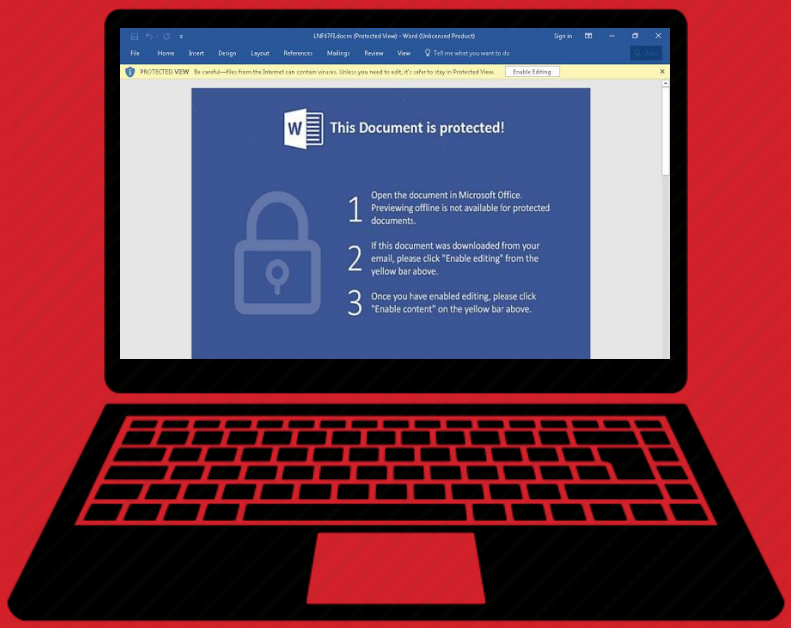
بررسی و تحلیل بدافزار

Jaff Ransomware



شبکه گستر
شرکت مهندسی شبکه گستر

عنوان سند: بررسی و تحلیل باج‌افزار Jaff
شناسه سند: SPT-A-0136-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ آخرین بازنگری: ۷ خرداد ۱۳۹۶ | شرح آخرین بازنگری: -

شبکه گستر

در اواخر اردیبهشت ماه ۱۳۹۶، محققان از ارسال ده‌ها میلیون ایمیل هرزنامه خبر دادند که هدف آنها آلوده کردن دستگاه قربانی به باج‌افزاری با عنوان Jaff بود. پیوست این هرزنامه‌ها فایلی PDF بود که در آن یک فایل Word حاوی ماکروی مخرب تزریق شده بود. در صورت باز شدن فایل پیوست و اجرای ماکروی مخرب، دستگاه به باج‌افزار آلوده شده و فایل‌های با یکی از پسوند هدف قرار گرفته شده رمزگذاری می‌شدند.

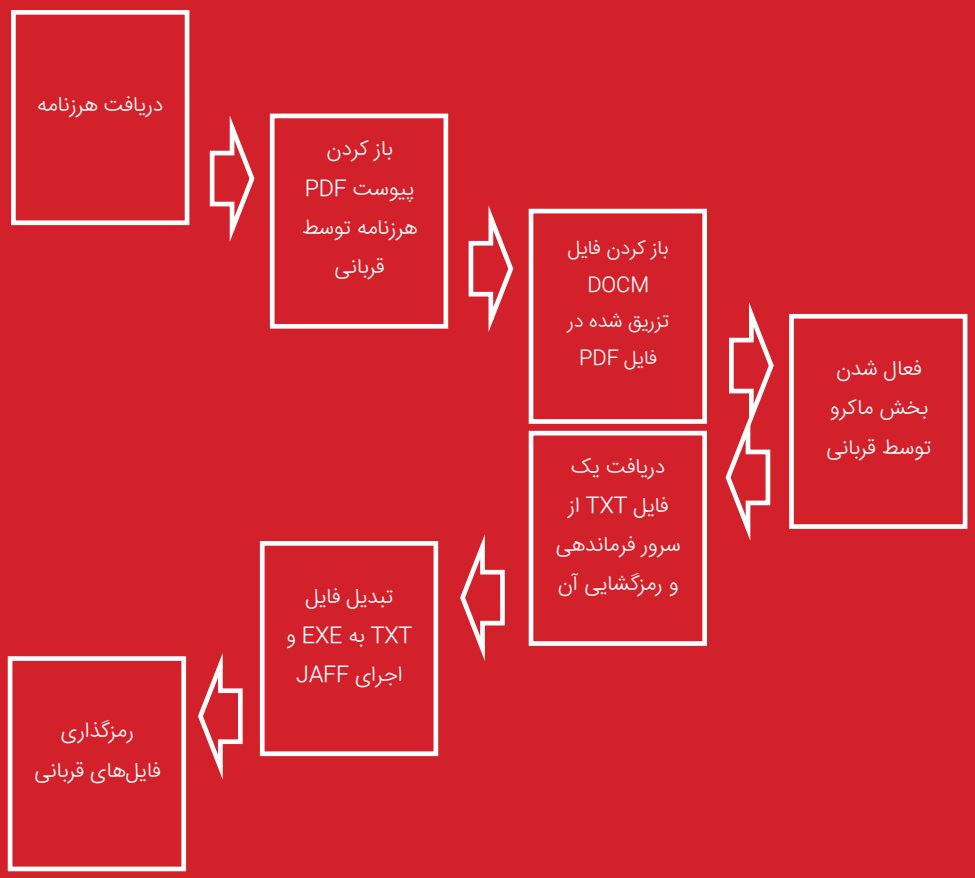
در نخستین نسخه از این باج افزار پسوند فایل‌های رمزگذاری شده به به jaff. تغییر داده می‌شد. ضمن اینکه مبلغ اخاذی شده در این نسخه حدود ۲/۰۴۷ بیت‌کوین (معادل بیش از ۱۷۰ میلیون ریال) بود که در مقایسه با اکثر باج‌افزارها، مبلغی بالا و غیررایج محسوب می‌شد.

