بـــاج افـزارهای رمـــزکننده

Master Boot Record

شبکه گستر
شـرکت مهندسی شـبکه گسـتر

عنوان سند: بررسی و تحلیل باج‌افزارهای رمزکننده بخش Master Boot Record

شناسه سند: SPT-A-0125-00

تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

آخرین بازنگری: بهمن ۱۳۹۵

شبکه گستر

بیش از یک سال است که نوع جدیدی از باج‌افزارها با روشی خاص اقدام به قطع کامل دسترسی کاربر به کامپیوتر می‌کنند.

این باج‌افزارها با رمزگذاری بخش Master Boot Record دیسک سخت، کامپیوتر را غیرقابل راه‌اندازی می‌کنند.

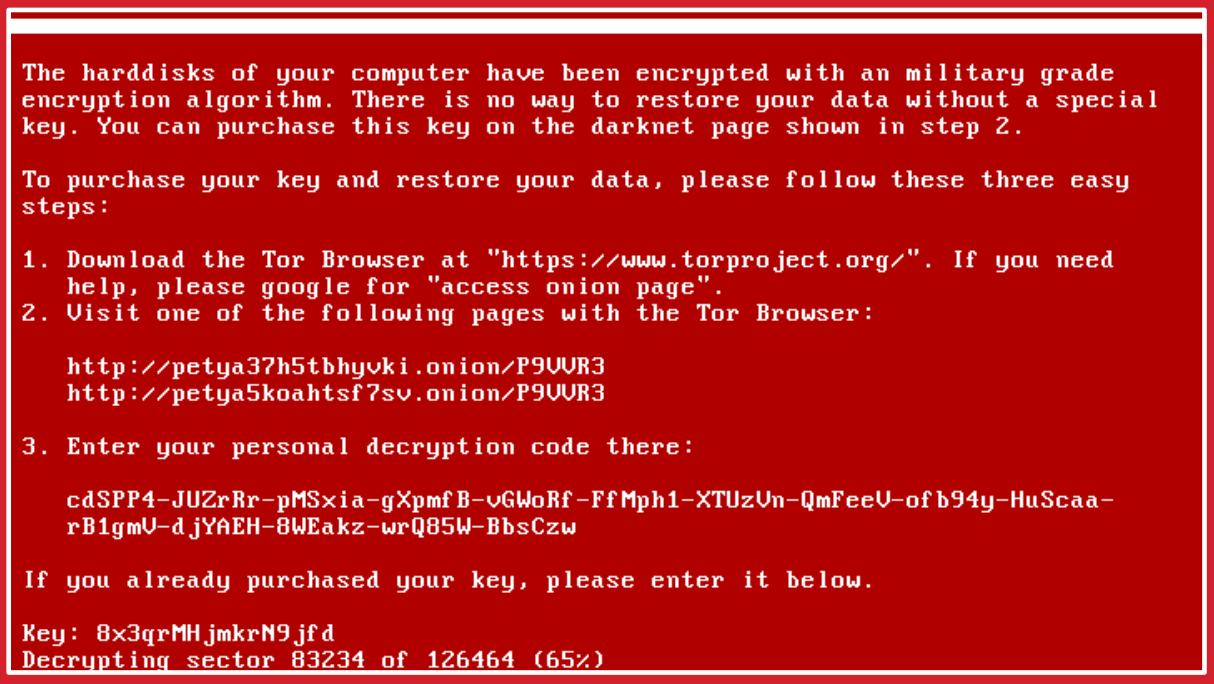
بخش Master Boot Record در قسمت‌های ابتدایی دیسک سخت ذخیره و نگهداری می‌شود. این بخش شامل اطلاعاتی درباره ساختار دیسک و برنامه‌ای که سیستم عامل را به اجرا در می‌آورد، می‌باشد. بدون یک Master Boot Record سالم و صحیح، کامپیوتر نمی‌داند که سیستم عامل بر روی کدام قسمت از دیسک سخت است و چگونه باید راه‌اندازی و اجرا شود.

نخستین بار، باج‌افزار Petya با بکارگیری این روش توجه کارشناسان امنیتی را به خود جلب کرد.

نویسنده این باج‌افزار پس از مدتی اقدام به استفاده همزمان از دو باج‌افزار Petya و Mischa به‌صورت ترکیبی نمود تا اگر به هر دلیلی امکان رونویسی بخش Master Boot Record فراهم نشد با استفاده از باج‌افزار Mischa فایل‌های قربانی رمزگذاری شود.

هر چند عمده فعالیت این باج‌افزار در کشور آلمان بوده اما نمونه‌هایی از آلودگی سیستم‌ها در کشورهای دیگر از جمله ایران به این باج‌افزار گزارش شده است.

در این گزارش عملکرد نسخه‌های مختلف باج‌افزار Petya مورد بررسی و تحلیل قرار گرفته است.

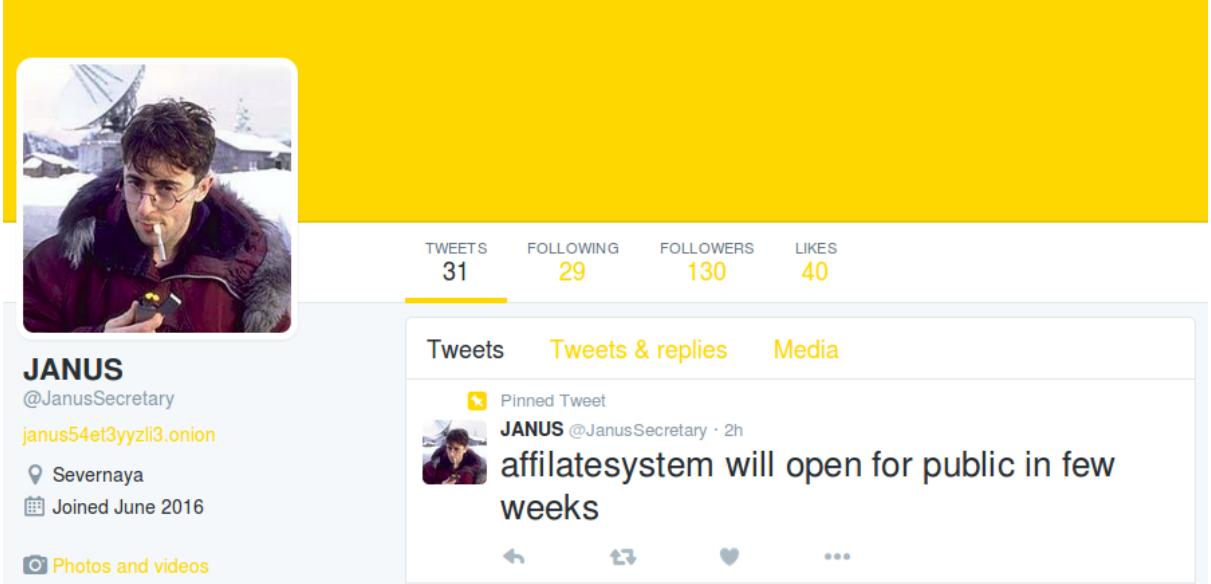


شکل ۱: نمونه‌ای از اطلاعیه باج‌گیری Petya پس از معرفی کلید رمزگشایی به آن

در اواخر سال ۱۳۹۴، یکی از شرکت‌های ضدویروس از انتشار باج‌افزار جدیدی به نام Petya در بین سازمان‌های آلمانی خبر داد که اقدام به رمزگذاری بخش Master Boot Record – به اختصار MBR – دیسک سخت[۱] کرده و با این روش کامپیوتر را غیرقابل راه‌اندازی[۲] می‌کرد.

