به نام خدا

مقدمه

اخیرا طیف خاصی از بدافزارهای مخرب در سطح شبکه اینترنت منتشر شده اند که با آسیب واردکردن به اطلاعات و داده های کاربران اقدام به اخاذی از آنها می کنند. با توجه به گزارش موارد متعددی از این حملات در سطح کشور و زیان های جبران ناپذیر وارد شده از جانب این حملات، گزارشی به شرح زیر جهت اطلاع رسانی تدوین شده است.

بدافزار CTB Locker چیست؟

یکی از انواع باج افزار است که با نام Critroni نیز شناخته می شود. اولین موارد CBT Locker در تیرماه ۱۳۹۳، در روسیه و اوکراین مشاهده شده است .این باج افزار میتواند سیستم عاملهای ویندوزXP ، ویستا، ۷ و ویندوز 8 را آلوده سازد. روش عمل این بدافزار این گونه است که فایلهایی با پسوندهای ، db، mp4،pem و jpg، docx، doc و سایر فایلهای با محتوای غنی را با یک کلید نامشخص رمزگذاری می کند، به نحوی که شناسایی کلید و بازگرداندن آنها تقریباً غیر ممکن است.

شناسایی دامنه های آلوده به بدافزار CTB Locker و لزوم مسدود نمودن دامنه های مذکور

این فایل ها پس از نصب، فایل اصلی بدافزار را دانلود و نصب می کنند. پس از اجرا روی سیستم، فایل های سیستم رمز شده و تنها با پرداخت پول درخواستی (bitcoin) ، کاربر می تواند فایل های خود را رمزگشایی نماید.

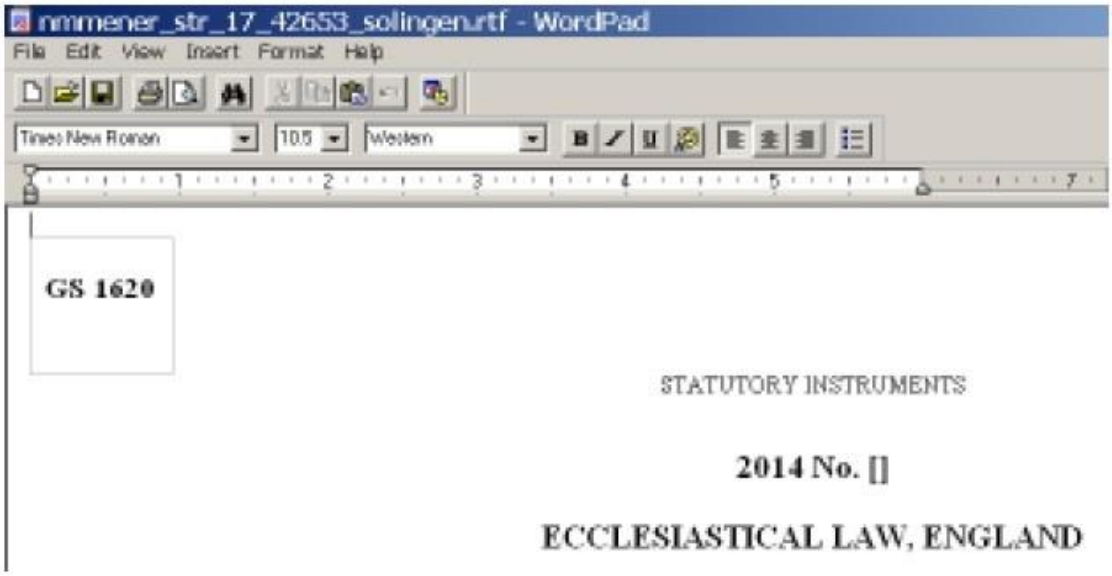
نحوه آلوده سازی

همان طور که مشاهده می شود ایمیلی با ظاهر عادی برای کاربر ارسال گردیده است که در ظاهر مشکلی ندارد.

بعد از دانلود فایل مشاهده می شود که فایل ظاهرا Screen saver است. ولی با اجرای آن بدافزار اصلی روی سیستم دانلود خواهد شد.

MD5:BCE620ECF70A52B92D89649698FDCC08

پس از اجرای فایل، فایل wordpad با مضمون یک فاکس مشاهده می گردد.



ولی در حقیقت سیستم آلوده از طریق اتصال به اینترنت، فایل های ذیل که فایل های اصلی بدافزار است، دانلود و اجرا می کند.