منابع مختلفی کارزار توزیع‌کننده Jaff را کارزاری موسوم به Malspam می‌دانند که انتشار باج‌افزار معروف Locky و بدافزار مشهور بانکی Dridex را در کارنامه خود دارد. این کارزار از شبکه مخرب Necurs به‌منظور توزیع هرزنامه‌های خود بهره می‌گیرد.

از اوایل خرداد ماه ۹۶ نیز، کارزار مذکور اقدام به توزیع نسخه جدیدی از باج‌افزار Jaff نموده که در مقایسه با نسخه پیشین آن تکامل‌های قابل توجهی یافته است.

در نسخه جدید پسوند فایل‌های رمزنگاری شده به wlu. تغییر داده می‌شود.

در این گزارش ساختار و عملکرد آخرین نسخه از باج‌افزار Jaff مورد بررسی و تحلیل قرار گرفته است.



شکل ۱: مراحل انتشار و اجرای باج‌افزار Jaff

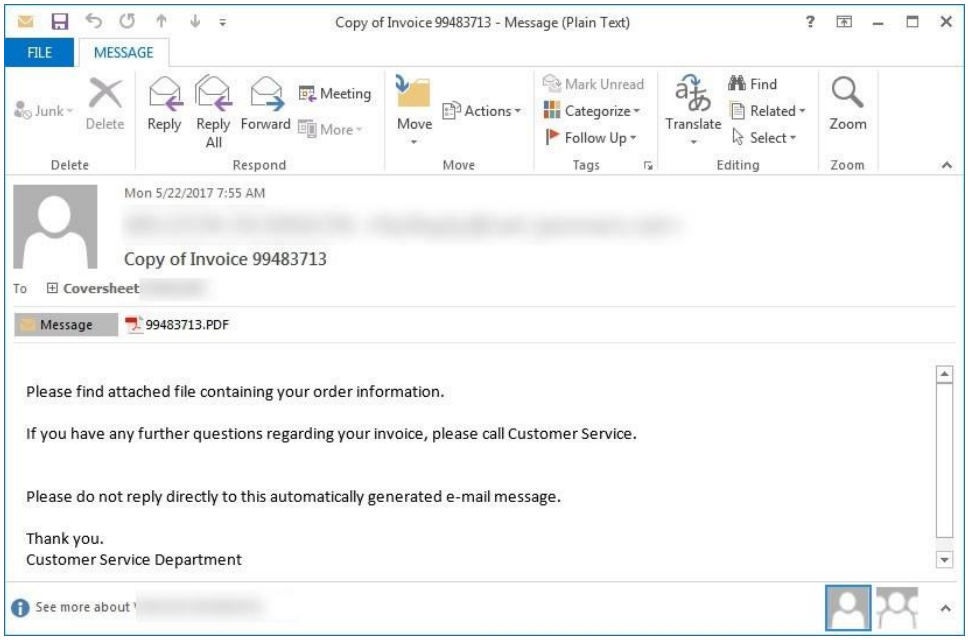
توزیع جدیدترین نسخه از باج‌افزار Jaff، از طریق هرزنامه‌هایی[1] با عناوین صدور صورت حساب صورت می‌پذیرد. برخی عناوین گزارش شده این هرزنامه‌ها به شرح زیر است:

- Invoice(00-5523)
- Invoice(00-5832)
- Invoice(08-4031)
- Invoice(09-5337)
- Invoice(19-9273)
- Invoice(23-0458)
- Invoice(27-7813)
- Invoice(53-3366)
- Invoice(54-9434)
- Invoice(61-7808)
- Invoice(68-4200)
- Invoice(68-5182)
- Invoice(68-6414)
- Invoice(72-6353)
- Invoice(88-6908)
- Invoice(95-1750)
- Invoice(98-3753)
- Invoice(98-9897)
- Invoice(78-8672)
- Invoice(28-3137)

همچنین عنوان برخی نمونه‌های این هرزنامه‌ها در قالب الگوی Copy of Invoice ######## بوده است. (شکل ۲)

پیوست هرزنامه‌های مذکور، فایلی PDF است که به‌نظر می‌رسد برای هر ارسال نام آن بر اساس اعدادی تصادفی ایجاد می‌شود. فهرست زیر برخی نام‌های مشاهده شده این پیوست‌ها را نمایش می‌دهد:

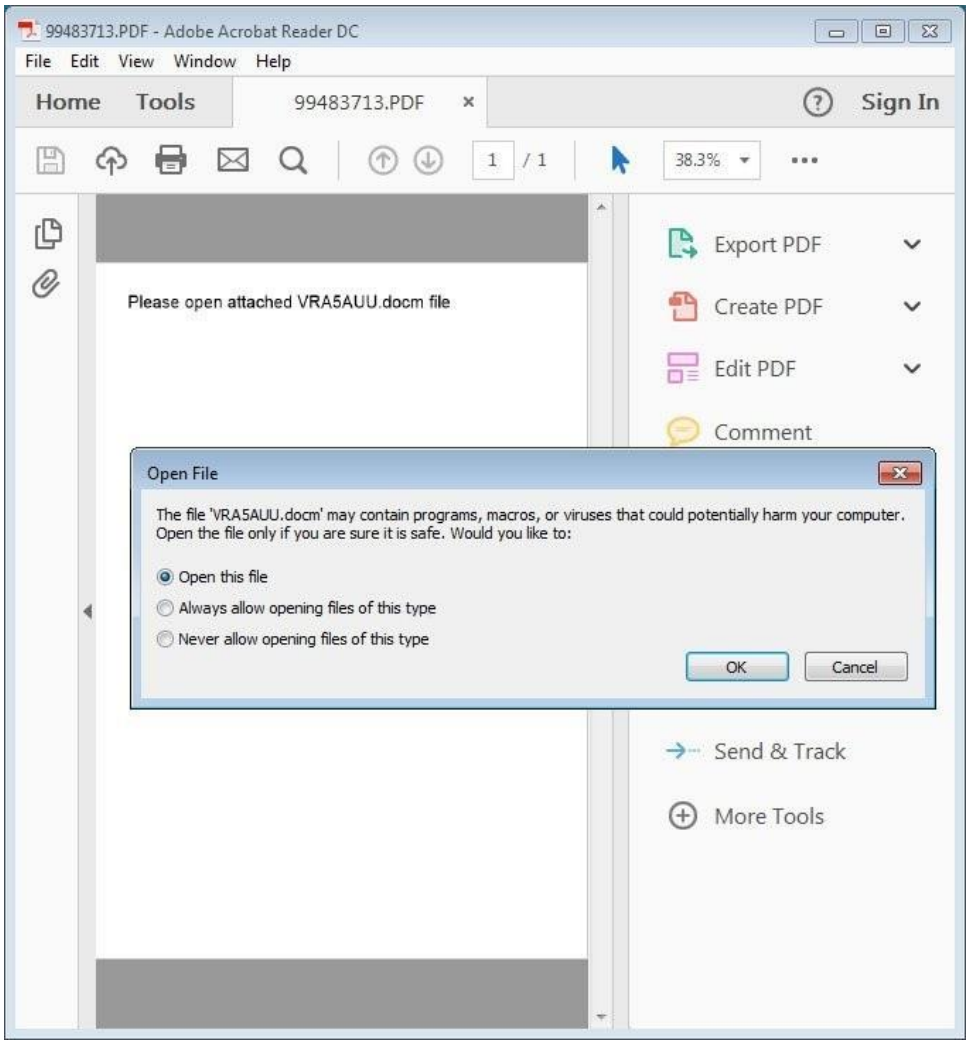
- 68-5182.pdf
- 98-9897.pdf
- 95-1750.pdf
- 78-8672.pdf
- 54-9434.pdf
- 23-0458.pdf
- 88-6908.pdf
- 72-6353.pdf
- 68-6414.pdf
- 68-4200.pdf
- 00-5832.pdf
- 27-7813.pdf
- 19-9273.pdf
- 09-5337.pdf
- 28-3137.pdf
- 53-3366.pdf
- 61-7808.pdf
- 98-3753.pdf
- 08-4031.pdf
- 00-5523.pdf



شکل ۲: نمونه‌ای از هرزنامه توزیع‌کننده باج‌افزار

[1] Spam

زمانی که فایل PDF پیوست شده به هرزنامه، توسط قربانی باز می‌شود، بسته به نرم‌افزار نمایش‌دهنده محتوای PDF، اعلانی جهت باز کردن یک سند توکار DOCM نمایش داده خواهد شد. (شکل ۳)



شکل ۳: نمونه‌ای از فایل پیوست شده به هرزنامه توزیع‌کننده باج‌افزار

در فایل DOCM یک ماکروی مخرب تزریق شده است.

یکی از روش‌های رایج انتشار باج‌افزارها، ارسال هرزنامه با پیوست حاوی ماکرو است.

برخی محصولات شرکت مایکروسافت، از جمله نرم‌افزار Office، بخشی با عنوان VBA – Visual Basic for Applications – دارند.

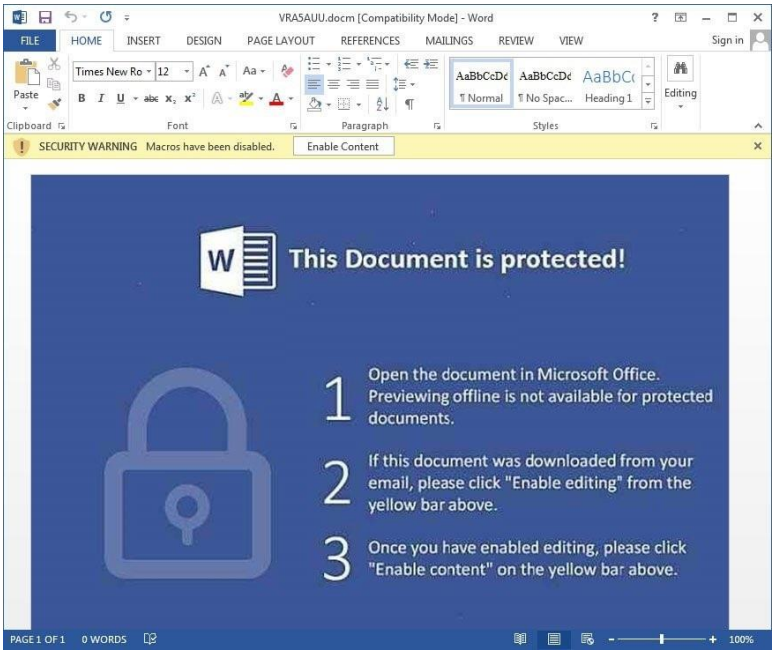
کاربرانی همچون حسابداران، مهندسان صنایع و مدیران سیستم‌ها می‌توانند از کدهای VBA در درون فایل‌هایی همچون Word و Excel استفاده کنند. فایل‌های حاوی کدهای VBA به ماکرو[۲] معروف هستند. ماکروها سبب سرعت بخشیدن به اموری می‌شوند که روالی تکرار شونده دارند. اما سرعت بخشیدن به کار بسیاری از کارکنان تنها خاصیت ماکرو نیست. نفوذگران معمولاً از ماکرو برای آلوده کردن سیستم‌های کاربران و رخنه به شبکه سازمان سوءاستفاده می‌کنند.

