ماهنامه

امنیت فناوری اطلاعات

مهر 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 مهر ماه ۱۳۹۸ پرداخته شده است.

در مهر ماه محققان موفق به ساخت ابزاری شدند که امکان رمزگشایی ۱۴۸ گونه از باج‌افزار مخرب STOP را فراهم می‌کند. بر اساس گزارشی که در شهریور ماه سایت BleepingComputer آن را منتشر کرد، STOP، فعال‌ترین باج‌افزار سال میلادی جاری بوده است. مهاجمان این باج‌افزار به کرات سیستم کاربران و سازمان‌های ایرانی را هدف حملات خود قرار داده‌اند. بی‌شک انتشار ابزار رمزگشایی جدید دستاورد بزرگی برای جامعه امنیت فناوی اطلاعات در مقابله با تهبکاران و باج‌گیران سایبری است. در این ماهنامه، ضمن بررسی ابزار رمزگشایی STOP به چند ابزار و راهکار رمزگشایی باج‌افزارهای دیگر پرداخته شده است.

ذکر این نکته ضروری است که علیرغم ناکامی برخی گردانندگان این بدافزارهای مخرب، باج‌گیران سایبری همچنان در حال جولان دادن و به گروگان گرفتن فایل‌های ذخیره شده بر روی سیستم‌های کاربران و سازمان‌های ایرانی هستند. برای مثال در هفته‌های اخیر گزارش‌های متعددی در خصوص مشاهده آلودگی بر روی سیستم برخی کاربران ایرانی به نسخه‌های جدید باج‌افزار Phobos به شرکت مهندسی شبکه گستر واصل شده است. Phobos که نخستین نسخه آن در اواخر سال ۱۳۹۷ شناسایی شد، همچنان سهم قابل‌توجهی از آلودگی‌ها را به خود اختصاص داده است. لذا همچون همیشه بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها و مقاوم‌سازی پودمان RDP برای ایمن ماندن از گزند این بدافزارهای مخرب توصیه می‌شود.

همچنین در اوایل هفتمین ماه ۱۳۹۸، عرضه دو اصلاحیه امنیتی توسط مایکروسافت خارج از برنامه زمانبندی معمول خود (سه‌شنبه دوم هر ماه میلادی) خبرساز شد. یکی از این اصلاحیه‌ها یک آسیب‌پذیری به تهدیدات اجرای کد به‌صورت از راه دور (Remote Code Execution) را در مرورگر Internet Explorer ترمیم می‌کند. این آسیب‌پذیری با شناسه CVE-2019-1367 و با درجه اهمیت "حیاتی" (Critical) که توسط یکی از محققان گوگل شناسایی شده و مواردی از بهره‌جویی از آن نیز توسط حداقل یک گروه از هکرها گزارش شده است، مهاجم را قادر به در اختیار گرفتن کنترل سیستم و اجرای کد به‌صورت از راه دور بر روی آن می‌کند. همانطور که در این ماهنامه به تفصیل به آن پرداخته شده نصب اصلاحیه مذکور در اسرع وقت بر روی کلیه سیستم‌ها توصیه می‌شود. در مهر ماه علاوه بر مایکروسافت، شرکت‌های ادوبی، اپل، سیسکو، جونیپر نت‌ورکز، گوگل و اوراکل و بنیاد وردپرس اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند که جزییات آنها در این ماهنامه قابل مطالعه 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 تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشـدارهـای امنـیـتی

کاربران و سازمان‌های ایرانی
هدف باج‌افزار مخرب Phobos

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

Phobos که نخستین نسخه آن در اواخر سال ۱۳۹۷ شناسایی شد، همچنان سهم قابل‌توجهی از آلودگی‌ها را به خود اختصاص داده است.

کدنویسی و عملکرد Phobos از جهات بسیاری مشابه باج‌افزار معروف Dharma - که با نام CrySis نیز شناخته می‌شود - 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 ناقل فایل / لینک مخرب یا با بهره‌جویی (Exploiting) از آسیب‌پذیری‌های امنیتی منتشر شده‌اند.

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

Phobos برای ماندگاری طولانی‌تر، علاوه بر نگهداری نسخه‌ای از خود در پوشه Startup اقدام به ایجاد کلیدهایی نیز در محضرخانه (Registry) سیستم عامل می‌کند.

پیش از آغاز رمزگذاری، باج‌افزار، پروسه‌های زیر را متوقف می‌کند:

msftesql.exe, sqlagent.exe, sqlbrowser.exe, sqlservr.exe, sqlwriter.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, agntsvc.exe, mydesktopqos.exe, isqlplussvc.exe, xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe, agntsvc.exe, agntsvc.exe, agntsvc.exe, encsvc.exe, firefoxconfig.exe, tbirdconfig.exe, ocomm.exe, mysqld.exe, mysqld-nt.exe, mysqld-opt.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, steam.exe, thebat.exe, thebat64.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe

هدف از انجام این کار فراهم شدن امکان رمزگذاری فایل‌های مورد استفاده این پروسه‌هاست.
به گزارش شرکت مهندسی شبکه گستر، Phobos به فایل‌های رمزگذاری شده، پسوندی با قالب زیر الصاق می‌کند:

id[random numbers].[email].extension

در قالب مذکور، قسمت extension یکی از کلمات زیر می‌تواند باشد:

acute, actin, Acton, actor, Acuff, Acuna, acute, adage, Adair, Adame, banhu, banjo, Banks, Banta, Barak, Caleb, Cales, Caley, calix, Calle, Calum, Calvo, deuce, Dever, devil, Devoe, Devon, Devos, dewar, eight, eject, eking, Elbie, elbow, elderphobos, help, blend, bqux, com, mamba, KARLOS, DDoS, phoenix, PLUT, karma, bbc, CAPITAL

