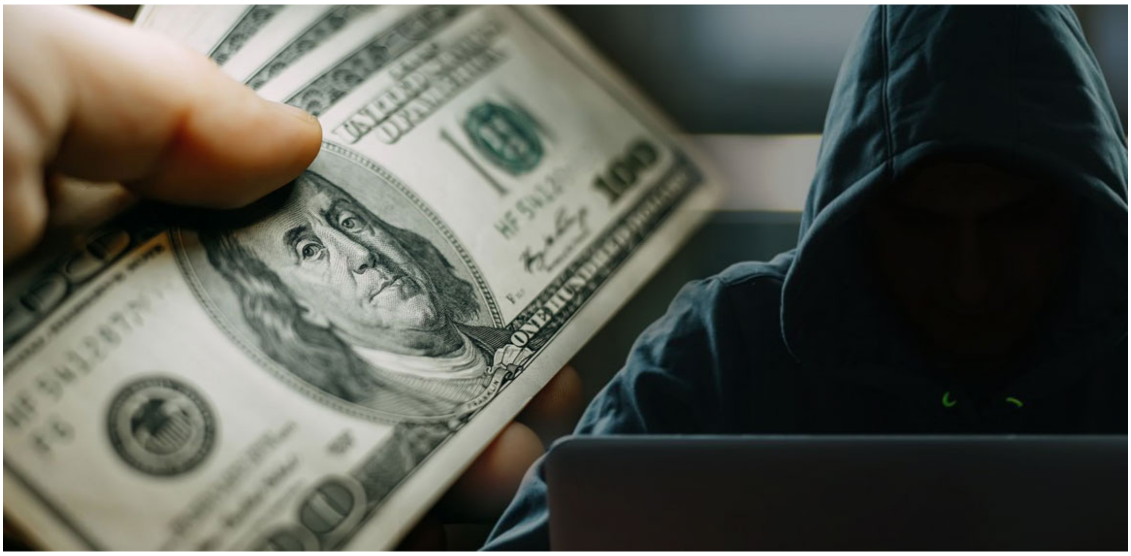
نخستین نسخه از بدافزار Conficker در آبان ۱۳۸۷ شناسایی شد. این بدافزار با روش‌های متعدد از جمله سوءاستفاده از یک آسیب‌پذیری امنیتی، در مدتی بسیار کوتاه موفق به تسخیر میلیون‌ها دستگاه در بیش از ۱۹۰ کشور جهان شد.

نکته قابل توجه اینکه علیرغم گذشت حدود ۱۲ سال از عرضه اصلاحیه امنیتی آسیب‌پذیری مورد بهره‌جویی این بدافزار و غیرفعال شدن مکانیزم به‌روزرسانی آن، Conficker همچنان در حال جولان دادن در شبکه بسیاری از سازمان‌ها در کشورهای مختلف از جمله ایران است.

در این گزارش ضمن بررسی و تحلیل عملکرد Conficker به راه‌های مقابله با این بدافزار و پاکسازی آن پرداخته شده است.

برای دریافت این گزارش بر روی تصویر زیر کلیک شود.

افزایش دو برابری
میانگین مبلغ اخاذی شده توسط باج‌افزارها

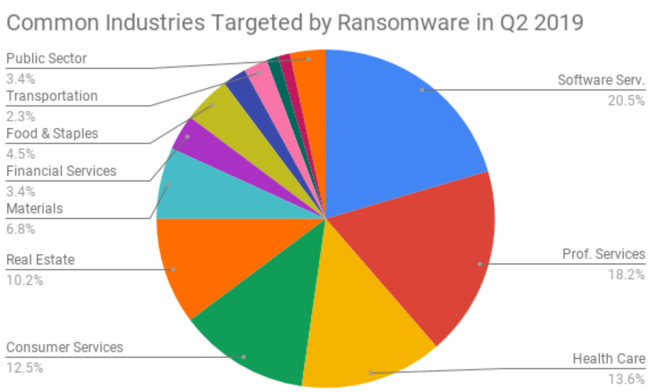


بر اساس گزارشی که شرکت کوور آن را منتشر کرده است میانگین مبلغ اخاذی شده در جریان حملات باج‌افزاری در سه‌ماهه دوم سال میلادی جاری با افزایشی ۱۸٤ درصدی در مقایسه با سه‌ماهه قبل از آن به بیش از ۳٦ هزار دلار رسیده است.

فعالیت گسترده دو باج‌افزار Ryuk و Sodinokibi و تمرکز نویسندگان آنها بر روی سازمان‌های بزرگ از اصلی‌ترین دلایل این افزایش اعلام شده است.

میانگین زمان اکار[۱] در نتیجه آلوده شدن سیستم‌ها به باج‌افزار نیز از ۷/۳ روز در سه‌ماهه اول ۲۰۱۹ به ۹/٦ روز در سه‌ماهه دوم سال میلادی جاری رسیده است.

در این دوره مهاجمان موفق به اخاذی صدها هزار دلار از ادارات عمومی آمریکا شده‌اند. به نحوی که میانگین مبلغ پرداخت شده از سوی این قربانیان حدود ۳٤۰ هزار دلار گزارش شده است. این در حالی است که ادارات عمومی آمریکا تنها ۳/٤ درصد از قربانیان باج‌افزار را در سه‌ماهه دوم ۲۰۱۹ تشکیل داده‌اند.

