انتشار نوع جدیدی از باج‌افزار dharma با افزونه پسوند brrr.

این هفته نوع جدیدی از باج‌افزار Dharma منتشر شد که افزونه brrr. را به فایل‌های رمزگذاری شده اضافه می‌کند. این نوع جدید اولین بار توسط Jakub Kroustek کشف شد که نمونه آن را در اختیار VirusTotal قرار داد.

در زیر مشخص شده که چگونه این باج‌افزار کامپیوتر را آلوده می‌کند و زمانی که اطلاعات شما رمزگذاری می‌شوند چگونه می‌توانید از اطلاعاتتان محافظت کنید، درحالیکه متاسفانه هیچ راهی برای رمزگشایی فایل‌های آلوده شده با باج‌افزار Dharma Brrr وجود ندارد.

خانواده باج‌افزارDharma از جمله نوع brrr آن، توسط مهاجمان به صورت دستی روی رایانه‌ها از طریق پروتکل‌های سرویس از راه دور یا RDP نصب می‌شود. مهاجمان فضای اینترنت را برای رایانه‌هایی که پروتوکل RDP را اجرا می‌کنند و معمولا بر روی پورت TCP ۳۳۸۹ هستند، جستجو می‌کنند، و تلاش می‌کنند تا رمز عبور آن‌ها را بشکنند و واردشان شوند.

همچنین سایت‌هایی زیرزمینی هستند که اطلاعات مربوط به رایانه‌های قابل دسترس از طریق پروتکل‌های سرویس از راه دور را می‌فروشند و مهاجمان می‌توانند این اطلاعات را خریداری کنند.

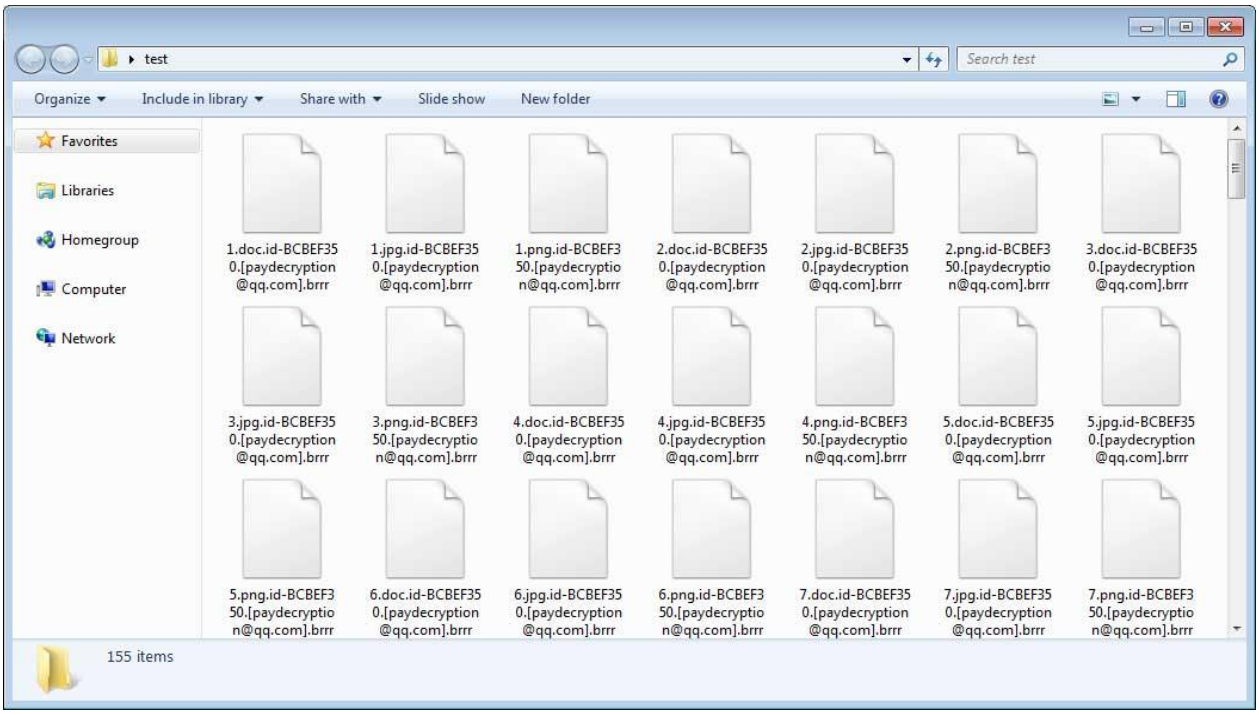
هنگامی که مهاجمان به کامپیوتر هدف دسترسی پیدا می‌کنند، باج‌افزار را نصب کرده و کامپیوتر را رمزگذاری می‌کنند. اگر مهاجمان قادر به رمزگذاری رایانه‌های دیگر در شبکه باشند، تلاش خواهند کرد که این کار را نیز انجام دهند.

باج‌افزار brrr Dharma چگونه کامپیوتر را رمزگذاری می‌کند

هنگامی که باج‌افزار نوع brrr روی کامپیوتری قرار گیرد، ابتدا کامپیوتر را برای فایل ها اسکن می‌کند و سپس آنها را رمزگذاری می‌کند. هنگام رمزگذاری یک فایل، پسوند آن را در قالب id-[id].[email].brrr. اضافه می کند. به عنوان مثال، اگر فایلی با نام test.jpg رمزگذاری شود به test.jpg.id-BCBEF350.[paydecryption@qq.com].brrr تغییر نام می‌دهد.

لازم به ذکر است که این باج‌افزار درایوهای اشتراکی در یک شبکه و همچنین درایوهای مجازی مشترک را هم رمزگذاری می‌کند. 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 پوشه‌ای رمزگذاری شده توسط باج‌افزار نوع brrr را در زیر ببینید



هنگامی که فایل‌ها رمزگذاری می‌شوند، 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 می‌شود توسط یک autorun اجرا می‌شود.

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

هر دو این فایل‌ها شامل دستورالعمل‌هایی برای تماس با paydecryption@qq.com جهت دریافت دستورالعمل‌های پرداخت باج 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 می دهد تا فایل های جدید ایجاد شده از زمان آخرین اجرای خود را رمزگذاری کند.

چگونه خود را از باج‌افزار brrr dharma 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 نرم افزار 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 حمله ی 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 نمی دانید 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 معمولا توسط توزیع‌کنندگان مخرب مورد سوء استفاده قرار می‌گیرند. بنابراین مهم است که آنها را به‌روز نگه‌دارید.
- 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 مستقیما به اینترنت وصل نکنید. در عوض آن را تنها با استفاده از یک VPN قابل دسترسی کنید.