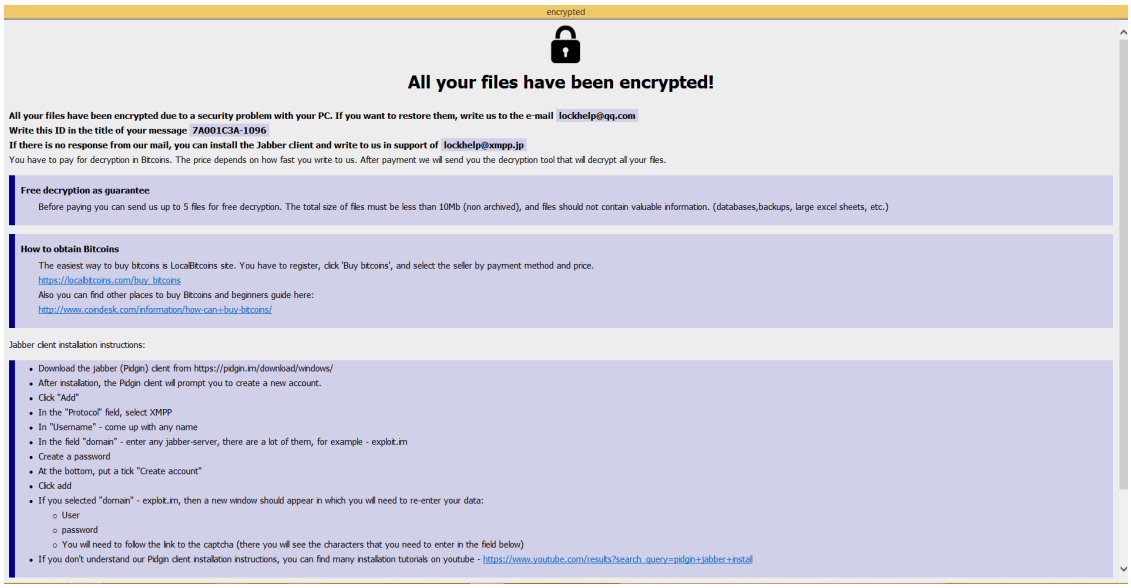
برای مثال، در یکی از جدیدترین نمونه‌های این باج‌افزار در ایران، عبارت زیر به هر فایل رمزگذاری شده چسبانده می‌شود:

id[5ED##A##-####].[eccentric_inventor@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	barcelona_100@aol.com
barcelona_100@aol.com	beltoro905073@aol.com	Cadillac.407@aol.com
datadecryption@countermail.com	decryptyourdata@qq	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
meachemvasili@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		

اطلاعیه باج‌گیری (Ransom Note) در قالب دو فایل - با پسوند txt و hta - به کاربر ارائه می‌شود؛ فایل با پسوند hta پس از اتمام فرایند رمزگذاری در قالب یک پنجره بالاپر (Popup) که نمونه‌ای از آن در تصویر زیر قابل مشاهده است ظاهر می‌گردد.



Phobos فایل‌های با هر یک از پسوندهای زیر را بر روی کلیه درایوهای محلی و شبکه‌ای (Mapped) و حافظه‌های جداشدنی متصل به دستگاه مورد دست‌درازی قرار می‌دهد:

sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pk-.pass, .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

این باج‌افزار ضمن صرف‌نظر کردن از رمزگذاری کلیه فایل‌های ذخیره شده در پوشه Windows و زیرپوشه‌های آن از دست‌درازی به فایل‌های با هر یک از پسوندهای زیر خودداری می‌کند:

1cd, 3ds, 3fr, 3g2, 3gp, 7z, accda, accdb, accdc, accde, accdt, accdw, adb, adp, ai, ai3, ai4, ai5, ai6, ai7, ai8, anim, arw, as, asa, asc, ascx, asm, asmx, asp, aspx, asr, asx, avi, avs, backup, bak, bay, bd, bin, bmp, bz2, c, cdr, cer, cf, cfc, cfm, cfml, cfu, chm, cin, class, clx, config, cpp, cr2, crt, crw, cs, css, csv, cub, dae, dat, db, dbf, dbx, dc3, dcm, dcr, der, dib, dic, dif, divx, djvu, dng, doc, docm, docx, dot, dotm, dotx, dpx, dqy, dsn, dt, dtd, dwg, dwt, dx, dxf, edml, efd, elf, emf, emz, epf, eps, epsf, epsp, erf, exr, f4v, fido, flm, flv, frm, fxg, geo, gif, grs, gz, h, hdr, hpp, hta, htc, htm, html, icb, ics, iff, inc, indd, ini, iqy, j2c, j2k, java, jp2, jpc, jpe, jpeg, jpf, jpg, jpx, js, jsf, json, jsp, kdc, kmz, kwm, lasso, lbi, lgf, lgp, log, m1v, m4a, m4v, max, md, mda, mdb, mde, mdf, mdw, mef, mft, mfw, mht, mhtml, mka, mkidx, mkv, mos, mov, mp3, mp4, mpeg, mpg, mpv, mrw, msg, mxl, myd, myi, nef, nrw, obj, odb, odc, odm, odp, ods, oft, one, onepkg, onetoc2, opt, oqy, orf, p12, p7b, p7c, pam, pbm, pct, pcx, pdd, pdf, pdp, pef, pem, pff, pfm, pfx, pgm, php, php3, php4, php5, phtml, pict, pl, pls, pm, png, pnm, pot, potm, potx, ppa, ppam, ppm, pps, ppsm, ppt, pptm, pptx, prn, ps, psb, psd, pst, ptx, pub, pwm, pxr, py, qt, r3d, raf, rar, raw, rdf, rgbe, rle, rqy, rss, rtf, rw2, rwl, safe, sct, sdpx, shtm, shtml, slk, sln, sql, sr2, srf, srw, ssi, st, stm, svg, svgz, swf, tab, tar, tbb, tbi, tbk, tdi, tga, thmx, tif, tiff, tld, torrent, tpl, txt, u3d, udl, uxdc, vb, vbs, vcs, vda, vdr, vdw, vdx, vrp, vsd, vss, vst, vsw, vsx, vtm, vtml, vtx , wb2, wav, wbm, wbmp, wim, wmf, wml, wmv, wpd, wps, x3f, xl, xla, xlam, xlk, xlm, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, xml, xps, xsd, xsf, xsl, xslt, xsn, xtp, xtp2, xyze, xz, zip

همچنین Phobos با اجرای فرامین زیر اقدام به حذف Shadow، غیرفعال کردن امکان راه‌اندازی سیستم در یکی از حالات موسوم به Recovery، حذف نسخه پشتیبان Catalog و متوقف نمودن دیواره آتش می‌کند:

vssadmin delete shadows /all /quiet

wmic shadowcopy delete

bcdedit /set {default} bootstatuspolicy ignoreallfailures

bcdedit /set {default} recoveryenabled no

wbadmin delete catalog -quiet

netsh advfirewall set currentprofile state off

netsh firewall set opmode mode=disable

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

توضیح اینکه نمونه بررسی شده در این خبر با نام‌های زیر شناسایی می‌شود:

Bitdefender:

-Trojan.Ransom.Phobos.F

McAfee :

-Ransom-Phobos!C9E480CC558A

Sophos:

-Troj/Phobos-B

اخباری خوش
در کنار هشداری همیشگی

بتازگی نویسنده HildaCrypt در اقدامی عجیب، خود کلیدهای رمزگشایی این باج‌افزار را منتشر کرده است. با استفاده از این کلیدها امکان بازگرداندن فایل‌های رمز شده توسط HildaCrypt به رایگان فراهم می‌شود. به نظر می‌رسد که هدف نویسنده HildaCrypt از این اقدام اثبات متفاوت بودن باج‌افزار خود از باج‌افزار معروف STOP بوده است. ماجرا از آنجا آغاز می‌شود که یکی از محققان امنیتی پس از کشف نمونه‌ای از HildaCrypt در حساب توییترش آن را نسخه‌ای جدید از STOP معرفی می‌کند.

