شیوه‌های زورگیری اینترنتی و ارائه راهکارهای امنیتی

داود عبیری[1]

محمدرضا ولوی[2]

تاریخ دریافت: ۱۳۹٤/٥/۲۰

تاریخ پذیرش: ۱۳۹٤/۷/۱۲

چکیده

زورگیری صرفاً در محیط فیزیکی زندگی بشر اتفاق نمی‌افتد، با گسترش فضای سایبر، زورگیری به این فضا هم سرایت کرده و برابر سوابق، مستندات و گزارش‌های مراکز امنیتی فعال در حوزه فضای سایبر نظیر مرکز ماهر[3] مرکز جرائم رایانه‌ای اتحادیه اروپا، اداره مرکزی پلیس اروپا، آژانس اطلاعات مرکزی امریکا، اداره تحقیقات فدرال (اف.بی.آی) و سایر مراجع دیگر، چند سالی است که مجرمان سایبری ازطریق بدافزارهای باج‌گیر (زورگیر) اینترنتی به روش‌های مختلف از جمله ایمیل‌های آلوده‌کننده، هدایت کاربران به سمت لینک‌های آلوده، دانلود و نصب نرم‌افزارهای آلوده، سوءاستفاده از آسیب‌پذیری‌ها، نقاط ضعف یا باگ سیستم‌های رایانه‌ای و...، سیستم‌های رایانه‌ای را در سطح جهان آلوده کرده و با رمزکردن داده‌های مورد نیاز کاربر، قفل‌کردن سیستم، قفل‌کردن صفحه نمایش همراه با نمایش تصاویر مستهجن، تهدید کاربران مبنی بر بازدید از سایت‌های غیرقانونی (سایت‌های تروریستی، مستهجن، کودک‌آزاری) کاربران را مجبور به پرداخت مبالغی می‌نمایند. در پاره‌ای از مواقع، مجرمان با پوشش پلیس و اعلام مواردی به‌عنوان تخلف از سوی کاربر، کاربران را تهدید و مجبور به پرداخت جریمه می‌نمایند و در برخی از موارد نیز با جسارت تمام، بدون هیچ پوششی، کاربر را مجبور به پرداخت وجه تعیین شده می‌نمایند؛ چرا که رایانه کاربر قفل شده و کار نمی‌کند و یا اینکه داده‌های مورد نیاز و حساس وی، رمز می‌شود؛ بنابراین برای دسترسی به رایانه و یا دسترسی به اطلاعات، کاربر مجبور به پرداخت هزینه می‌باشد.

تجارب ثبت شده، نشان داده که در اکثر مواقع کاربر حتی با پرداخت هزینه تعیین‌شده، باز هم موفق به دسترسی به رایانه و اطلاعات رایانه خود نمی‌شود. بنابراین آگاهی کاربران از روش‌های مجرمان، انجام اقدام‌های لازم برای جلوگیری از آلوده‌شدن سیستم‌ها به بدافزارهای زورگیر، مشکلات پاکسازی رایانه آلوده‌شده و جلوگیری از پرداخت هزینه غیرقانونی به مجرمان، از جمله مواردی است که این مقاله به آن پرداخته و از روش توصیفی و ابزار گردآوری اطلاعات کتابخانه‌ای همراه با تجزیه و تحلیل، راهکارهای لازم را در پایان ارائه نموده است.

کلید واژه‌ها:

زورگیری اینترنتی/ راهکار امنیتی/ سایت‌های غیر قانونی/ مجرمان سایبری.

---

۱. دانشجوی دکترای امنیت فضای سایبر (نویسنده مسئول)

۲. عضو هیئت علمی دانشگاه مالک اشتر

بدافزار باج‌گیر چیست؟

بدافزار باج‌گیر، نرم‌افزاری است که بر خلاف خواسته کاربر عمل می‌کند و به‌منظور اخاذی از کاربران، اقدام به قفل‌کردن رایانه یا غیرقابل استفاده کردن فایل‌ها می‌نماید (مرکز محافظت بدافزار مایکروسافت، ۲۰۱۵).

برابر بررسی‌ها و گزارش‌های اعلام شده از سوی مراکز امنیتی، مدتی است بدافزارهای باج‌گیر با نام‌های Police Ransomware، Crypto Locker، Torrent Locker، CryptoWall، CTB locker، FBI Moneypak، ویروس FBI و... در کشورها از جمله کشورمان، رواج پیدا کرده و این امر مشکلاتی را برای شرکت‌ها، سازمان‌ها، کاربران خانگی و مجموعه‌هایی که با اینترنت بیشتر سروکار دارند، رواج پیدا کرده است.

روند ترویج بدافزارهای باج‌گیر اینترنتی با انتشار بدافزاری تحت عنوان «ویروس پلیس» آغاز و در برخی از آن‌ها با استفاده از آرم و علائم پلیس، اقدام به ترساندن و باج‌گیری از کاربران به دلایل قانون‌گریزی و عدم رعایت استانداردهای اینترنتی، می‌نمایند و موفق شدند مبالغ زیادی را به‌عنوان جریمه نقدی از کاربران ساده‌لوح اخاذی کنند.

با گذشت زمان، باج‌افزارها به‌جای تظاهرکردن از سمت قانون (پلیس)، با شهامت کامل خود را یک بدافزار خطرناک معرفی کرده و فایل‌های کاربران را با الگوریتم پیشرفته‌ای رمزگذاری می‌کنند. بدافزار ادعا می‌کند که با دریافت مبالغ تعیین‌شده، کلید رمز را در اختیارشان قرار می‌دهد که البته هیچ‌گونه تضمینی برای بازگشت فایل‌های نابودشدهٔ آن‌ها وجود نخواهد داشت.