در طی این یک سال نسخه‌های متعددی از این باج‌افزار منتشر شده است. Petya پس از رمزگذاری MBR، اطلاعیه باجگیری[۳] را در قالب یک تصویر جمجمه که با حروف ASCII ساخته شده، نمایش می‌دهد. رنگ جمجمه در برخی نسخه‌های این باج‌افزار تغییر کرده است.

فردی با شناسه Janus خود را به‌عنوان نویسنده و صاحب این باج‌افزار معرفی کرده است. او تا اکتبر سال ۲۰۱۶ میلادی سایت Janus Cybercrime را اداره می‌کرد و در این سایت Petya را به عنوان باج‌افزار به‌عنوان سرویس[۴] اجاره می‌داد. Janus در ماه جولای ۲۰۱۶ اقدام به انتشار کلیدهای رمزگشایی یکی از باج‌افزارهای هم‌قطار و رقیبش با نام Chimera کرد.



شکل ۲: نمایه Janus در شبکه Twitter

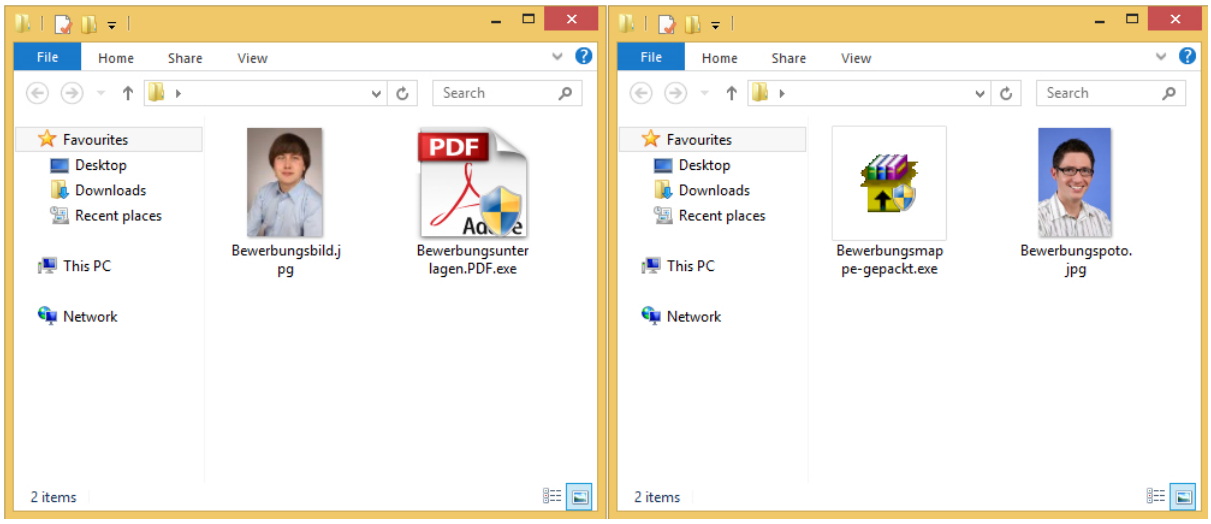
روش انتشار

اصلی‌ترین روش انتشار باج‌افزار Petya ، ایمیل‌های ناخواسته و مزاحم هرزنامه[۵] – معمولاً در ظاهر درخواست استخدام – بوده است.

در برخی نسخه‌های این باج‌افزار هرزنامه‌های ارسالی حاوی پیوند[۶] به یک شاخه به اشتراک گذاشته شده بر روی سرویس‌های ذخیره‌سازی ابری[۷] نظیر DropBox بوده‌اند. در این شاخه یک فایل تصویری که در ظاهر عکسی از متقاضی استخدام است قرار دارد. علاوه بر آن یک فایل اجرایی نیز قرار دارد که نشان[۸] آن در برخی نمونه‌ها مشابه فایل‌های فشرده شده و در برخی نمونه‌ها به‌صورت یک فایل PDF است. در صورت دریافت و اجرای فایل اجرایی، باج‌افزار Petya نصب و فعال می‌شود.

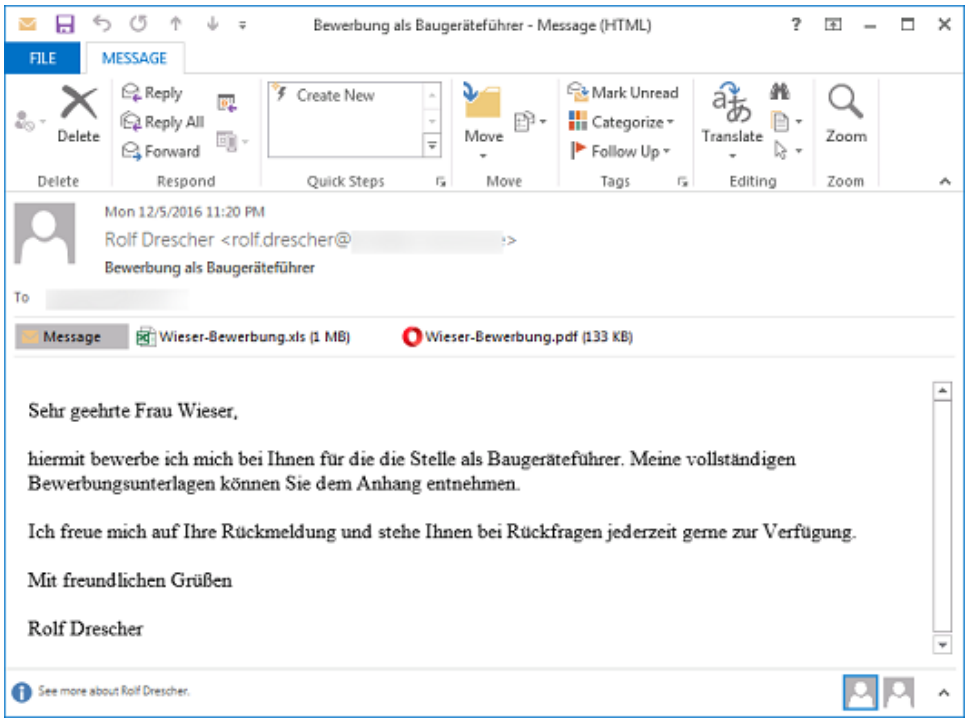
---

۱ Hard Disk
۲ Boot
۳ Ransom Note
۴ Ransomware-as-a-Service
۵ Spam
۶ Link
۷ Cloud
۸ Icon



شکل ۳: نمونه فایل‌های مخرب Petya، اشتراک گذاشته شده بر روی سرویس‌های ذخیره‌سازی ابری

در برخی نمونه‌های دیگر از این باج‌افزار، هرزنامه‌های ارسالی حاوی دو فایل PDF و Excel هستند.



شکل ٤: نمونه هرزنامه با پیوست فایل ماکروی ناقل Petya

فایل پیوست PDF، رزومه‌ای جعلی است که به‌خوبی می‌تواند کارکنان بخش منابع انسانی سازمان‌ها را به دام بیندازد.

