شبکه گستر

مروری بر بدافزار CTB-Locker

ویژه مشترکین McAfee

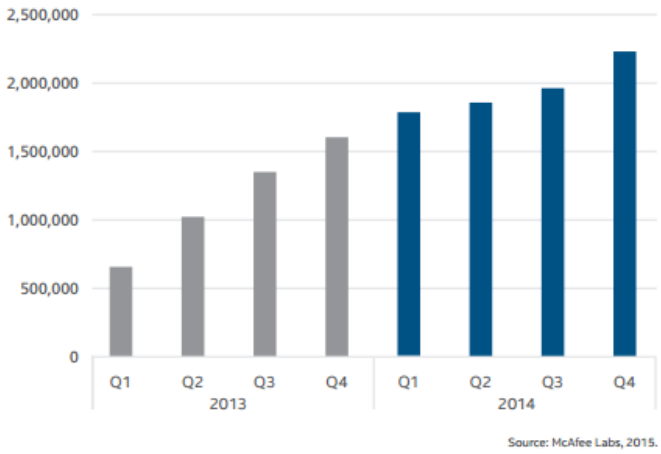
تهیه کننده: گروه تحقیق، توسعه و آموزش شرکت مهندسی شبکه گستر

تاریخ انتشار: اردیبهشت ۱۳۹۴

شماره: ۹۴-۰۱

پیشگفتار

هر چند که سالها از ظهور اولین باج‌افزار (Ransomware) می گذرد اما اوج موفقیت این نوع بدافزارها به باج‌افزار Cryptolocker در سال ۱۳۹۲ باز می‌گردد. گردانندگان Cryptolocker موفق شدند در مدتی کوتاه، از طریق بدافزار GameOver Zeus دهها هزار سیستم را آلوده و میلیون‌ها دلار از کاربران اخاذی کنند. شبکه مخرب GameOver Zeus در خرداد سال گذشته توسط اداره تحقیقات فدرال (FBI) و با همراهی شرکت‌های امنیتی و نهادهای قانونی چند کشور متلاشی و انتشار Cryptolocker متوقف شد.[1]



▲ **شکل ۱: تعداد باج‌افزارها در بین سال‌های ۲۰۱۴ و ۲۰۱۵**

اما اندکی بعد CTB-Locker به صحنه آمد. CTB مخفف Curve-Tor-Bitcoin Locker است و در حقیقت، نشان‌دهنده سه مشخصه اصلی این بدافزار می‌باشد: استفاده از الگوریتم رمزگذاری به نام Elliptic Curve Cryptography، استفاده از سامانه نرم‌افزاری Tor برای ناشناس ماندن و استفاده از واحد پول سایبری Bitcoin برای دریافت باج از قربانیان خود. برنامه‌نویسان CTB-Locker توابع فایل Tor.exe را بصورت حرفه‌ای در بدنه بدافزار جاسازی کرده‌اند. نسخه‌های اولیه این بدافزار عمدتاً از طریق سوء استفاده از حفره های امنیتی منتشر می شد. اما گونه آخر این بدافزار، در قالب پیوست هرزنامه‌ها، منتشر شده و قربانیانی در نقاط مختلف دنیا و از جمله کشور ایران می‌گیرد. یک روز با عنوان "نسخه جدید مرورگر Chrome" و یک روز در قالب "صورتحساب و فاکتور فروش" سعی می‌کند تا کاربرانی را فریب داده و آنها را به کلیک کردن بر روی پیوند و فایل پیوست مخرب، تشویق و ترغیب کند.

پس از آن فایل‌های ذخیره‌شده بر روی کامپیوتر قربانی رمزگذاری شده و سپس از او برای بازگشایی آنها، درخواست باج خواهد شد. باج را که یک گونه از CTB-Locker با نرخ دو Bitcoin و گونه دیگر با نرخ سه Bitcoin تعیین می‌کنند، باید در مهلت تعیین شده پرداخت کنید تا این بدافزار خوش‌قول هم فوراً از راه دور اقدام به رمزگشایی فایل‌های قفل‌شده، کند.

با توجه به نوع خاص رمزگذاری بدافزار CTB-Locker و طول کلید رمزگذاری، امکان رمزگشایی و بازگرداندن فایل‌های رمزشده با سعی و خطا توسط روش جستجوی فراگیر عملاً غیر ممکن است.