81F68349B12F22BEB8D4CF50EA54D854EAA39C89 Win32/FileCoder.DA

0D4B6401EB5F89FF3A2CF7262872F6B3D903B737 Win32/FileCoder.DA

نتیجه کار مانند بدافزارهای CryptoLocker و TorrentLocker است که فایل هایی با پسوند .jpg, .doc,.db.cer,.mp4,.pem. و غیره با یک کلید نامشخص رمز می شوند که تقریبا بازگرداندن آنها غیرممکن می باشد.
بدافزار پس از پایان کار خود پیامی را روی صفحه با مضمون زیر و زبان های مختلف نشان می دهد.حتی برای اطمینان به کاربر اجازه می دهد تا ۵ فایل دلخواه خود را رمزگشایی کند.سپس صفحه ای جهت پرداخت، مشاهده خواهد شد .

راه های مقابله و پیشگیری

درست است که تکنیک مورد استفاده این بدافزارها طوری است که امکان رمزگشایی و بازیابی فایل ها در آن وجود ندارد، اما با روش های زیر به راحتی می توان با این بدافزارها مقابله کرد :

گرفتن فایل پشتیبان (Backup) از اطلاعات مهم

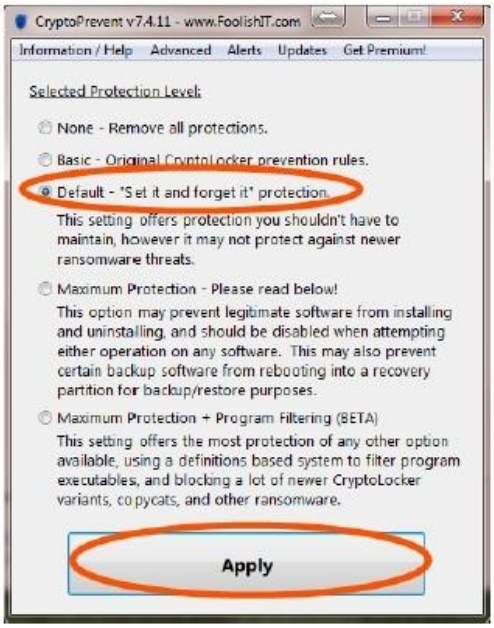
- به کارگیری راه حل های امنیتی جهت ایمیل ها.
- خودداری از بازکردن ضمایم ایمیل هایی که با ارسال کننده ناشناس آمده است.
- پاک کردن یا اسپم کردن ایمیل های مشکوک
- استفاده از ابزارهای امنیتی مناسب در شبکه
- از ابزارهایی مانند CryptoPrevent به منظور حذف برخی دسترسیهای مورد استفاده باج افزارها استفاده شود(در ادامه در این مورد توضیحات بیشتری داده خواهد شد)
- **گرفتن فایل پشتیبان (Backup) از اطلاعات مهم**

ابزار CryptoPrevent چیست؟

CryptoPrevent نرم افزاری است که با اعمال سیاست ها و ایجاد تغییراتی در سیستم عامل ویندوز، مسیرهای شناخته شده اجرای باج افزارها را مسدود می نماید .این نرم افزار رایگان است و استفاده از آن ساده می باشد. از آدرس زیر می توان این ابزار را دریافت نمود:

http://62.60.136.44/CryptoPreventSetup.zip

پس از دریافت فایل و نصب و اجرای آن، تنظیمات مطابق مراحل زیر انجام شود.



در صورت نیاز کامپیوتر خود را ری استارت کنید.

توجه داشته باشید که در صورت انتخاب گزینه های Maximum Protection یا Maximum Protection + Program Filtering را انتخاب نمایید، سیستم از سطح امنیتی بیشتری برخوردار خواهد بود .اما انتخاب این دو گزینه موجب می شود در انجام عملیاتی مانند نصب برنامه ها یا اجرای برخی برنامه های کاربردی اختلال ایجاد شود.

همچنین با انتخاب گزینه None(اولین گزینه)کلیه تنظیمات امنیتی اعمال شده توسط این برنامه حذف می شود و سیستم به حالت عادی باز میگردد .بنابراین در صورت ایجاد اختلال در اجرای برخی برنامه ها می توانید از این گزینه استفاده کنید.

از آدرس زیر می توان اطلاعات تکمیلی در مورد این باج افزار را دریافت نمود:

http://www.bleepingcomputer.com/virus-removal/ctb-locker-ransomwareinformation