

## انتشار نوع جدیدی از باج افزار Cmb Dharma

در روز پنج شنبه نسخه جدیدی از باج افزار Dharma منتشر شد که افزونه cmb. را به فایل های رمزگذاری شده اضافه می کند.

نوع Cmb از باج افزار Dharma اولین بار توسط Michael Gillespie هنگامی که نمونه های آپلود شده از شناسه باج افزار را بررسی می کرد، کشف شد و بعد از خبررسانی در مورد آن، Jakub Kroustek نمونه ای از مقدار هش آن را منتشر کرد :

c2ab289cbd2573572c39cac3f234d77fdf769e48a1715a14feddaea8ae9d9702 - [paymentbtc@firemail.cc].cmb + FILES  
ENCRYPTED.txt

Sample submitted to @virusbay\_io <https://t.co/3NCEyTPEKn>

Jakub Kroustek (@JakubKroustek) August 10, 2018

در توضیحات زیر مشخص شده که چگونه این خانواده باج افزار کامپیوتر را آلوده می کند و زمانی که شما با نوع Cmb از این باج افزار آلوده می شوید، چگونه از خودتان محافظت کنید درحالیکه متأسفانه، هیچ راهی برای رمزگشایی فایل های آلوده با باج افزار Dharma Cmb به صورت رایگان وجود ندارد.

### توزیع شده از طریق هک سرویس های دسکتاپ از راه دور

خانواده باج افزار Dharma از جمله نوع Cmb آن، توسط مهاجمان به صورت دستی روی کامپیوترها از طریق پروتکل های سرویس از راه دور (RDP) نصب می شود. مهاجمان اینترنت را برای رایانه هایی که پروتکل RDP را اجرا می کنند و معمولاً بر روی پورت ۳۳۸۹ TCP هستند، جستجو می کنند، و تلاش می کنند تا رمز عبور آن ها را بشکنند و وارد شوند.

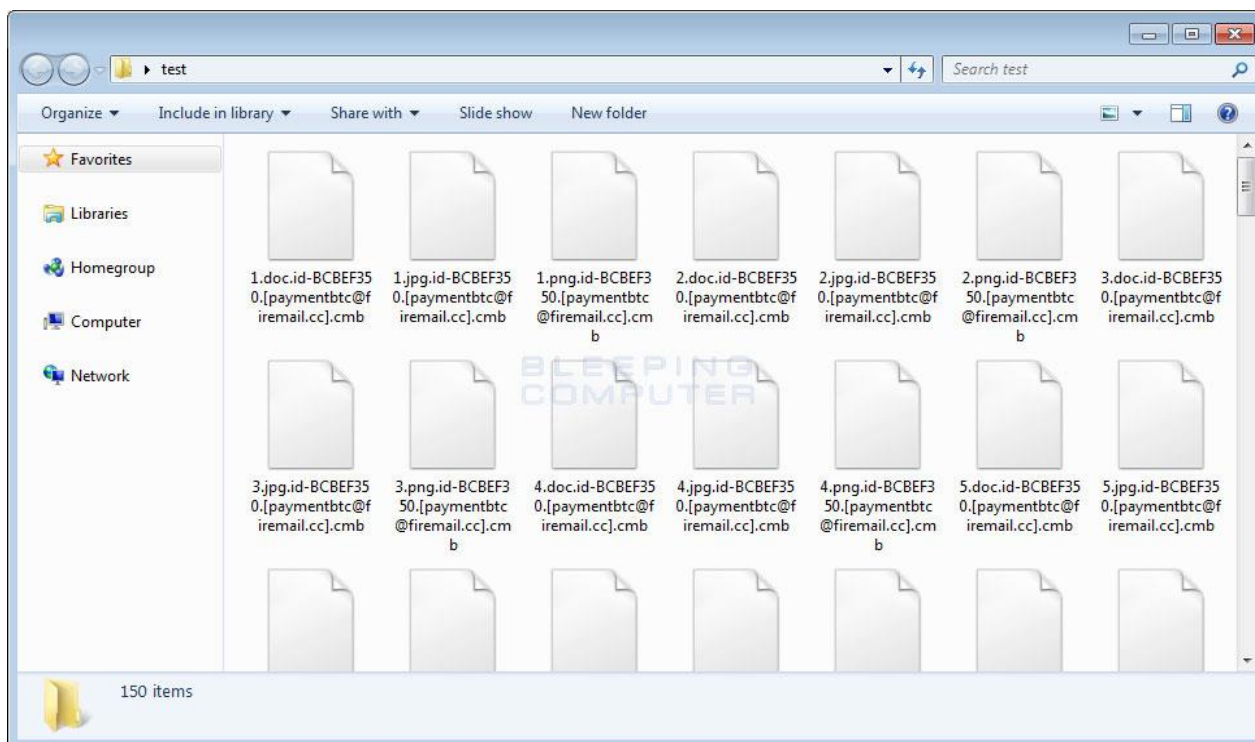
هنگامی که مهاجمان به کامپیوتر هدف دسترسی پیدا می کنند، باج افزار را نصب کرده و کامپیوتر را رمزگذاری می کنند. اگر مهاجمان قادر به رمزگذاری رایانه های دیگر در شبکه باشند، تلاش خواهند کرد که این کار را نیز انجام دهند.