در پاسخ به انتشار خبر مذکور، نویسنده HildaCrypt کلیدهای بکار گرفته شده توسط این باج‌افزار را در اختیار همه قرار می‌دهد. در نتیجه آن، ابزاری رایگان برای قربانیان HildaCrypt در اینجا در دسترس قرار گرفته است. ذکر این توضیح خالی از لطف نیست که خلق HildaCrypt توسط نویسنده آن طور که خودش می‌گوید بیشتر با نیت سرگرمی انجام شده بوده تا اخاذی!

دیگر خبر خوش باج‌افزاری، افشای کلیدهای رمزگشایی Muhstik توسط یکی از قربانیان آن است. حدود یک ماه است که نویسنده یا نویسندگان Muhstik با هک آن دسته از دستگاه‌های موسوم به ذخیره‌ساز متصل به شبکه (NAS) ساخت شرکت کیونپ که در بستر اینترنت به طریقی غیرامن در دسترس قرار گرفته‌اند، اقدام به رمزگذاری فایل‌های ذخیره شده بر روی آنها کرده و در ازای آنچه که بازگرداندن فایل‌ها به حالت اولیه می‌خوانند، مبلغ ۰/۰۹ بیت‌کوین (معادل حدود ۷۰۰ دلار) را اخاذی می‌کنند. اما یکی از قربانیان این باج‌افزار در اقدامی تلافی‌جویانه با هک سرور فرماندهی (C۲) باج‌افزار Muhstik موفق به دستیابی به حدود ۳ هزار کلید آن شده است. جالب اینجاست که این قربانی پیش از هک کردن سرورهای فرماندهی Muhstik خود مبلغ ٦٧٠ دلار را به گردانندگان این باج‌افزار پرداخت کرده بود!

```
hey guys,
good news for you all, bad news for me cause i paid already... maybe someone can
give me a tip for my hard work ^^
my wallet: 1JrwK1hpNXHVebByLD2te4E2KzxyMnvhb

i hacked back this criminal and get the whole database with keys, here it is:
https://pastebin.com/N8ahWBni

decryption software:
https://mega.nz/#!O9Jg3QYZ!5Gj8VrBXl4ebp_MaPDPE7JpzqdUaeUa5m9kL5fEmkVs

manual:
upload to nas:
"chmod +x decrypt"
"sudo ./decrypt YOURDECRYPTIONKEY"

and yeah, i know it was not legal from me too but he used already hacked servers
with several webshells on it... and im not the bad guy here :D

but its really sad, i lost 670 € to this criminal :'(

cheers
battleck aka tobias frömel
```

در پی افشای این کلیدها، چندین ابزار رمزگشای باج‌افزار Muhstik عرضه شدند که دو نمونه از آنها در اینجا و اینجا قابل دسترس است.

اخبار خوش برای قربانیان حملات باج‌گیران سایبری به همین جا ختم نمی‌شود. در روزهای اخیر محققان امنیتی موفق به ساخت ابزاری برای بازگرداند فایل‌های رمز شده توسط برخی از نسخه‌های باج‌افزار Nemty شدند. Nemty طی دو ماه گذشته سهم قابل‌توجهی از آلودگی‌ها به باج‌افزار را به خود اختصاص داده است. این باج‌افزار با استفاده از بسته بهره‌جوی RIG اقدام به رخنه به دستگاه‌های آسیب‌پذیر می‌کند. RIG از ضعف‌هایی همچون CVE-2018-15982 در نرم‌افزار Flash Player و CVE-2018-8174 در مرورگر Internet Explorer سوءاستفاده می‌کند.

اما در کنار این اخبار خوش در هفته‌های اخیر گزارش‌های متعددی در خصوص مشاهده آلودگی بر روی سیستم برخی کاربران و سازمان‌های ایرانی به نسخه جدید باج‌افزارهای مخربی همچون STOP، Phobos و Dharma به شرکت مهندسی شبکه گستر واصل شده است. لذا همچون همیشه بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها و مقاوم سازی پودمان RDP برای ایمن ماندن از گزند این بدافزارهای مخرب توصیه می‌شود.

خبری بسیار خوش برای
قربانیان باج‌افزار STOP

شرکت ام‌سی‌سافت با مشارکت یک محقق امنیتی موفق به ساخت ابزاری شده که امکان رمزگشایی ۱۴۸ گونه از باج‌افزار مخرب STOP را فراهم می‌کند.

گرچه پیش‌تر نیز ابزاری برای این منظور عرضه شده بود اما ابزار قبلی صرفا قادر به رمزگشایی فایل‌های آن دسته از سیستم‌های آلوده شده به STOP بود که در جریان دست‌درازی به فایل‌ها، از کلید رمزگذاری آفلاین (و نه آنلاین) استفاده می‌شد.

بر اساس گزارشی که در شهریور ماه سایت BleepingComputer آن را منتشر کرد، STOP، فعال‌ترین باج‌افزار سال میلادی جاری بوده است. مهاجمان این باج‌افزار به کرات سیستم کاربران و سازمان‌های ایرانی را هدف حملات خود قرار داده‌اند.

به گزارش شرکت مهندسی شبکه گستر، 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 را 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.

