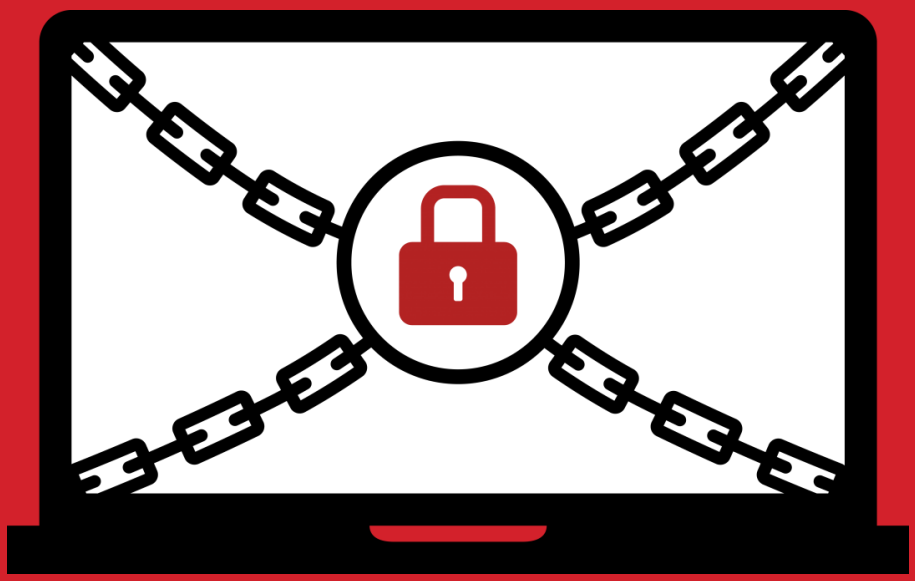
بـررسـی و تحلیل بـــاج‌افـــزار

VIRLOCK



شبکه گستر
شـرکت مهندسی شـبکه گسـتر

عنوان سند: بررسی و تحلیل باج‌افزار VirLock

شناسه سند: SPT-A-0123-00

تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

آخرین بازنگری: بهمن ۱۳۹۵

در آذر ماه ۱۳۹۳، کارشناسان شرکت امنیتی Sophos به نمونه باج‌افزاری دست یافتد که ضمن مسدود نمودن دسترسی کاربر به دستگاه، کد مخرب آلوده‌کننده به باج‌افزار را نیز به انواع فایل‌ها از جمله فایل‌های اجرایی تزریق می‌کرد. در نتیجه آن، دستگاه هر کاربری که اقدام به باز کردن این فایل‌های آلوده شده می‌کرد نیز به باج‌افزار آلوده می‌شد.

عملکرد ویروسی این باج‌افزار سبب معروف شدن آن به VirLock، VirLocker و VirRansom شد.

از دیگر ویژگی‌های خاص این باج‌افزار قابلیت چندریختی بودن آن بود که سبب تغییر درهم‌ساز هر فایل حاوی کد مخرب VirLock می‌شد. قابلیتی که ضدویروس‌های سنتی را از شناسایی این باج‌افزار ناتوان می‌کرد.

ترکیب قابلیت باج‌افزار، ویروس چندریختی و تزریق کد به فایل‌های سالم، VirLock را به بدافزاری مخرب و خطرناک تبدیل کرده که قادر است به‌سرعت در شبکه یک سازمان یا بسترهای رایانش ابری منتشر شود.

در طی این دو سال نویسنده یا نویسندگان این باج‌افزار نسخه‌های جدیدی از آن را منتشر کردند.

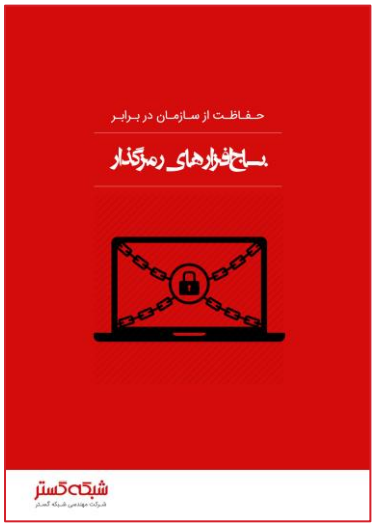
در این مقاله دو نمونه اخیر از باج‌افزار VirLock و نحوه رمزگشایی فایل‌های آلوده شده به آن بدون نیاز به پرداخت باج مورد بررسی و تحلیل قرار گرفته است.