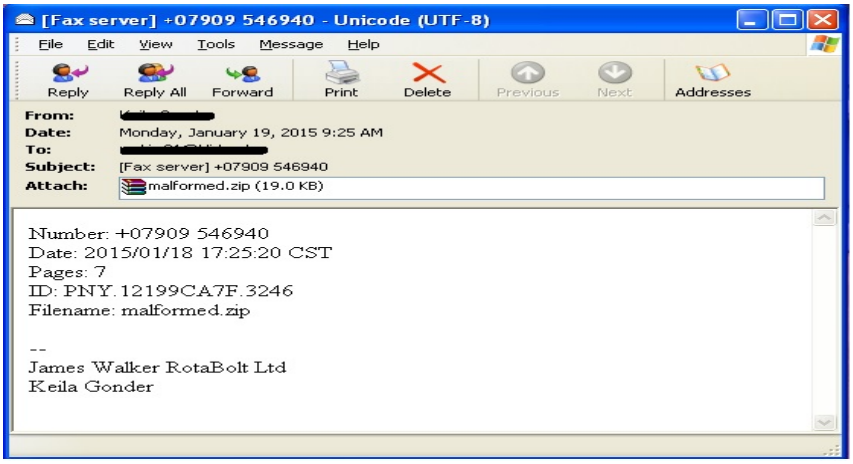
اهمیت و ضرورت تحقیق

امروزه بخش اعظمی از فعالیت کاربران با استفاده از سیستم‌های رایانه‌ای به‌خصوص در بستر اینترنت انجام می‌پذیرد، بنابراین عدم دسترسی به رایانه و داده‌های رایانه‌ای کاربر می‌تواند مشکلاتی را برای کاربران فراهم نماید و از طرفی پرداخت پول غیرقانونی و یا اجباری به مجرمان، می‌تواند علاوه بر صدمات مالی به کاربر و کشورها، باعث تقویت و ارتقای روش‌ها، سیستم‌ها و فعالیت مجرمان شود. در این راستا انجام اقدام‌های پیشگیرانه، بازدارنده و همچنین مقابله‌ای، امری بسیار لازم و ضروری می‌باشد. بنابراین انجام این تحقیق می‌تواند در کاهش صدمه‌ها و خسارت‌ها نقش بسزایی ایفا نماید.

روش کار و نحوه فعالیت بدافزارهای باج‌گیر

مجرمان سایبری با استفاده از تکنیک‌های مهندسی اجتماعی و ازطریق هرزنامه‌ها، لینک‌های ناشناخته، شبکه‌های مجازی اجتماعی، نرم‌افزارهای آلوده و سایر موارد، کاربران را به نوعی فریب داده و فایل آلوده را به سیستم آن‌ها منتقل و رایانه‌ها را آلوده می‌کنند. البته برخی از نسخه‌های این بدافزار می‌تواند ازطریق فایل‌های فشرده شده یا Zip و به‌صورت پیوست ایمیل، با یکی از نام‌های simoniac.zip، malformed.zip، plenitude.zip، inquires.zip، faltboat.zip، incurably.zip، payloads.zip،

dessiatine.zip بدافزار را برای کاربر ارسال و سیستم را آلوده نماید (دانشگاه تهران، پردیس بین‌المللی کیش، ۱۳۹٤).



برابر بررسی صورت گرفته، متأسفانه روش‌ها، شیوه‌ها و تکنیک‌های مورد استفاده مجرمان توسط بدافزارهای باج‌گیر، اغلب ناشناخته و بدیع است و بسیاری از مجرمان با استفاده از این بدافزارها در انجمن‌های زیرزمینی فعالیت می‌کنند. عدم آگاهی کاربران و وجود ضعف‌های امنیتی (باگ‌ها) رایانه، بیشترین قربانی را در این خصوص به‌دنبال داشته است، بنابراین لازم است کاربران درخصوص رفع مشکلات سیستم‌ها اقدام و آگاهی کاربران در زمینه شیوه و روش‌های این‌گونه بدافزارها، افزایش یابد تا در دام این مجرمان گرفتار نشوند.

عمده روش‌ها و تکنیک‌های مشخص‌شده توسط این بدافزارها از جمله بدافزار پلیس[۱] پاک‌کردن اطلاعات، رمزنگاری فایل‌ها، قفل‌کردن صفحه نمایش کاربر، قفل‌کردن صفحه نمایش همراه با نمایش تصاویر جنسی (در این مورد برخی از کاربران از شرم نمایش تصاویر جنسی و عدم امکان حذف آن و همچنین ترس از دیگران، بدنام‌شدن کاربر، احتمال تحت تعقیب قرار گرفتن و...، اقدام به پرداخت مبلغ درخواستی می‌نمایند)، تهدید کاربر تحت عنوان بازدید از سایت‌های تروریسم، مستهجن و کودک‌آزاری (هر چند که کاربر از این سایت بازدید نداشته است)، روشن‌کردن وِب‌کم رایانه و نمایش

۱ Police Ransomware

تصویر وب‌کم در یک پنجره قفل‌شده، هَک سایت‌ها و هدایت ترافیک در مسیر مدنظر مجرمان به‌خصوص سایت‌های آلوده به بدافزارها، مهندسی اجتماعی و تشویق کاربر به انجام اقدام‌های دلخواه مجرمان و... مشخص شده که این روش‌ها باتوجه به فرهنگ، موقعیت جغرافیایی (کشور)، نوع اطلاعات کاربران، نوع سرویس‌های ارائه شده از سوی سایت‌ها و... متفاوت می‌باشد (مرکز جرائم سایبری اتحادیه اروپا، ۲۰۱٤).

یکی دیگر از روش‌های مجرمان، به دام انداختن کاربرانی است که از سایت‌های پورنو بازدید می‌نمایند. در این روش چنانچه کاربر از سایت‌های خاص (پورنو، کودک‌آزاری و...) بازدید نماید، این بدافزار تحت پوشش پلیس، عمل کاربر را جرم اعلام می‌نماید و کاربر را مجبور به پرداخت مبلغ خاص می‌نماید.

متأسفانه بعد از آلوده‌شدن رایانه به بدافزارهای مخرب باج‌گیر، نرم‌افزارهای امنیتی از جمله ضد ویروس‌ها، سامانه‌های رمزگشایی و... هیچ کاری از پیش نخواهند برد و در نهایت فایل‌های باارزش کاربر که جزو دارایی‌های مهم او محسوب می‌شود، غیرقابل بهره‌برداری یا غیرقابل استفاده خواهد شد. شکل زیر، نمونه‌ای از عملکرد بدافزار باج‌گیر با پوشش FBI است که ضمن قفل‌کردن صفحه رایانه، با نمایش تصویر وب‌کم، دلایل قفل‌شدن رایانه را (دسترسی به سایت‌های پورنو، انجام اقدام‌های خلاف قانون و....) بیان کرده است (Anand Ajjan, 2013).

