حفاظت از سازمان در برابر

باج‌افزارهای رمزگذار

شبکه گستر
شرکت مهندسی شبکه گستر

عنوان سند: حفاظت از سازمان در برابر باج‌افزارهای رمزگذار

شناسه سند: SPT-A-0121-00

تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

تاریخ تهیه: دی ماه ۱۳۹۵

انتشار اولین نسخه از باج‌افزار معروف CryptoLocker در خرداد ماه سال ۱۳۹۳ و موفقیت‌های کم‌نظیر آن در اخاذی از کاربران را می توان سرآغاز دوره‌ای جدید در دنیای ویروس‌نویسان دانست؛ دوره ای که در آن نوع جدیدی از بدافزارها موسوم به باج‌افزارهای رمزگذار کاربران و سازمان‌های کوچک تا بزرگ را به‌صورت گسترده هدف قرار داده‌اند.

باج‌افزارهای رمزگذار یکی از پرطرفدارترین و متأسفانه مخرب‌ترین بدافزارهایی هستند که در دو سال اخیر مورد استفاده تبهکاران سایبری قرار گرفته‌اند.

محدود کردن دسترسی به داده‌های حساس از طریق رمزنگاری، ارعاب کاربر و بدنبال آن اخاذی در ازای بازگرداندن این داده‌ها، هدف اصلی این نوع باج‌افزارها است. رمزگشایی فایل‌هایی که با طراحی زیرکانه به این روش رمزنگاری می‌شوند دشوارتر و در بسیاری مواقع غیرممکن است.

برآورد می‌شود گردانندگان باج‌افزار در سال میلادی ۲۰۱۶، در مجموع ۱ میلیارد دلار از راه باج‌گیری درآمد کسب کرده باشند.

اما دلایل موفقیت باج‌افزارهای رمزگذار چیست؟ کدام راهکار امنیتی می‌تواند بهترین حفاظت را برای سازمان در برابر این نوع تهدیدات فراهم کند؟

در این مقاله ضمن بررسی باج‌افزارهای رمزگذار به راه‌های مقابله با این تهدیدات پرداخته شده است.

شبکه گستر

انواع باج‌افزار

باج‌افزار یا Ransomware گونه‌ای بدافزار است که دسترسی به فایل‌های کاربر را محدود ساخته و برای دسترسی مجدد، از او درخواست باج می‌کند.

این محدودسازی ممکن است به چند روش انجام شود. در یک روش ساده، با نمایش دائمی یک تصویر بر روی صفحه، به‌نحوی که کاربر قادر به بستن و یا باز کردن پنجره دیگری نباشد، دسترسی کاربر محدود می‌شود. در تصاویر نمایش داده شده توسط این گونه باج‌افزارها، معمولاً، این طور القا می‌شود که قفل شدن کامپیوتر توسط نهادهای امنیتی و به دلیل نقض قوانین، انجام شده است.

شکل ۱: نمونه‌ای از تصویر نمایش داده شده توسط یک باج‌افزار قفل‌کننده صفحه

در این حالت با پاکسازی کامپیوتر توسط دیسک‌های نجات[۱] مجهز به ضدویروس دسترسی به اطلاعات مجدداً میسر می‌شود.

اما در روش‌های پیشرفته‌تر، ممکن است باج‌افزار اقدام به رمز کردن فایل‌های کامپیوتر کند. این نوع بدافزارها به باج‌افزارهای رمزگذار[۲] موسوم هستند. هدف از رمز کردن[۳]، محدود کردن دسترسی است؛ به‌نحوی که تنها با داشتن کلید رمزگشایی بتوان به محتوای فایل دست پیدا کرد. پیچیدگی و قدرت این کلیدها بر اساس تعداد بیت بکار رفته در ساخت کلید است. هر چه تعداد این بیت‌ها بیشتر باشد شانس یافتن آن هم دشوارتر و در تعداد بیت بالا عملاً غیرممکن می‌شود.