باج‌افزار[۱] گونه‌ای بدافزار است که از راه‌های مختلف دسترسی به فایل‌های کاربر را محدود ساخته و برای دسترسی مجدد، از او درخواست باج می‌کند.

این محدودسازی ممکن است به چند روش انجام شود.

در یک روش ساده، با نمایش دائمی یک تصویر بر روی صفحه کامل نمایشگر به‌نحوی که کاربر قادر به بستن و یا باز کردن پنجره دیگری نباشد، دسترسی کاربر محدود می‌شود. در تصاویر نمایش داده شده توسط این گونه باج‌افزارها، معمولاً، این‌طور القاء می‌شود که قفل شدن کامپیوتر توسط نهادهای امنیتی و به دلیل نقض قوانین، انجام شده است.

در این حالت با پاکسازی کامپیوتر توسط ضدویروس‌ها دسترسی به اطلاعات مجدداً میسر می‌شود.



اما در روش‌های پیشرفته‌تر، ممکن است باج‌افزار اقدام به رمز کردن فایل‌های کامپیوتر کند.

در سال‌های اخیر آن دسته از باج‌افزارهایی که از طریق رمزنگاری اقدام به محدودسازی دسترسی کاربر به فایل‌ها می‌کنند موفقیت‌های بی‌مثالی را نصیب گردانندگان تبهکار خود کرده‌اند و بر اساس آمار، تعداد این نوع باج‌افزارها که به باج‌افزارهای رمزگذار[۲] معروف شده‌اند بشدت در حال افزایش است. در این نوع محدودسازی، هدف از رمز کردن، تغییر ساختار فایل است؛ به‌نحوی که تنها با داشتن کلید رمزگشایی[۳] بتوان به محتوای فایل دسترسی پیدا کرد. پیچیدگی و قدرت این کلیدها بر اساس تعداد بیت بکار رفته در ساخت کلید است. هر چه تعداد این بیت‌ها بیشتر باشد شانس یافتن آن هم دشوارتر و در تعداد بیت بالا عملاً غیرممکن می‌شود.

هر چند هرزنامه‌ها[۴] و بسته‌های بهره‌جو[۵] اصلی‌ترین ابزارهای انتشار باج‌افزارها محسوب می‌شوند اما VirLock از روش‌هایی خاص، مؤثر و مخرب به‌منظور انتشار خود بهره می‌گیرد.

VirLock، نه تنها فایل‌های قربانی را رمزنگاری می‌کند بلکه به آنها کد مخرب آلوده‌کننده به باج‌افزار نیز تزریق می‌کند. در حقیقت، هر فایل رمز شده، خود به یک VirLock تبدیل می‌شود!

انتشار این باج‌افزار معمولاً از طریق پوشه‌های اشتراکی شبکه‌ای[۶] یا ابری[۷] و همچنین حافظه‌های USB انجام می‌شود. حتی در برخی نمونه‌ها، VirLock در بدافزاری دیگر نیز ادغام شده است.

---

۱ Ransomware
۲ Crypto Ransomware
۳ Decryption Key
۴ Spam
۵ Exploit Kit
۶ Network Shared Folder
۷ Cloud

به‌محض اجرا شدن، سه فایل با نام‌های تصادفی بر روی دستگاه کاربر ایجاد می‌شود. این سه فایل از نوع چندریختی[۸] بوده و بنابراین درهم‌ساز[۹] آنها در هر فایل آلوده شده متفاوت است. دو فایل از این سه فایل مخرب وظیفه آلوده نمودن سایر فایل‌های کاربر به بدافزار را بر عهده دارند.

همچنین این دو فایل کلیدهای جدیدی را در محضرخانه[۱۰] ایجاد می‌کنند تا با هر بار راه‌اندازی دستگاه، به‌صورت خودکار اجرا شوند.

سومین فایل مخرب نیز خود را به‌عنوان یک سرویس در سیستم عامل ثبت می‌کند.

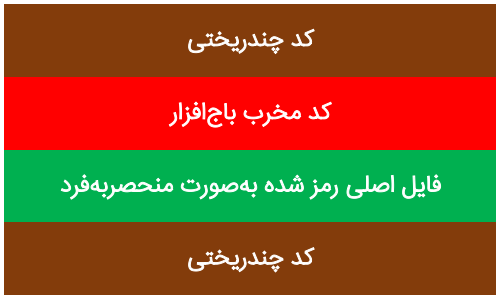
VirLock بخش‌های Task Manager و Registry Editor سیستم عامل را غیرفعال می‌کند. همچنین با دست‌درازی به کلیدهای زیر تنظیمات محضرخانه را به‌نحوی تغییر می‌دهد که فایل‌های مخفی شده و پسوندهای شناخته شده بر روی دستگاه قابل نمایش نبوده و بخش User Access Control سیستم عامل نیز غیرفعال شود:

```
Registry Key:
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
Value Name: Hidden
Value Data: 2

Registry Key:
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
Value Name: HideFileExt
Value Data: 1

Registry Key:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
Value Name: EnableLUA
Value Data: 0
```

باج‌افزار Virlock دامنه گسترده‌ای از پسوندها را رمزنگاری می‌کند.