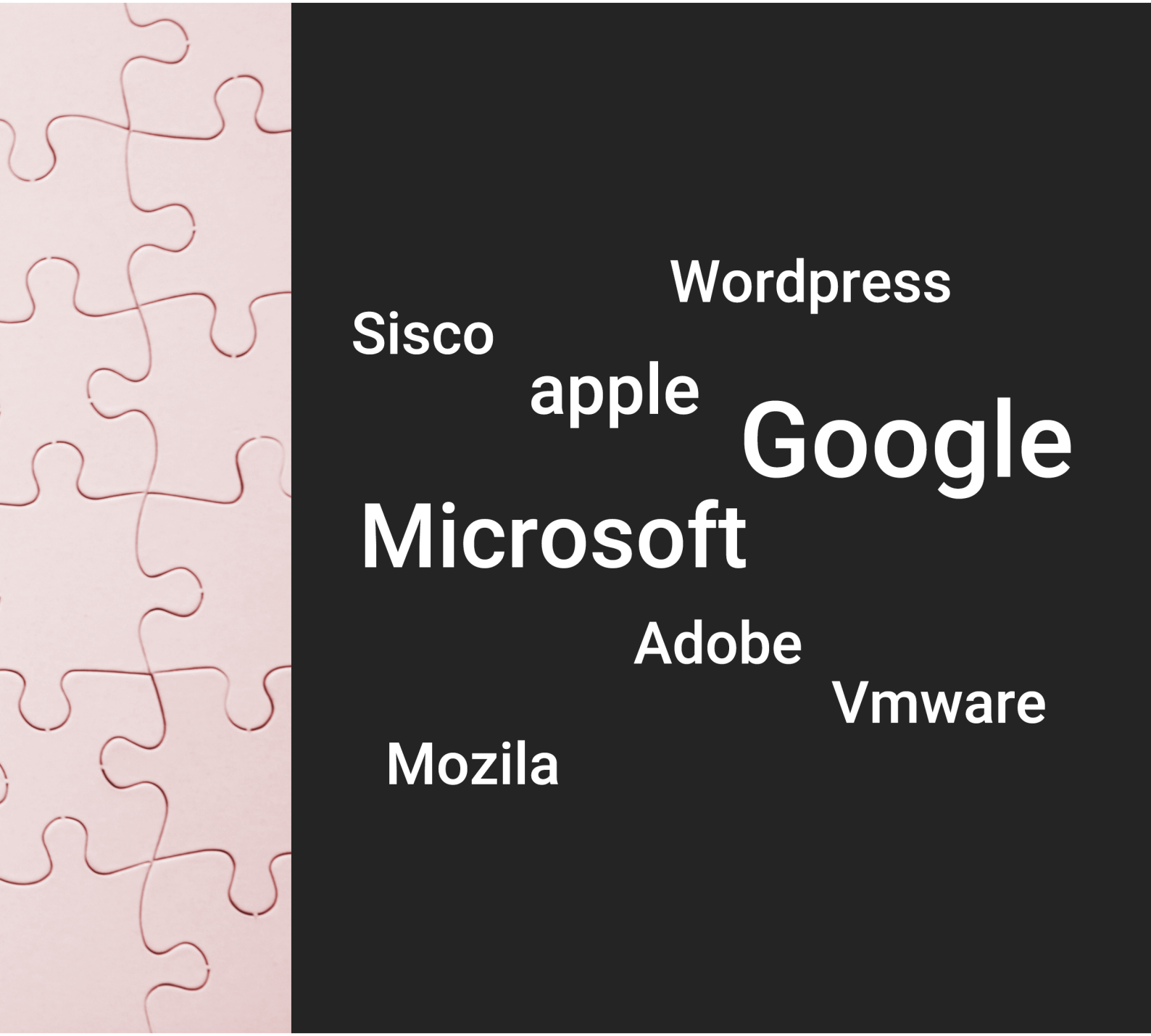
از جمله برنامه‌های مورد استفاده توسط نویسندگان STOP می‌توان به Crack نرم‌افزارهای KMSPico، Cubase، Photoshop و برنامه‌های ضدویروس اشاره کرد.

انتشار ابزار رمزگشایی جدید دستاورد بزرگی برای جامعه امنیت فناوی اطلاعات در مقابله با تهبکاران و باج‌گیران سایبری است.

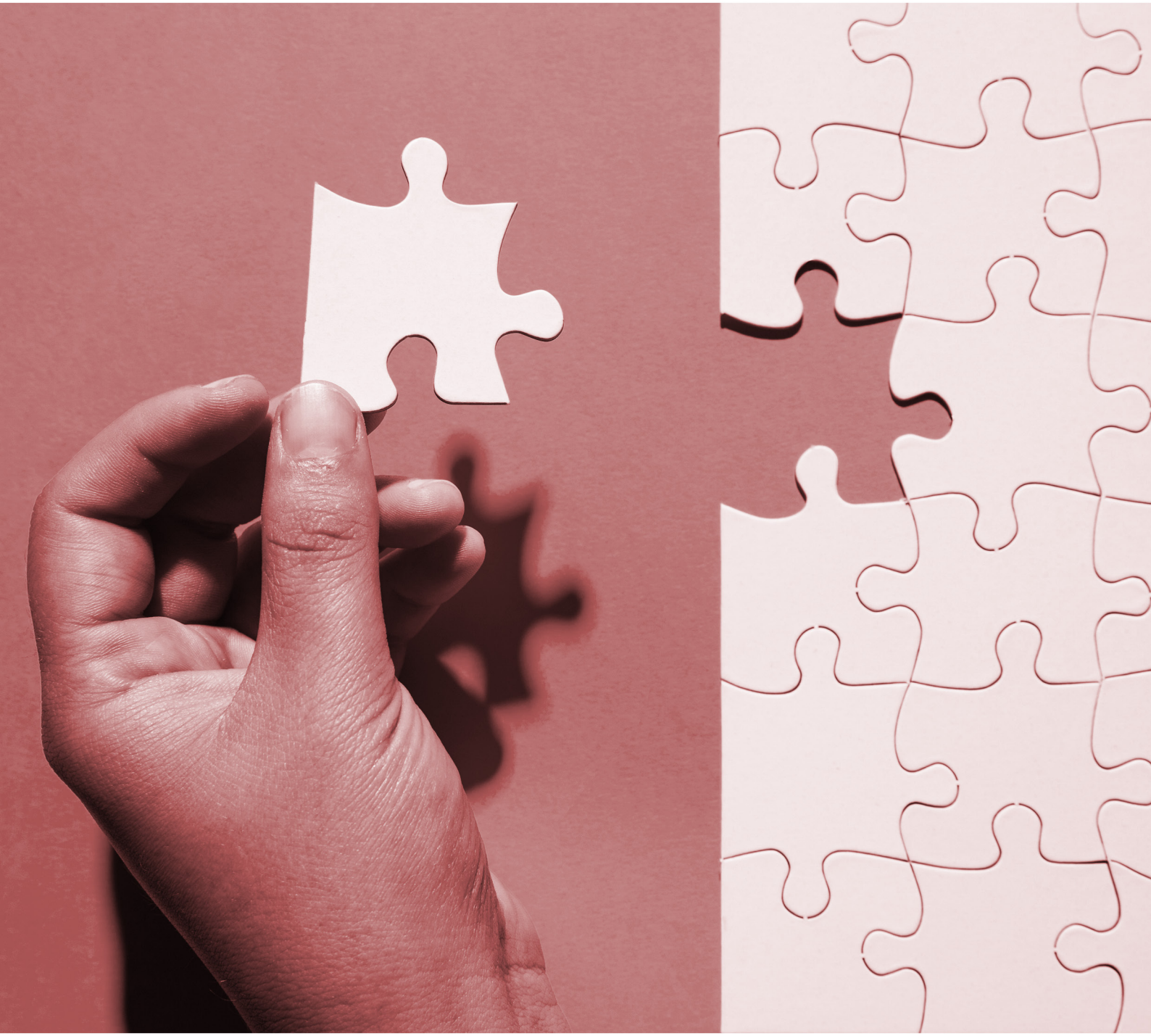
ابزار عرضه شده جدید که در اینجا قابل استفاده است از پسوندهای زیر پشتیبانی می‌کند:

.shadow, .djvu, .djvur, .djvuu, .udjvu, .uudjvu, .djvuq, .djvus, .djvur, .djvut, .pdff, .tro, .tfude, .tfudet, .tfudeq, .rumba, .adobe, .adobee, .blower, .promos, .promoz, .promorad, .promock, .promok, .promorad2, .kroput, .kroput1, .pulsar1, .kropun1, .charck, .klope, .kropun, .charcl, .doples, .luces, .luceq, .chech, .proden, .drume, .tronas, .trosak, .grovas, .grovat, .roland, .refols, .raldug, .etols, .guvara, .browec, .norvas, .moresa, .vorasto, .hrosas, .kiratos, .todarius, .hofos, .roldat, .dutan, .sarut, .fedasot, .berost, .forasom, .fordan, .codnat, .codnat1, .bufas, .dotmap, .radman, .ferosas, .rectot, .skymap, .mogera, .rezuc, .stone, .redmat, .lanset, .davda,

.poret, .pidom, .pidon, .heroset, .boston, .muslat, .gerosan, .vesad, .horon, .neras, .truke, .dalle, .lotep, .nusar, .litar, .besub, .cezor, .lokas, .godes, .budak, .vusad, .herad, .berosuce, .gehad, .gusau, .madek, .darus, .tocue, .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, .cetori, .stare, .carote


Wordpress
Sisco
apple
Google
Microsoft
Adobe
Vmware
Mozila

آسیب‌پذیری‌ها
و اصلاحیه‌های امنیتی



انتشار دو اصلاحیه اضطراری
توسط مایکروسافت

به گزارش شرکت مهندسی شبکه گستر، شرکت مایکروسافت دو اصلاحیه امنیتی را خارج از برنامه زمانبندی معمول خود (سه‌شنبه دوم هر ماه میلادی) عرضه کرده است. این اصلاحیه‌ها یک آسیب‌پذیری به تهدیدات اجرای کد به‌صورت از راه دور (Remote Code Execution) و یک ضعف امنیتی به حملات از کاراندازی سرویس (Denial of Service) را به‌ترتیب در Internet Explorer و Windows Defender ترمیم می‌کنند.

آسیب‌پذیری نخست با شناسه CVE-2019-1367 و با درجه اهمیت "حیاتی" (Critical) که توسط یکی از محققان گوگل شناسایی شده و مواردی از بهره‌جویی از آن نیز توسط حداقل یک گروه از هکرها گزارش شده است مهاجم را قادر به در اختیار گرفتن کنترل سیستم و اجرای کد به‌صورت از راه دور بر روی آن می‌کند.

هدایت قربانی به صفحه اینترنتی حاوی بهره‌جوی (Exploit) آسیب‌پذیری مذکور و در ادامه آلوده شدن دستگاه به‌محض فراخوانی صفحه در Internet Explorer از جمله سناریوهای احتمالی بکارگیری CVE-2019-1367 برای آلوده‌سازی دستگاه‌ها به بدافزار بدون نیاز به هر گونه دخالت کاربر است.

با توجه به گزارش سوءاستفاده مهاجمان از آسیب‌پذیری CVE-2019-1367، نصب اصلاحیه مربوطه در اسرع وقت بر روی کلیه سیستم‌ها توصیه می‌شود.

جزییات بیشتر در خصوص این ضعف امنیتی و اصلاحیه منتشر شده در لینک زیر قابل دریافت و مطالعه است:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367

همزمان مایکروسافت ضعفی دیگر با شناسه CVE-2019-1255 را در ضدویروس این شرکت، Windows Defender ترمیم و اصلاح کرده است.

بهره‌جویی از CVE-2019-1255 به مهاجم امکان می‌دهد تا مانع از اجرای برنامه‌ها و فایل‌های مورد نظر خود بر روی سیستم قربانی شود. از آنجا که سوءاستفاده موفق از این ضعف مستلزم دخالت کاربر است درجه حساسیت آن "بااهمیت" (Important) اعلام شده است.

در صورت فعال بودن قابلیت به‌روزرسانی خودکار بخش Malware Protection Engine و دسترسی دستگاه به اینترنت فرایند نصب اصلاحیه به صورت خودکار انجام خواهد شد. توضیحات بیشتر در لینک زیر در دسترس است:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1255

انتشار این دو اصلاحیه در حالی صورت می‌گیرد که حدود دو هفته پیش مایکروسافت مجموعه اصلاحیه‌های ماه میلادی سپتامبر خود را منتشر کرده بود.

اصلاحیه‌های امنیتی مایکروسافت
برای ماه میلادی اکتبر

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه ۱۶ مهر، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی اکتبر منتشر کرد. این اصلاحیه‌ها در مجموع، ۵۹ آسیب‌پذیری را در سیستم عامل Windows و محصولات زیر ترمیم می‌کنند:

- Internet Explorer
- Microsoft Edge
- ChakraCore
- Microsoft Office, Office Services and Web Apps
- SQL Server Management Studio
- Open Source Software
- Microsoft Dynamics 365
- Windows Update Assistant

درجه اهمیت ۹ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical)، ۴۹ مورد "بااهمیت" (Important) و یک مورد "متوسط" (Moderate) اعلام شده است.
پس از مدت‌ها، در این ماه هیچ کدام از ضعف‌های ترمیم شده توسط اصلاحیه‌های مایکروسافت، روز صفر (Zero-day) اعلام نشده‌اند.

آسیب‌پذیری‌های حیاتی ترمیم‌شده

CVE-2019-1238 و CVE-2019-1239 از جمله آسیب‌پذیری‌های حیاتی اصلاح شده در این ماه هستند که از اشکالی در بخش مدیریت‌کننده VBScript در مرورگر Internet Explorer ناشی می‌شوند. آسیب‌پذیری‌های مذکور به مهاجم امکان می‌دهند تا با ارسال یک فایل یا از طریق صفحه اینترنتی حاوی بهره‌جو (Exploit) کد مورد نظر خود را بر روی دستگاه قربانی اجرا کند.

CVE-2019-1333 نیز دیگر ضعف امنیتی برجسته ترمیم شده در این ماه است که سوءاستفاده از آن مهاجم را قادر می‌کند تا از روی سرور تحت کنترل خود اقدام به اجرای کد بر روی هر دستگاه آسیب‌پذیری که از طریق پودمان RDP به آن متصل شده کند.