در گونه‌های حرفه‌ای باج‌افزارها، در هنگام رمزنگاری، برای هر دستگاه یک کلید خصوصی[۴] منحصربه‌فرد تولید شده و سپس به نویسنده باج‌افزار فرستاده می‌شود. بنابراین در صورت داشتن کلید خصوصی یک دستگاه رمز شده، نمی‌توان از آن برای دستگاه‌های دیگری که به آن باج‌افزار آلوده شده‌اند استفاده کرد. رمزگشایی فایل‌هایی که با طراحی زیرکانه به این روش رمزنگاری می‌شوند دشوارتر و در بسیاری مواقع غیرممکن است.

---

[۱] Rescue Disk
[۲] Crypto-ransomware
[۳] Encryption
[۴] Private Key

دلایل موفقیت باج‌افزارها

کم نیستند سازمان‌هایی که با وجود استفاده از محصولات امنیتی، قربانی حملات باج‌افزارها می‌شوند. اما رمز موفقیت باج‌گیران سایبری چیست؟

۱ تکنیک‌های پیشرفته و نوآوری مستمر در باج‌افزارهای رمزگذار

- گردانندگان باج‌افزارهای رمزگذار از ترفندهای مهندسی اجتماعی[۵] ماهرانه، برای تشویق کاربر به اجرای باج‌افزار استفاده می‌کنند.
- ارائه "باج‌افزار به عنوان سرویس"[۶] که حتی تبهکاران با دانش کم برنامه‌نویسی را نیز قادر به استفاده از باج‌افزارهای حرفه‌ای می‌کند. در این روش مبلغ اخاذی شده بین نویسنده و اجاره‌کننده باج‌افزار تقسیم می‌شود.

۲ ضعف‌های امنیتی سازمان‌ها

- نبود استراتژی صحیح تهیه نسخه پشتیبان[۷]
- عدم نصب مستمر اصلاحیه‌های امنیتی[۸] سیستم‌های عامل و نرم‌افزارها
- تخصیص نادرست حق دسترسی به کاربران و پوشه‌های اشتراکی[۹]
- عدم آگاهی‌رسانی به کاربران در خصوص نحوه برخورد با ایمیل‌ها و فایل‌های مشکوک
- نبود سیستم‌های امنیتی نظیر پویشگرهای ویروس[۱۰]، دیواره آتش[۱۱]، نفوذیاب[۱۲]، کنترل‌کننده وب[۱۳]، ضدهرزنامه[۱۴] و یا عدم پیکربندی صحیح آنها
- عدم تقسیم‌بندی شبکه‌ای[۱۵] سیستم‌های حساس و بااهمیت
- نبود سیاست‌های امنیتی جامع و صحیح؛ برای مثال مسدود نشدن ایمیل‌های با فایل پیوست حاوی ماکرو
- اولویت‌بندی نادرست و چشم‌پوشی از الزامات امنیتی با بیان عباراتی نظیر "ما می‌دانیم این روش امن نیست، اما کارکنان ما باید کار کنند!"

۳ کمبود فناوری پیشرفته حفاظتی در سازمان‌ها

- بسیاری از سازمان‌ها از راهکارهای امنیتی غیرجامع یا نامناسب بهره می‌گیرند.
- باج‌افزارها به‌طور پیوسته در حال تکامل بوده و فناوری‌های حفاظتی را دور می‌زنند.
- مقابله با نمونه‌های پیشرفته باج‌افزارهای رمزگذار مستلزم استفاده از محصولات امنیتی خاص است.

---

۵ Social Engineering
۶ Ransomware as a Service
۷ Backup
۸ Security Patches
۹ Shared Folder
۱۰ Antivirus
۱۱ Firewall
۱۲ Intrusion Prevention
۱۳ Web Control
۱۴ Antispam
۱۵ Network Segmentation

روش‌های انتشار

هرزنامه‌های با پیوست فایل آلوده و سایت‌های مخرب یا تسخیر شده حاوی بسته بهره‌جو از روش‌های رایج مورد استفاده تبهکاران سایبری برای انتشار باج‌افزارها هستند.