این باج‌افزار، به فایل‌های رمز شده غیراجرایی، پسوند exe را الصاق می‌کند. برای مثال فایلی با نام help-world.pdf به help-world.pdf.exe تغییر نام پیدا می‌کند.

شکل ۱ ساختار یک فایل آلوده شده به VirLock را نمایش می‌دهد.



شکل ۱: ساختار یک فایل آلوده شده به VirLock

[۸] Polymorphic
[۹] Hash
[۱۰] Registry

این باج افزار فایل‌هایی که در مسیر آنها کلمات زیر قرار دارند را استثناء می‌کند:

- \Program
- \Temp
- \Windows

در انتها در اقدامی کاملاً مشابه با باج‌افزارهای غیررمزگذار با نمایش یک تصویر این طور القاء می‌شود که در نتیجه نقض قانون حق تکثیر[1]، دستگاه قفل شده و کاربر می‌بایست مبلغی را به عنوان جریمه پرداخت کند. (شکل‌های ۲ و ۳)

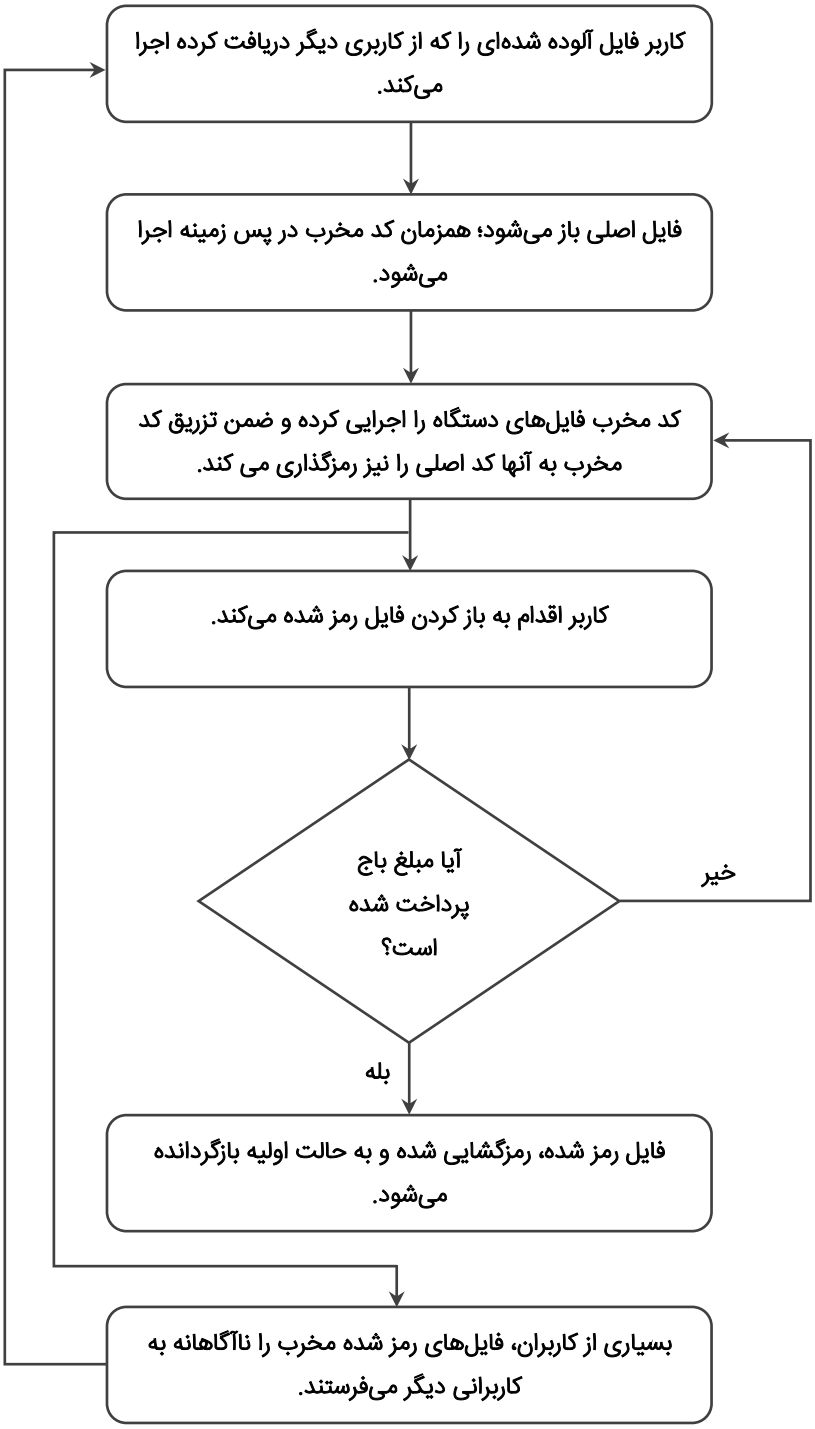
شکل ۲: اطلاعیه باج‌گیری در نمونه منتشر شده در آبان ماه ۱۳۹۵