سایر آسیب‌پذیری‌های "حیاتی" این ماه عبارتند از:

CVE-2019-1372 CVE-2019-1366 CVE-2019-1060 CVE-2019-1307 CVE-2019-1308 CVE-2019-1335

آسیب‌پذیری‌های بااهمیت وصله‌شده

از میان آسیب‌پذیری‌های "بااهمیت" برطرف شده در این ماه، دو ضعف از نوع عبور از سد تنظیمات امنیتی در بخش اصالت‌سنجی NTLM در سیستم عامل Windows بیش از سایرین جلب توجه می‌کنند. این دو آسیب‌پذیری با شناسه‌های CVE 2019-1166 و CVE-2019-1338 مهاجمان را قادر می‌کنند که کل دامنه (Domain) را در یک شبکه به تسخیر خود آورند.

سایر آسیب‌پذیری‌های با درجه "بااهمیت" این ماه عبارتند از:

CVE-2019-1371	CVE-2019-1364	CVE-2019-1328	CVE-2019-1347	CVE-2019-1318	CVE-2019-1343
CVE-2019-0608	CVE-2019-1363	CVE-2019-1070	CVE-2019-1315	CVE-2019-1320	CVE-2019-1334
CVE-2019-1357	CVE-2019-1358	CVE-2019-1340	CVE-2019-1346	CVE-2019-1369	CVE-2019-1345
CVE-2019-1314	CVE-2019-1359	CVE-2019-1339	CVE-2019-1317	CVE-2019-1368	CVE-2019-1326
CVE-2019-1375	CVE-2019-1331	CVE-2019-1316	CVE-2019-1321	CVE-2019-1376	CVE-2019-1323
CVE-2019-1356	CVE-2019-1327	CVE-2019-1342	CVE-2019-1322	CVE-2019-1313	CVE-2019-1337
CVE-2019-1361	CVE-2019-1330	CVE-2019-1311	CVE-2019-1341	CVE-2019-1230	CVE-2019-1336
CVE-2019-1362	CVE-2019-1329	CVE-2019-1344	CVE-2019-1319	CVE-2019-1365	

آسیب‌پذیری متوسط برطرف‌شده

CVE-2019-1325 تنها آسیب‌پذیری با درجه اهمیت "متوسط" این ماه است که سیستم عامل Windows از آن تأثیر می‌پذیرد.

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.

لازم به ذکر است که در کنار اعلام انتشار مجموعه اصلاحیه‌های ماه اکتبر، مایکروسافت نزدیک بودن پایان پشتیبانی این شرکت از سیستم‌های عامل Windows 7 و Windows Server 2008 R2 را برای چندمین بار به کاربران و راهبران شبکه یادآوری کرده است. بر طبق اعلام مایکروسافت این شرکت پشتیبانی از این دو سیستم عامل را کمتر از چهار ماه دیگر پایان خواهد داد و از ۲۵ دی به بعد، هیچ اصلاحیه امنیتی و پشتیبانی فنی برای این محصولات ارائه نخواهد شد. لذا به تمامی راهبران شبکه توصیه می‌شود که در فرصت باقی مانده اقدام به ارتقای دستگاه‌های با Windows 7 و Windows Server 2008 R2 خود به نسخه‌های جدیدتر و قابل پشتیبانی کنند.

اصلاحیه‌های عرضه شده
در مهـر ۱۳۹۸

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

در اوایل مهر ماه، عرضه دو اصلاحیه امنیتی توسط مایکروسافت خارج از برنامه زمانبندی معمول خود (سه‌شنبه دوم هر ماه میلادی) خبرساز شد. این اصلاحیه‌ها یک آسیب‌پذیری به تهدیدات اجرای کد به‌صورت از راه دور (Remote Code Execution) و یک ضعف امنیتی به حملات از کاراندازی سرویس (Denial of Service) را به‌ترتیب در Internet Explorer و Windows Defender ترمیم می‌کنند. آسیب‌پذیری نخست با شناسه CVE-2019-1367 و با درجه اهمیت "حیاتی" (Critical) که توسط یکی از محققان گوگل شناسایی شده و مواردی از بهره‌جویی از آن نیز توسط حداقل یک گروه از هکرها گزارش شده است، مهاجم را قادر به در اختیار گرفتن کنترل سیستم و اجرای کد به‌صورت از راه دور بر روی آن می‌کند. هدایت قربانی به صفحه اینترنتی حاوی بهره‌جوی (Exploit) آسیب‌پذیری مذکور و در ادامه آلوده شدن دستگاه به‌محض فراخوانی صفحه در Internet Explorer از جمله سناریوهای احتمالی بکارگیری CVE-2019-1367 برای آلوده‌سازی دستگاه‌ها به بدافزار بدون نیاز به هر گونه دخالت کاربر است. با توجه به گزارش سوءاستفاده مهاجمان از آسیب‌پذیری CVE-2019-1367، نصب اصلاحیه مربوطه در اسرع وقت بر روی کلیه سیستم‌ها توصیه می‌شود. اصلاحیه دوم نیز ضعفی با شناسه CVE-2019-1255 را در ضدویروس این شرکت، Windows Defender ترمیم و اصلاح کرده است. بهره‌جویی از CVE-2019-1255 به مهاجم امکان می‌دهد تا مانع از اجرای برنامه‌ها و فایل‌های مورد نظر خود بر روی سیستم قربانی شود. از آنجا که سوءاستفاده موفق از این ضعف مستلزم دخالت کاربر است درجه حساسیت آن "بااهمیت" (Important) اعلام شده است.

مایکروسافت، سه‌شنبه ١٦ مهر نیز اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی اکتبر منتشر کرد که پیش‌تر در این خبر به‌طور مفصل به آنها پرداخته شد.

در مهر ماه ادوبی در دو نوبت اقدام به عرضه به‌روزرسانی امنیتی کرد؛ محصولات زیر از این به‌روزرسانی‌ها تأثیر می‌پذیرند:

ColdFusion

Experience Manager

Acrobat and Reader

Experience Manager Forms

Download Manager

بهره‌جویی موفق از برخی از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند.

در ماهی که گذشت، شرکت اپل نیز با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در سیستم‌های عامل iOS، iPadOS، macOS، tvOS و محصولات Safari، iTunes و iCloud ترمیم و اصلاح کرد. سوءاستفاده از برخی از این ضعف‌ها که جزییات آنها در اینجا قابل دریافت است امکان در اختیار گرفتن کنترل سیستم را برای مهاجم فراهم می‌کند.

به گزارش شرکت مهندسی شبکه گستر، در مهر ماه، سیسکو در چندین نوبت اقدام به انتشار به‌روزرسانی‌های امنیتی کرد. این به‌روزرسانی‌ها در مجموع، ۱۰۱ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۳ مورد از این آسیب‌پذیری‌ها "حیاتی" و ۳۵ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون اجرای کد به‌صورت از راه دور و عبور از سد تنظیمات امنیتی، از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید است. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در اینجا قابل دسترس است.