### باج افزار Cmb Dharma چگونه کامپیوتر را رمزگذاری می کند

هنگامی که باج افزار نوع Cmb روی کامپیوتری قرار گیرد، ابتدا کامپیوتر را برای فایل ها اسکن می کند و سپس آنها را رمزگذاری می کند. هنگام رمزگذاری یک فایل، پسوند آن را در قالب [email].cmb[id- [id]].id- اضافه می کند. به عنوان مثال، اگر یک فایل با نام test.jpg رمزگذاری شود به test.jpg.id-BCBEF350.[paymentbtc@firemail.cc].cmb تغییر نام می دهد.

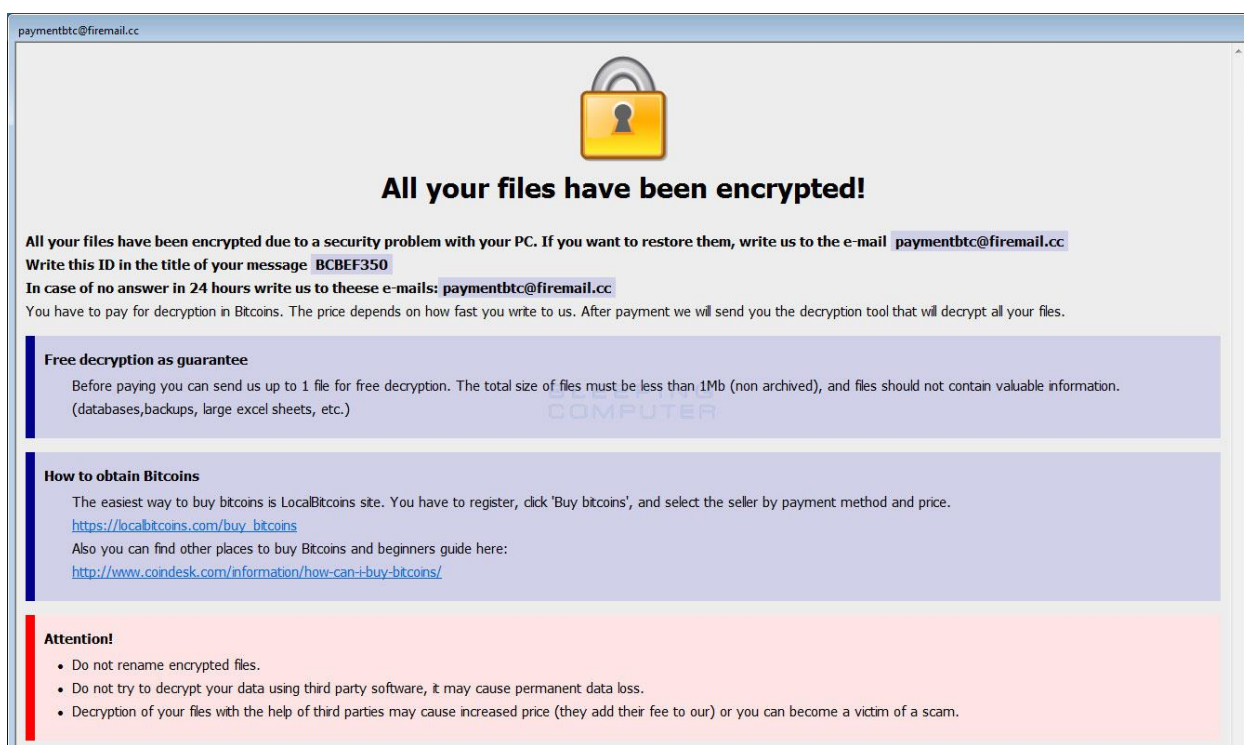
لازم به ذکر است که این باج افزار درایوهای اشتراکی در یک شبکه و همچنین درایوهای مجازی مشترک را هم رمزگذاری می کند. بنابراین مهم است که مطمئن شوید شبکه اشتراک اطلاعاتتان به خوبی قفل شده و محافظت شده است، به طوری که فقط کسانی که نیاز به دسترسی شبکه دارند، مجوز دسترسی داشته باشند.