مجرمان فعال در این زمینه به‌منظور جلوگیری از ردیابی و گرفتارشدن در دام قانون، علاوه بر فعالیت در انجمن‌های زیر زمینی، از تکنیک‌های امنیتی نظیر VPN (تونل‌های امن برای دریافت مبلغ و...) و سایر تجهیزات و روش‌ها استفاده می‌نمایند.

در گذشته نرم‌افزار باج‌گیر معروفی که با نمایش جعلی‌بودن نرم‌افزار ضد ویروس، کاربر را مجبور به خرید نرم‌افزار ضد ویروس می‌کرد و از این طریق کلاهبرداری‌های متعددی صورت گرفت. تحقیقات نشان می‌دهد بسیاری از افرادی که با بیان جعلی‌بودن ضد ویروس، کاربران را فریب می‌دادند، درحال حاضر متولی ارائه بدافزارهای پلیس هستند.

بدافزار پلیس[۱] اولین بار در سال ۲۰۱۱ در اتحادیه اروپا منتشر شد و پس از آن در سطح جهان شروع به فعالیت نمود. امروزه تکنیک‌ها و روش‌های باج‌گیری ازطریق این نرم‌افزار تکامل یافته و با انواع تایمر شمارش معکوس، تهدید و فشار و... کاربر را مجبور به پرداخت مبلغ تعیین‌شده می‌نمایند.

۱ police ransomware

به‌منظور جلوگیری از ردیابی مجرمان توسط قانون، مجرمان بعضاً از واحد پول بین‌المللی جدیدی به نام بیت‌کوینت[۱] استفاده می‌کنند.[۲]

نمونه‌ای از باج‌گیری که با واحد پولی بیت‌کوینت، درخواست باج شده است را در تصویر زیر مشاهده می‌کنید.

۱. bitcoins

۲. در این روش افراد با خرید یک کوپن حاوی یک کد چند رقمی و واردکردن کددر پنجره پاپ آپ، می‌توانند مبلغ مدنظر جهانی را مبادله (پرداخت) نمایند. در اکثر کشورها، خرید طریق صرافی‌های آنلاین با انتقال پول از حساب بانکی خود و یا کوپن (کاغذهای حاوی کد چند رقمی) را می‌توان به‌راحتی از بسیاری از دکه‌ها، مغازه‌های خرده‌فروشی، فروشگاه‌ها، پمپ بنزین‌ها، دستگاه‌های خودپرداز، کیوسک‌ها و یا آنلاین با پرداخت هزینه، خریداری کرد.

در مجموع روند استفاده از نرم‌افزارهای باج‌گیر رو به افزایش است.

قربانیان (افرادی که رایانه آن‌ها مورد حمله قرار گرفته و به یکی از روش‌ها گرفتار شده‌اند) به دلایلی از جمله: ترس از دوستان، همکاران، والدین و...، عدم آگاهی از تهدیدهای آنلاین، ترس از پلیس و قانون مبنی بر اعلام گزارش جرم ناشی از تماس یا مشاهده وب‌سایت‌های غیرقانونی، عدم امکان کنترل مجدد رایانه، عدم برگرداندن اطلاعات رایانه و...، بدون فوت وقت اقدام به پرداخت غرامت می‌نمایند و با این اقدام به مدل کسب و کار پر سود مجرمان، کمک می‌کنند (مرکز جرائم سایبری اتحادیه اروپا، ۲۰۱٤).

در کشور ما ایران هرچند که زمینه و بستر لازم برای پرداخت مبالغ تعیین شده (توسط باج‌گیران) فراهم نیست و در این خصوص نگرانی کمتری وجود دارد، اما آنچه که مشکل آفرین شده و خواهد شد، از بین رفتن اسناد دیجیتالی باارزش کاربران است و معمولاً در صورت آلوده شدن سیستم، بازگشت اطلاعات به حالت اولیه تقریباً غیر ممکن است.

بررسی نمونه‌هایی از بدافزار باج‌گیر

۱. بدافزار CTB locker

این بدافزار که اخیراً بیشترین فعالیت را دارد، ازطریق پیوست‌های ایمیل انتشار پیدا کرده و با رمزکردن فایل‌های کاربر، برای بازگرداندن آن‌ها درخواست باج (پول) می‌کند. این بدافزار مانند دیگر بدافزارهای باج‌گیر از قبیل Crypto Locker، Torrent Locker،

فایل‌هایی با پسوندهای mp4، pem، jpg، doc، cer، db و... که معمولاً فایل‌های اصلی کاربر می‌باشد را با یک کلید نامشخص رمز می‌کند؛ به گونه‌ای که کاربر نمی‌تواند از فایل‌های خود استفاده کند. سپس این بدافزار پس از پایان کار خود پیامی را روی صفحه کاربر با زبان‌های مختلف (مطابق با منطقه) نشان می‌دهد، حتی برای اطمینان به کاربر اجازه می‌دهد تا ۵ فایل دلخواه خود را رمزگشایی کند. سپس صفحه‌ای برای پرداخت پول، به صاحب سیستم نمایش می‌دهد.

در گونه جدید CTB-Locker، مبلغ اخاذی به ۳ بیت‌کوین (حدود ۷۵۰ دلار) افزایش پیدا کرد. ضمن اینکه مهلت پرداخت باج از ۷۲ ساعت به ۹۶ ساعت تغییر یافته است (www.irkaspersky.com).

در نسخه‌های مختلف CTB-Locker، گاهی کار با کدگذاری فایل‌ها تمام نمی‌شود و بدافزار لیست ایمیل مخاطبان کاربر را هم یک کپی گرفته و از آن به منظور شناسایی قربانیان بعدی استفاده می‌کند. شاید بخش نگران‌کننده این باشد که فرد کلاهبردار با یک آدرس ایمیل جعلی، قربانیان را مورد حمله قرار می‌دهد. بنابراین احتمال دارد هرزنامه از طرف یکی از دوستان خود برایتان ارسال شود.