فایل Excel نیز نصاب[۹] اصلی باج‌افزار محسوب می‌شود. این فایل حاوی ماکرویی مخرب است که در صورت فعال شدن توسط کاربر اقدام به درج رشته‌هایی در فایلی اجرایی در پوشه Temp کرده و سپس آن را اجرا می‌کند. با این کار پروسه رمزنگاری بر روی دستگاه فعال می‌شود. کد ماکروی مخرب نیز مبهم‌سازی[۱۰] شده است.

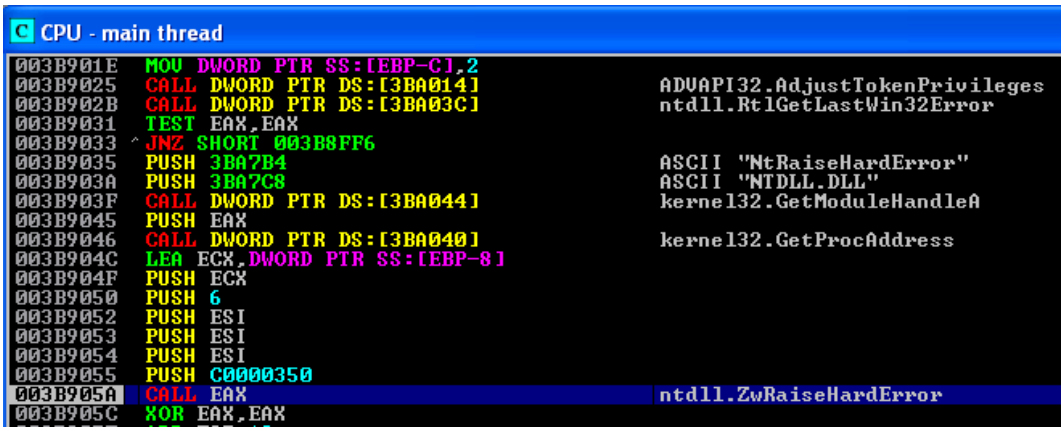
---

[۹] Installer

[۱۰] Obfuscation

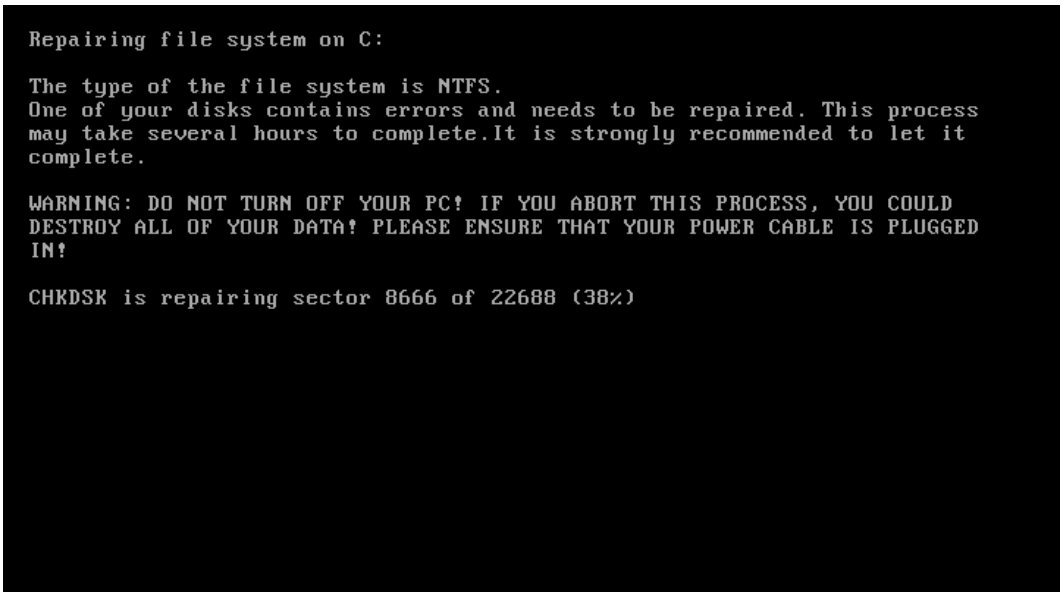
رمزنگاری

با اجرا شدن باج‌افزار، در اولین مرحله بخش MBR و برخی قسمت‌های دیگر از دیسک سخت توسط کدهای باج‌افزار با استفاده از الگوریتم Salsa20 رمزگذاری می‌شوند. در ادامه با استفاده از رابط کاربری[11] NtRaiseHardError یک خطای حاد سیستمی ایجاد شده و در نتیجه آن دستگاه راه‌اندازی مجدد[12] می‌شود.



شکل ۵: رابط کاربری NtRaiseHardError در باج‌افزار Petya

با راه‌اندازی مجدد دستگاه، باج‌افزار اقدام به نمایش یک پیام CHKDSK جعلی می‌کند. هدف از این کار مخفی نمودن ادامه فرآیند رمزنگاری سکتورهای در نظر گرفته شده از چشم کاربر است. در پیام دروغین CHKDSK پیشرفت کار به‌صورت درصد به قربانی نمایش داده می‌شود.



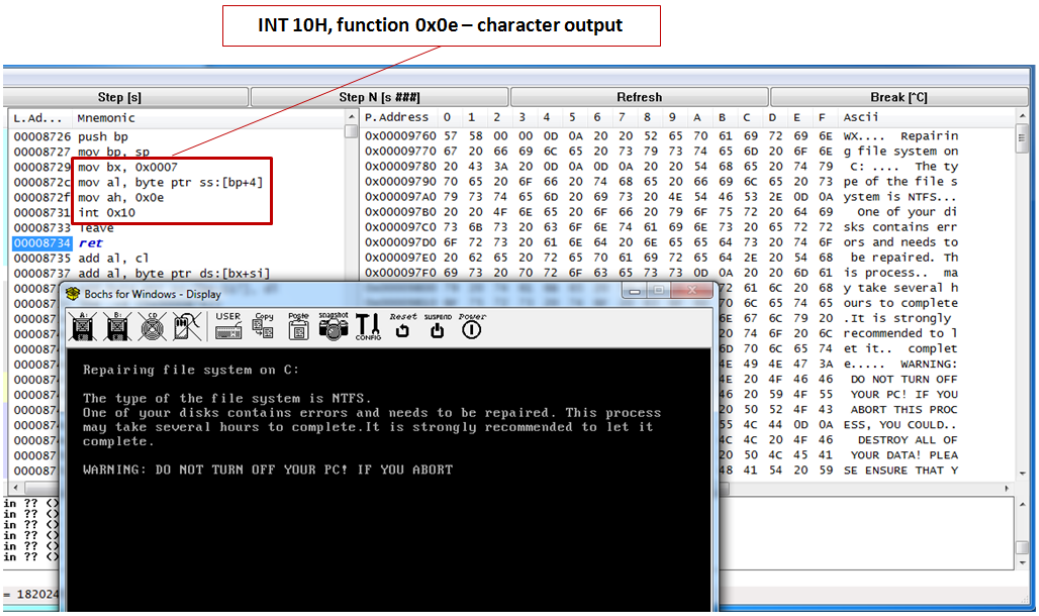
شکل ٦: پیام دروغین CHKDSK

باید توجه داشت که در زمان راه‌اندازی شدن دستگاه، هیچ رابط کاربری Windows در دسترس نیست. بنابراین باج‌افزار از برخی توابع INT 13H برای اجرای فرامینی نظیر خواندن و انتقال کد بهره‌گیری می‌کند. همچنین به‌منظور نمایش پیام CHKDSK جعلی از برخی توابع INT 10H استفاده کرده و پیام را به‌صورت نویسه نویسه درج می‌کند. (شکل ۷)