شکل ۳: اطلاعیه باج‌گیری در نمونه منتشر شده در بهمن ماه ۱۳۹۵

[1] Copyright

مبلغ اخاذی شده در دو نمونه جدید این باج‌افزار ۰/۳۷۸ و ۰/۲۸۳ بیت‌کوین[۱۴] بوده است.

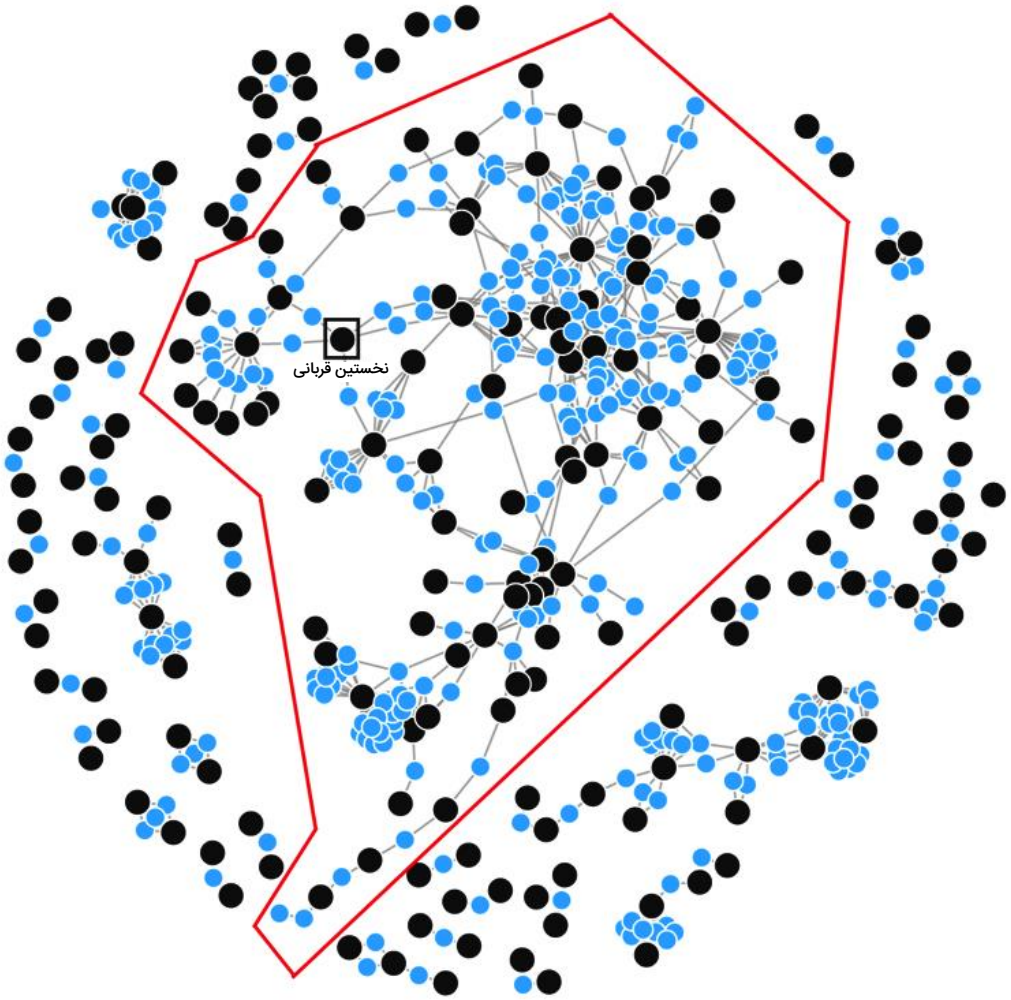
زمانی که یکی از فایل‌های رمز شده آلوده بر روی دستگاه اجرا می‌شود ابتدا پرداخت شدن باج مورد بررسی قرار می‌گیرد. در صورت پرداخت شدن باج، فایل رمزگشایی شده و به حالت اولیه باز می‌گردد. در غیر اینصورت فرآیند مذکور مجدداً بر روی دستگاه تکرار می‌شود. همچنین با توجه به عدم نمایش پسوند فایل‌های شناخته شده بر روی دستگاه بسیاری از کاربران متوجه اجرایی شدن – و در عین حال ناقل باج‌افزار شدن – فایل‌ها نشده و ممکن است که ناآگاهانه برخی از آنها را به کاربران دیگر ارسال کنند. (شکل ۴)