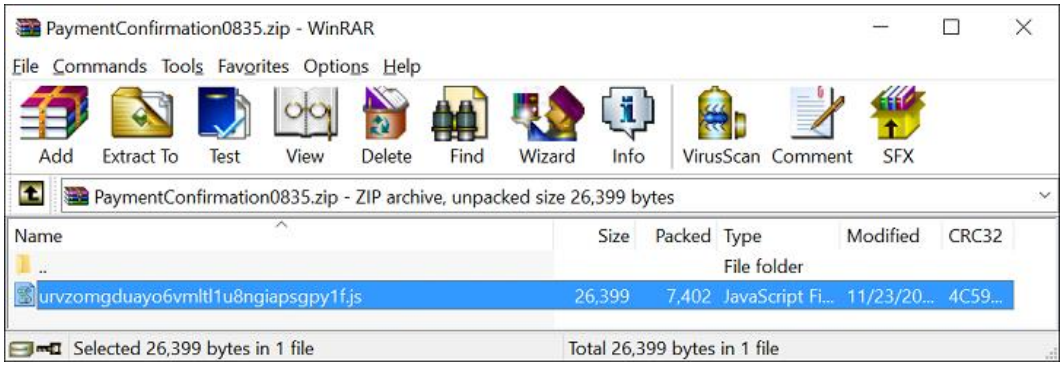
هرزنامه[۱۶]

در این روش مهاجمان با استفاده از ترفندهای مهندسی اجتماعی با ساخت ایمیل‌های فریبنده دریافت‌کنندگان ایمیل را تشویق به اجرای فایل مخرب پیوست شده به ایمیل می‌کنند. پیوست این ایمیل‌ها – در حقیقت هرزنامه‌ها – معمولاً نقش دانلودکننده[۱۷] باج‌افزار را بر عهده دارد. در حملات هدفمند عنوان، محتوا و پیوست هرزنامه ارسال شده مرتبط با کسب‌وکار سازمان یا واحد سازمانی هدف قرار گرفته شده است. برای نمونه، نویسنده باج‌افزار Petya، هرزنامه‌های ناقل این باج‌افزار را در ظاهر رزومه فردی که متقاضی استخدام است به بخش منابع انسانی سازمان‌ها ارسال می‌کند.

پیوست ایمیل‌های ناقل باج‌افزار معمولاً یکی از موارد زیر است:

- فایل‌های مرتبط با نرم‌افزار Office نظیر DOC.، و XML. – در این فایل‌ها از بخش Visual Basic for Applications – VBA – که به ماکرو[۱۸] معروف است سوءاستفاده می‌شود. به این نوع فایل‌ها، ماکروی مخرب اطلاق می‌شود.
- HTA.[۱۹] – فایل‌های HTA، قابلیت اجرا شدن بر روی مرورگر – فارغ از محدودیت‌های امنیتی لحاظ شده در آن مرورگر – را دارا هستند.
- JS. – این فایل‌ها، حاوی کدهای JavaScript هستند.
- VBS. – این فایل‌ها، حاوی کدهای VB Script هستند.
- JSE.[۲۰] – این نوع فایل‌ها که می‌توانند حاوی اسکریپت باشند برای محافظت کدگذاری شده‌اند.
- WSF.[۲۱] – فایل‌های متنی حاوی کدهای XML هستند. این نوع فایل‌ها با هر دو زبان اسکریپت‌نویسی JavaScript و VBScript سازگار بوده و برنامه‌نویس حتی می‌تواند از هر دوی این زبان‌ها در یک فایل WSF استفاده کند.
- CHM.[۲۲] – این فایل‌ها می‌توانند حاوی کدهای HTML و زبان‌های اسکریپت‌نویسی باشند.
- LNK.[۲۳] – فایل‌های LNK میانبری برای اجرای یک برنامه یا فایل هستند. برخی گردانندگان باج‌افزار از این نوع فایل برای اجرای کد مخرب باج افزار از طریق پروسه‌های مجازی نظیر Windows PowerShell استفاده می‌کنند.

