بررسی و تحلیل باج‌افزار

PETYA

شبکه گستر
شرکت مهندسی شبکه گستر

عنوان سند: بررسی و تحلیل باج‌افزار Petya

شناسه سند: SPT-A-0138-00

تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

آخرین بازنگری: ۷ تیر ۱۳۹۶

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.

در ششم تیر ماه ۱۳۹۶، نسخه جدیدی از Petya با بهره‌جویی از آسیب‌پذیری بخش SMB و بکارگیری چندین روش اجرای از راه دور کد، خاصیت کرم گونه به خود گرفت و در در عرض چند ساعت سازمان‌ها و شرکت‌های متعددی را، ابتدا در اوکراین و سپس در کشورهای دیگر عمدتاً در اروپا به خود آلوده کرد. هر چند که یکی از شرکت‌های ضدویروس بر این باور است که باج‌افزار مذکور بدافزاری متفاوت و مستقل از Petya بوده و بر همین اساس آن را NotPetya نامگذاری کرده است.

با توجه به تعطیلی ششم تیر ماه در ایران بیم آن می‌رود که در صورت عدم توجه به موقع کاربران و راهبران شبکه به راهکارهای پیشگیرانه بررسی شده در این گزارش، سازمان‌های ایرانی نیز به جمع قربانیان این باج‌افزار افزوده شوند.

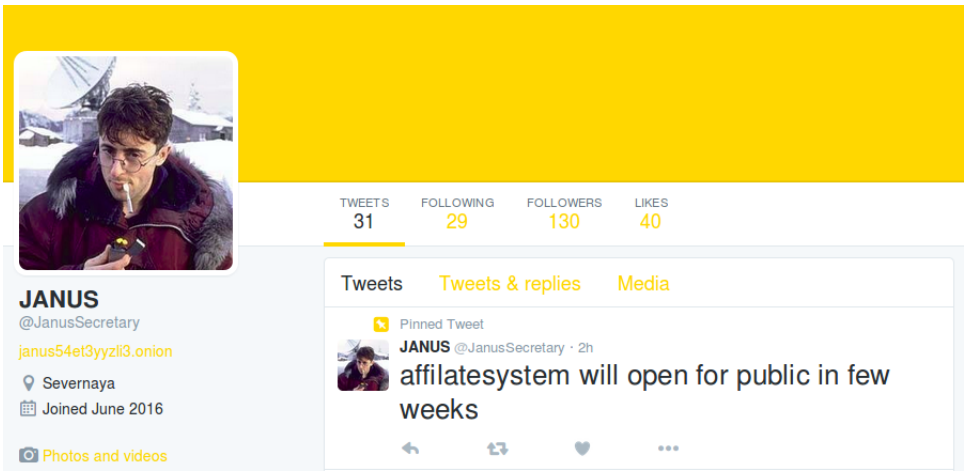
در این گزارش عملکرد نسخه‌های مختلف باج‌افزار Petya مورد بررسی و تحلیل قرار گرفته است.

شکل ۱: آلودگی گسترده سیستم‌ها به باج‌افزار Petya در ششم تیر ماه ۹۶

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.

از آن زمان تا کنون نسخه‌های متعددی از این باج‌افزار منتشر شده است. در بسیاری از نسخه‌های Petya، پس از رمزگذاری MBR، اطلاعیه باجگیری[۳] در قالب یک تصویر جمجمه که با حروف ASCII ساخته شده، نمایش داده می‌شود. 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

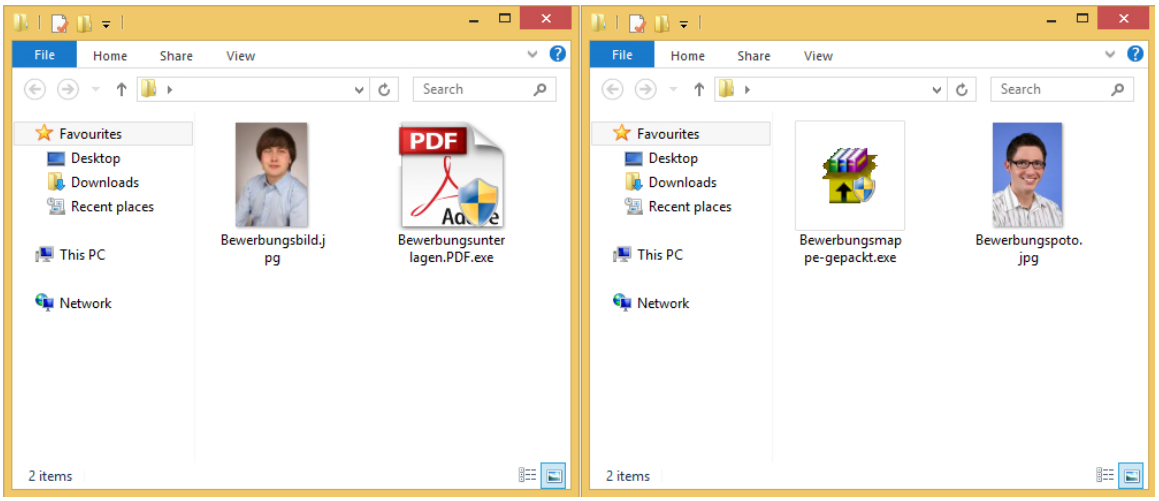
روش انتشار

تا پیش از عرضه نسخه تیر ماه، اصلی‌ترین روش انتشار باج‌افزار Petya، ایمیل‌های ناخواسته و مزاحم هرزنامه[۵] – معمولاً در ظاهر درخواست استخدام – بود.

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.

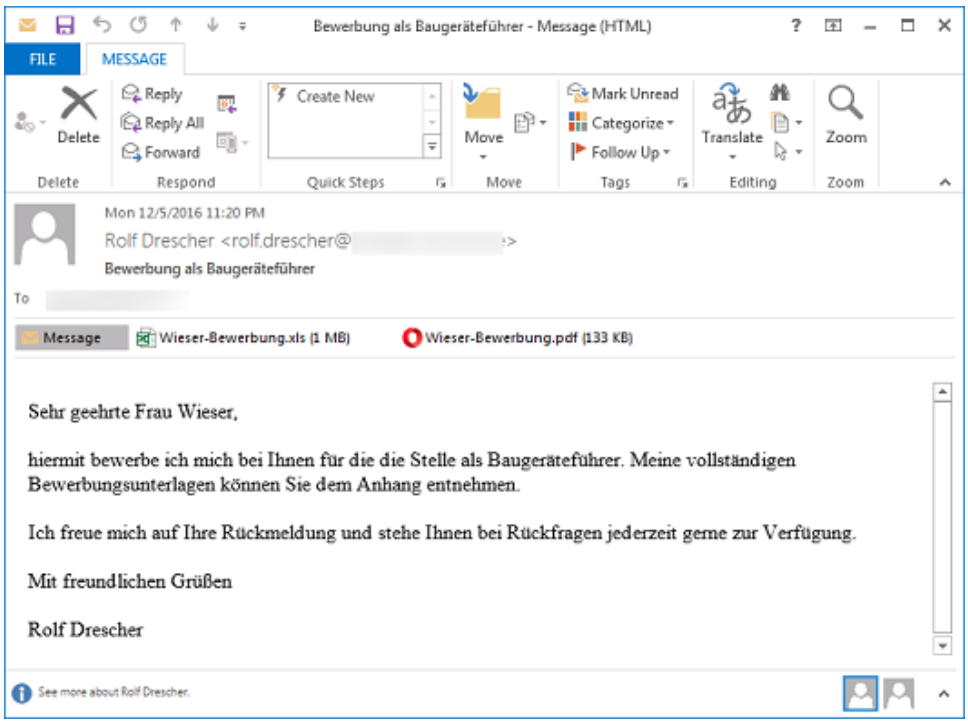
---

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 ۴: 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

اما در نسخه تیر ماه این باج‌افزار از دو روش زیر به‌منظور ورود و رخنه به سیستم‌ها بهره گرفته شده است:

- ارسال هرزنامه‌هایی با پیوست فایل Excel که در آن از یک ضعف امنیتی با شناسه CVE-2017-0199 در نرم‌افزار Office بهره‌جویی می‌شود؛ شرکت مایکروسافت این آسیب‌پذیری را در ۲۲ فروردین ۱۳۹۶ ترمیم کرده بود.
- ارسال نسخه آلوده شده‌ای از نرم‌افزار M.E.Doc در قالب فایل به‌روز رسانی به سازمان‌های استفاده کننده این نرم‌افزار؛ برای این منظور مهاجم اقدام به هک سرور مرکزی M.E.Doc و تزریق کد مخرب خود در این نرم‌افزار کرده بود. سازمان‌های متعدد در صنایع مختلف در کشور اوکراین از نرم‌افزار M.E.Doc استفاده می‌کنند.