به‌صورت پیش‌فرض در نرم‌افزار Office، بخش ماکرو غیر فعال است؛ اما در عین حال در زمان باز کردن فایل حاوی ماکرو، پیامی ظاهر شده و از کاربر خواسته می‌شود تا برای استفاده از کدهای بکار رفته در فایل، تنظیمات امنیتی خود را تغییر دهد.

---

[۲] Macro

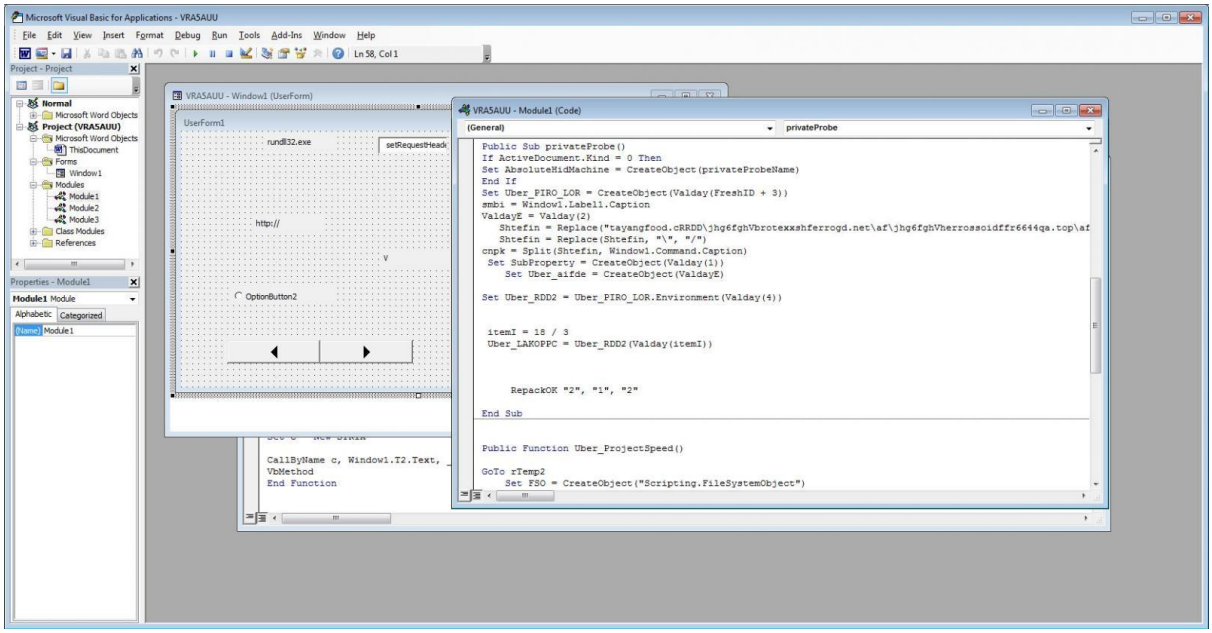
در نمونه بررسی شده در این گزارش نیز، در زمان باز شدن فایل DOCM در نرم‌افزار Word پیام مذکور نمایش داده می‌شود.



شکل ۴: اعلان فعال نمودن بخش ماکرو در فایل DOCM

زمانی که کاربر بر روی دگمه Enable Content کلیک می‌کند، ماکروی مخرب یک نسخه از باج‌افزار Jaff را دانلود کرده و پس از ذخیره نمودن آن با نام levinsky8.exe در مسیر زیر، اقدام به اجرای آن می‌کند:

- `C:\Users\[username]\AppData\Local\Temp\`



شکل ۵: ماکروی مخرب در فایل DOCM

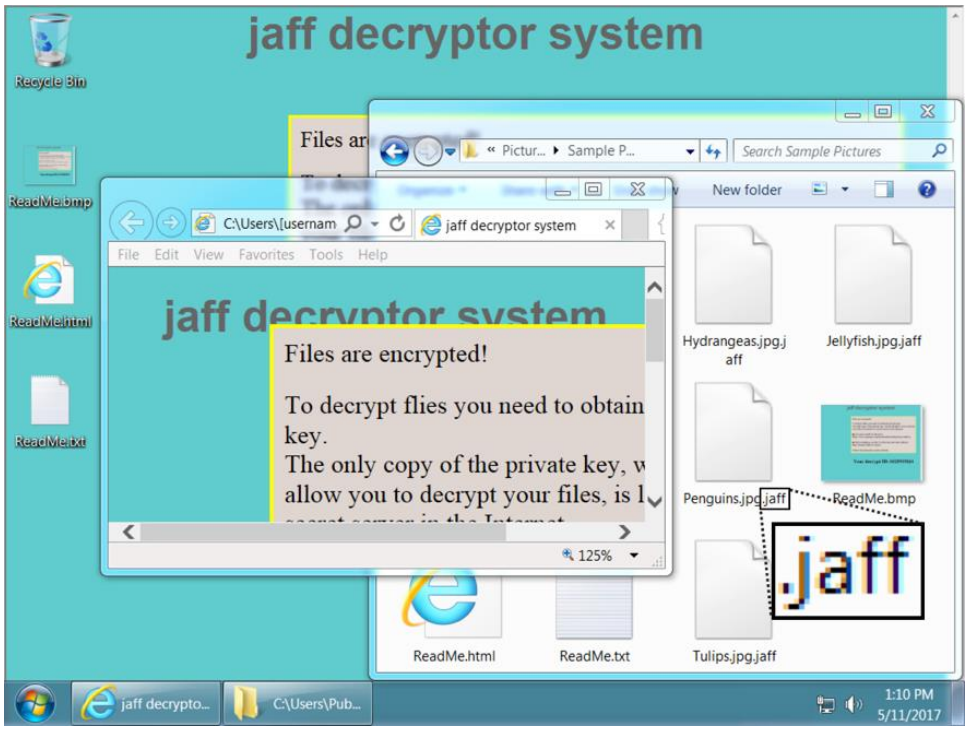
به‌محض اجرا شدن، باج‌افزار اقدام به پویش سیستم برای یافتن فایل‌های با هر یک از پسوندهای مورد نظر خود می‌کند. در حال حاضر باج‌افزار Jaff پسوندهای زیر را هدف قرار می‌دهد:

```
.001, .002, .004, .005, .006, .007, .008, .009, .010, .1cd, .3dm, .3ds, .3fr, .3g2, .3pr, .7ZIP,
.MPEG, .aac, .ab4, .accdb, .accde, .accdt, .acd, .ach, .acr, .act, .adb, .adp, .ads, .agdl, .aif,
.aiff, .ait, .aoi, .apj, .arw, .as4, .asf, .asm, .asp, .aspx, .asx, .avi, .awg, .back, .backup,
```