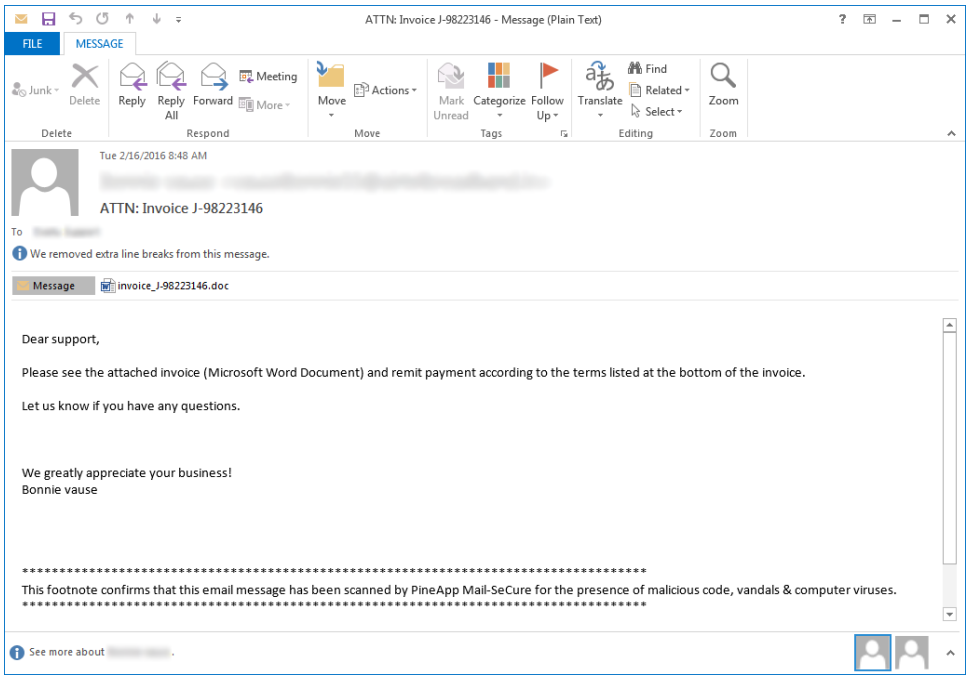
توضیح اینکه در اکثر نمونه‌ها فایل‌های مذکور به‌صورت فشرده شده به هرزنامه پیوست می‌شوند.



شکل ۲: نمونه فایل مخرب JS که در یک فایل ZIP با عنوان جذاب فشرده شده است

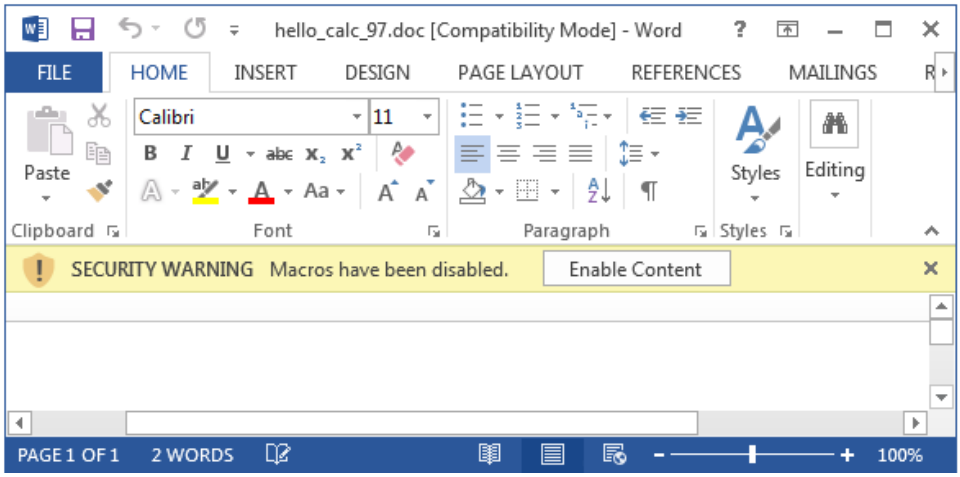
[۱۶] Spam
[۱۷] Downloader
[۱۸] Macro
[۱۹] HTML Application
[۲۰] JScript.Encode
[۲۱] Windows Script File
[۲۲] Compiled HTML
[۲۳] Link Shortcut