همچنین نسخه تیر ماه این باج‌افزار قابلیت کرم[۱۱] گونه نیز داشته و قادر است از راه‌های مختلف به‌سرعت در سطح شبکه منتشر شود. این نسخه مجهز به بهره‌جوی[۱۲] موسوم به EternalBlue است. ماجرای این بهره‌جو به حدود دو ماه 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 دارد – توسط گروه Shadow Brokers بر روی اینترنت به اشتراک گذاشته شدند. یک ماه پیش از درز این اطلاعات، شرکت مایکروسافت اقدام به عرضه اصلاحیه‌ای با شناسه MS17-010 به‌منظور ترمیم آسیب‌پذیری مذکور نموده بود.

باج افزار WannaCry که تهاجمی‌ترین باج‌افزار تاریخ نام گرفته است از ۲۲ اردیبهشت ماه با بکارگیری بهره‌جوی EternalBlue بطور گسترده در سطح جهان منتشر شده است.

نسخه تیر ماه Petya پس از رخنه به دستگاه، نشانی‌های IP تخصیص داده شده به تمامی کارت‌های شبکه، اسامی سرورها – از طریق NetBIOS – و فهرست نشانی‌های IP تخصیص داده شده از سوی DHCP را شناسایی کرده و در ادامه با روش‌های زیر اقدام به آلوده‌سازی سایر دستگاه‌های شبکه به صورت از راه دور می‌کند:

- بکارگیری بهره‌جوی EternalBlue و پویش درگاه‌های 445 و 139 به‌منظور شناسایی دستگاه‌های آسیب‌پذیر
- بررسی پروسه مجاز lsass.exe به منظور بکارگیری اطلاعات اصالت‌سنجی[۱۳] موسوم به Current User Windows Token در یکی از دو ابزار مجاز زیر:

۱. ابزار Psexec در قالب فرمان زیر:

```
C:\WINDOWS\dllhost.dat \\w.x.y.z -accepteula -s -d
C:\Windows\System32\rundll32.exe C:\Windows\perfc.dat,#1
```

۲. بخش Windows Management Instrumentation – به اختصار WMI – در قالب فرمان زیر:

```
Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process
call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1"
```

منظور از "w.x.y.z" در بندهای ۱ و ۲ نشانی IP است.

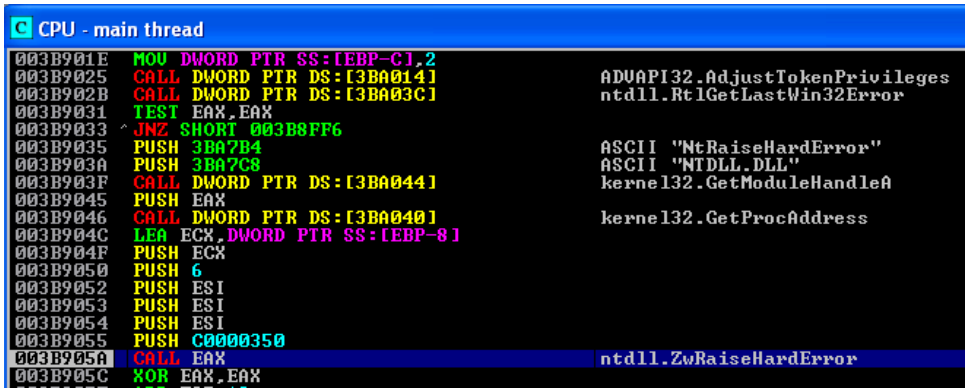
بدیهی است چنانچه کاربر دستگاه آلوده شده حق دسترسی بالایی همچون Domain Admin در سطح شبکه داشته باشد این خطر وجود خواهد داشت که دستگاه‌های دیگر شبکه نیز به باج‌افزار Petya آلوده شوند.

---

[۱۱] Worm
[۱۲] Exploit
[۱۳] Credential

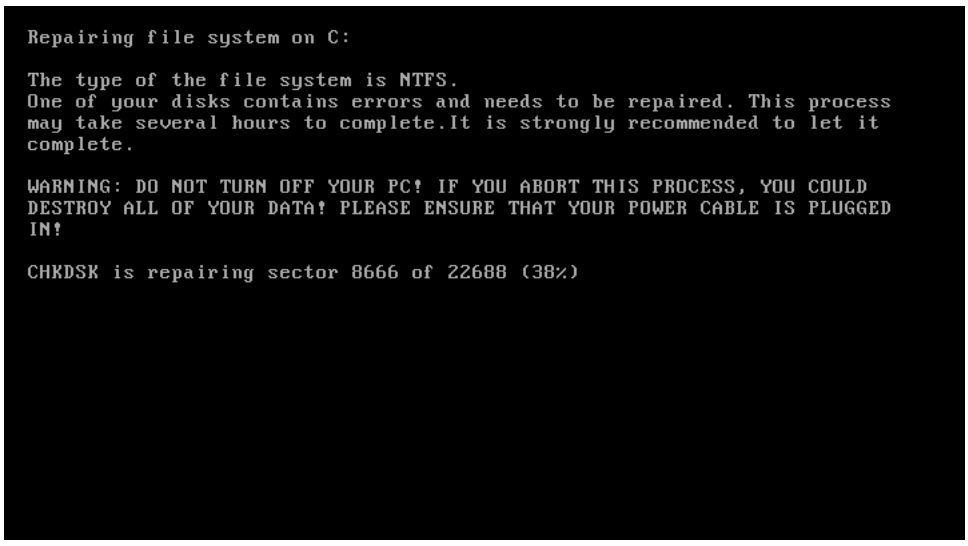
رمزنگاری

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[۱۴] NtRaiseHardError یک خطای حاد سیستمی ایجاد شده و در نتیجه آن دستگاه راه‌اندازی مجدد[۱۵] 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.



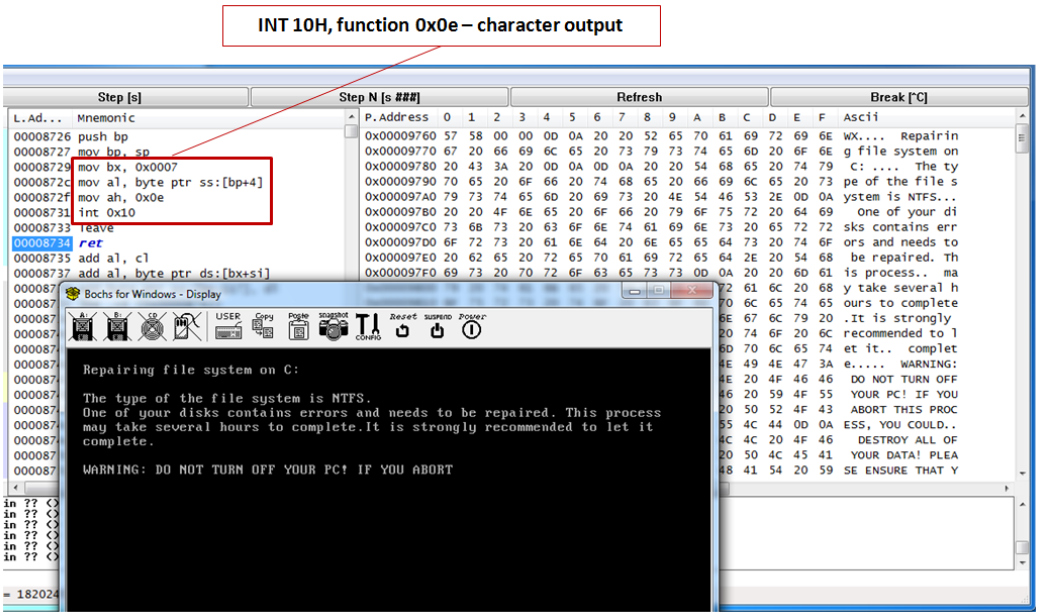
شکل ۶: پیام دروغین CHKDSK

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 درج می‌کند. (شکل ۷)