---

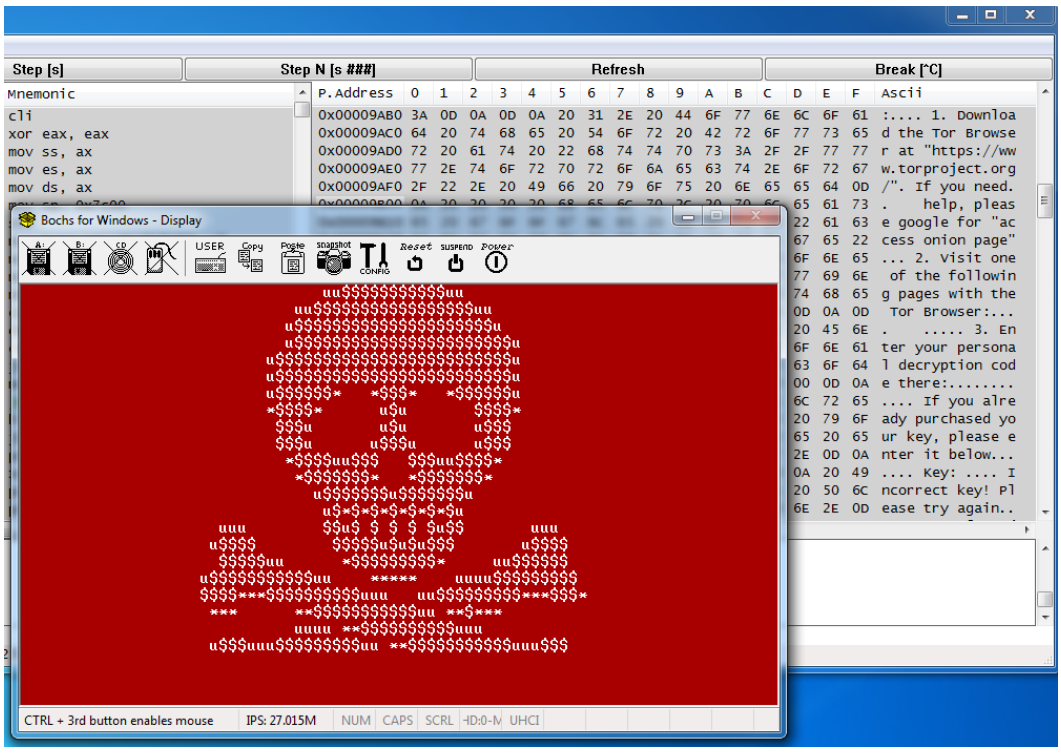
[11] API

[12] Reboot

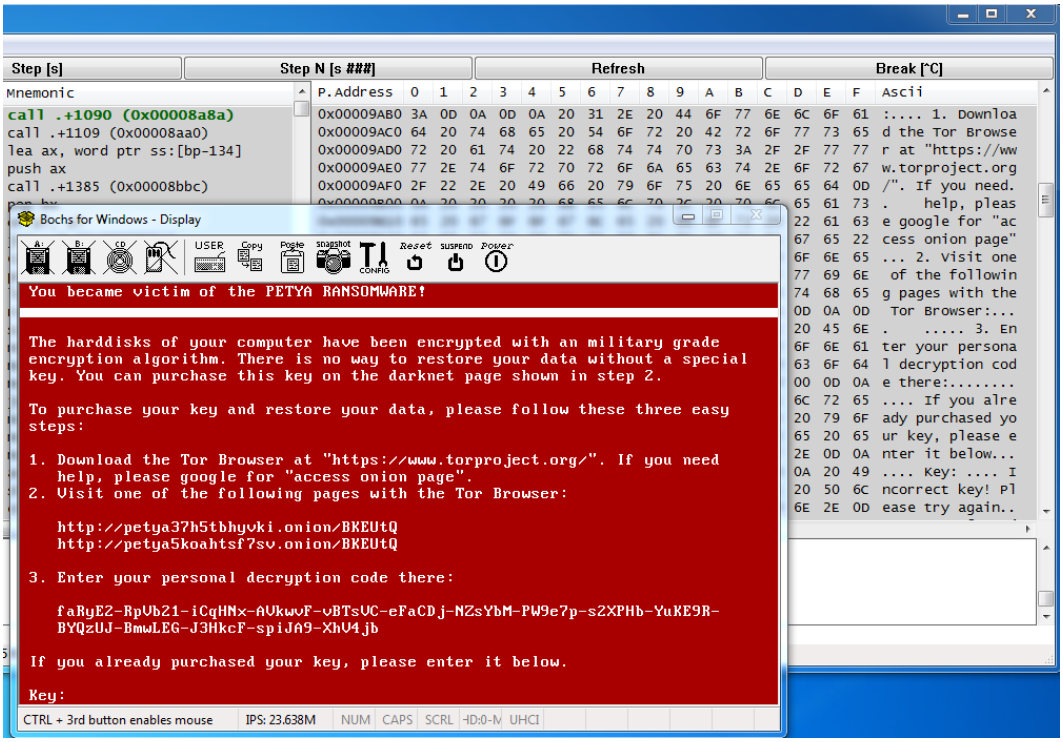


شکل ۷: فراخوانی تابع INT 10H

پس از آن نوبت به ایجاد تصویر یک جمجمه با نویسه‌های ASCII و نمایش آن به صورت چشمک‌زن می‌رسد. رنگ این جمجمه در نسخه‌های مختلف این باج‌افزار متغیر بوده است. پس از آن، هر بار راه‌اندازی شدن سیستم منجر به نمایش تصویر مذکور شده و با فشردن هر کلیدی توسط کاربر، اطلاعیه باج‌گیری ظاهر می‌شود.



شکل ۸: تصویر جمجمه Petya



شکل ۹: اطلاعیه باج‌گیری Petya

ترکیب باج‌افزارهای Petya و Mischa

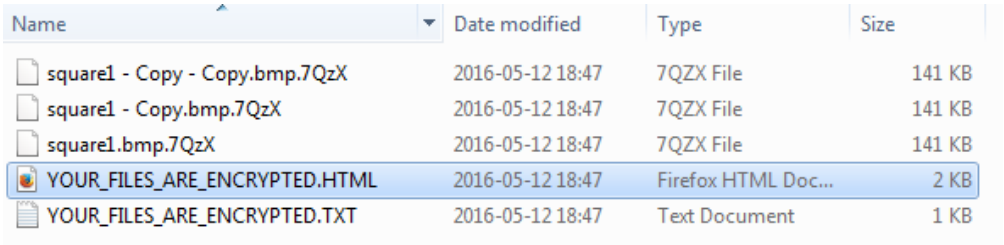
در اواسط سال ۱۳۹۵، دو باج‌افزار Petya و Mischa به‌صورت ترکیبی کاربران را هدف قرار دادند. در یکی از این نمونه‌ها باج‌افزار ابتدا تلاش می‌کرد که بخش MBR دیسک را رمزگذاری کند و تنها در صورت عدم موفقیت در انجام این کار اقدام به اجرای باج‌افزار Mischa بر روی سیستم می‌کرد.

اما در گونه‌های جدیدتر، Mischa در همان ابتدا – مشابه باج‌افزارهای رمزگذار رایج – اقدام به رمزنگاری فایل‌های بر روی دستگاه کرده و به فایل‌های رمز شده پسوندی تصادفی الصاق می‌کند.