شکل ۳، نمونه‌ای از هرزنامه ناقل یک باج‌افزار با پیوست فایل Word را نمایش می‌دهد.



شکل ۳: نمونه هرزنامه ارسال شده توسط گردانندگان باج‌افزار رمزگذار Locky

به‌صورت پیش‌فرض در زمان باز شدن فایل‌های حاوی ماکرو پیامی ظاهر شده و از کاربر خواسته می‌شود تا برای استفاده از کدهای به کار رفته در فایل، تنظیمات امنیتی خود را تغییر دهد.

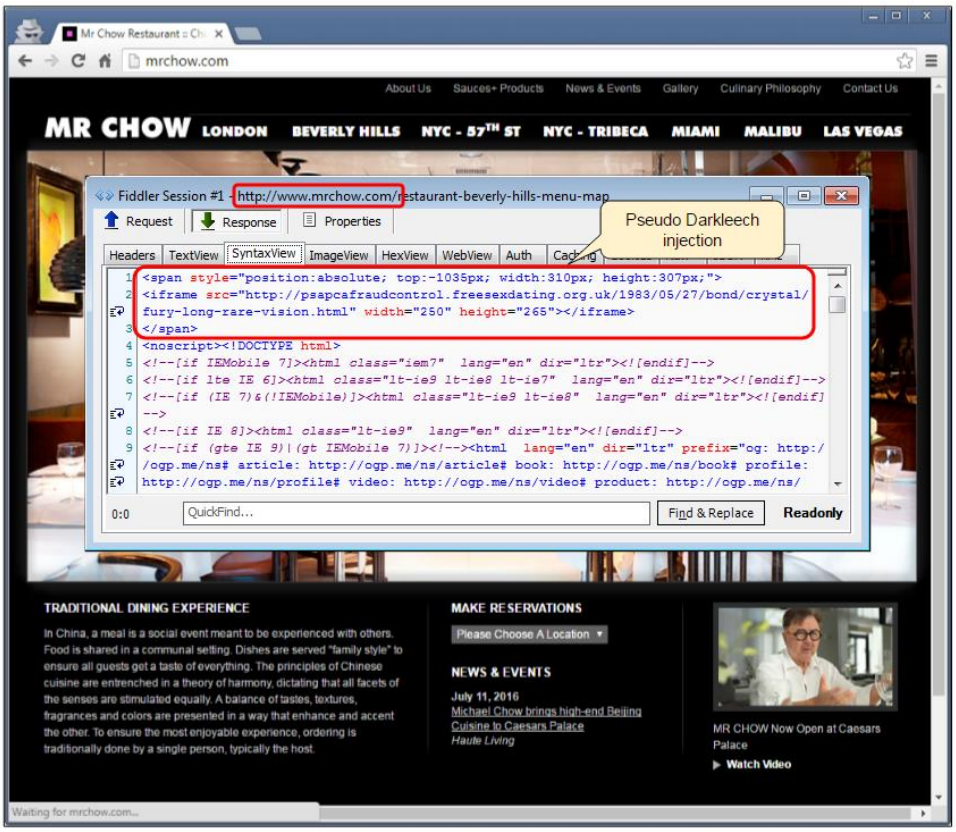


شکل ۴: نمونه فایل Word حاوی ماکرو

با کلیک کاربر بر روی Enable Content، بخش ماکرو فعال شده و پس از دانلود شدن فایل مخرب باج افزار بر روی دستگاه کاربر اجرا می‌شود.