---

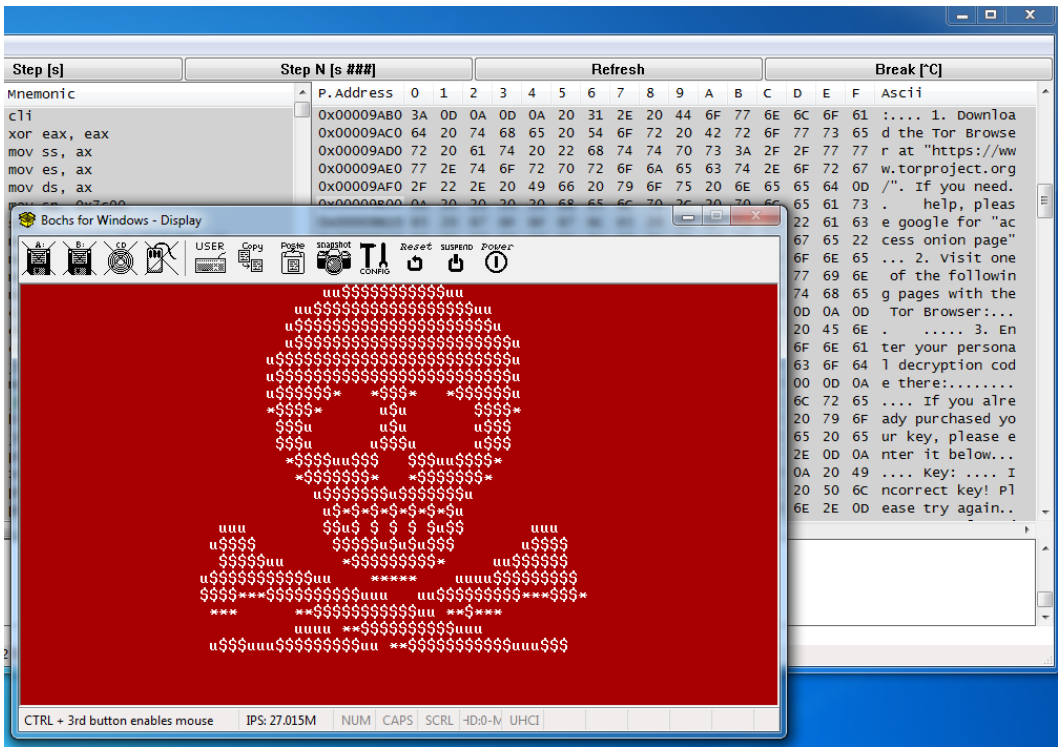
[۱۴] API

[۱۵] Reboot

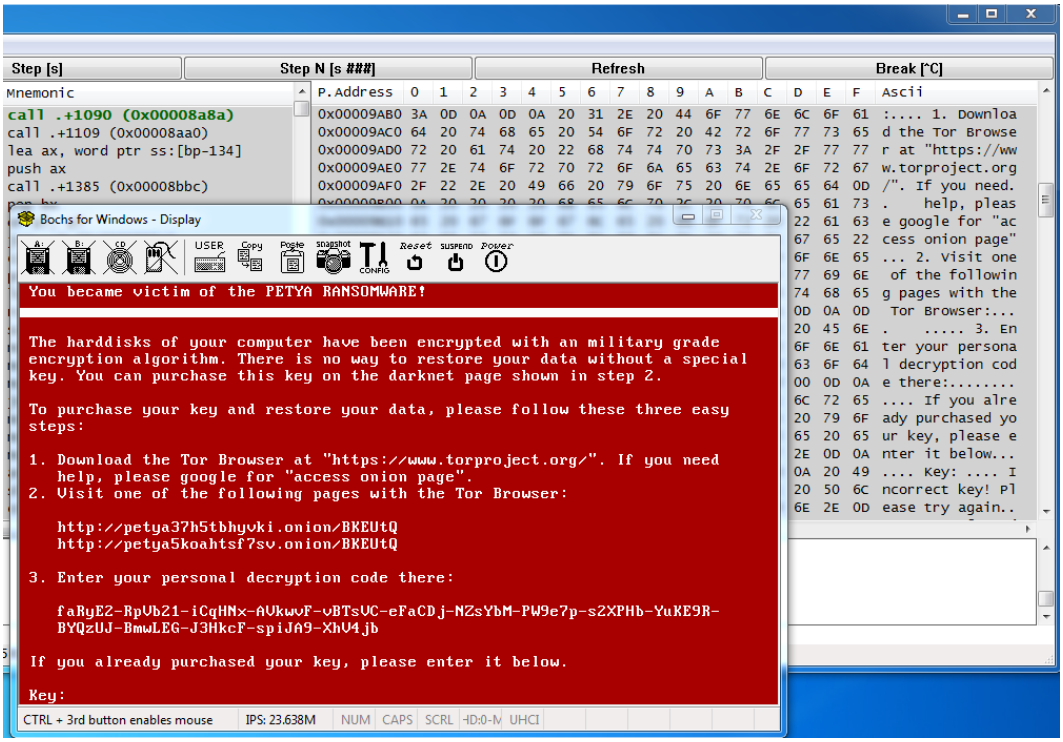


شکل ۷: فراخوانی تابع INT 10H

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.

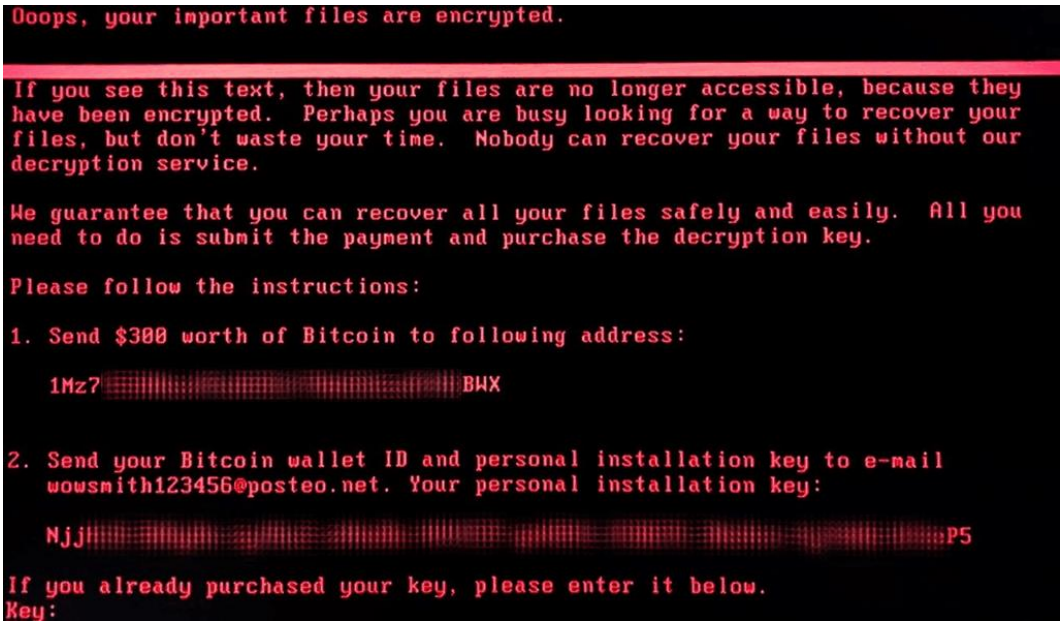


شکل ۸: تصویر جمجمه Petya



شکل ۹: اطلاعیه باج‌گیری Petya

همچنین شکل ۱۰ نمونه‌ای از اطلاعیه باج‌گیری نسخه تیر ماه Petya را نمایش می‌دهد. در این نسخه از قربانی خواسته می‌شود مبلغ ۳۰۰ دلار به بیت‌کوین پرداخت شود.



شکل ۱۰: اطلاعیه باج‌گیری در نسخه تیر ماه Petya

ترکیب باج‌افزارهای Petya و Mischa

از 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.