.backupdb, .bak, .bank, .bay, .bdb, .bgt, .bik, .bin, .bkp, .blend, .bmp, .bpw, .cad, .cbr, .cdf, .cdr, .cdr3, .cdr4, .cdr5, .cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfg, .cgm, .cib, .class, .cls, .cmt, .config, .contact, .cpi, .cpp, .cr2, .craw, .crt, .crw, .csh, .csl, .css, .csv, .dac, .dat, .db3, .db_journal, .dbf, .dbx, .dc2, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .deb, .der, .des, .design, .dgc, .dit, .djvu, .dng, .doc, .docm, .docx, .dot, .dotm, .dotx, .drf, .drw, .dsr, .dtd, .dwg, .dxb, .dxf, .dxg, .edb, .eml, .eps, .erbsql, .erd, .exf, .fdb, .ffd, .fff, .fhd, .fif, .fla, .flac, .flv, .flvv, .fpx, .fxg, .gif, .gray, .grey, .groups, .gry, .gz, .hbk, .hdd, .hdr, .hpp, .htm, .html, .ibank, .ibd, .ibz, .ico, .ics, .idf, .idx, .iff, .iif, .iiq, .incpas, .indd, .iso, .java, .jnt, .jpe, .jpeg, .jpg, .kc2, .kdbx, .kdc, .key, .kpdx, .kwm, .laccdb, .lit, .log, .lua, .m2ts, .m3u, .m4a, .m4p, .m4v, .mapimail, .max, .mbx, .mdb, .mdc, .mdf, .mdi, .mef, .mfw, .mid, .mix, .mkv, .mlb, .mmw, .mny, .moneywell, .mos, .mov, .mp3, .mp4, .mpd, .mpg, .msg, .myd, .ndd, .ndf, .nef, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg, .nsh, .nvram, .nwb, .nx2, .nxl, .nyf, .oab, .obd, .obj, .obt, .odb, .odc, .odf, .odg, .odm, .odp, .ods, .odt, .ogg, .oil, .ord, .ost, .otg, .oth, .otp, .ots, .ott, .ova, .p12, .p7b, .p7c, .pab, .pages, .par, .pas, .pat, .pcd, .pct, .pdb, .pdd, .pdf, .pef, .pem, .pfx, .php, .pif, .plc, .plus_muhd, .png, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .prn, .psafe3, .psd, .pspimage, .pst, .ptx, .pub, .pwm, .qba, .qbb, .qbm, .qbw, .qbx, .qby, .qcow, .qcow2, .qed, .r3d, .raf, .rar, .rat, .raw, .rdb, .rpm, .rtf, .rvt, .rw2, .rwz, .s3db, .safe, .sas7bdat, .sav, .save, .say, .sd0, .sda, .sdf, .sitx, .sldm, .sldx, .sql, .sqlite, .sqlite3, .sqlitedb, .srf, .srt, .srw, .st4, .st5, .st6, .st7, .st8, .stc, .std, .sti, .stl, .stm, .stw, .stx, .svg, .swf, .swm, .sxc, .sxd, .sxg, .sxi, .sxm, .sxw, .tar, .tex, .tga, .thm, .tib, .tif, .tlg, .txt, .vbox, .vcf, .vdi, .veg, .vhd, .vhdx, .vib, .vmdk, .vmsd, .vmx, .vmxf, .vob, .vsc, .vsd, .wab, .wad, .wallet, .wav, .waw, .wb2, .wbk, .wda, .wma, .wmv, .wpd, .wps, .x11, .x3f, .xis, .xla, .xlam, .xlk, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .xmod, .ycbcra, .zip, .zipx, .zpf