همان‌طورکه قبلاً اشاره شد، یکی از روش‌های آلوده‌شدن سیستم‌ها ازطریق پیوست ایمیل است و تاکنون مواردی که در قسمت موضوع[1] ایمیل‌ها گزارش شده، به قرار زیراست:

- [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

عنوان CTB برگرفته از عبارت Curve Tor Bitcoin است که در آن Curve معرف رمزگذاری پیچیده Elliptical Curve Encryption می‌باشد. بسیاری از نرم‌افزارهای

۱. Subject

ضدویروس قادر به شناسایی این بدافزار هستند و ضدویروس مکافی ضمن بررسی و ارائه راهکارهای پیشگیرانه، نحوه استفاده از ضدویروس و مقابله با بدافزار را در سایت و سند تنظیمات مربوط ارائه کرده که عبارت‌اند از: (Mcafee Labs Threat advisory CTB-Locker, 2015).

الف. شناسایی و جلوگیری از آلوده‌شدن به بدافزار

باتوجه به شیوع گسترده این بدافزار در سراسر دنیا، متأسفانه هنوز هیچ ابزاری که بتواند فایل‌های کدگذاری یا رمزگذاری شده را بازیابی کند، پیدا نشده است. بدافزار CTB-Locker ازطریق ایمیل و یک فایل zip وارد سیستم شده و پس از اینکه از حالت فشرده خارج شود، شروع به دانلود بدافزار ازطریق شبکه می‌کند. پس از بارگذاری، این بدافزار شروع به رمزگذاری فایل‌ها کرده و سپس از کاربر برای رمزگشایی این فایل‌ها درخواست پول می‌کند.

برای جلوگیری از ورود این بدافزار به سیستم، نیاز به تنظیماتی است که در این بخش به بررسی تنظیمات مربوط می‌پردازیم تا از نفوذ خودکار این بدافزار ازطریق فایل zip جلوگیری شود.

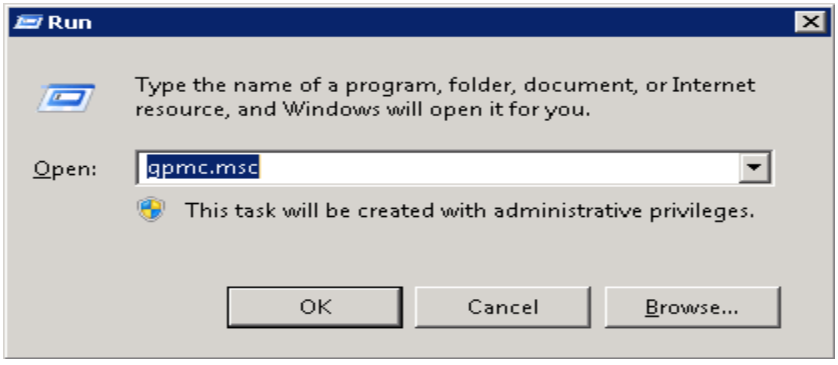
این بدافزار فایل‌های اجرایی خود را به مسیر ٪TEMP٪ منتقل می‌کند و شما به‌صورت دستی یا ازطریق آنتی ویروس خود می‌توانید آن‌ها را پاک کنید. برای بازگردانی فایل‌های خود نیز ممکن است بتوانید از نرم‌افزارهای بازگردانی اطلاعات از جمله Recuva استفاده کنید تا نسخه‌های پیشین فایل‌های خود را بیابید.

مهم‌ترین نکته برای جلوگیری از ورود این بدافزار، آگاهسازی کاربران برای عدم بازگشایی ایمیل‌های ناخواسته می‌باشد. معمولاً کاربران برای بازکردن فایل‌های ضمیمه ازطریق خود ایمیل این کار را انجام می‌دهند و چون این بدافزار ازطریق فایل zip منتشر می‌شود، می‌توان مراحل زیر را نیز برای جلوگیری از بازشدن این فایل‌ها به‌صورت غیر عمدی توسط کاربران انجام داد. این مراحل بر روی Active Directory و بر روی یک سیستم Local توضیح داده شده‌اند.

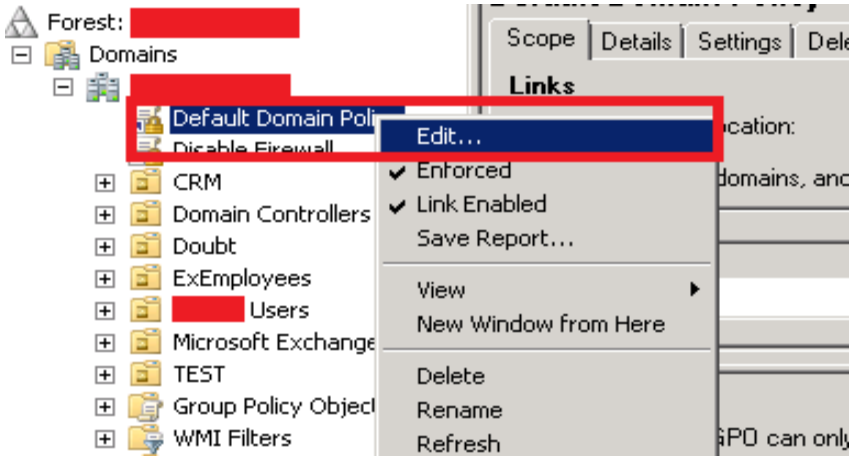
نکته مهم: باتوجه به اینکه نوع سیستم عامل رایانه‌ها و نوع سرویس‌ها یا خدماتی که ارائه می‌کنند، متفاوت می‌باشد، اعمال تنظیمات زیر نیاز به دانش تخصصی دارد، چرا که برخی از تنظیمات ممکن است مشکلاتی را برای رایانه به‌وجود آورد. بنابراین اعمال تنظیمات برای تمام رایانه‌ها توصیه نمی‌شود و در صورت تسلط بر رایانه و سرویس‌هایی که ارائه می‌شود و همچنین شناخت دستورها، متناسب با نیاز تنظیمات اعمال گردد. ضمن اینکه سایر راهکارها نیز بررسی و متناسب با نوع فعالیت رایانه‌ها، اقدام پیشگیرانه لازم صورت پذیرد.