تضمینی هم نیست که بدافزار همیشه و فقط از وسیله ایمیل برای انتشار خود استفاده کند. حمله از طریق مرورگرها، محصولات پرمصرف Adobe، ابزارهایی مانند Java و Flash که اینترنت بدون آنها معنای دیگری خواهد داشت، نرم‌افزارهای کاربردی اداری و ... پایان و انتهایی ندارد. وقتی هم که قربانی و میزبان مورد تعرض قرار گرفت، داده‌های سرقت شده می‌تواند به روش‌های مختلف خسارات مادی و حیثیتی برای سازمان به همراه داشته باشد.

با وجود ضعف‌های امنیتی فراوان در سیستم های عامل و دیگر نرم‌افزارهای کاربردی، حضور کاربران کم‌تجربه و وابستگی بسیاری از سیستم‌های امنیتی امروزی به انتخاب کاربر، نمی توان انتظار داشت که افرادی که امروز دنیای سایبری را به جولانگاهی برای خرابکاری های خود مبدل ساخته اند، به این زودی ها محو و نابود شوند.

[1] http://blog.shabakeh.net/15054

باید روش‌های نوینی برای دیده‌بانی کاربران و حساب های کاربری در شبکه بکار گرفته شوند تا علائم تعرض، نفوذ و استفاده های نا صحیح شناسایی شوند و بتوان سازمان و شبکه خود را در برابر کاربرانی که قربانی انواع حقه‌ها و فریب‌های سایبری می شوند، محافظت کرد. بسیاری از ابزارهای دیده‌بانی، ردیابی و شناسایی در برابر بدافزارهایی نظیر CTB-Locker ناکام خواهند بود مگر آنکه از لحاظ برنامه‌نویسی و مشخصه‌های رفتاری مشابه گونه‌های قبلی و شناخته شده باشند. البته شاید شانس بیشتری در مرحله شناسایی هرزنامه (Spam) برای مهار این باج‌افزار داشته باشیم ولی حملات همیشه از طریق ایمیل نخواهد بود.

باج‌افزارهایی نظیر CTB-Locker باید حداقل دو درس به ما، کارشناسان امنیتی و مدیران سازمان‌ها داده باشند. درس اول، آموزش کاربران حتی در دوره‌های دبیرستان، دانشگاه و استخدام. درس دوم، کاربران دست به کارهای خطرساز خواهند زد و سیستم‌ها مورد تعرض قرار خواهند گرفت. آموزش کاربران شانس موفقیت بیشتری را در برابر هرزنامه‌ها و روش‌های فریب بدافزارها فراهم خواهد کرد. ولی در نهایت، همیشه کاربری خواهد بود که روی آن پیوند فریبنده و فایل وسوسه‌کننده کلیک کند. پس بعد از آموزش نیز اقداماتی نظیر بایگانی صحیح و دستورالعمل‌های بازیابی/بازسازی می‌تواند کمک موثری در مهار صدمات بدافزارهایی نظیر CTB-Locker باشد.

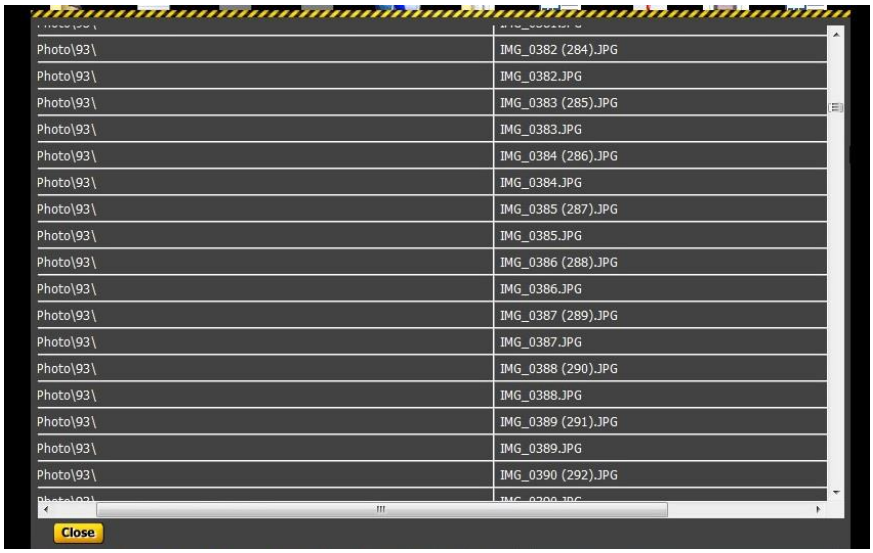
عملکرد بدافزار

پس از آلوده شدن کامپیوتر به باج‌افزار CTB-Locker، پیام‌هایی برای کاربر به نمایش درمی‌آید. در این بخش، از اولین پیام باج‌افزار که کاربر را از اتفاقی که افتاده مطلع می‌کند تا پیام‌های بعدی که کاربر را برای پرداخت باج و رمزگشایی داده‌های کامپیوتر، راهنمایی می‌نمایند، نشان داده می‌شود.