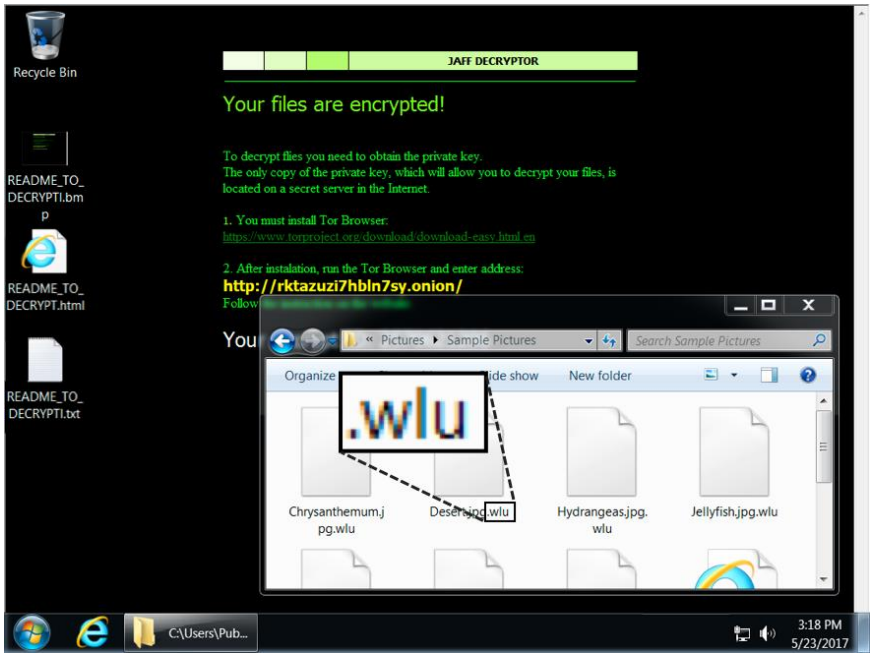
Jaff با استفاده از الگوریتم رمزگذاری AES هر فایل شناسایی شده را رمزنگاری می‌کند.

همانطور که پیش‌تر اشاره شد در نسخه نخست این باج‌افزار، پسوند فایل‌های رمزگذاری شده به jaff. تغییر داده می‌شد. (شکل ۶)



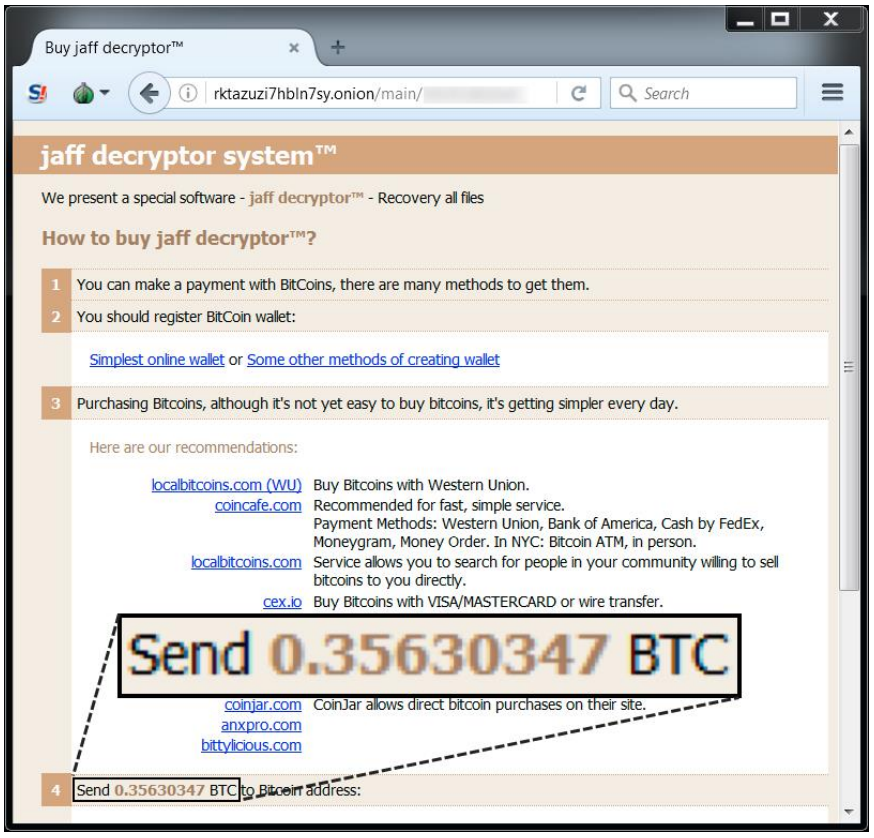
شکل ۶: فایل‌های رمزگذاری شده در نسخه قبلی باج‌افزار Jaff

اما در نسخه جدید، در زمان رمزنگاری پسوند wlu. به انتهای نام فایل‌های رمزنگاری شده اضافه می‌شود. (شکل ۷)



شکل ۷: فایل‌های رمزگذاری شده در نسخه جدید باج‌افزار Jaff

مبلغ اخاذی شده در نمونه بررسی شده در این گزارش، ۰/۳۶ بیت‌کوین[۳] (معادل حدود ۳۰ میلیون ریال) است.



شکل ۸: میزان باج در نسخه جدید باج‌افزار Jaff

[۳] Bitcoin

نتیجه‌گیری

متأسفانه در زمان نگارش این گزارش امکان رمزگشایی فایل‌های رمزنگاری شده توسط باج‌افزار Jaff بدون پرداخت باج ممکن نیست. تنها راه بازیابی فایل‌ها استفاده از فایل‌های پشتیبان است. هر چند که در موارد نادر، استفاده از Shadow Volume Copies ممکن است منجر به بازیابی فایل‌ها شود. برای ایمن ماندن از گزند باج افزارهای رمزگذار رعایت موارد زیر توصیه می‌شود:

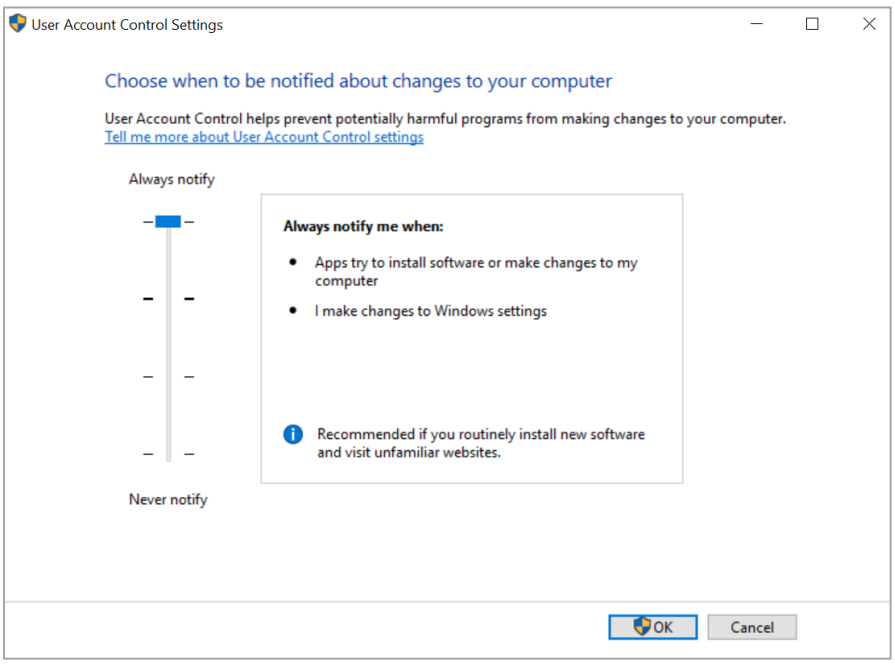
۱ تهیه نسخه پشتیبان

از اطلاعات سازمانی به‌صورت دوره‌ای نسخه پشتیبان تهیه شود. پیروی از قاعده ۳-۲-۱ برای داده‌های حیاتی توصیه می‌شود. بر طبق این قاعده، از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه به‌عنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود. همچنین رمزگذاری فایل‌های پشتیبان برای حفاظت از آنها در برابر افراد غیرمجاز نیز توصیه می‌شود.

۲ محدود کردن سطح دسترسی

همه کاربران، حتی مدیر سیستم می‌بایست با حداقل سطح دسترسی مورد نیاز به هر سیستم وارد شوند. در صورت محدود بودن سطح دسترسی حتی در صورت اجرای فایل مخرب توسط کاربر، دستگاه به باج‌افزار آلوده نخواهد شد. همچنین برخی محصولات کنترل برنامه نظیر McAfee Application Control نیز می‌توانند به‌نحوی مؤثر از اجرا شدن فایل‌های غیرمجاز از جمله باج‌افزارها جلوگیری کنند.

همچنین توصیه می‌شود بخش User Account Control Settings در حالت Always notify me قرار داده شود.



شکل ۹: تنظیمات بخش User Account Control

برای اعمال این پیکربندی بر روی تمامی دستگاه‌های سازمان از طریق Group Policy می‌توان از این راهنما استفاده کرد.

۳ نصب اصلاحیه‌ها در اولین فرصت ممکن و استمرار در انجام آن

بسیاری از بهره‌جویی‌ها از طریق سوءاستفاده از ضعف‌های امنیتی نرم‌افزارهای پرکاربردی نظیر Adobe Flash، Office و مرورگرها صورت می‌پذیرد. هر چه زودتر اصلاحیه نصب شود آسیب کمتری متوجه سازمان می‌شود.

٤ استفاده از فناوری‌های حفاظتی پیشرفته

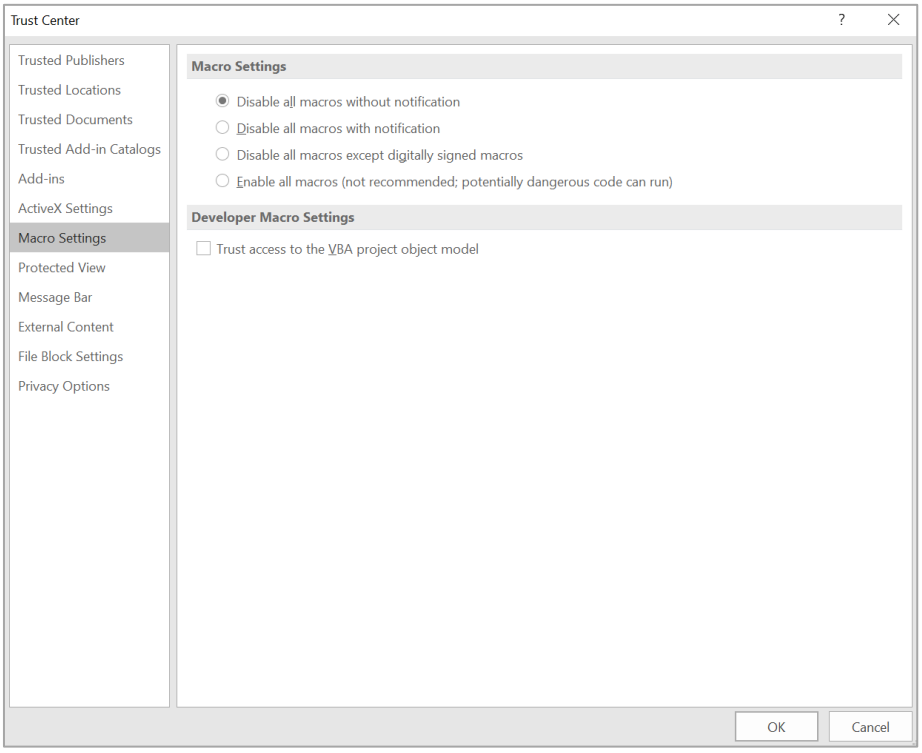
استفاده از ضدویروس قدرتمند و به‌روز جهت مقابله با باج‌افزارهای رمزگذار ضروری است. اما در کنار آن می‌بایست از راهکارهای نفوذیاب، ضدهرزنامه، کنترل‌کننده وب و دیواره آتش نیز استفاده کرد. همچنین برخی محصولات امنیتی نظیر McAfee و Bitdefender دارای راهکارهایی ویژه و خاص برای شناسایی و مقابله با باج‌افزارهای رمزگذار هستند.