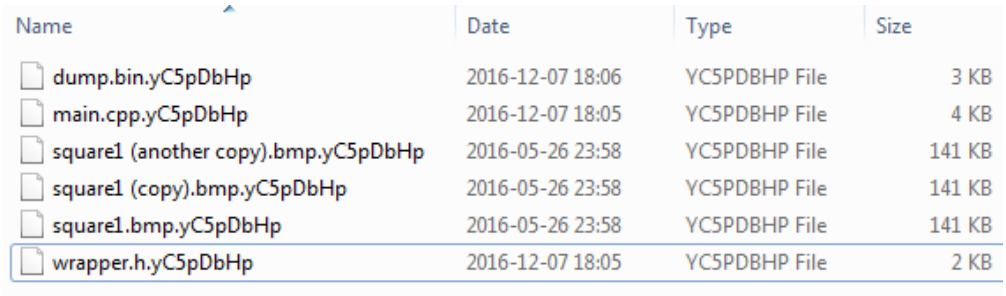
Mischa از محدود باج‌افزارهایی است که فایل‌های اجرایی را نیز رمزگذاری می‌کند. البته فایل‌های موجود در مسیرهای زیر در این باج‌افزار مستثنی شده‌اند:

- \Windows
- \$Recycle.Bin
- \Microsoft
- \Mozilla Firefox
- \Opera
- \Internet Explorer
- \Temp
- \Local
- \LocalLow
- \Chrome

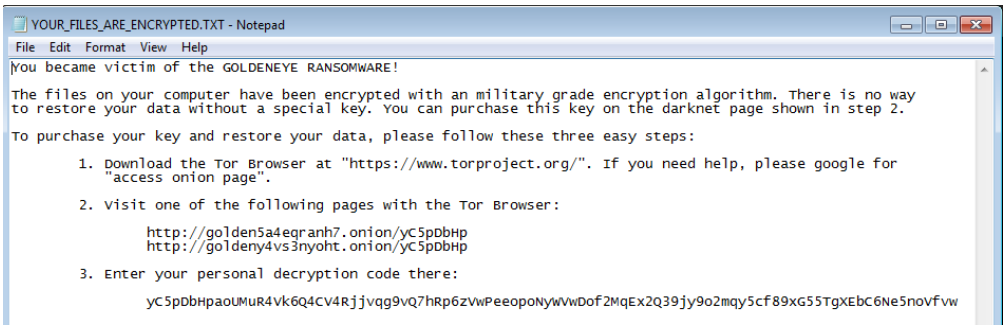
Mischa در هر پوشه‌ای که حداقل یکی از فایل‌های آن رمزنگاری شده اطلاعیه باج‌گیری را در قالب دو فایل با نام‌های YOUR_FILES_ARE_ENCRYPTED.TXT و YOUR_FILES_ARE_ENCRYPTED.HTML کپی می‌کند.



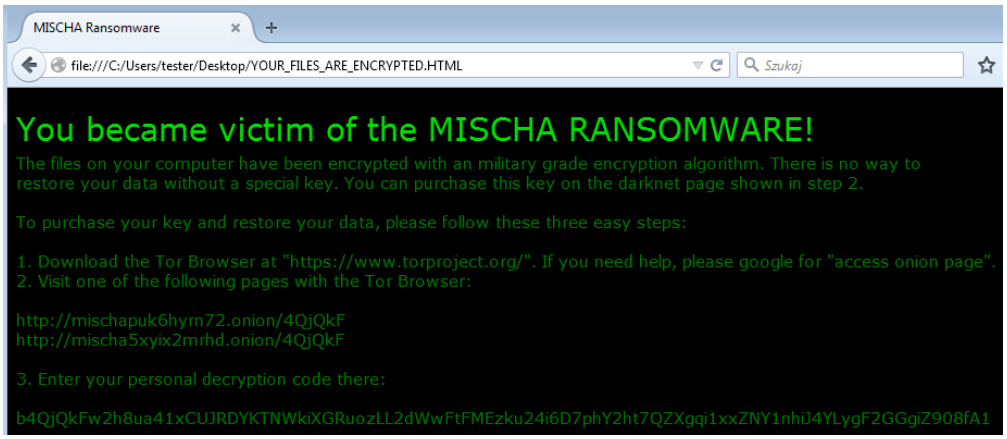
شکل ۱۰: فایل‌های رمزگذاری شده در یکی از نسخه‌های Petya



شکل ۱۱: فایل‌های رمزگذاری شده در یکی از نسخه‌های Petya



شکل ۱۲: اطلاعیه باج‌گیری در یکی از نسخه‌های Petya



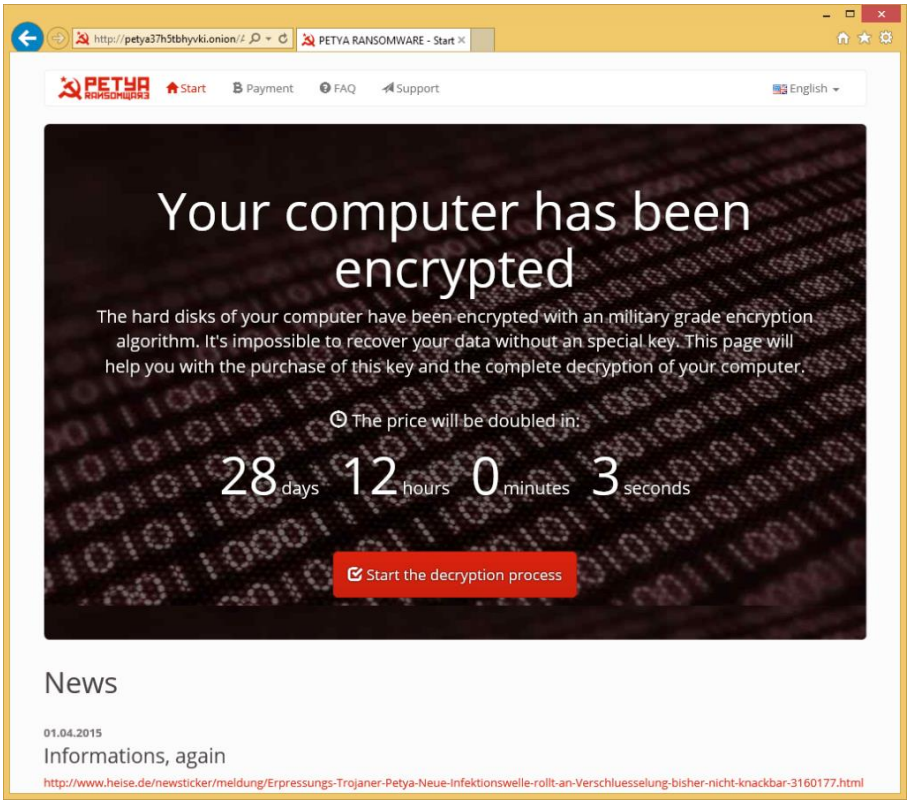
شکل ۱۳: اطلاعیه باج‌گیری در یکی از نسخه‌های Petya

در مرحله بعد دستگاه راه‌اندازی مجدد شده و فرآیند رمزگذاری Petya مشابه نسخه‌های پیشین ادامه می‌یابد.