در برخی نسخه‌ها، باج‌افزار Mischa 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

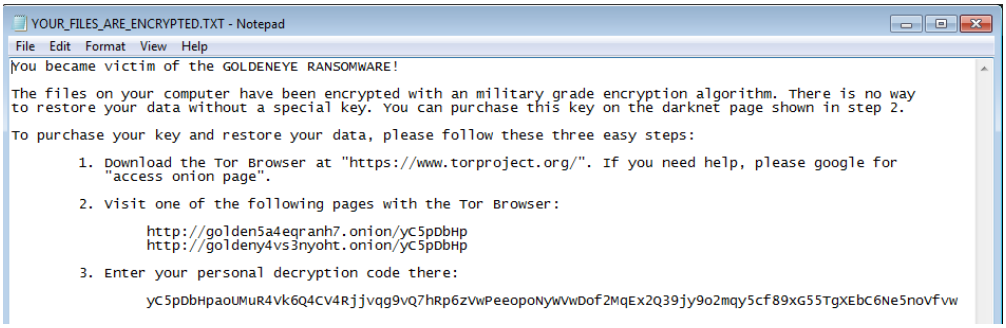
Mischa در هر پوشه‌ای که حداقل یکی از فایل‌های آن رمزنگاری شده اطلاعیه باج‌گیری را در قالب دو فایل با نام‌های YOUR_FILES_ARE_ENCRYPTED.TXT و YOUR_FILES_ARE_ENCRYPTED.HTML کپی می‌کند.

Name	Date modified	Type	Size
square1 - Copy - Copy.bmp.7QzX	2016-05-12 18:47	7QZX File	141 KB
square1 - Copy.bmp.7QzX	2016-05-12 18:47	7QZX File	141 KB
square1.bmp.7QzX	2016-05-12 18:47	7QZX File	141 KB
YOUR_FILES_ARE_ENCRYPTED.HTML	2016-05-12 18:47	Firefox HTML Doc...	2 KB
YOUR_FILES_ARE_ENCRYPTED.TXT	2016-05-12 18:47	Text Document	1 KB

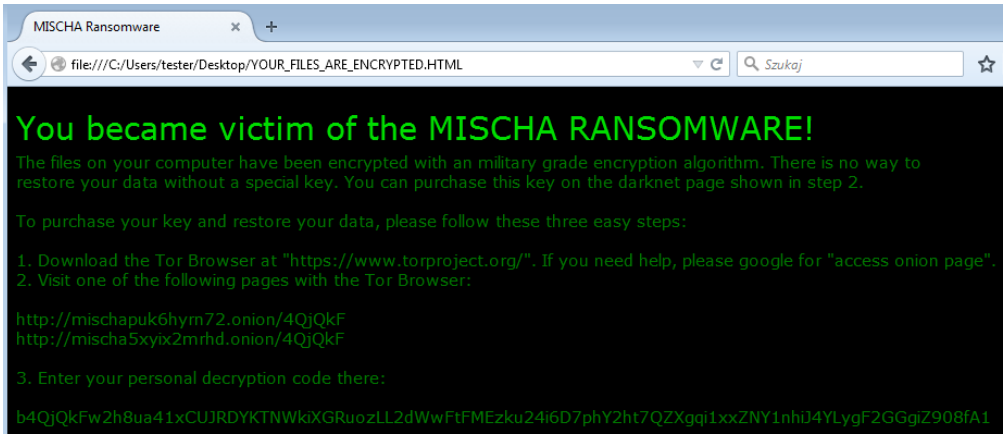
شکل ۱۱: فایل‌های رمزگذاری شده در یکی از نسخه‌های Petya

Name	Date	Type	Size
dump.bin.yC5pDbHp	2016-12-07 18:06	YC5PDBHP File	3 KB
main.cpp.yC5pDbHp	2016-12-07 18:05	YC5PDBHP File	4 KB
square1 (another copy).bmp.yC5pDbHp	2016-05-26 23:58	YC5PDBHP File	141 KB
square1 (copy).bmp.yC5pDbHp	2016-05-26 23:58	YC5PDBHP File	141 KB
square1.bmp.yC5pDbHp	2016-05-26 23:58	YC5PDBHP File	141 KB
wrapper.h.yC5pDbHp	2016-12-07 18:05	YC5PDBHP File	2 KB

شکل ۱۲: فایل‌های رمزگذاری شده در یکی از نسخه‌های Petya



شکل ۱۳: اطلاعیه باج‌گیری در یکی از نسخه‌های Petya



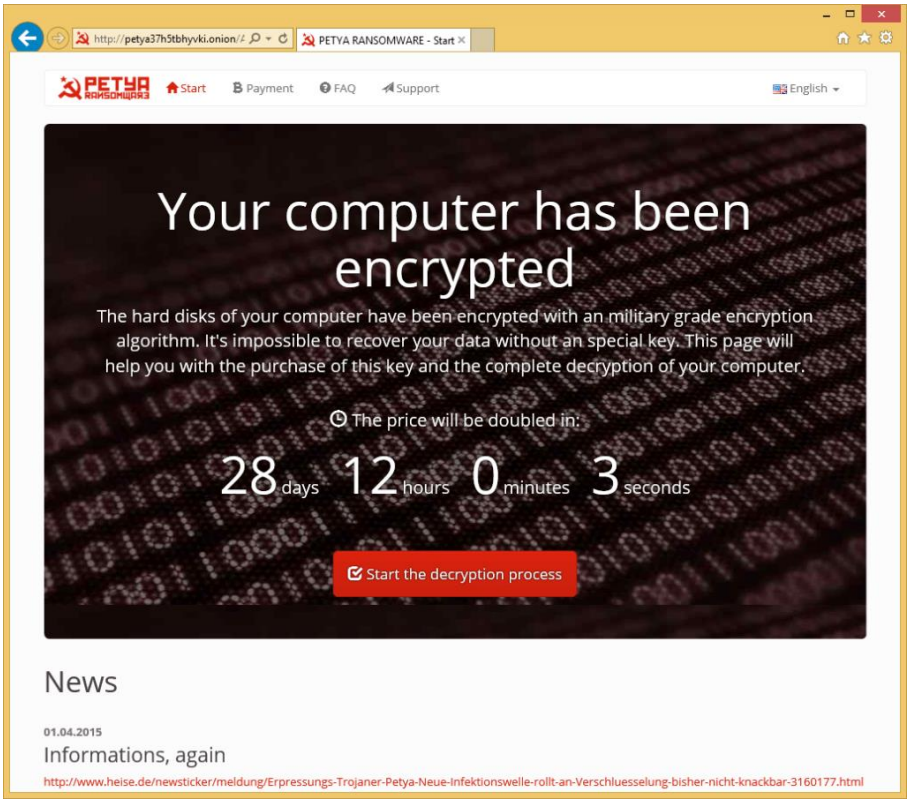
شکل ۱۴: اطلاعیه باج‌گیری در یکی از نسخه‌های Petya

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

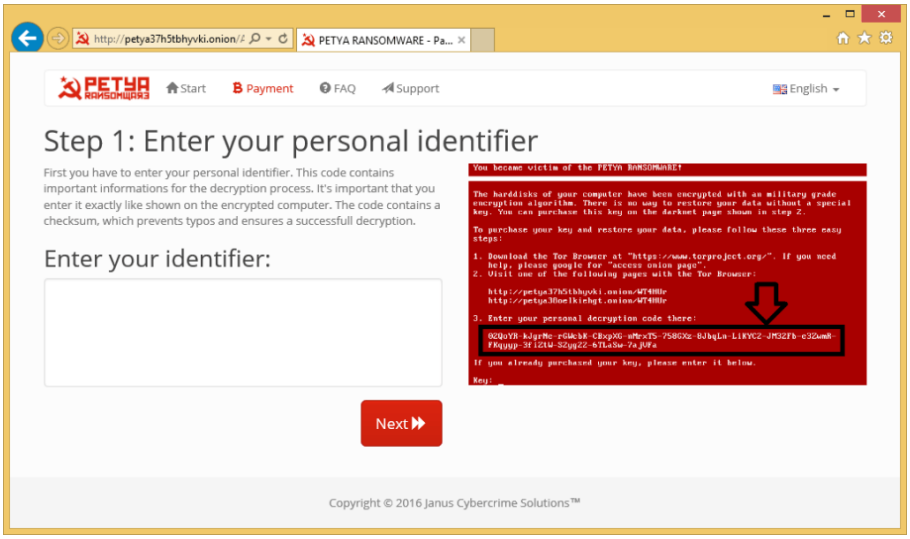
پرداخت باج

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.