شما می توانید یک نمونه از پوشه ای رمزگذاری شده توسط باج افزار نوع Cmb را در زیر ببینید

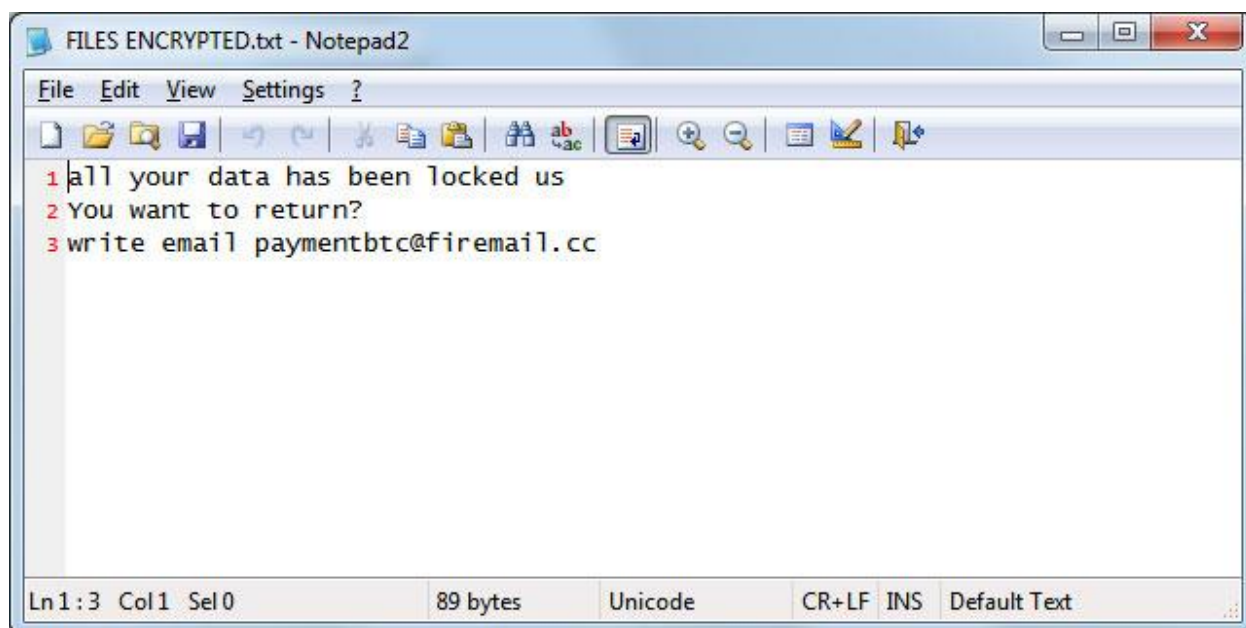


هنگامی که فایل ها رمزگذاری می شوند، این باج افزار دو نوع فایل مختلف را در کامپیوتر آلوده ایجاد می کند.

فایل اول Info.hta است که زمانی که کاربر وارد سیستم می شود توسط یک autorun اجرا می شود.