با اولین پیام، کاربر از آلوده شدن به بدافزار CTB-Locker مطلع می‌شود. در این پیام توضیح داده شده که داده‌های کاربر رمزگذاری شده و برای بازگرداندن آن به حالت اولیه، باید ظرف ۹۶ ساعت، باج درخواستی پرداخت شود. همچنین به کاربر هشدار داده می‌شود که اقدام به پاکسازی بدافزار نکند، زیرا با اینکار برخی فایل‌های مرتبط با بدافزار حذف می‌شود و امکان رمزگشایی داده‌ها دیگر وجود نخواهد داشت (شکل ۲).

▲ شکل ۲

در پیام اول، گزینه View وجود دارد که با زدن دگمه آن، فهرستی از فایل‌های رمزگذاری شده کاربر برای اثبات، به نمایش درمی‌آید (شکل۳).

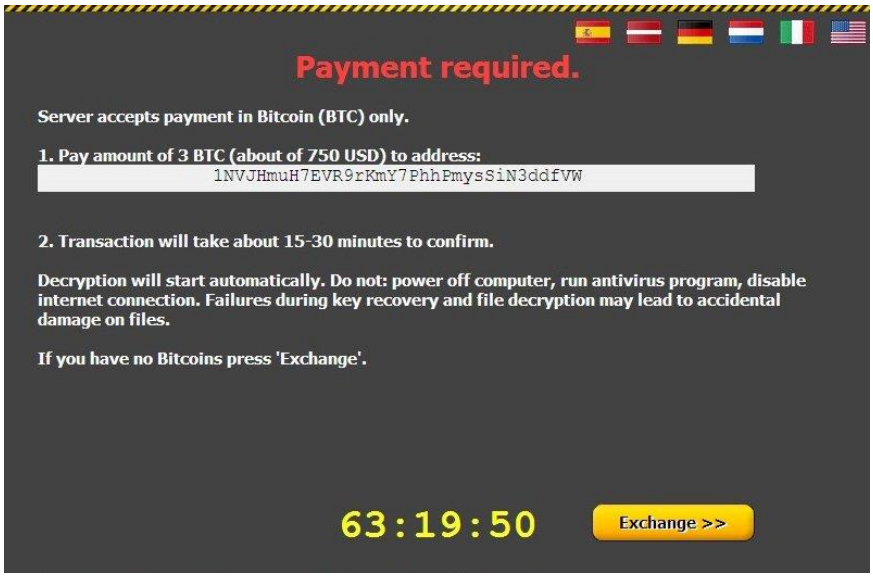


▲ شکل ۳

در پیام اول، دگمه Next وجود دارد که با زدن آن، پیام جدیدی ظاهر می‌شود (شکل ۴). در این پیام، برای نشان دادن توانایی بدافزار در رمزگشایی داده‌ها، فرصت رمزگشایی چند فایل که بطور تصادفی انتخاب می‌شوند، داده شده است.