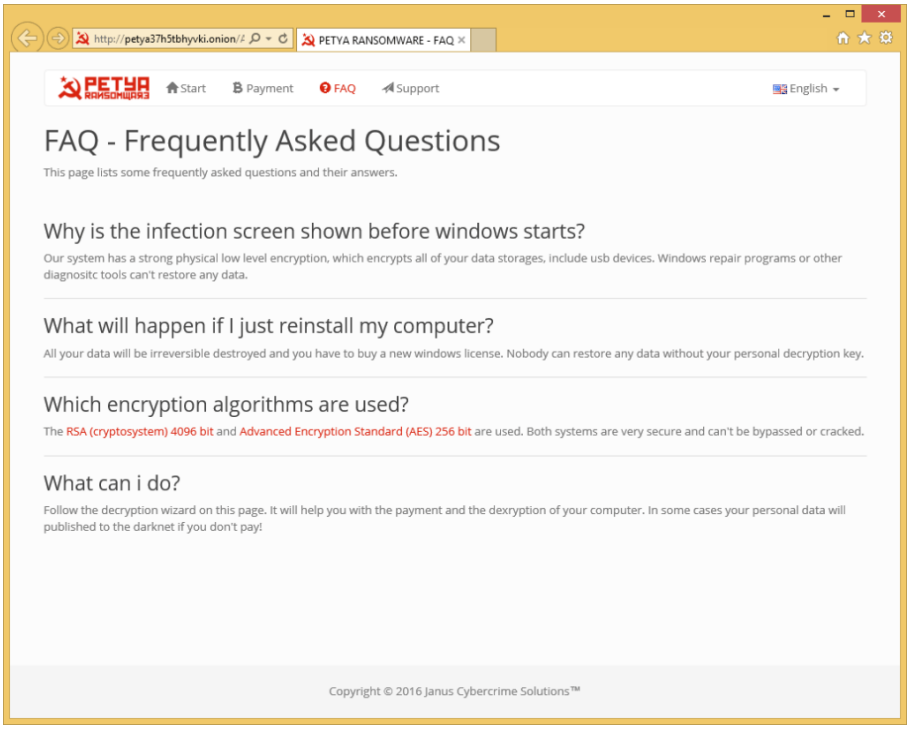
در برخی نسخه های Petya در پیام باج‌گیری از کاربر خواسته می‌شود که به سایتی در شبکه اینترنتی ناشناس TOR مراجعه کرده و شماره منحصربه‌فردی را که نشان‌دهنده کامپیوتر کاربر به باجگیران است، وارد کند.



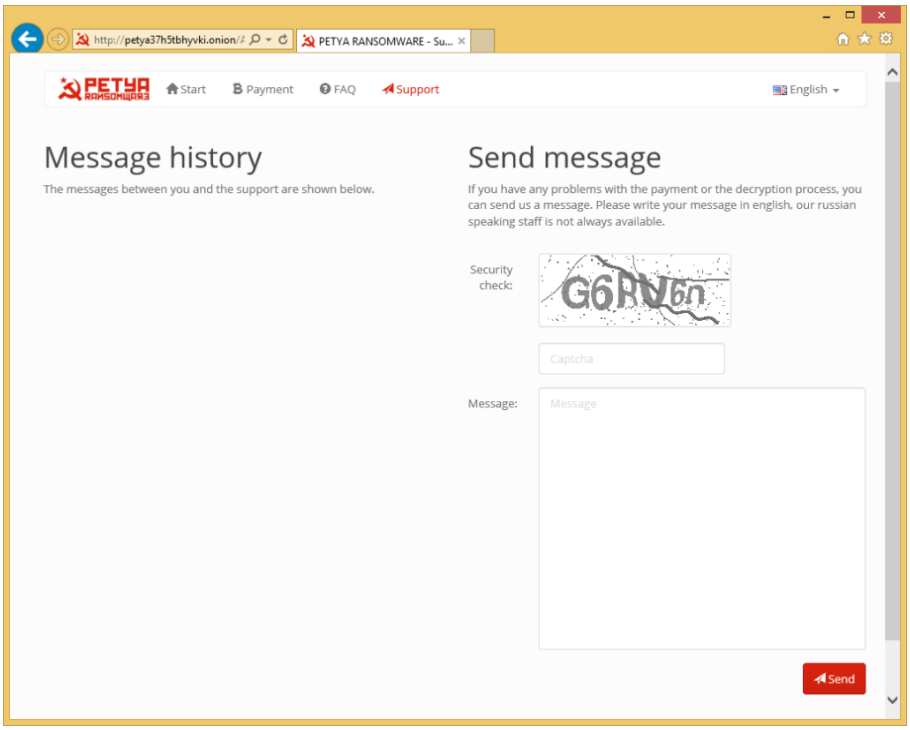
شکل ۱۵: پورتال قربانی در سایت Petya



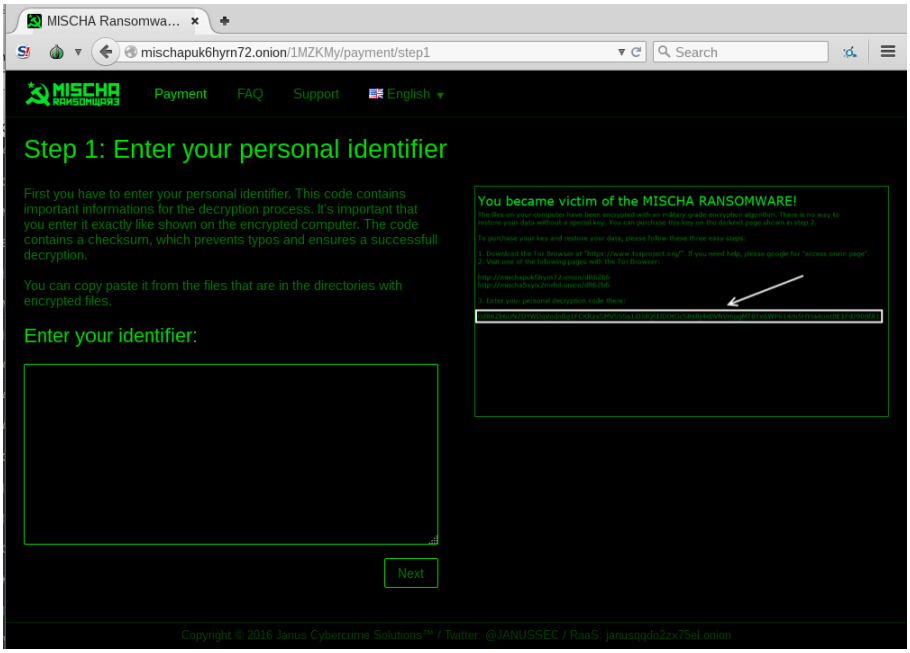
شکل ۱۶: پورتال قربانی در سایت Petya



شکل ۱۷: پورتال قربانی در سایت Petya



شکل ۱۸: پورتال قربانی در سایت Petya



شکل ۱۹: پورتال قربانی در سایت Mischa

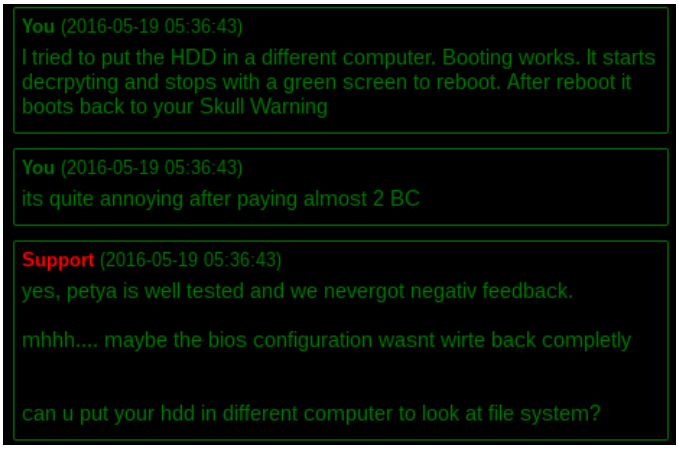
در اطلاعیه باج‌گیری نسخه تیر ماه Petya از قربانی خواسته می‌شود که پس از پرداخت باج موضوع از طریق ایمیل wowsmith123456@posteo[.]net به اطلاع نویسنده باج‌افزار رسانده شود.