محدودکردن فایل‌های ZIP در زمان Extract شدن در Active Directory

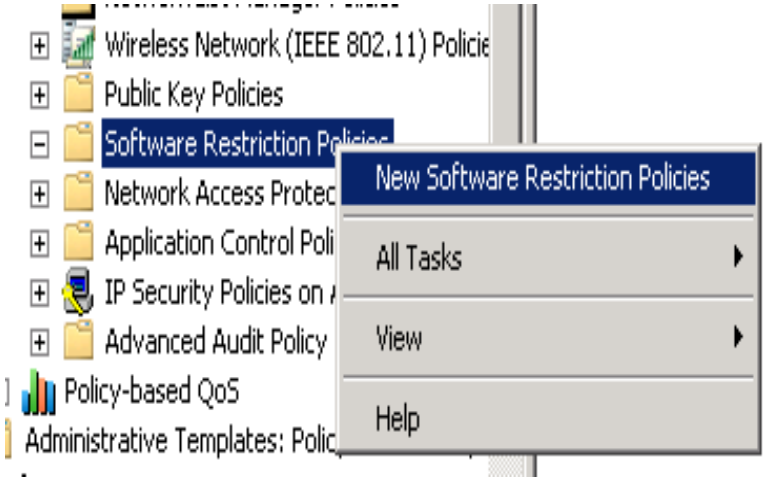
ابتدا بر روی سرور AD خود در Run گزینه gpmc.msc را وارد کنید.



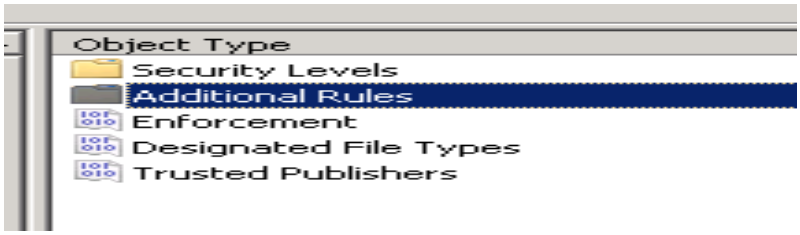
سپس مانند تصویر بروی Policy مربوطه کلیک راست کرده و گزینه Edit را انتخاب کنید.



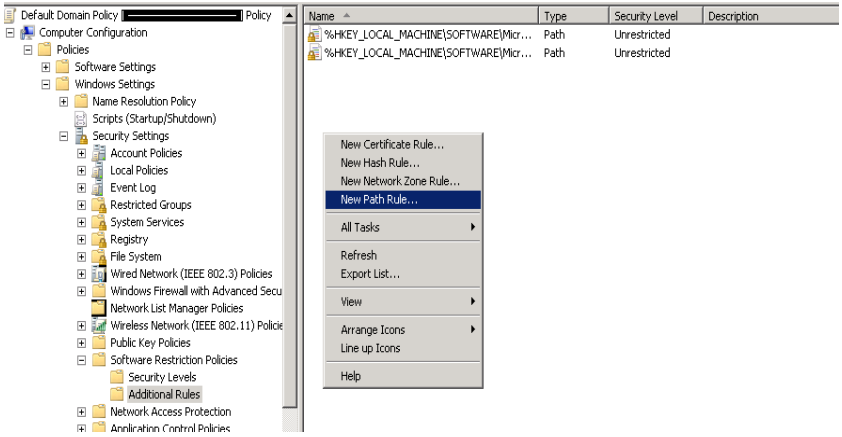
پس از این کار، بر روی قسمت Software Restriction Policy کلیک راست کرده و گزینه New Software Restriction Policy را انتخاب کنید.



سپس به Additional Rules وارد شوید.



سپس کلیک راست کرده و گزینه New Path Rule را انتخاب کنید.



در پنجره باز شده در قسمت Path، مسیرهای زیر را وارد کرده و Security Levelرا بر روی Disallowed قرار دهید.

```
%AppData%\*.exe
%UserProfile%\Local Settings\*.exe
%LocalAppData%\*.exe
%AppData%\*\*.exe
%UserProfile%\Local Settings\*\*.exe
%LocalAppData%\*\*.exe
%UserProfile%\Local Settings\Temp\Rar*\*.exe
%LocalAppData%\Temp\Rar*\*.exe
%UserProfile%\Local Settings\Temp\7z*\*.exe
%LocalAppData%\Temp\7z*\*.exe
%UserProfile%\Local Settings\Temp\wz*\*.exe
%LocalAppData%\Temp\wz*\*.exe
%UserProfile%\Local Settings\Temp\*.zip\*.exe
%LocalAppData%\Temp\*.zip\*.exe
```

برای تغییر در سیستم‌ها به‌صورت Local نیز در Run گزینه SecPol.msc وارد کرده و همین روال را بروید (www.irkaspersky.com).

گونه‌های جدید این بدافزار با نام‌های BackDoor-FCKQ، Downloader-FAMV و Injector-FMZ توسط ضدویروس McAfee شناسایی می‌شوند (دانشگاه تهران پردیس بین‌المللی کیش، ۱۳۹٤).

ب. بازگشت به حالت اولیه (قبل از آلوده شدن)

از نظر فنی راه‌حلی برای بازگرداندن فایل‌های رمز شده وجود ندارد و اگر هم وجود داشته باشد، بسیار پیچیده، سخت و نیاز به زمان طولانی و هزینه گزاف دارد، اما احتمال بازیابی برخی از فایل‌ها (نسخه قدیمی) وجود دارد. بنابراین استفاده از نرم‌افزارهای بازیابی اطلاعات از جمله Recuva و... ممکن است بتواند بخشی از اطلاعات ارزشمند را بازیابی کند.