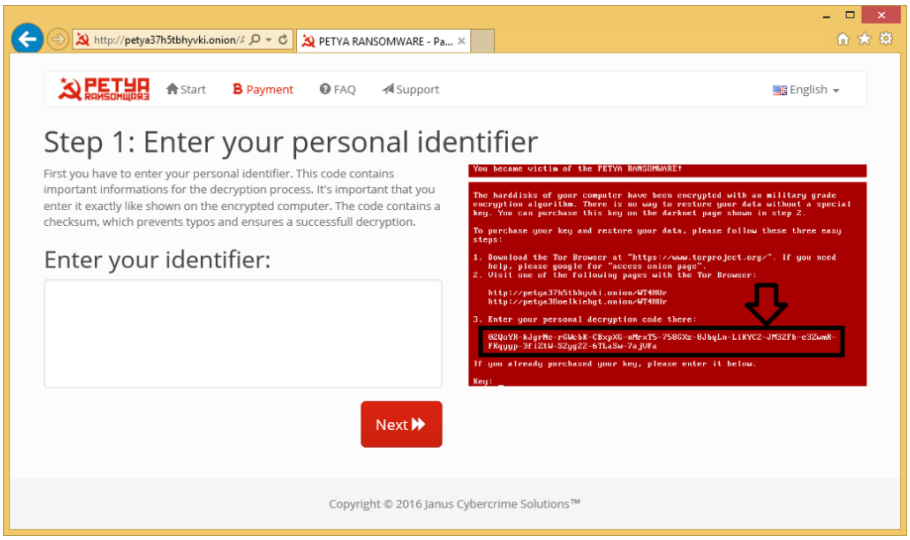
پرداخت باج

با توجه به عدم دسترسی کاربر به دستگاه، قربانی ناچار است که با مراجعه به سایتی دیگر اقدام به پرداخت باج کند. لازم به ذکر است که هیچ تضمینی برای بازگردانی سیستم به حالت اولیه در صورت پرداخت مبلغ اخاذی شده وجود ندارد.

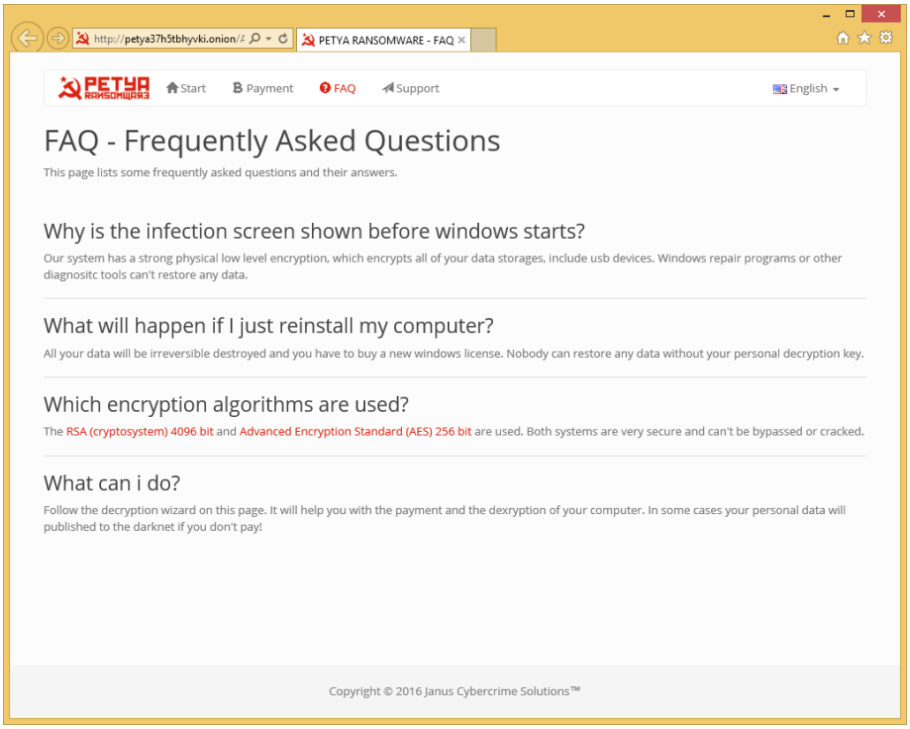
در پیام باج‌گیری از کاربر خواسته می‌شود که به سایتی در شبکه اینترنتی ناشناس TOR مراجعه کرده و شماره منحصربفردی را که نشان‌دهنده کامپیوتر کاربر به باجگیران است، وارد کند.