این در حالی است که پس از انتشار گسترده Petya، مدیران posteo.net اقدام به مسدود نمودن این حساب ایمیل کرده‌اند. بنابراین حتی در صورت پرداخت باج حداقل در زمان نگارش این گزارش امکان بازگردانی فایل‌ها فراهم نخواهد بود.

شکل ۲۰: اعلام مسدود شدن حساب ایمیل درج شده در اطلاعیه باج‌گیری

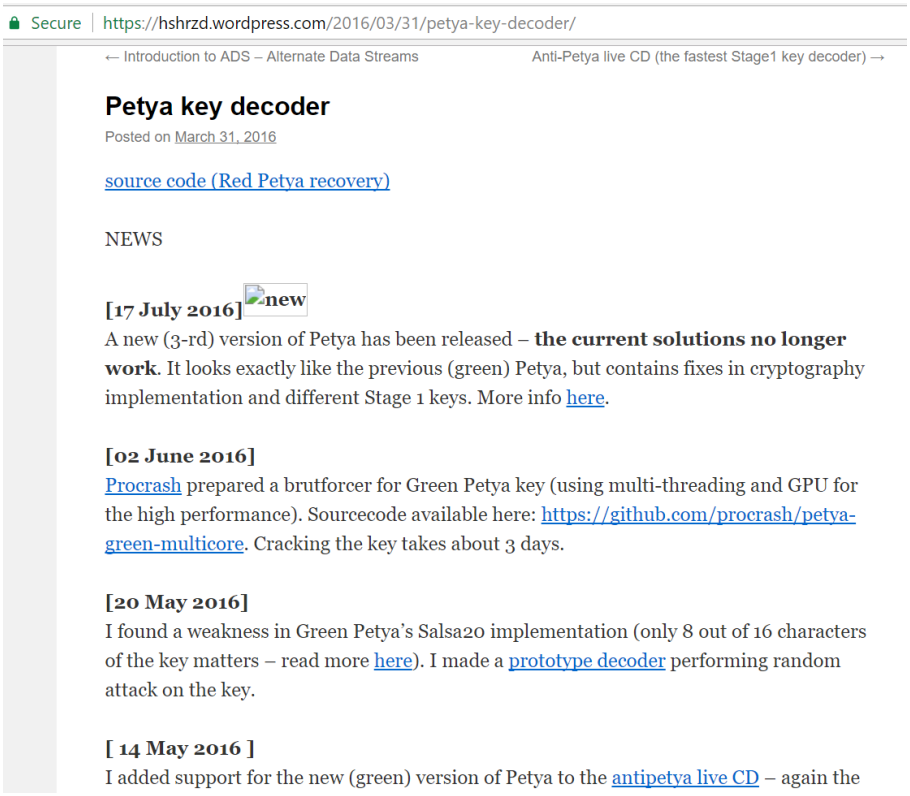
اشکالات نرم‌افزاری

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



شکل ۲۱: 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.

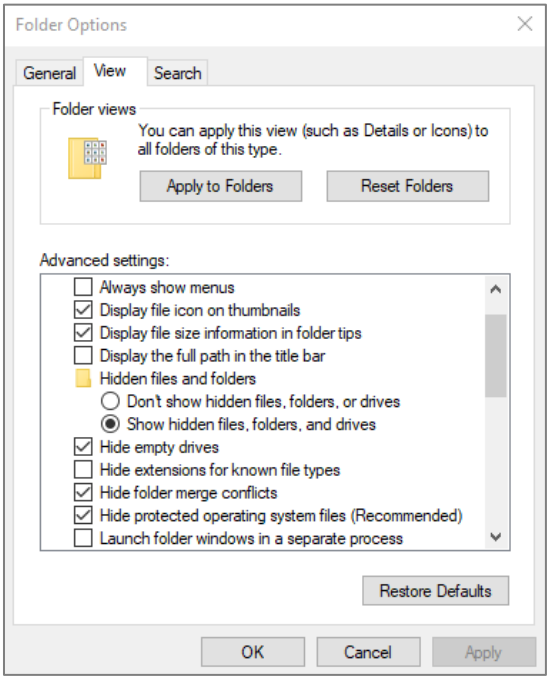


شکل ۲۲: ابزارهای رمزگشایی باج‌افزار Petya

واکسن تیر ماه!

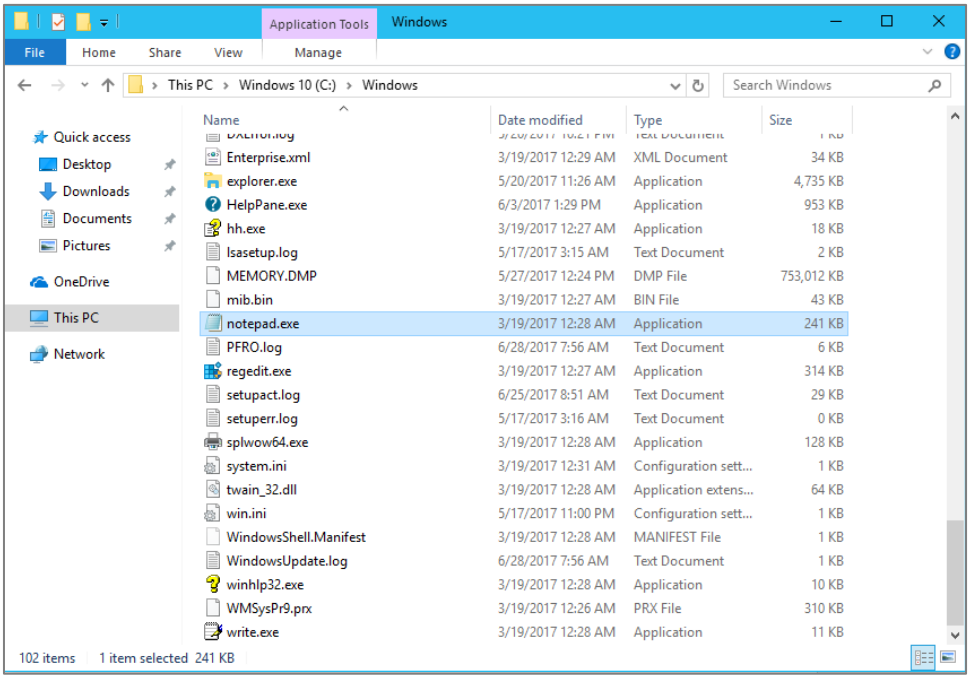
بر اساس روش انتشار از راه دور نسخه تیر ماه Petya، یکی از محققان راهکاری را در خصوص پیشگیری از آلودگی به این نسخه ارائه کرده است. برای این منظور مراحل زیر باید دنبال شود:

۱. در سربرگ View در بخش Folder Options گزینه Hide extensions for known file types غیرفعال شود.



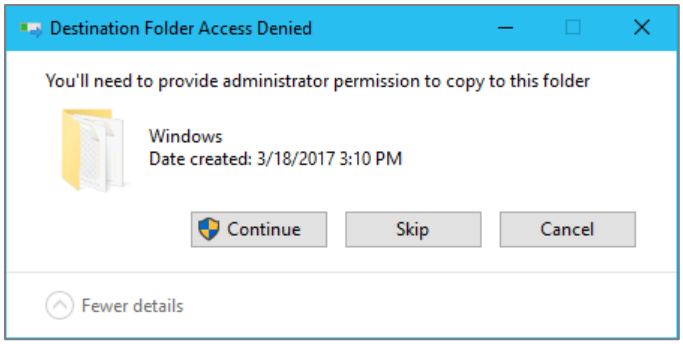
شکل ۲۳: پنجره Folder Options

۲. در مرحله بعد وارد پوشه C:\Windows شده و برنامه notepad.exe انتخاب شود.