فایل دوم FILES ENCRYPTED.txt است و بر روی دسکتاپ یافت شود.



هر دو این فایل‌ها شامل دستورالعمل‌هایی برای تماس با paymentbtc@firemail.cc جهت دریافت دستورالعمل‌های پرداخت می‌باشند.

و در نهایت، این باج‌افزار خود را به گونه‌ای پیکربندی خواهد کرد تا به صورت خودکار هنگام ورود به سیستم ویندوز شروع شود که این کار اجازه می‌دهد تا فایل‌های جدید ایجاد شده از زمان آخرین اجرای خود را رمزگذاری کند.

### چگونه خود را از باج‌افزار Dharma Cmb محافظت کنیم

به منظور محافظت از خود در برابر باج‌افزار Dharma و یا هر باج‌افزار دیگری، مهم است که شما از عادت‌های کامپیوتری خوبی برخوردار باشید و نرم‌افزار امنیتی استفاده کنید.

اول و مهمتر از همه، همیشه بایستی یک فایل پشتیبان مطمئن و آزمایش شده از داده‌های خود داشته باشید که می‌تواند در موارد اضطراری مانند حمله‌ی باج‌افزار اطلاعات بازگردانده شود.

باج‌افزار Dharma به طور معمول از طریق سرویس‌های دسکتاپ از راه دور نفوذ می‌کند پس بسیار مهم است که مطمئن شوید این سرویس‌ها به درستی محافظت شده‌اند. پس باید مطمئن شوید که هیچ کامپیوتری با سرویس‌های دسکتاپ از راه دور یا RDP به

طور مستقیم به اینترنت وصل نشود و در عوض VPN هایی را قبل از کامپیوترهای با سرویس‌های دسکتاپ از راه دور قرار دهیم به طوری که در شبکه شما کامپیوترها فقط برای کسانی که حساب‌های VPN دارند در دسترس باشند.

همچنین مهم است که قفل حساب کاربری ویندوز را طوری تنظیم کنید تا حساب‌ها برای خدمات دسکتاپ از راه دور قابل نفوذ نباشند.

شما همچنین باید نرم‌افزاری امنیتی داشته باشید که شکل و نوع رفتار باج‌افزار را شناسایی کند و نه فقط تشخیص امضا یا روش‌های اکتشافی را شامل شود. به عنوان مثال Emsisoft Anti-Malware و Malwarebytes Anti-Malware هر دو دارای شناسایی رفتاری هستند که می‌توانند از بسیاری از آلودگی‌های باج‌افزاری و رمزگذاری کامپیوترها جلوگیری کنند.

و در آخر اطمینان حاصل کنید که نکات امنیت اینترنتی زیر را رعایت کنید که در بسیاری از موارد مهم‌ترین نکات برای پیشگیری از قربانی شدن هستند :

- پشتیبان‌گیری
- فایل‌های ضمیمه را باز نکنید، اگر نمی‌دانید چه کسی آنها را فرستاد.
- اسکن فایل‌های ضمیمه با ابزارهایی مانند VirusTotal.
- اطمینان حاصل کنید که همه بروزرسانی ویندوز در اسرع وقت نصب می‌شوند. همچنین اطمینان حاصل کنید که تمام برنامه‌ها، به ویژه جاوا، فلش و Adobe Reader را بروزرسانی می‌کنید. برنامه‌های قدیمی‌تر شامل آسیب‌پذیری‌های امنیتی هستند که معمولاً توسط توزیع‌کنندگان مخرب مورد سوء استفاده قرار می‌گیرند. بنابراین مهم است که آنها را به‌روز نگه دارید.
- اطمینان حاصل کنید که از نوع خاصی از نرم‌افزار امنیتی استفاده می‌کنید.
- از رمزهای عبور سخت استفاده کنید و رمز عبور مشابهی را در چندین سایت استفاده نکنید.
- اگر از سرویس‌های Remote Desktop Services استفاده می‌کنید، آن را مستقیماً به اینترنت وصل نکنید. در عوض آن را تنها با استفاده از یک VPN قابل دسترسی کنید.