۲. CryptoLocker

همان‌طور از نام این بدافزار پیداست، این بدافزار ازطریق رمزکردن داده اقدام به زورگیری می‌کند و در دنیای فناوری اطلاعات و ارتباطات، فعالیت‌های تخریبی زیادی داشته است.

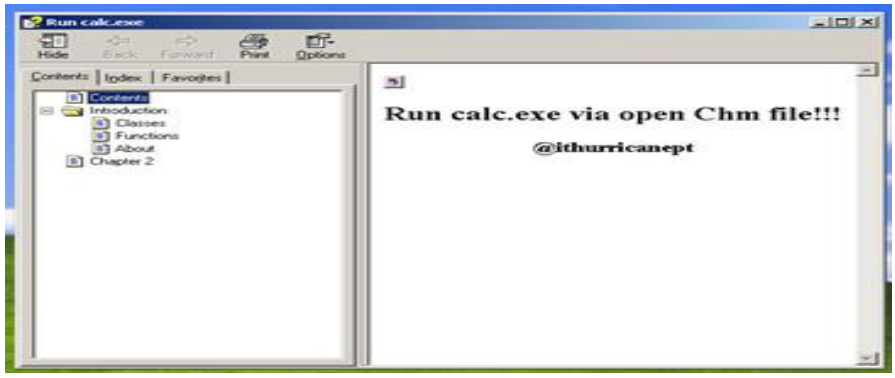
برخی از شرکت‌ها و مؤسسه‌های امنیتی توصیه کردند که در صورت گرفتارشدن در دام این باج‌گیر اینترنتی (کریپتولاکر) اگر فایل‌های شما رمزنگاری شد و حتی هیچ‌گونه نسخه پشتیبانی از آن‌ها در دست نداشتید، باز هم هیچ‌گونه هزینه‌ای برای بازیافت (رمزگشایی) فایل‌های خود پرداخت نکنید؛ چرا که تجربه نشان داده حتی در صورت پرداخت هزینه، باز هم نتیجه‌ای نخواهید گرفت.

این بدافزار (CryptoLocker) که بدنام‌ترین باج‌افزارهای فضای سایبر به حساب می‌آید، در سال‌های گذشته فعالیت‌های تخریبی فراوانی را در سوابق خود به ثبت رسانده و مبالغ هنگفتی را از کاربران دریافت کرده و از آن به‌عنوان یک «مدل تجاری» نام برده می‌شود. روش کار آن مانند باج‌گیرهای دیگر، رمزنگاری برخی فایل‌های کاربران است و برای آزادسازی اطلاعات (رمزگشایی)، مبالغ هنگفتی را از کاربران اخاذی می‌کند.

این بدافزار در کشورهای امریکا، کانادا، انگلیس، استرالیا و هند به ترتیب بیشترین فعالیت را داشته و ازطریق واحد پولی دلار امریکا و بیت‌کوینت، زورگیری می‌کند (Cryptolocker Q&AMenace of the Year , 2015).

۳. بدافزار CryptoWall

براساس گزارش ارائه شده در نشریه SC امنیت حرفه‌ای برای فناوری اطلاعات، در تاریخ ۲۹ آگوست ۲۰۱٤ اعلام نموده که بدافزار CryptoWall در یک دوره پنج‌ماهه بیش از ٦۲۵۰۰۰ قربانی در سراسر جهان داشته و حدود ۵/۲۵۰/۰۰۰/۰۰۰ فایل را آلوده و بیش از ۱,۱ میلیون دلار غرامت جمع‌آوری کرده است.

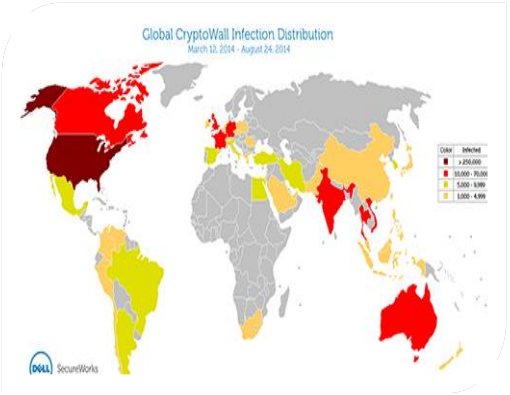


بدافزار باج‌گیر Cryptowall ازطریق ایمیل و با استفاده از فایل‌های chm و فایل‌های راهنما[1] سیستم‌ها را آلوده می‌کند. محققان آزمایشگاه شرکت Bitdefender معتقدند که هدف مهاجمان از نفوذ به سیستم کاربران، دسترسی به شبکه‌های خصوصی سازمان‌های مختلف می‌باشد.

با اجرا یا مشاهده فایل‌های آلوده از جمله پسوند chm، کدهای تخریبی از مسیر سرور http: //**********/putty.exe دانلود و در مسیر %temp%\natmasla2.exe ذخیره و بدافزار به‌طور اتوماتیک اجرا و در طول اجرای بدافزار مذکور، پنجره اجرای فرامین ویندوز باز می‌گردد (Help Net Security,2015).

۱ Help

بر اساس گزارش Dell secure works که در تاریخ ۲۷ آگوست ۲۰۱٤ ارائه شده، کشورمان ایران نیز قربانیان فراوانی از ناحیه این بدافزار داشته و بر همین اساس در صدر کشورهای آلوده‌شده به این بدافزار می‌باشد (رتبه سوم در جهان). جزئیات نحوه آلوده‌شدن سیستم‌ها، پاکسازی سیستم‌های آلوده شده و فرایند کار و سایر موارد به‌صورت مشروح در این گزارش قید شده است[۱] (Dell SecureWorks, 2014).