۱۸ مهر ماه، جونیپر نت‌ورکز نیز با ارائه به‌روزرسانی چند ضعف امنیتی را در تجهیزات ساخت این شرکت ترمیم کرد. سوءاستفاده از برخی از ضعف‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. جزییات بیشتر در اینجا قابل مطالعه است.

در مهر ماه شرکت گوگل هم اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه عرضه شده از این مرورگر 77.0.3865.120 است. فهرست اشکالات مرتفع شده در این نسخه نیز در اینجا قابل دریافت و مشاهده است.

۲۲ مهر بنیاد وردپرس نسخه 5.2.4 سامانه مدیریت محتوای WordPress را عرضه کرد. در نسخه مذکور ضعف‌هایی ترمیم شده که سوءاستفاده از برخی آنها به مهاجم امکان می‌دهد تا کنترل سایت تحت مدیریت این سامانه را به دست بگیرد. اطلاعات بیشتر در این مورد در اینجا قابل دریافت است.

اوراکل طبق برنامه زمانبندی شده سه‌ماهه خود، سه‌شنبه، ۲۳ مهر، با انتشار به‌روزرسانی‌های امنیتی، در مجموع، ۲۱۹ آسیب‌پذیری را در ده‌ها محصول ساخت این شرکت ترمیم و اصلاح کرد. جزییات کامل در اینجا ارائه شده است.

در مهر ماه، آژانس CISA آمریکا نسبت به وجود آسیب‌پذیری در بخش مدیریت کننده ارتباطات VPN محصولات امنیتی Palo Alto، FortiGuard و Pulse هشدار داد. این آژانس به راهبران شبکه توصیه کرده تا با مراجعه به توصیه‌نامه های منتشر شده از سوی شرکت‌های سازنده این محصولات نسبت به ترمیم آسیب‌پذیری‌ها اقدام کنند. فهرست این توصیه‌نامه‌ها به شرح زیر است:

https://securityadvisories.paloaltonetworks.com/(X(1)S(klphdezgerjfyhnvfqkwlgqu))/Home/Detail/158?AspxAutoDetectCookieSupport=1

https://fortiguard.com/psirt/FG-IR-18-384

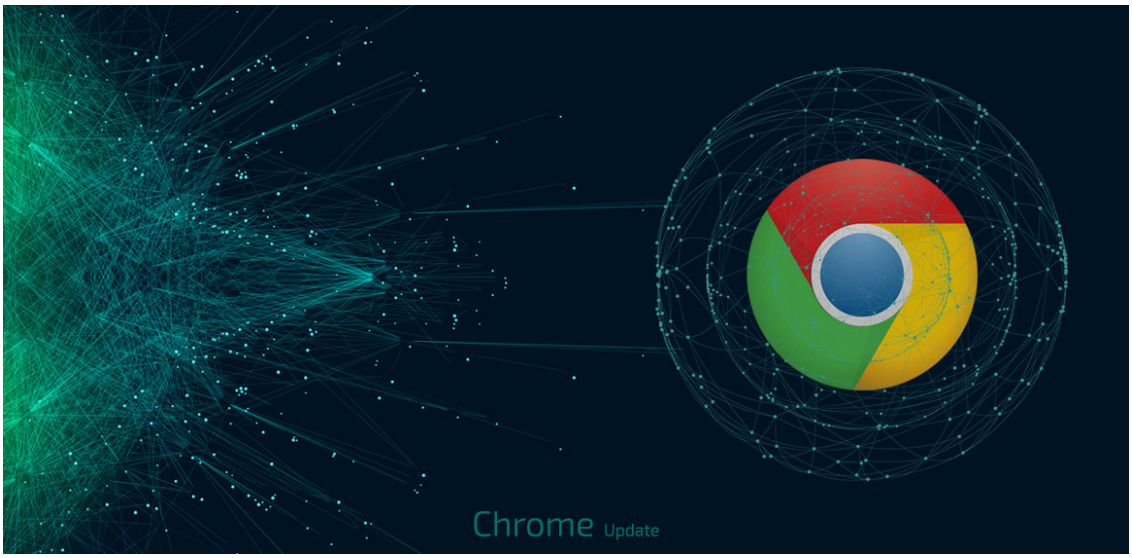
https://fortiguard.com/psirt/FG-IR-18-388

https://fortiguard.com/psirt/FG-IR-18-389

https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

همچنین در ماهی که گذشت مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) با انتشار چندین مطلب به بررسی آسیب‌پذیری‌های نرم‌فزار Foxit Reader، ابزار Sudo، فایروال Cybroam، پیام‌رسان Whatsapp، سرویس‌دهنده ایمیل Exim و نرم‌افزارهای مدیریت محتوای WordPress و phpMyAdmin پرداخت که جزییات آن در سایت این مرکز قابل مطالعه است.

ترمیم یک آسیب‌پذیری روز صفر
در مرورگر Chrome



شرکت گوگل با عرضه نسخه‌ای جدید از Chrome دو ضعف امنیتی در این مرورگر را ترمیم و اصلاح کرده است. سوءاستفاده از هر یک از این دو ضعف امنیتی مهاجم را قادر به در اختیار گرفتن کنترل سیستم آسیب‌پذیر می‌کند.

به گزارش شرکت مهندسی شبکه گستر، یکی از ضعف‌های مذکور که به آن شناسه CVE-2019-13720 تخصیص داده شده، مورد بهره‌جویی حداقل یک گروه از مهاجمان قرار گرفته است.

جزییات کامل در مورد این آسیب‌پذیری‌ها هنوز به‌صورت عمومی منتشر نشده و مطابق معمول گوگل انتشار آنها را به بعد از به‌روزرسانی Chrome توسط اکثر کاربران موکول کرده است.

با نصب نسخه جدید Chrome، نگارش این مرورگر به 78.0.3904.87 تغییر خواهد یافت.

با توجه به مورد بهره‌جویی قرار گرفتن آسیب‌پذیری CVE-2019-13720 توسط مهاجمان، به کاربران و راهبران شبکه توصیه می‌گردد که در اسرع وقت نسبت به ارتقای این محصول اقدام کنند.

اطلاعات بیشتر در خصوص نگارش 78.0.3904.87 مرورگر Chrome در اینجا قابل دریافت و مطالعه است.

گـزارش‌هـا

پلیدهای ابدی؛
بدافزار Sality

Sality بدافزاری از نوع ویروس است که با چسباندن کد مخرب به فایل‌های اجرایی سالم، آنها را آلوده و تبدیل به ناقلی از خود می‌کند. ضمن اینکه با کپی فایل‌های آلوده بر روی حافظه‌های جداشدنی، پوشه‌های اشتراکی و در برخی از نسخه‌ها سوءاستفاده از آسیب‌پذیری‌های امنیتی سیستم عامل، خود را به‌سرعت در سطح شبکه توزیع می‌کند.