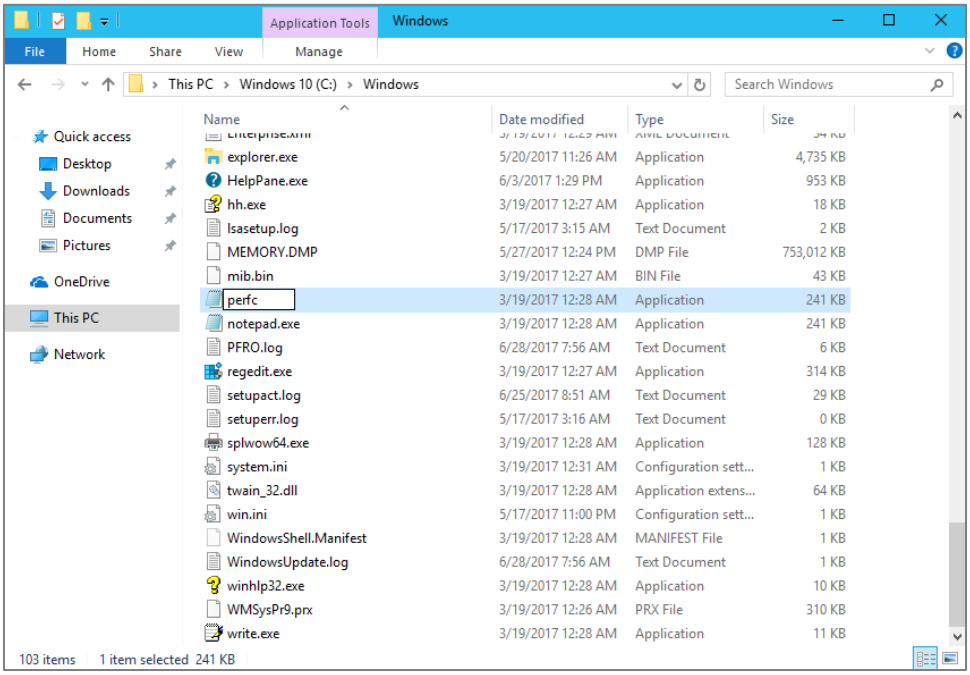
شکل ۲۴: فایل notepad.exe در پوشه Windows

۳. کلیدهای CTR+c برای کپی و CTR+v برای ذخیره نسخه ای از آن در همان مسیر فشرده شوند. در زمان ذخیره شدن یک پیام مبنی بر مجوز دادن نمایش داده می‌شود.



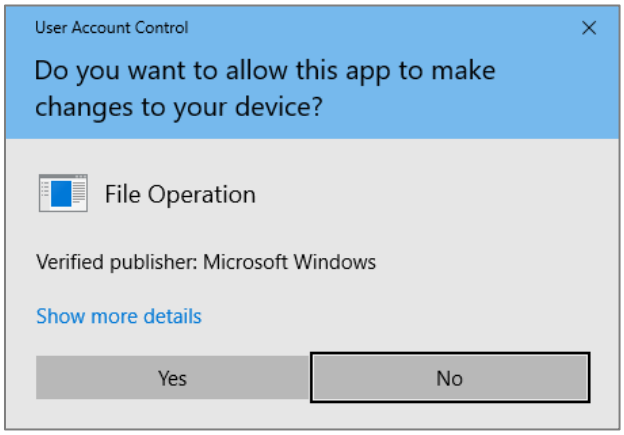
شکل ۲۵: پنجره هشدار کپی فایل در پوشه Windows

۴. با کلیک بر روی دگمه Continue فایلی با نام notepad - Copy.exe ساخته می‌شود. نام فایل مذکور به perfc تغییر داده شود.



شکل ۲۶: تغییر نام فایل کپی شده

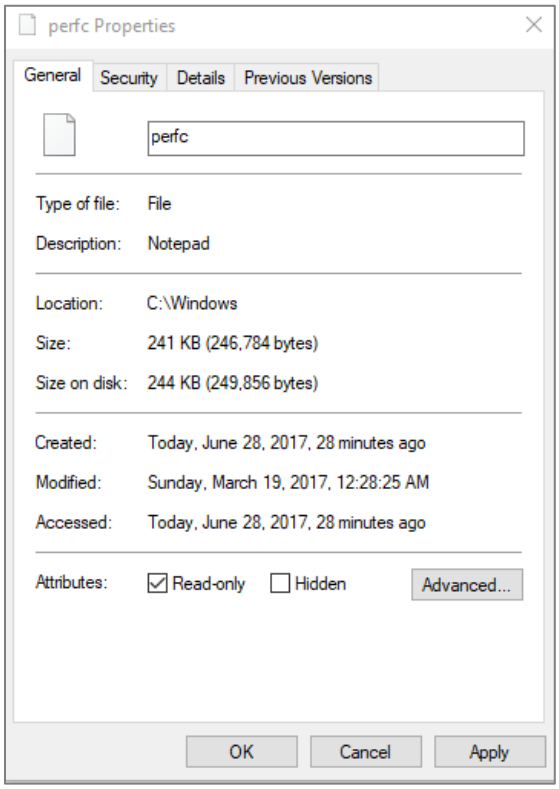
۵. پس از تغییر نام فایل به perfc، کلید Enter فشرده شود. در صورت نمایش پنجره UAC نیز بر روی دگمه Yes کلیک شود.



شکل ۲۷: پنجره UAC

۶. بر روی فایل perfc ایجاد شده کلیک راست شده و گزینه Properties انتخاب شود.

۷. در پنجره باز شده گزینه Read-only انتخاب شود.

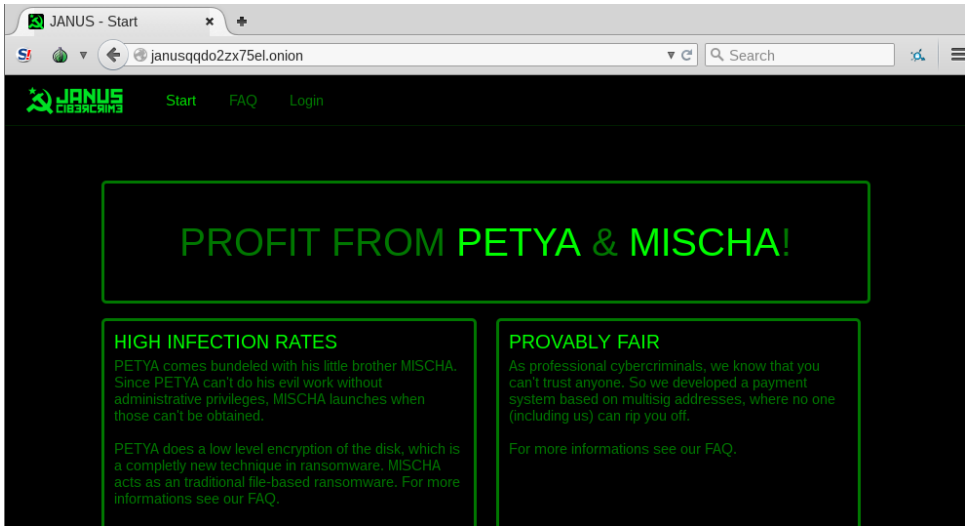


شکل ۲۸: فعال کردن ویژگی "فقط خواندنی" فایل perfc

۸. در مرحله آخر بر روی دگمه Apply و سپس OK کلیک شود.

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 می‌گیرند. اکنون با افزوده شدن قابلیت کرم گونه به این باج‌افزار باید انتظار افزایش چشمگیر آلودگی‌ها به این باج‌افزار را داشت.



شکل ۲۹: 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.

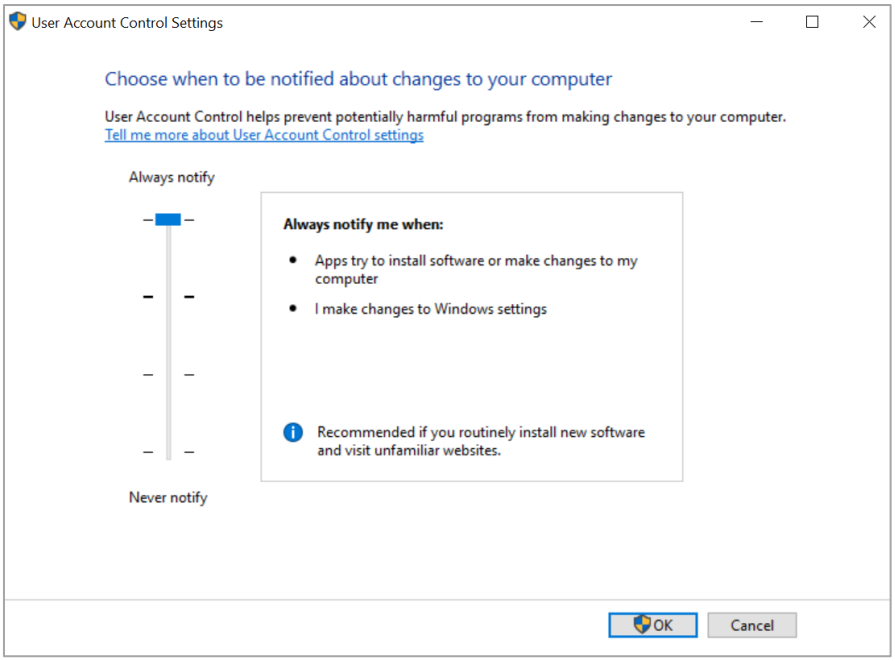
۱ تهیه نسخه پشتیبان

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 ۳۰: 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

در خصوص باج‌افزار Petya نصب اصلاحیه‌های زیر در زودترین زمان ممکن توصیه می‌شود:

```
Security Update for Microsoft Windows SMB Server: March 14, 2017:
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Security update for Office 2016: April 11, 2017:
https://support.microsoft.com/en-us/help/3178703/description-of-the-security-update-for-office-2016-april-11-2017
```

شایان ذکر است 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.