COUNTRY	INFECTED SYSTEMS	PERCENTAGE OF TOTAL
India	266	27.5%
United States	141	14.6%
Iran	112	11.6%
Singapore	93	9.6%
Poland	55	5.7%
Pakistan	49	5.1%
Turkey	42	4.3%
Brazil	40	4.1%
Sri Lanka	27	2.8%
Indonesia	23	2.4%

تجزیه و تحلیل

برابر مطالعات انجام شده، ضعف سیستم‌ها، عدم آگاهی کاربران، ابزارهای نوین و پیشرفته در فضای سایبر برای سوء استفاده، دانش بالای مجرمان و... مواردی هستند که باعث می‌شود مجرمان یک گام جلوتر از کاربران باشند و برای اغفال کاربران، صدمه‌زدن به سیستم‌ها و باج‌گیری اقدام نمایند. معمولاً اطلاع‌رسانی به مردم درخصوص شیوه و شگردهای مجرمان و بدافزارها بنا به دلایلی، یا با تأخیر انجام می‌شود و یا به لحاظ ملاحظات امنیتی ناقص یا به شکل کلی‌گویی، اطلاع‌رسانی می‌شود و از طرفی تخصصی‌بودن موضوع‌ها منجر به افزایش سوء استفاده شده است. یقیناً با افزایش آگاهی مردم و افشای شیوه و شگردهای بدافزارهای باج‌گیر نظیر بدافزار باج‌گیر پلیس، آمار قربانیان در این زمینه کاهش خواهد یافت و به‌طور مطمئن مجرمان به‌دنبال روش‌های جدید خواهند رفت.

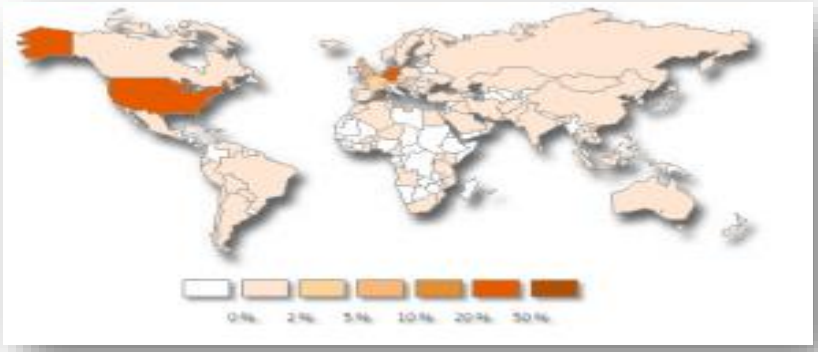
۱ . در صورت نیاز به اطلاعات بیشتر به سایت زیر مراجعه شود

http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware

باتوجه به اینکه رمزگشایی موارد رمز شده بسیار پیچیده و نیاز به کلید خصوصی دارد و ازآنجاکه این کلید صرفاً در اختیار مجرمان قرار دارد، با استفاده از روش‌های نوین، در آینده هزینه‌های هنگفتی از سوی قربانیان به جیب مجرمان واریز خواهد شد. مردم بسیاری از توصیه‌ها را جدی نمی‌گیرند و یا اینکه توان اجرای برخی از ملاحظه‌های امنیتی را ندارند، بنابراین زمینه را برای سوء استفاده مجرمان فراهم می‌نمایند.

تجربه نشان داده تا جرمی فراوانی آن بالا نباشد، متولیان امر اقدام جدّی انجام نمی‌دهند، اما برخی از مواقع یک مورد هم ممکن است خطرآفرین و مشکل‌ساز باشد، مثلاً رمزشدن داده‌های بانکی! یا سیستم‌های حساس و مهم.

همان‌طورکه در تصویر روبه‌رو مشاهده می‌شود، بدافزارهای باج‌گیر تقریباً در سطح جهان رواج پیدا کرده و روز به روز درحال افزایش و گسترش هستند. کشورمان نیز در زمره کشورهای آلوده به این بدافزارها می‌باشد.



Ransomware: A Growing Menace, Symantec security response,2012

تمام مراجع و مراکز امنیتی مهم و غیر مهم جهان، اولین و مهم‌ترین نکته‌ای که یادآوری می‌کنند، تهیه نسخه پشتیبان یا بکاپ از اطلاعات است. بنابراین قبل از هر اقدامی، تهیه نسخه پشتیبان برای تمام اطلاعات باارزش و حتی سیستم عامل رایانه برای بازگشت به حالتِ قبل از آلودگی، توصیه می‌شود.

راهکارها و پیشنهادها

باتوجه به اهمیت و حساسیت سیستم‌های رایانه‌ای و نقش آن‌ها در زندگی روزمره و اداره نمودن جامعه و... مهم‌ترین راهکارها و پیشنهادها به‌منظور پیشگیری و جلوگیری از به دام افتادن بدافزارهای زورگیر، به‌شرح زیر بیان می‌گردد:

۱. رصد شیوه و شگردهای کلاهبرداری از جمله زورگیری در بستر فضای سایبر توسط نیروی انتظامی و سایر مراجع مرتبط؛
۲. برخورد با متخلفان و مجرمانی که در فضای سایبر اقدام به کلاهبرداری یا زورگیری می‌کنند؛
۳. اطلاع‌رسانی در مورد آخرین شیوه و شگردهای احصا شده توسط نیروی انتظامی به جامعه، به‌منظور پیشگیری از ارتکاب جرائم؛
٤. تصویب قوانین و مقررات بازدارنده برای جلوگیری از زورگیری‌های اینترنتی، متناسب با پیشرفت فناوری و اهمیت دارایی‌ها در بستر فضای سایبر در سطح ملی و بین‌المللی؛
۵. تهیه نسخه بکاپ یا پشتیبان[۱] از تمام اطلاعات مهم و حتی سیستم عامل‌ها و... و نگهداری نسخه پشتیبان اطلاعات در محلی اَمن و خارج از سیستم مورد بهره‌برداری (با این روش حتی در صورتی که دیسک سخت‌افزاری (هارد) آسیب ببیند، باز هم فایل‌های از بین رفته به سادگی قابل استفاده خواهند بود)؛
٦. استفاده از ابزارهای امنیتی مناسب، از جمله نرم‌افزار ضدویروس قدرتمند و به‌روز برای تمامی رایانه‌ها؛
۷. سیستم عامل، نرم‌افزارهای کاربردی و سایر ابزارهای مورد استفاده خود را همیشه به‌روز نگه دارید و وصله‌های امنیتی[۲] منتشرشده را بلافاصله پس از انتشار نصب کنید تا هرچه سریع‌تر آسیب‌پذیری موجود در سیستم خود را برطرف کنید؛