سایت‌های مخرب

روش رایج دیگر انتشار باج‌افزارها هدایت کاربر به سایت‌های مخرب یا سایت‌های تسخیر شده[۲۴] حاوی بسته بهره‌جو[۲۵] است. حتی سایت‌های پربیننده مجاز نیز ممکن است توسط هکرها تسخیر شوند. در این صورت در زمان مراجعه به این سایت‌ها کاربر به صفحه‌ای حاوی بسته بهره‌جو هدایت شده و دستگاه آسیب‌پذیر کاربر به باج‌افزار آلوده می‌شود.



شکل ۵: نمونه‌ای از یک سایت اینترنتی تسخیر شده

بسته‌های بهره‌جو، مجموعه کدهایی هستند که سوءاستفاده از ضعف‌های امنیتی نرم‌افزارهای نصب شده بر روی کامپیوتر را بدون نیاز به دخالت کاربر ممکن می‌کنند.

رمزگذاری

پس از آلوده شدن اولیه از طریق هرزنامه یا سایت مخرب، باج‌افزار اقدامات زیر را انجام می‌دهد:

- با سرور فرماندهی مهاجم ارتباط برقرار کرده و ضمن ارسال اطلاعاتی در خصوص دستگاه آلوده شده کلید عمومی[۲۶] رمزگذاری را دریافت می‌کند.

[۲۴] Compromised Website
[۲۵] Exploit Kit
[۲۶] Public Key

- فایل‌های پراستفاده – که بسته به باج‌افزار می‌تواند متفاوت باشد - بر روی سیستم، حافظه‌های حذف‌شدنی[۲۷] متصل به آن و پوشه‌های به اشتراک گذاشته شده که کاربر دستگاه آلوده به آن دسترسی دارد را رمزگذاری می‌کند.
- سیستم‌های پشتیبان‌گیری سیستم عامل Windows، نظیر Shadow Copy معمولاً حذف می‌شوند تا امکان برگرداندن داده‌ها فراهم نشود.
- پیامی موسوم به اطلاعیه باج‌گیری[۲۸] نشان داده شده و در آن نحوه پرداخت باج شرح داده می‌شود.
- در برخی موارد باج‌افزار خود را حذف کرده و فایل‌های رمزگذاری شده و اطلاعیه باج را بر روی سیستم باقی می‌گذارد.

راه‌های پیشگیری و مقابله

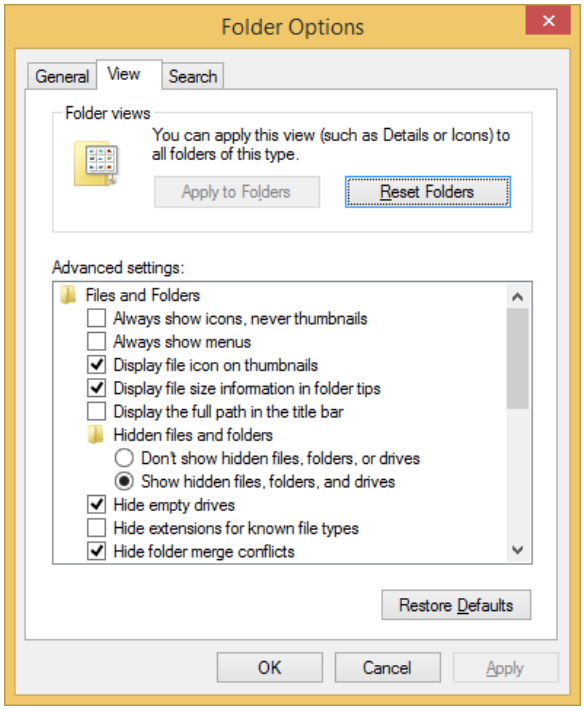
امن ماندن در برابر باج‌افزار رمزگذار تنها به داشتن آخرین راهکار امنیتی خلاصه نمی‌شود. بلکه مستلزم اجرای مجموعه‌ای از اقدامات زیر است.