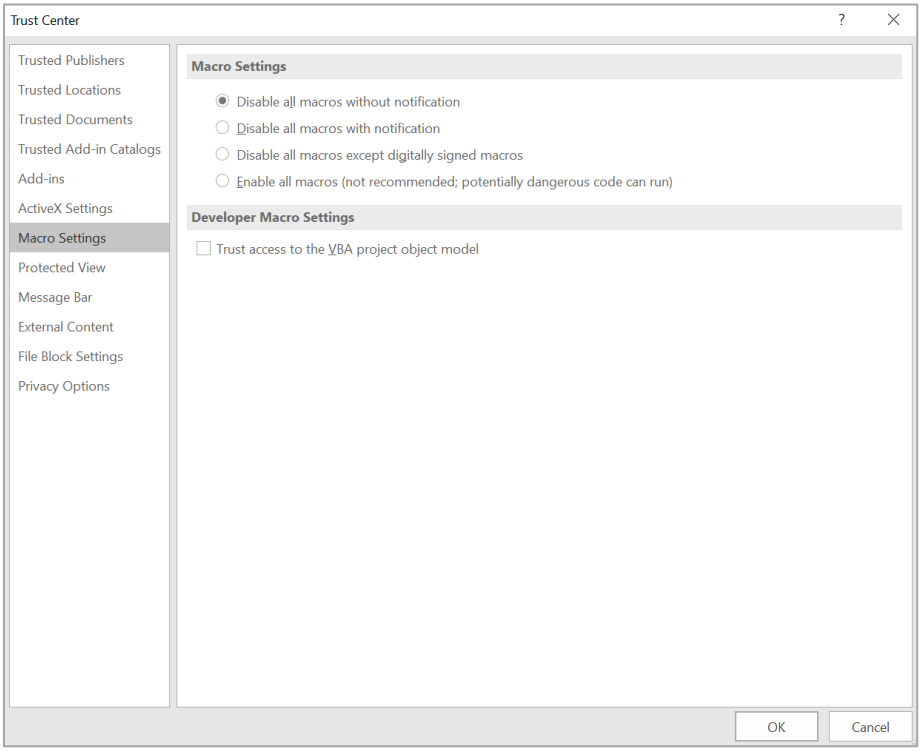
٤ استفاده از فناوری‌های حفاظتی پیشرفته

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 فناوری های ویژه و خاص برای شناسایی و مقابله با باج‌افزارهای رمزگذار هستند.

به کاربران راهکارهای McAfee توصیه می‌شود فایل به‌روزرسانی Extra DAT مربوطه را از اینجا دریافت کرده و با دنبال کردن این مراحل آن را در انباره ابزار مدیریتی McAfee ePolicy Orchestrator اضافه کنند.

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 ۳۱: 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.

۶ 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.

۷ به‌روز بودن در خصوص روش‌های جدید باج‌گیران

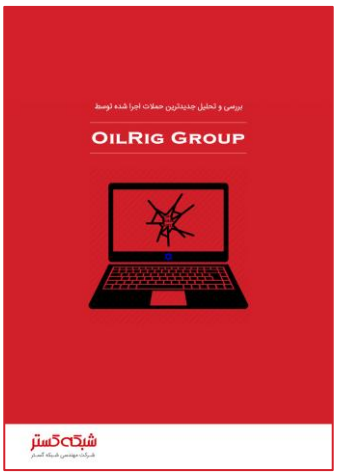
نویسندگان باج‌افزار دائماً در حال تغییر و تکامل روش‌های خود هستند. با مرور اخبار و حضور در دوره‌های آگاهی‌رسانی شرکت مهندسی شبکه گستر، از آخرین روش‌های مورد استفاده مهاجمان آگاه شده و سیاست‌ها پیشگرانه لازم را اعمال کنید.

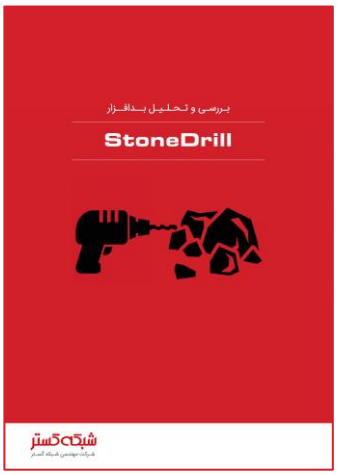
منابع

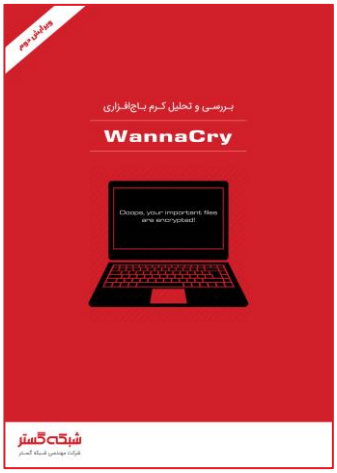
- https://blog.malwarebytes.com/threat-analysis/2016/04/recovery-from-petya-ransomware
- https://blog.malwarebytes.com/threat-analysis/2016/07/third-time-unlucky-improved-petya-is-out
- https://researchcenter.paloaltonetworks.com/2017/06/palo-alto-networks-protections-petya-ransomware
- https://blog.fortinet.com/2017/06/27/new-ransomware-follows-wannacry-exploits
- https://threatpost.com/complex-petya-like-ransomware-outbreak-worse-than-wannacry/126561
- https://posteo.de/blog/info-zur-ransomware-petrwrappetya-betroffenes-postfach-bereits-seit-mittag-gesperrt
- https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak
- https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine
- https://www.forbes.com/sites/thomasbrewster/2017/06/27/ransomware-spreads-rapidly-hitting-power-companies-banks-airlines-metro/#551fefa37abd
- http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html
- https://securelist.com/schroedingers-petya/78870
- https://www.bleepingcomputer.com/news/security/wannacry-d-j-vu-petya-ransomware-outbreak-wreaking-havoc-across-the-globe
- https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Petya-AQ.aspx
- https://kc.mcafee.com/corporate/index?page=content&id=KB89540
- https://labs.bitdefender.com/2017/06/massive-goldeneye-ransomware-campaign-slams-worldwide-users/?icid=overlaycall-pagesgoldeneye
- 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

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







شبکه گستر

با همکاری و مشارکت

کهکشان نور

سمینار کالبدشکافی باج‌افزار WannaCry

زمان: دوشنبه، ۱۲ تیر ماه ۱۳۹۶، از ساعت ۹ الی ۱۳

مکان: مؤسسه آموزشی کهکشان
تهران، یوسف‌آباد، خیابان سی‌ویکم، نبش خیابان ابن‌سینا، شماره ۱۱۱

هزینه: ۲ میلیون ریال

علاقمندان می توانند جهت شرکت در این سمینار با شماره ۰۲۱-۴۲۰۵۲ تماس حاصل نمایند.

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳
تلفن / دورنگار ۰۲۱-۴۲۰۵۲
تارنمای شرکت www.shabakeh.net
مرکز آموزش events.shabakeh.net
اتاق خبر newsroom.shabakeh.net

شبکه گستر

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 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 می‌نماید.

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 ضدویروس 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 پروژه‌های طراحی، نصب، راه‌اندازی و طولانی مدت‌ترین خدمات نگهداری 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

شبکه گستر

شـرکت 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