---

۱ backup

۲ Patch

۸. به‌کارگیری راه‌حل‌های امنیتی برای ایمیل‌ها، مانند فعال‌سازی فیلترکردن پسوند فایل‌های ضمیمه مانند scrها برای بلوکه‌کردن فایل‌های آلوده؛
۹. خودداری از بازکردن ضمایم ایمیل‌هایی که از سوی افراد ناشناس ارسال شده است، به‌خصوص فایل‌های Scr، zip و سایر موارد مشخص شده و مشکوک؛
۱۰. پاک‌کردن یا اِسپَم‌کردن ایمیل‌های مشکوک و هشدار به دیگران؛
۱۱. براساس گزارش مراکز امنیتی، مشخصات ایمیل‌های مشکوک و ناشناخته‌ای که اعلام شده خصوصاً مواردی که به همراه خود فایل ضمیمه دارند را از صندوق ورودی خود حذف کنید؛
۱۲. قابلیت «پنهان‌کردن پسوند فایل‌ها» که به‌طور پیش‌فرض روی ویندوز فعال است را غیر فعال کنید. با این اقدام، در صورت مشاهده فایل‌های مشکوکی که پسوند یک فایل اجرایی دارند، می‌توان آن‌ها را شناسایی و از کلیک‌کردن روی آن خودداری و آن‌ها را حذف کرد؛
۱۳. فعال‌سازی تمامی ماژول‌های حفاظتی و تنظیمات ارائه شده برای سیستم‌ها جهت مقابله با بدافزارهای باج‌گیر، امری الزامی است؛
۱٤. در صورتی که فایل‌ها توسط بدافزارها رمزنگاری شد و هیچ‌گونه نسخه پشتیبانی از آن‌ها در دست نداشتید، باز هم هیچ هزینه‌ای بابت بازیافت فایل‌های نابود یا رمزشدهٔ خود پرداخت نکنید؛ چرا که با این کار، مسیر تازه‌ای برای درآمدزایی مجرمان اینترنتی به‌وجود می‌آید و علاوه بر این، با پرداخت هزینه مقرر شده، هیچ‌گونه تضمینی برای بازیابی فایل‌های آسیب‌دیده وجود نخواهد داشت؛
۱۵. در صورتی که اطلاعات رایانه به یکی از ویروس‌های باج‌گیر آلوده و فایل‌ها حذف یا رمز شده باشد و همچنین نسخه پشتیبان از اطلاعات در اختیار ندارید، یکی از روش‌های احتمالی دسترسی به بخشی از اطلاعات، بازیابی[۱] کپی‌های قبلی از فایل‌های مدنظر است؛

۱ Recovery

۱٦. فقط فایل‌هایی را از اینترنت دانلود کنید که صددرصد به اعتبار و امنیت آن اعتماد دارید. اگر اندکی نسبت به امنیت یا اصالت فایلی تردید دارید، آن را دانلود نکنید و یا بعد از دانلود، قبل از هر اقدامی ازطریق ضدویروس مناسب آن را کنترل کنید؛

۱۷. مراقب فایل‌های فشرده (zip و rar) که حاوی فایل‌های اجرایی با پسوند exe و یا scr هستند، باشید؛

۱۸. برنامه‌های امنیتی و ضدویروس نصب‌شده بر روی سیستم‌ها را به‌طور دائم به‌روز کنید. سعی کنید از نرم‌افزارهایی استفاده کنید که علاوه بر اصلیت و رسمیت لایسنس، دارای پشتیبانی و خدمات فنی قابل قبول باشند؛

۱۹. در شبکه‌های سازمانی و حتی در رایانه‌های خانگی، دسترسی افراد به اینترنت را جدّی بگیرید و تحت کنترل دائم قرار دهید؛

۲۰. به‌صورت مداوم «فایل‌های موقت» اینترنتی و یا نرم‌افزاری سیستم[1] را به‌طور کامل پاک کنید؛

۲۱. حافظه‌های جانبی مانند فلش‌مموری، دیسک‌ها، پخش‌کننده‌های موسیقی و... می‌توانند حامل بدافزارهای باج‌گیر باشند، قبل از بازکردن درایو سخت‌افزاری، آن را کامل با برنامه ضدویروس اسکن کنید؛

۲۲. حتی‌الامکان سعی شود با شناسه کاربری سطح پایین در سیستم عامل‌ها فعالیت کنید؛

۲۳. از وبگردی در وب‌سایت‌های ناشناس و همچنین کلیک روی لینک‌های ناشناخته و مشکوک، خودداری کنید؛

۲٤. نسبت به تبلیغات سایت‌ها حساس باشید و بر روی لینک‌های تبلیغاتی ناشناخته کلیک نکنید.

---

۱ Temporary Files

منابع

- سایت http://www.irkaspersky.com، نماینده رسمی کاسپرسکای در ایران، جلوگیری از انتشار CTB-Locker.
- سایت http://kish.ut.ac.ir، دانشگاه تهران، پردیس بین‌المللی کیش، انتشار گونه جدیدی از باج‌افزار.
- سایت http://www.certcc.ir، مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای.
- سایت مرکز جرائم سایبری اتحادیه اروپا به آدرس:
- European cybercrime center ,EUROPOL PUBLIC INFORMATION, Police Ransomware Threat Assessment.
- سایت مرکز محافظت بدافزار مایکروسافت به آدرس:
- http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx.
- Anand Ajjan, Ransomware Next-Generation Fake Antivirus, ۲۰۱۳
- Mcafee Labs Threat advisory CTB-Locker, ۲۰۱۵
- Ransomware: A Growing Menace, Symantec security response,۲۰۱۲
- Cryptolocker Q&AMenace of the Year , ۲۰۱۵, http://www.symantec.com/ connect/blogs/cryptolocker-qa-menace-year.
- Cryptolocker Q&AMenace of the Year , ۲۰۱۵
- Help Net Security, Cryptowall makes a comeback via malicious help files, ۲۰۱۵
- Dell SecureWorks, CryptoWall Ransomware, http://www.secureworks.com/cyber-threat-intelligence/threats/ cryptowall-ransomware/ ۲۰۱٤