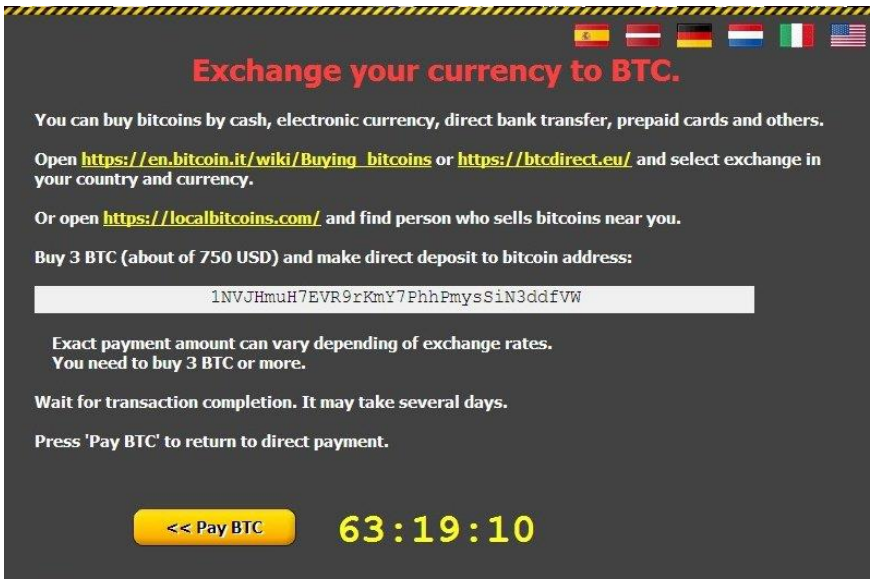
▲ شکل ۴

در پیام بعدی، جزئیات باجگیری ارائه می شود. در این پیام از کاربر خواسته می شود که مبلغ سه Bitcoin به یک شماره حساب واریز کند تا عملیات رمزگشایی داده‌ها بطور خودکار آغاز گردد (شکل ۵). شماره حساب ارائه‌شده منحصربه‌فرد و ویژه آن کامپیوتر خاص است. در حقیقت، از این شماره حساب برای تشخیص اینکه باج واریز شده بابت کدام کامپیوتر بوده است، استفاده می‌شود.



شکل ۵ ▲

نویسنده باج‌افزار CTB-Locker تمام جوانب کار را اندیشیده و برای هر مشکلی راه حلی دارد. اگر کاربر فاقد حساب و پول مجازی Bitcoin باشد، گزینه Exchange راهنمایی‌های لازم را به کاربر در این زمینه ارائه می‌کند (شکل ۶). از جمله پیوندها و وب‌گاه‌های مناسب برای خرید Bitcoin به کاربر پیشنهاد می‌شوند.



شکل ۶ ▲

در صورتیکه کاربر اقدام به خرید Bitcoin و واریز به حساب تعیین شده نماید، در مدت کمتر از نیم ساعت، پیامی مبنی بر آغاز رمزگشایی داده‌ها به نمایش درمی‌آید (شکل ۷). در نمونه‌هایی که توسط کارشناسان شبکه گستر جمع‌آوری شده‌اند، داده‌ها بطور کامل و سالم رمزگشایی شده و به حالت اولیه خود بازمی‌گردند.

شکل ۷

پس از تکمیل رمزگشایی داده‌های دیسک سخت کامپیوتر، بدافزار پیش از محو و نابود کردن خود، از کاربر می‌خواهد تا اگر داده‌های او بر روی حافظه‌های USB Flash هم رمزگذاری شده‌اند، آنها را یک‌به‌یک به کامپیوتر متصل کند تا CTB-Locker اقدام به رمزگشایی آنها نیز نماید (شکل ۸).

شکل ۸

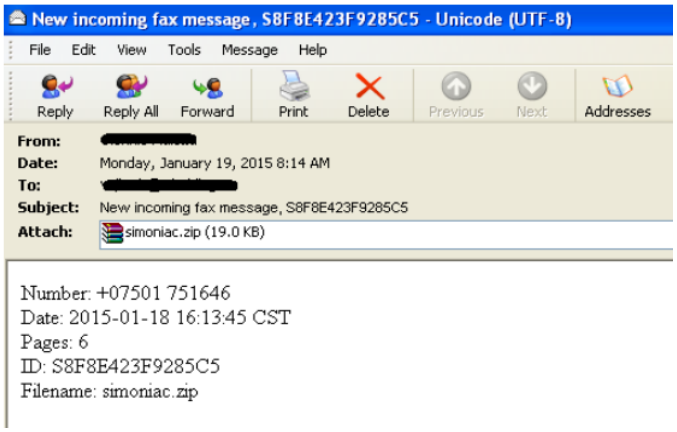
انتشار

آخرین گونه شناسایی شده در ایران، در قالب SCR و بصورت فایل ZIP یا CAB از طریق هرزنامه ها منتشر می‌شوند. اسامی نمونه‌هایی از این پیوست‌های آلوده بشرح زیر است:

- faltboat.zip
- incurably.zip
- payloads.zip
- dessiatin.zip
- malformed.zip
- plenitude.zip
- inquires.zip
- simoniac.zip