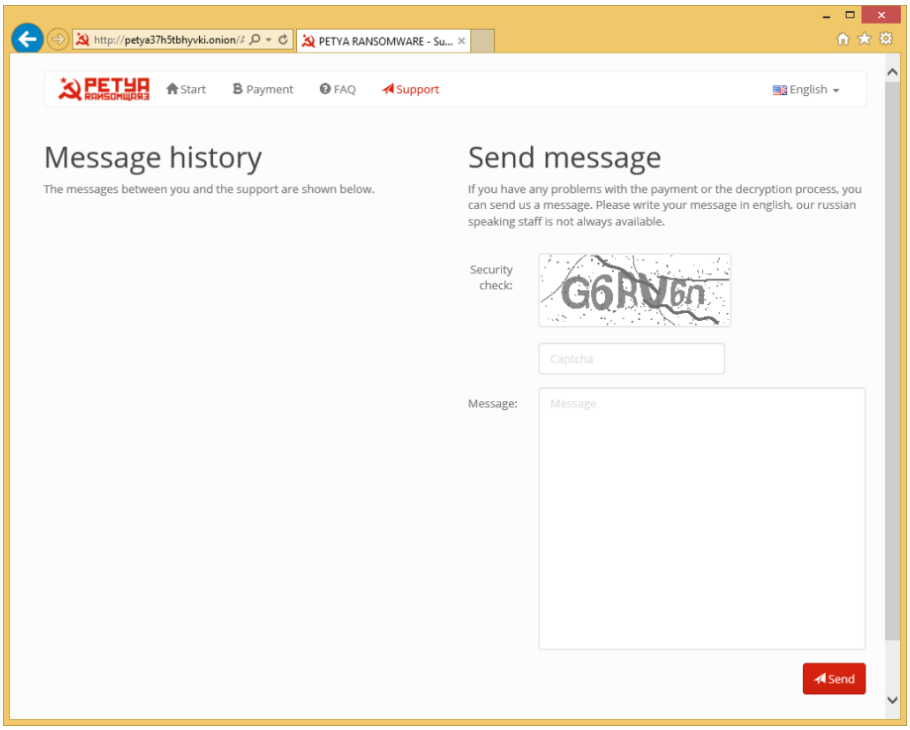
شکل ۱۴: پورتال قربانی در سایت Petya



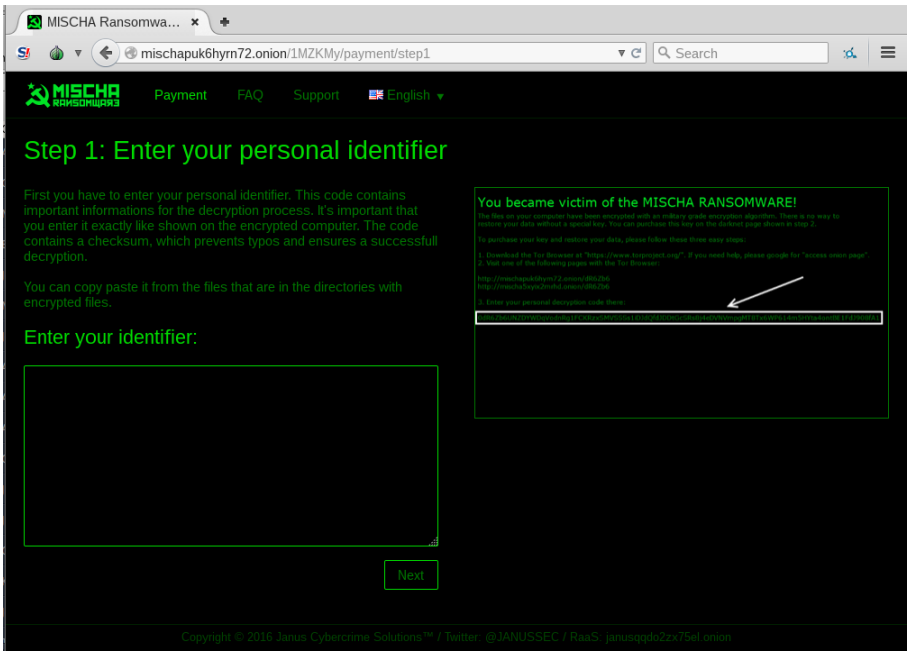
شکل ۱۵: پورتال قربانی در سایت Petya



شکل ۱۶: پورتال قربانی در سایت Petya



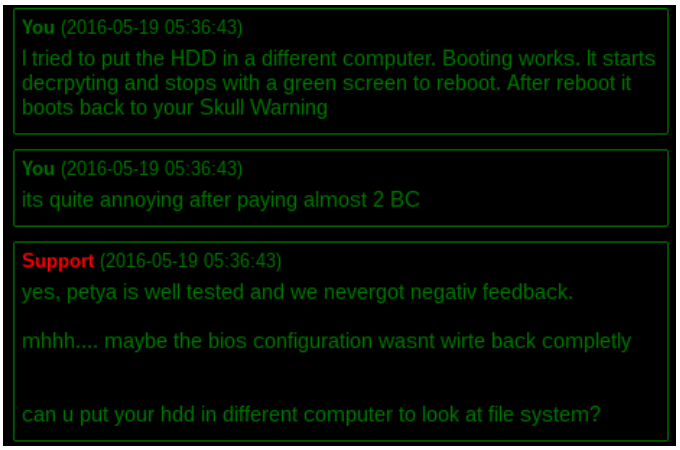
شکل ۱۷: پورتال قربانی در سایت Petya



شکل ۱۸: پورتال قربانی در سایت Mischa

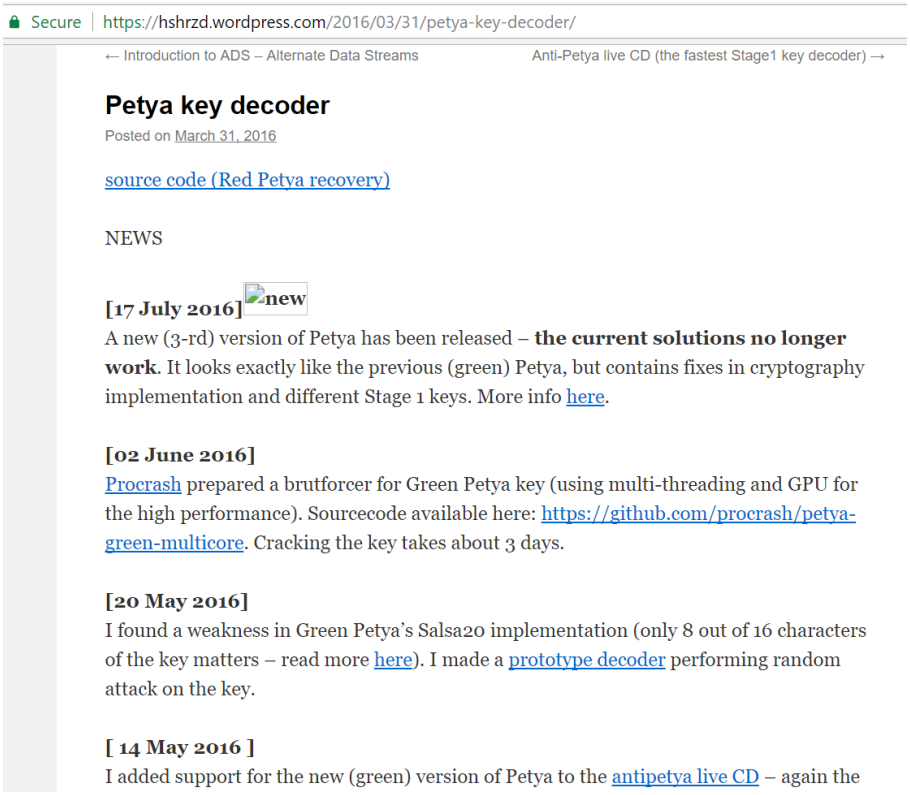
اشکالات نرم‌افزاری

نسخه‌های ابتدایی باج‌افزار Petya دارای اشکالاتی بود که حتی در صورت در اختیار داشتن کلید رمزگشایی، فرآیند بازگردانی با اشکال روبرو می‌شد.



شکل ۱۹: گزارش وجود اشکال در زمان رمزگشایی توسط یکی از قربانیان Petya

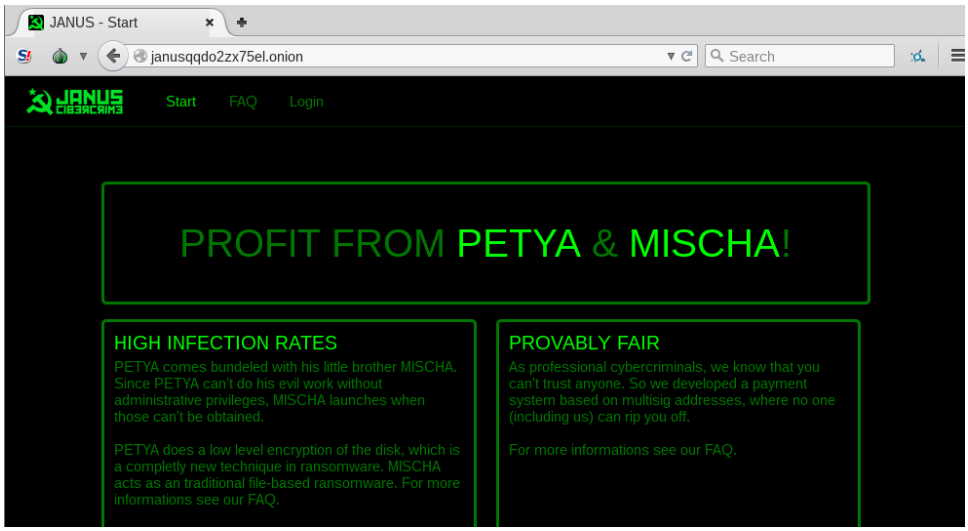
همچنین پیاده‌سازی فرآیند رمزگذاری در این باج‌افزار دارای اشکالاتی بود که محققان را قادر به ارائه ابزارهایی برای رمزگشایی Petya کرد. این اشکالات در نسخه‌های جدیدتر این باج‌افزار ترمیم شدند.