۱ تهیه نسخه پشتیبان

از اطلاعات سازمانی به‌صورت دوره‌ای نسخه پشتیبان تهیه شود. پیروی از قاعده ۳-۲-۱ برای داده‌های حیاتی توصیه می‌شود. بر طبق این قاعده، از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه به‌عنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود. همچنین رمزگذاری فایل‌های پشتیبان برای حفاظت از آنها در برابر افراد غیرمجاز نیز توصیه می‌شود.

۲ نمایش پسوند فایل‌ها

به‌صورت پیش‌فرض در سیستم عامل Windows پسوند فایل‌ها نمایش داده نمی‌شود. این بدان معناست که کاربر می‌بایست به نشان[۲۹] فایل اعتماد کند. موضوعی که سبب استفاده برخی ویروس‌نویسان از فایل های دو پسوندی برای فریب کاربران می شود. برای مثال فایل Hello.txt.js در حالت عادی به‌صورت Hello.txt نمایش داده می‌شود. توصیه می‌شود که در بخش Folder Options گزینه Show hidden files, folders, and drive فعال شده و گزینه Hide extensions for known file types غیرفعال شود.

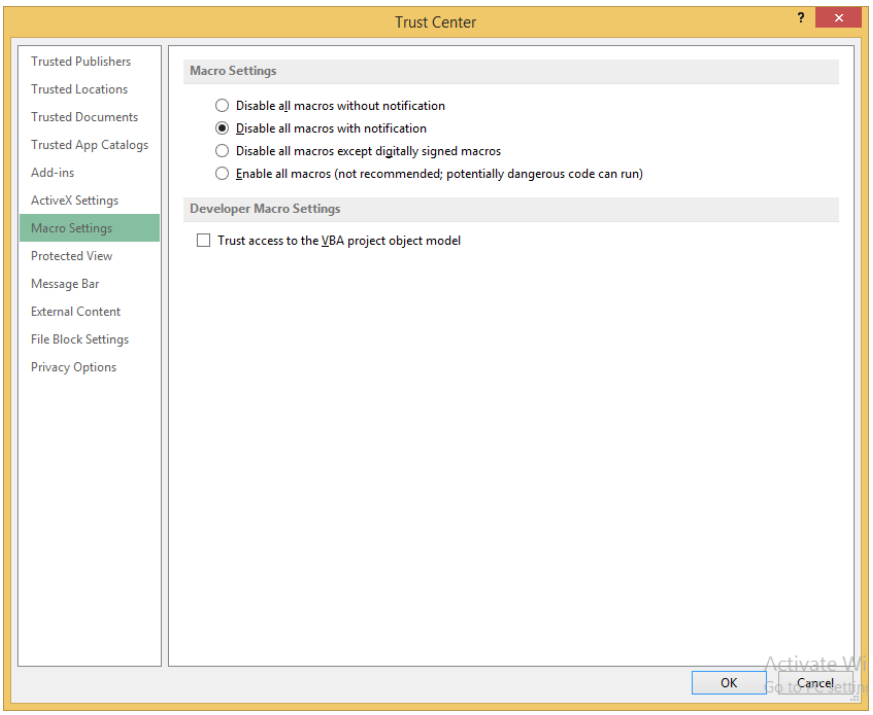


شکل ۶: تنظیمات Folder Options

[۲۷] Removable Storage
[۲۸] Ransom Note
[۲۹] Icon

۳ غیرفعال کردن بخش ماکرو

با توجه به انتشار بخش قابل توجهی از باج‌افزارها از طریق فایل‌های نرم‌افزار Office حاوی ماکروی مخرب، غیرفعال کردن بخش ماکرو برای کاربرانی که به این قابلیت نیاز کاری ندارند با فعال کردن گزینه Disable all macros without notification توصیه می‌شود.