شکل ۴: فرآیند آلوده‌سازی در باج‌افزار VirLock

[۱۴] Bitcoin

ترکیب قابلیت باج‌افزار، بدافزار چندریختی و تزریق کد به فایل‌های سالم، VirLock را به بدافزاری مخرب و خطرناک تبدیل کرده که قادر است به‌سرعت در بستر شبکه یک سازمان منتشر شود. کارکنان سازمانی را در نظر بگیرید که از سرویس‌های رایانش ابری برای به‌اشتراک‌گذاری فایل‌ها استفاده می‌کنند. برای مثال در شکل ۵ نقاط مشکی رنگ نمایانگر کاربران و نقاط آبی رنگ نشان‌دهنده فایل‌های اشتراکی در بستر رایانش ابری است. محدوده قرمز رنگ نیز معرف دستگاه‌های آلوده شده به این بدافزار در چند دقیقه اول است.



شکل ۵: گسترش آلودگی به باج‌افزار VirLock در چند دقیقه نخست در یک بستر رایانش ابری

نسخه منتشر شده در بهمن ماه ۱۳۹۵ حاوی باگی است که رمزگشایی فایل‌ها را بدون پرداخت باج میسر می‌کند. همانطور که در تصاویر ۲ و ۳ نمایش داده شد اطلاعیه باج‌گیری VirLock حاوی بخشی با عنوان Transfer ID است که قربانی پس از پرداخت باج می‌بایست شناسه دریافت شده از سوی نویسنده یا نویسندگان این باج‌افزار را در این قسمت وارد کند تا عملیات رمزگشایی بر روی سیستم اجرا شود. اما وارد کردن ۶۴ صفر (0) در این قسمت نیز منجر به فعال شدن بخش رمزگشایی باج‌افزار می‌شود. با این حال انتظار می‌رود نویسنده یا نویسندگان این باج‌افزار به‌سرعت اقدام به ترمیم این باگ کنند.

راه‌های پیشگیری و مقابله

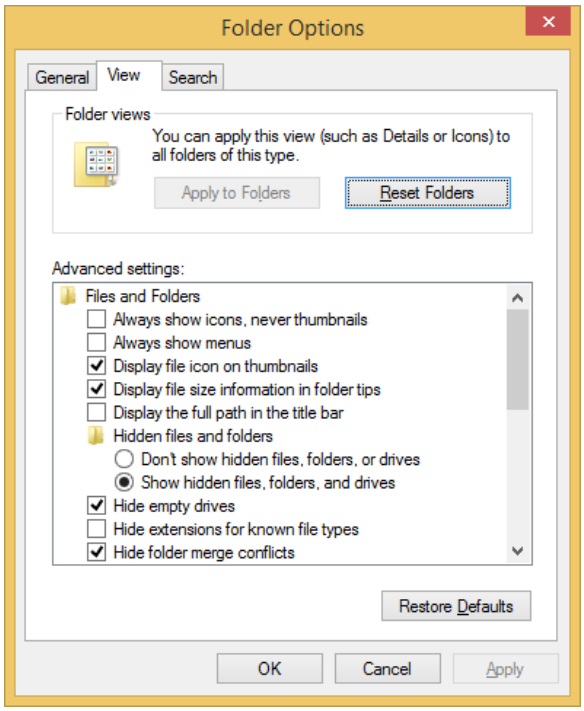
در امان ماندن از گزند این نوع باج‌افزارها تنها به داشتن آخرین راهکار امنیتی خلاصه نمی‌شود. بلکه مستلزم اجرای مجموعه‌ای از اقدامات زیر است.