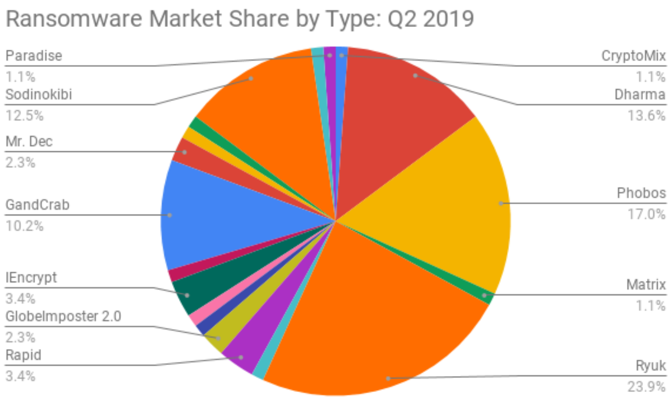


۱ Downtime

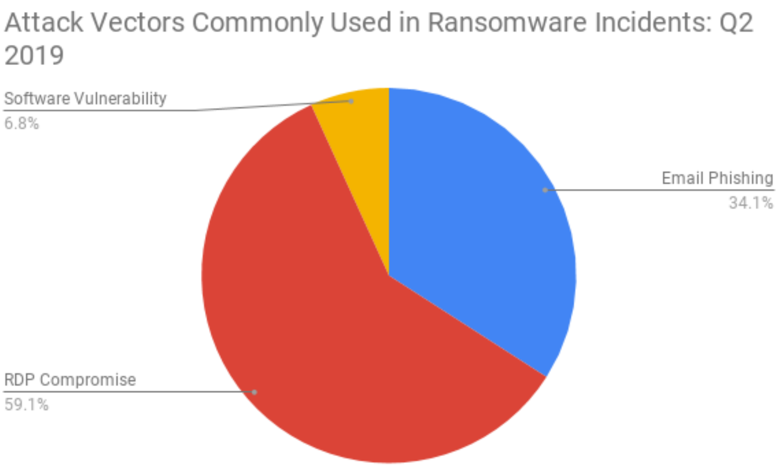
نکته نگران کننده، پرداخت باج، توسط ۹۶ درصد سازمان‌هایی است که سیستم یا سیستم‌های آنها به باج‌افزار آلوده شده است. موضوعی که بی‌شک سبب افزایش علاقه تبهکاران سایبری در ادامه اجرای این اقدامات مخرب می‌گردد.

علاوه بر آنکه تضمینی برای ارائه شدن ابزار رمزگشایی در ازای دریافت مبلغ اخاذی نیست، متأسفانه کم نیستند مواردی که ابزار ارائه شده قادر به بازگردانی صحیح کلیه فایل‌های رمزگذاری شده نبوده است.

همچنین بر طبق گزارش، Ryuk بیشتری سهم از آلودگی سازمان‌ها به باج‌افزار را به خود اختصاص داده است. Phobos و Dharma که ایران نیز همواره در فهرست اهداف آنها بوده است در جایگاه‌های دوم و سوم قرار گرفته‌اند.



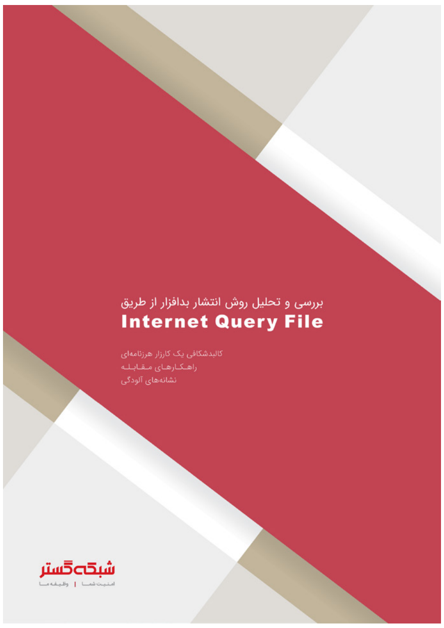
اتصال از راه دور مهاجمان از طریق پودمان Remote Desktop – به اختصار RDP – به دستگاه‌های با رمز عبور ضعیف و اجرای فایل مخرب باج‌افزار اصلی‌ترین روش انتشار باج‌افزارها در دوره مذکور بوده است.



لذا، همچون همیشه بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها و مقاوم سازی پودمان RDP برای ایمن ماندن از گزند باج‌افزارها توصیه می‌شود.

مشروح گزارش کوور در اینجا قابل دریافت و مطالعه است.

در اتاق خبر
شبکه گستر بخوانید...



شبکه‌گستر

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

CSQ

ISO 9001:2008

Cert No 9150.C528

شرکت مهندسی شبکه گستر

تهران ١٩٦٨٦، خیابان شهید دستگردی (ظفر)، شماره ٢٧٣

تلفن / دورنگار	٠٢١-٤٢٠٥٢
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