شکل ۷: تنظیمات امنیتی بخش ماکرو در نرم‌افزار Office

برای غیرفعال کردن این قابلیت، از طریق Group Policy، می‌توان از این راهنما و این راهنما استفاده کرد.

همچنین توصیه می‌شود ایمیل‌های دارای پیوست ماکرو در همان درگاه شبکه مسدود شوند. بدین منظور می‌توان از تجهیزات دیواره آتش، نظیر Sophos بهره گرفت.

٤ محدود کردن سطح دسترسی

همه کاربران، حتی مدیر سیستم می‌بایست با حداقل سطح دسترسی مورد نیاز به هر سیستم وارد شود. در صورت محدود بودن سطح دسترسی حتی در صورت اجرای فایل مخرب توسط کاربر، دستگاه به باج‌افزار آلوده نخواهد شد. همچنین برخی محصولات کنترل برنامه نظیر McAfee Application Control نیز می‌توانند به‌نحوی مؤثر از اجرا شدن فایل‌های غیرمجاز از جمله باج‌افزارها جلوگیری کنند.

۵ نصب اصلاحیه‌ها در اولین فرصت ممکن و استمرار در انجام آن

بسیاری از بهره‌جویی‌ها از طریق سوءاستفاده از ضعف‌های امنیتی نرم‌افزارهای پرکاربردی نظیر Adobe Flash، Office و مرورگرها صورت می‌پذیرد. هر چه زودتر اصلاحیه نصب شود آسیب کمتری متوجه سازمان می‌شود.

٦ استفاده از فناوری‌های حفاظتی پیشرفته

استفاده از ضدویروس قدرتمند و به روز جهت مقابله با باج افزارهای رمزگذار ضروری است. اما در کنار می بایست از راهکارهای نفوذیاب، ضدهرزنامه، کنترل‌کننده وب و دیواره آتش نیز استفاده کرد. همچنین برخی محصولات امنیتی نظیر McAfee و Bitdefender دارای راهکارهایی ویژه و خاص برای شناسایی و مقابله با باج‌افزارهای رمزگذار هستند.

۷ به روز بودن در خصوص روش‌های جدید باج‌گیران

با مرور اخبار و حضور در دوره‌های آگاهی‌رسانی شرکت مهندسی شبکه گستر، نظیر سیمنارهای فصلی مروری بر رخدادهای امنیت سایبری از آخرین روش‌های مورد استفاده مهاجمان آگاه شده و سیاست‌ها پیشگرانه لازم را اعمال کنید.

۸ آگاهی‌رسانی به کاربران

گردانندگان باج‌افزار به‌خوبی می‌دانند تا زمانی که کاربر فایل پیوست ایمیل را جذاب یا مرتبط تشخیص ندهد آن را باز نمی‌کند. آموزش و راهنمایی کاربران سازمان به صرف‌نظر کردن از فایل‌های حتی کمی مشکوک و باز نکردن آنها می‌تواند نقشی مؤثر در پیشگیری از اجرا شدن این فایل‌ها داشته باشد. برای این منظور می‌توانید از این داده‌نمایی‌ها استفاده کنید.

شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرد. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولید کننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" (Unified Threat Management – UTM) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر به‌عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می‌نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضد ویروس Bitdefender را به‌عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران، آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین و طولانی مدت‌ترین پروژه‌های طراحی، نصب، راه ندازی و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت‌افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

CSQ
ISO 9001:2008
Cert No 9150.C528

شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن / دورنگار	۴۲۰۵۲-۰۲۱
تارنمای شرکت	www.shabakeh.net
سامانه پشتیبانی	help.shabakeh.net
خدمات پس از فروش	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net