این بدافزار بخش ابتدایی فایل‌های اجرایی را با کدی پیچیده جایگزین می‌کند تا در زمان اجرای فایل، کد مخرب فراخوانی شده و در عین حال عملکرد اصلی فایل نیز حفظ شود.

نخستین نسخه از بدافزار Sality در ۱۷ فروردین ۱۳۸۲ شناسایی شد و طی یک دهه پس از آن، نسخه‌های متعددی از این بدافزار مخرب با کدهایی پویا و با قابلیت‌های پیشرفته عرضه شد. از جمله این قابلیت‌ها می‌توان به توانایی فعالیت به‌عنوان درب‌پشتی، جاسوس‌افزار و روت‌کیت اشاره کرد.

اگر چه چندین سال است که نسخه جدیدی از Sality ارائه نشده اما متأسفانه ایران در فهرست پنج کشوری است که این بدافزار در آنها بیشترین فعالیت را دارد.

شرکت مهندسی شبکه گستر در گزارشی ضمن بررسی روش کار نسخه های متداول Sality به راه های مقابله با این بدافزار مخرب پیر پرداخته است.

برای دریافت این گزارش بر روی تصویر زیر کلیک شود.

نسل جدید امکانات پیشرفته مقابله با تهدیدات
در محصولات سازمانی بیت‌دیفندر

شرکت بیت‌دیفندر به‌طور مستمر در حال بهبود راهکارهای امنیتی خود است و در همین راستا امکانات جدیدی شامل امنیت پست‌های الکترونیکی و قابلیت‌های ویژه مقابله با تهدیدات پیشرفته در حال افزوده شدن به راهکار GravityZone می‌باشد. تجهیز این راهکار به این امکانات درتاریخ‌های ۲۹ اکتبر (۷ آبان) و ۵ نوامبر (۱٤ آبان) به‌ترتیب بر روی بستر ابری (Cloud) و نسخه‌های مستقر در بستر شبکه (On-premise) صورت خواهد پذیرفت.

از جمله امکانات جدید در به‌روزرسانی پیش رو در بستر ابری می‌توان به موارد زیر اشاره کرد:

- امنیت پست‌های الکترونیک - شامل پشتیبانی از کلیه سرویس‌دهندگان پست‌های الکترونیک و همچنین محصول Office 365 می‌شود. این امکان شامل یک محافظت همه‌جانبه از تهدیدات مبتنی بر پست‌های الکترونیک شامل بدافزارها، هرزنامه‌ها، حملات فیشینگ و لینک‌های مخرب می‌شود.
- دفاع در برابر حملات درون‌شبکه‌ای - امکانی که با شناسایی ضعف‌های امنیتی درون شبکه، سطح جدیدی از محافظت را در برابر افرادی که قصد حمله به زیرساخت سازمان و دسترسی به منابع را دارند فراهم می‌کند.
- امکانات بازدارنده پیشرفته - امروزه تهدیدات پیچیده شامل حملات بدون فایل و حملات مبتنی بر اسکریپت بیش از پیش سازمان‌ها را در معرض خطر قرار داده است. امکان جدید Fileless Attack Defense که در نگارش ابری بسته‌های Advanced، Elite و Ultra اضافه خواهد شد کمک شایانی در مقابله با این گونه تهدیدات مخرب و فوق‌پیچیده و ناکام گذاشتن آنها خواهد کرد.
- مقابله با بهره‌جوها - با افزوده شدن امکان Exploit Defense و غنی‌تر شدن بانک داده بهره‌جوهای جدید در راهکار، با گونه‌های نو و حتی ناشناخته بهره‌جوها پیش از اجرا مقابله خواهد شد.

برخی از قابلیت های جدید در به‌روزرسانی نسخه مستقر در سازمان Bitdefender GravityZone نیز شامل موارد زیر می‌شود:

- دفاع در مقابل حملات شبکه‌ای - ناکام گذاشتن تهدیدات، با افزودن فناوری جدیدی جهت شناسایی آن دسته از حملات شبکه‌ای که با بهره‌گیری از تکنیک‌هایی نظیر حملات سعی‌وخطا (Brute-force) و یا روش‌های پیشرفته دیگر اقدام به رخنه در سیستم ها می‌کنند.
- امنیت زیرساخت - با ایجاد امکان ساخت VPN Clustering ارتباط سرویس‌های مختلف بر روی بستر GravityZone را بیش از قبل امن می‌کند.
- بررسی اشکالات به‌صورت از راه دور - امکان جمع‌آوری لاگ‌ها از روی سیستم‌های مستقر در شبکه را مستقیماً از طریق کنسول مدیریتی GravityZone فراهم می‌سازد.

- ضدبهره‌جوی پیشرفته - موجب مجهز شدن راهکار به سه تکنیک جدید برای شناسایی تهدیدات خاص مبتنی برای بهره‌جوها شامل Shell Code Export Address Filtering، VBScript Generic و Emerging Exploits می‌گردد.
- مدیریت نصب اصلاحیه‌های امنیتی برروی نقاط پایانی - دیگر امکان جدیدی است که در به‌روزرسانی جدید لحاظ خواهد شد.
- جعبه‌شنی (Sandbox) پیشرفته - ابزاری پیشرفته را برای بررسی فایل‌های آلوده و مشکوک در اختیار راهبران امنیت سازمان قرار می‌دهد.

شرکت بیت‌دیفندر در سال ۲۰۰۱ میلادی در کشور رومانی تاسیس شد و در زمانی اندک، به یکی از سازندگان مطرح نرم‌افزارهای ضدویروس تبدیل شد. شرکت بیت‌دیفندر سازنده یکی از سریع‌ترین و کارآمدترین نرم‌افزارهای ضدویروس در دنیا است.

محصولات بیت‌دیفندر دارنده ده‌ها نشان از مؤسسات ارزیابی مستقل نظیر AV-Comparatives و AV-Test هستند. همچنین محصولات بیت‌دیفندر به دفعات از سوی این مؤسسات معتبر به عنوان برترین ضدویروس سال معرفی شده‌اند.

محصولات متنوع بیت‌دیفندر صدها میلیون کاربر خانگی و سازمانی را در اقصی نقاط جهان در برابر تهدیدات سایبری محافظت می‌کنند. محصولات بیت‌دیفندر توسط نمایندگان محلی این شرکت در بیش از ۲۰۰ کشور دنیا توزیع و پشتیبانی می‌شوند. ضمن اینکه بیت‌دیفندر جزو معدود شرکت‌های عرضه‌کننده ضدویروس در جهان است که حضور مستقیم در بازار ایران دارد.

بسیاری از شرکت‌های عرضه کننده محصولات امنیتی از جمله eScan، Bullguard، Qihoo، GData، F-Secure و IBM از فناوری شناسایی بیت‌دیفندر بهره می‌گیرند.

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