همچنین، عباراتی که در ادامه آمده‌اند نمونه‌هایی از عناوین این هرزنامه‌ها می‌باشند:

- [Fax server] +07909 546940
- copy from +07540040842
- Message H4H2LC68B7167E4F4
- New incoming fax message, S8F8E423F9285C5
- Incoming fax from +07843-982843
- [Fax server]:+07725-855368
- Fax ZC9257943991110
- New fax message from +07862-678057



▲ شکل ۹

اقدامات پیشگیرانه

گونه‌های جدید این بدافزار با DAT 7781، توسط ضدویروس McAfee با نام‌های BackDoor-FCKQ، Downloader-FAMV، Injector-FMZ، Downloader-CTB و Ransom-CTB شناسایی می‌شوند. با این حال، استفاده از فایل به‌روزرسانی موقت (EXTRA DAT) که حاوی فرمول شناسایی آخرین گونه‌های بدافزار CTB-Locker می‌باشد نیز توصیه می‌گردد.

برای گسترش فایل به‌روزرسانی موقت[۲] از طریق ابزار مدیریتی McAfee ePolicy Orchestrator مراحل زیر می‌بایست دنبال شوند:

۱. فایل را از اینجا دریافت کنید؛
۲. فایل دریافتی را باز کنید و آنرا از حالت فشرده در آورید (نام فایل EXTRA.DAT)؛
۳. در کنسول ePolicy Orchestrator بر روی Menu کلیک و در قسمت Software گزینه Master Repository را انتخاب نمایید؛
۴. بر روی دگمه Actions کلیک کرده و گزینه Check In Package را انتخاب کنید؛
۵. پس از فعال کردن گزینه Extra DAT بر روی گمه Browse کلیک نموده و فایل EXTRA.DAT را انتخاب کنید. در ادامه بر روی دگمه Next کلیک نمایید؛
۶. پس از ظاهر شدن مشخصات فایل، بر روی دگمه Save کلیک کنید تا فایل در انباره قرار گیرد.

علاوه بر استفاده از ضدویروس قدرتمند و به‌روزرسانی مداوم آن، رعایت موارد ذیل، آسان‌ترین و ارزان‌ترین راه برای حفاظت از اطلاعات در برابر خرابکاران و مجرمان باجگیر خواهد بود:

- آموزش کاربران؛

[۲] اعتبار این فایل تا پایان اردیبهشت ۱۳۹۴ می‌باشد.

- تهیه پشتیبان از داده های بااهمیت بصورت دوره‌ای؛ پیروی از قاعده ۱-۲-۳ برای داده های حیاتی توصیه می شود. بر طبق این قاعده، از هر فایل سه نسخه می بایست نگهداری شود (یکی اصلی و دو نسخه بعنوان پشتیبان)، فایل‌ها باید بر روی دو رسانه ذخیره سازی مختلف حفظ شوند. یک نسخه از فایلها می بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود؛
- بهره‌گیری از نرم‌افزارها و سخت‌افزارهای ضدهرزنامه (Anti-Spam)؛
- محدود کردن سطح دسترسی کاربران بمنظور جلوگیری از آلوده شدن دستگاه حتی در صورت اجرا شدن فایل مخرب توسط کاربر.

پیوندهای مفید

- هشدار جدی مرکز ماهر در خصوص بدافزار CTB locker:

http://www.certcc.ir/index.php?module=cdk&func=loadmodule&system=cdk&sismodule=user/content_view.php&cnt_id=220380&ctp_id=19&id=3797&sisOp=view

- McAfee Labs Threat Advisory - CTB-Locker:

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25696/en_US/McAfee_Labs_Threat_Advisory-CTB-Locker.pdf

- باج‌افزار:

http://fa.wikipedia.org/wiki/%D8%A8%D8%A7%D8%AC%E2%80%8C%D8%A7%D9%81%D8%B2%D8%A7%D8%B1

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

گروه فروش ۵۷ – ۵۳ ۸۲ ۶۵ ۸۸ | sales@shabakeh.net
گروه پشتیبانی ۸۵ – ۸۱ ۲۴ ۲۰ ۸۸ | support@shabakeh.net

تارنمای شرکت www.shabakeh.net
سامانه پشتیبانی help.shabakeh.net
پایگاه اطلاع رسانی blog.shabakeh.net
خدمات پس از فروش my.shabakeh.net