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 نمایش پسوند فایل‌ها

به‌صورت پیش‌فرض در سیستم عامل Windows پسوند فایل‌ها نمایش داده نمی‌شود. این بدان معناست که کاربر می‌بایست به نشان[۱۳] فایل اعتماد کند. موضوعی که سبب استفاده برخی ویروس‌نویسان از فایل های دو پسوندی برای فریب کاربران می شود. برای مثال فایل Hello.txt.js در حالت عادی به‌صورت Hello.txt نمایش داده می‌شود. توصیه می‌شود که در بخش Folder Options گزینه Show hidden files, folders, and drive فعال شده و گزینه Hide extensions for known file types غیرفعال شود.



شکل ۶: تنظیمات Folder Options

۳ استفاده از ابزارهای کنترل‌کننده حافظه‌های USB

استفاده از ابزارهایی نظیر Device Control برای مدیریت و محدودسازی دسترسی به حافظه‌های مبتنی بر USB در سیستم‌های سازمان می‌تواند نقشی مؤثر در جلوگیری از انتشار انواع بدافزارهای از نوع کرم[۱۴] و همچنین این نمونه از باج‌افزار داشته باشد.

---

[۱۳] Icon

[۱۴] Worm

٤ محدود کردن سطح دسترسی

همه کاربران، حتی مدیر سیستم می‌بایست با حداقل سطح دسترسی مورد نیاز به هر سیستم وارد شود. 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.

٥ 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.

٦ استفاده از فناوری‌های حفاظتی پیشرفته

استفاده از ضدویروس قدرتمند و به روز جهت مقابله با باج افزارهای رمزگذار ضروری است. اما در کنار می بایست 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.

٧ به روز بودن در خصوص روش‌های جدید باج‌گیران

با مرور اخبار و حضور در دوره‌های آگاهی‌رسانی شرکت مهندسی شبکه گستر، نظیر سیمنارهای فصلی مروری بر رخدادهای امنیت سایبری از آخرین روش‌های مورد استفاده مهاجمان آگاه شده و سیاست‌ها پیشگرانه لازم را اعمال کنید.

٨ آگاهی‌رسانی به کاربران

گردانندگان باج‌افزار به‌خوبی می‌دانند تا زمانی که کاربر فایل پیوست ایمیل را جذاب یا مرتبط تشخیص ندهد آن را باز نمی‌کند. 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 این فایل‌ها داشته باشد. برای این منظور می‌توانید از این داده‌نمایی‌ها استفاده کنید.

پیوست – درهم‌ساز MD5 نمونه‌های بررسی شده

- ad9216a81088d9c6cfd3f7ddd14e33ff
- d577c2418ff7513f897c3fe56c59a59c
- 28e8b1e88cc8aa33c5ae49299c24a460
- DF0B3DD3E412EF5373372EA207577C00
- DE2297B150DA6785A301F690C909F96D
- F0286F192D8E0A58F19FC887AAA8B2C0
- cbea60d561de150819ec799d25a491bf
- 17465534071253l1d471fe1c722b2539
- ac7bd8b6b5f8393617d026e4a2cef01c
- cdcbe8bf3f7b391dcecb947ae7cca492
- ac5624a9c37c8fb324a0162c4d5d244e
- cc340c5e4911e8be185eed73b22d596b
- c4f066f5220f7bb949ac2c7a49b0385e

منابع

- https://www.bleepingcomputer.com/forums/t/559220/operation-global-iii-ransomware-not-only-encrypts-but-infects-your-data-as-well/
- https://blog.malwarebytes.com/threat-analysis/2017/01/virlockers-comeback-including-recovery-instructions/
- https://www.bleepingcomputer.com/news/security/virlocker-ransomware-returns-just-as-virulent-as-ever/
- http://newsroom.shabakeh.net/17845/virlock-a-polymorphic-ransomware.html
- https://blogs.sophos.com/2016/01/11/the-current-state-of-ransomware-virlock-threatfinder-crypvault-and-powershell-based/#more-30514
- https://nakedsecurity.sophos.com/2014/12/05/notes-from-sophoslabs-Ransomware-with-a-difference-this-one-is-a-true-virus
- https://www.netskope.com/blog/cloud-malware-fan-virlock-ransomware/

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 (تولید کننده 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 – UTM) 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

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