شکل ۲۰: ابزارهای رمزگشایی باج‌افزار Petya

نتیجه‌گیری

Petya را می‌توان آغازگر نوع جدیدی از باج‌افزارها دانست. گردانندگان Petya و Mischa یک طرح مشارکت نیز به راه انداخته‌اند و با جذب دیگر تبهکاران سایبری و شراکت با آنها بر سر باج‌های به دست آمده، از آنها برای توزیع هر چه بیشتر و گسترده‌تر این دو باج‌افزار کمک می گیرند. بدین ترتیب باید در انتظار آلودگی‌های بیشتر به این دو باج‌افزار بود.

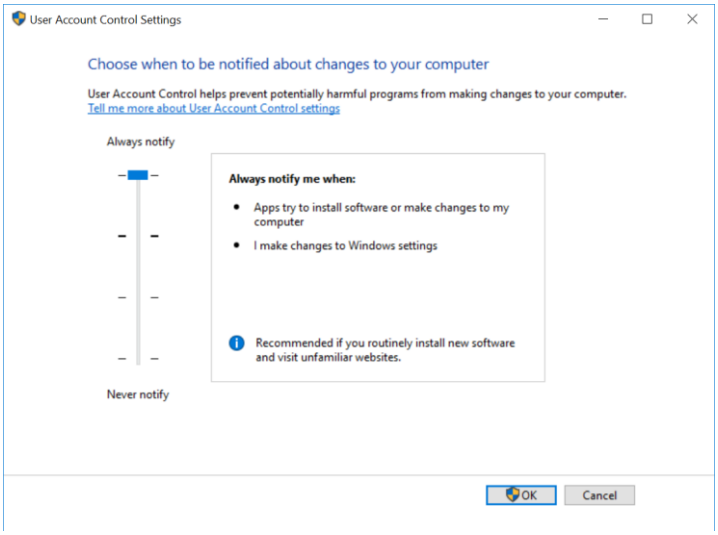


شکل ۲۱: ارائه باج‌افزارهای Petya و Mischa به‌صورت باج‌افزار به‌عنوان سرویس توسط گردانندگان این باج‌افزارها

رعایت موارد زیر آسان‌ترین و ارزان‌ترین راه برای مقابله با باج‌افزارها است.

۱ اطیمنان از فعال بودن بخش User Account Control

بخش User Account Control Settings در حالت Always notify me قرار داده شده و به پیام‌های این بخش توجه شود.

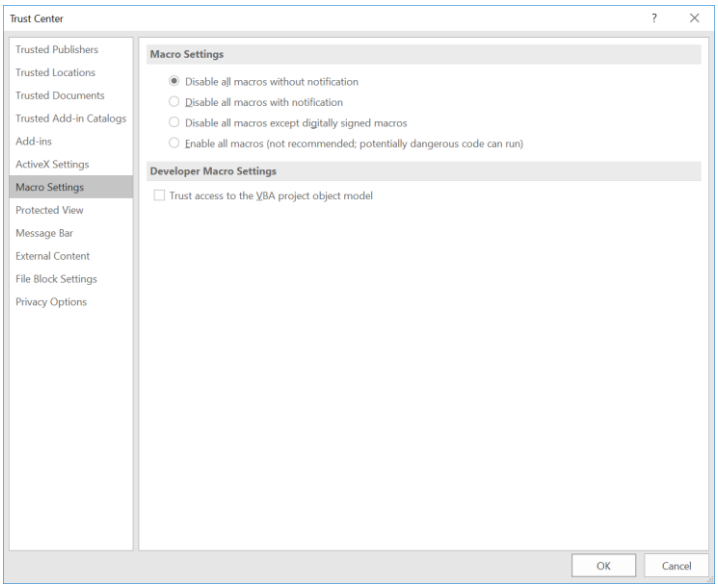


شکل ۲۲: تنظیمات بخش User Account Control

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

۲ 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 ۲۳: 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.

۳ 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.

٤ به روز 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.

پیوست

پسوندهای هدف Mischa

txt doc docx docm odt ods odp odf odc odm odb rtf xlsm xlsb xlk xls xlsx pps ppt pptm pptx pub epub pdf jpg jpeg frm wdb ldf myi vmx xml xsl wps cmf vbs accdb ini cdr svg conf cfg config wb2 msg azw azw1 azw3 azw4 lit apnx mobi p12 p7b p7c pfx pem cer key der mdb htm html class java asp aspx cgi cpp php jsp bak dat pst eml xps sqllite sql jar wpd crt csv prf cnf indd number pages lnk dcu pas dfm directory pbk yml dtd rll lib cert cat inf mui props idl result localstorage ost default json sqlite log bat ico dll exe x3f srw pef raf orf nrw nef mrw mef kdc dcr crw eip fff iiq k25 crwl bay sr2 ari srf arw cr2 raw rwl rw2 r3d 3fr eps pdd dng dxf dwg psd png jpe bmp gif tiff gfx jge tga jfif emf 3dm 3ds max obj a2c dds pspimage yuv 3g2 3gp asf asx mpg mpeg avi mov flv wma wmv ogg swf ptx ape aif wav ram m3u movie mp1 mp2 mp3 mp4 mp4v mpa mpe mpv2 rpf vlc m4a aac aa3 amr mkv dvd mts vob 3ga m4v srt aepx camproj dash zip rar gzip vmdk mdf iso bin cue dbf erf dmg toast vcd ccd disc nrg nri cdi

منابع

- http://newsroom.shabakeh.net/17039/petya-ransomware-encrypts-mbr.html
- http://newsroom.shabakeh.net/17512/chimera-decryption-keys-leaked-by-rival-gang.html
- http://newsroom.shabakeh.net/18124/petya-goldeneye.html
- https://nakedsecurity.sophos.com/2016/04/04/new-ransomware-with-an-old-trick-petya-parties-like-its-1989
- https://nakedsecurity.sophos.com/2016/04/12/petya-ransomware-decryption-tool-sets-your-files-free
- https://en.wikipedia.org/wiki/Salsa20
- https://www.bleepingcomputer.com/news/security/petya-ransomware-skips-the-files-and-encrypts-your-hard-drive-instead
- https://www.bleepingcomputer.com/news/security/petya-ransomwares-encryption-defeated-and-password-generator-released
- https://blog.fortinet.com/2017/02/01/ransomware-and-the-boot-process
- https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/
- https://blog.malwarebytes.com/threat-analysis/2016/05/petya-and-mischa-ransomware-duet-p1
- https://blog.malwarebytes.com/threat-analysis/2016/06/petya-and-mischa-ransomware-duet-p2
- https://blog.malwarebytes.com/threat-analysis/2016/12/goldeneye-ransomware-the-petyamischa-combo-rebranded
- https://blog.malwarebytes.com/threat-analysis/2016/04/recovery-from-petya-ransomware
- https://blog.malwarebytes.com/threat-analysis/2016/07/third-time-unlucky-improved-petya-is-out

شبکه گستر

شرکت مهندسی شبـکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولیـن شـرکت ایـرانـی است کـه در زمینه نرم‌افزارهای ضـدویـروس فعـالیت تخصصی و متمـرکـزی را آغـاز کـرد. در ابتـدا، همکـاری مشتـرکی بیـن شرکت مهندسی شبـکه گستـر 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، بـه تـدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سـال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمـاینـدگان بیـن‌المللی فعـالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شـرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سـال ۱۳۸۴ شـرکت مهندسی شبـکه گستر مـوفـق بـه کسب نـمـایـنـدگی رسمـی و انحصـاری شـرکت آلمانی Astaro، سـازنـده محصولات "مـدیریت یکپـارچـه تهـدیـدات" (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.

CSQ
ISO 9001:2008
Cert No 9150.C528

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