توضیح اینکه نمونه بررسی شده در این گزارش توسط ضدویروس‌های McAfee، Bitdefender و ESET با نام‌های زیر شناسایی می‌شود:

Bitdefender: Trojan.GenericKD.5148703
McAfee: RDN/Trojan-FMTJ
ESET: Win32/Filecoder.Jaff.B

۵ غیرفعال کردن بخش ماکرو

با توجه به انتشار بخش قابل توجهی از باج‌افزارها از جمله Sage از طریق فایل‌های نرم‌افزار Office حاوی ماکروی مخرب، غیرفعال کردن بخش ماکرو برای کاربرانی که به این قابلیت نیاز کاری ندارند با فعال کردن گزینه Disable all macros without notification توصیه می‌شود.



شکل ۱۰: تنظیمات امنیتی بخش ماکرو در نرم‌افزار Office

برای غیرفعال کردن این قابلیت، از طریق Group Policy، می‌توان از این راهنما و این راهنما استفاده کرد.

همچنین توصیه می‌شود ایمیل‌های دارای پیوست ماکرو در همان درگاه شبکه مسدود شوند. بدین منظور می‌توان از تجهیزات دیواره آتش مجهز به این قابلیت بهره گرفت.

٦ احتیاط در زمان باز کردن ایمیل‌ها

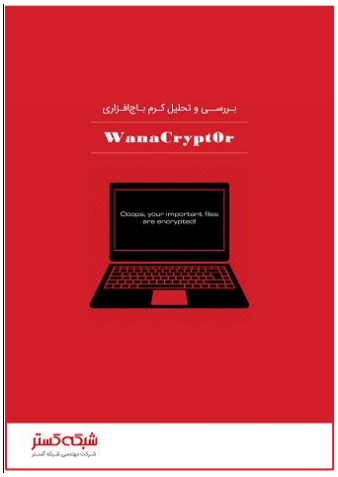
آموزش و راهنمایی کاربران سازمان به صرف‌نظر کردن از فایل‌های حتی کمی مشکوک و باز نکردن آنها می‌تواند نقشی مؤثر در پیشگیری از اجرا شدن پیوست‌های مخرب داشته باشد. برای این منظور می‌توانید از این داده‌نمایی‌ها استفاده کنید.

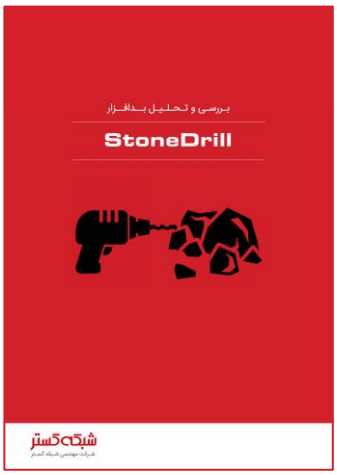
٧ به‌روز بودن در خصوص روش‌های جدید باج‌گیران

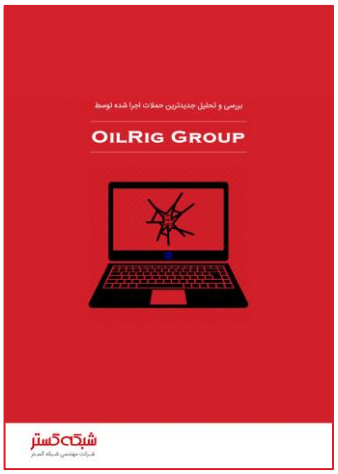
نویسندگان باج‌افزار دائماً در حال تغییر و تکامل روش‌های خود هستند. با مرور اخبار و حضور در دوره‌های آگاهی‌رسانی شرکت مهندسی شبکه گستر، از آخرین روش‌های مورد استفاده مهاجمان آگاه شده و سیاست‌ها پیشگرانه لازم را اعمال کنید.

منابع

- https://isc.sans.edu/forums/diary/Jaff+ransomware+gets+a+makeover/22446/
- http://blog.checkpoint.com/2017/05/11/jaff-new-ransomware-town-widely-spread-infamous-necurs-botnet/
- http://blog.emsisoft.com/2017/05/11/jaff-ransomware-the-new-locky/
- https://www.tripwire.com/state-of-security/latest-security-news/newly-designed-jaff-ransomware-now-encrypts-data-wlu-extension/
- https://blog.malwarebytes.com/cybercrime/2017/05/new-jaff-ransomware-via-necurs-asks-for-2-btc/
- http://blog.talosintelligence.com/2017/05/jaff-ransomware.html







شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرد. 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 به‌عنوان 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. در حال حاضر نیز شرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری 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 به‌عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می‌نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضد ویروس Bitdefender را به‌عنوان 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 است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و 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 و طولانی مدت‌ترین پروژه‌های طراحی، نصب، راه‌اندازی و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت‌افزاری فایروال 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.

ISO 9001:2008
Cert No 9150.C528

شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن / دورنگار	۰۲۱-۴۲۰۵۲
تارنمای شرکت	www.shabakeh.net
سامانه پشتیبانی	help.shabakeh.net
خدمات پس از فروش	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net