

گروگان گرفته نشوید!

حفاظت از سازمان در برابر باج افزارها

انواع باج افزار
انتشار و آلوده سازی
نمونه های شاخص
راه های پیشگیری و مقابله

شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

۱ خلاصه مدیریتی
۲ انواع باج افزارها
۲ باج افزارهای قفل کننده صفحه
۳ باج افزارهای رمزگذار فایل
۴ باج افزارهای کنترل کننده بخش راه انداز
۵ دلایل موفقیت باج افزارها
۶ انتشار و آلوده سازی
۶ انتشار از طریق هرزنامه
۸ بهره جویی از آسیب پذیری امنیتی
۹ اتصال از طریق پودمان RDP
۱۰ رمزگذاری و اخاذی
۱۱ چند نمونه شاخص
۱۱ WannaCry
۱۲ Petya
۱۳ Karmen
۱۴ Spora
۱۵ PooleZoor
۱۷ راه های پیشگیری و مقابله

خلاصه مدیریتی

انتشار اولین نسخه از باج‌افزار معروف CryptoLocker در خرداد ماه سال ۱۳۹۳ و موفقیت‌های کم‌نظیر آن در اخذی از کاربران را می‌توان سرآغاز دوره‌ای جدید در دنیای ویروس‌نویسان دانست؛ دوره‌ای که در آن نوع جدیدی از بدافزارها موسوم به باج‌افزارهای رمزگذار^۱ کاربران و سازمان‌های کوچک تا بزرگ را به‌صورت گسترده هدف قرار داده‌اند.

باج‌افزارهای رمزگذار یکی از پرتعدادترین و متأسفانه مخرب‌ترین بدافزارهایی هستند که در نیم‌دهه اخیر مورد استفاده تبهکاران سایبری قرار گرفته‌اند.

محدود کردن دسترسی به داده‌های حساس از طریق رمزنگاری، ارباب کاربر و بدنال آن اخذی در ازای بازگرداندن این داده‌ها، هدف اصلی این نوع باج‌افزارهاست. رمزگشایی^۲ فایل‌هایی که با طراحی زیرکانه به این روش رمزنگاری می‌شوند دشوارتر و در بسیاری مواقع غیرممکن است.

برآورد می‌شود گردانندگان باج‌افزار، تا کنون بیش از یک میلیارد دلار از راه باج‌گیری درآمد کسب کرده باشند.

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

در این گزارش ضمن بررسی و کالبدشکافی باج‌افزارها به راه‌های مقابله با این تهدیدات پرداخته شده است.



WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud






DESCRIPTION

Aliases: Evgeniy Bogachev, Evgeniy Mikhailovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	Hair: Brown (usually shaves his head)
Eyes: Brown	Height: Approximately 5'9"
Weight: Approximately 180 pounds	Sex: Male
Race: White	Occupation: Bogachev works in the Information Technology field.
NCIC: #890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to \$1 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

REMARKS

Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

CAUTION

Evgeniy Mikhailovich Bogachev, using the online monikers "lucky12345" and "slavik", is wanted for his alleged involvement in a wide-ranging racketeering enterprise and scheme that installed, without authorization, malicious software known as "Zeus" on victims' computers. The software was used to capture bank account numbers, passwords, personal identification numbers, and other information necessary to log into online banking accounts. While Bogachev knowingly acted in a role as an administrator, others involved in the scheme conspired to distribute spam and phishing emails, which contained links to compromised web sites. Victims who visited these web sites were infected with the malware, which Bogachev and others utilized to steal money from the victims' bank accounts. This online account takeover fraud has been investigated by the FBI since the summer of 2009.

Starting in September of 2011, the FBI began investigating a modified version of the Zeus Trojan, known as GameOver Zeus (GOZ). It is believed GOZ is responsible for more than one million computer infections, resulting in financial losses of more than \$100 million.

شکل ۱: اطلاعاتی تحت تعقیب بودن یکی از گردانندگان شبکه مخرب منتشر کننده باج‌افزار CryptoLocker و پاداش ۳ میلیون دلاری FBI در ازای اطلاعاتی که منجر به دستگیری او شود. این باج‌افزار در سال ۱۳۹۳، ده‌ها میلیون دستگاه را در بسیاری از کشورها آلوده کرد.

Crypto Ransomware ^۱
Decrypt ^۲

انواع باج افزارها

باج افزار 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 که در ادامه این بخش به بررسی آنها پرداخته شده است.

باج افزارهای قفل‌کننده صفحه

در این باج‌افزارها، با نمایش دائمی یک تصویر بر روی صفحه، به نحوی 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. در این حالت با پاکسازی کامپیوتر توسط دیسک‌های نجات^۳ مجهز به ضدویروس، دسترسی به اطلاعات مجدداً میسر می‌شود.

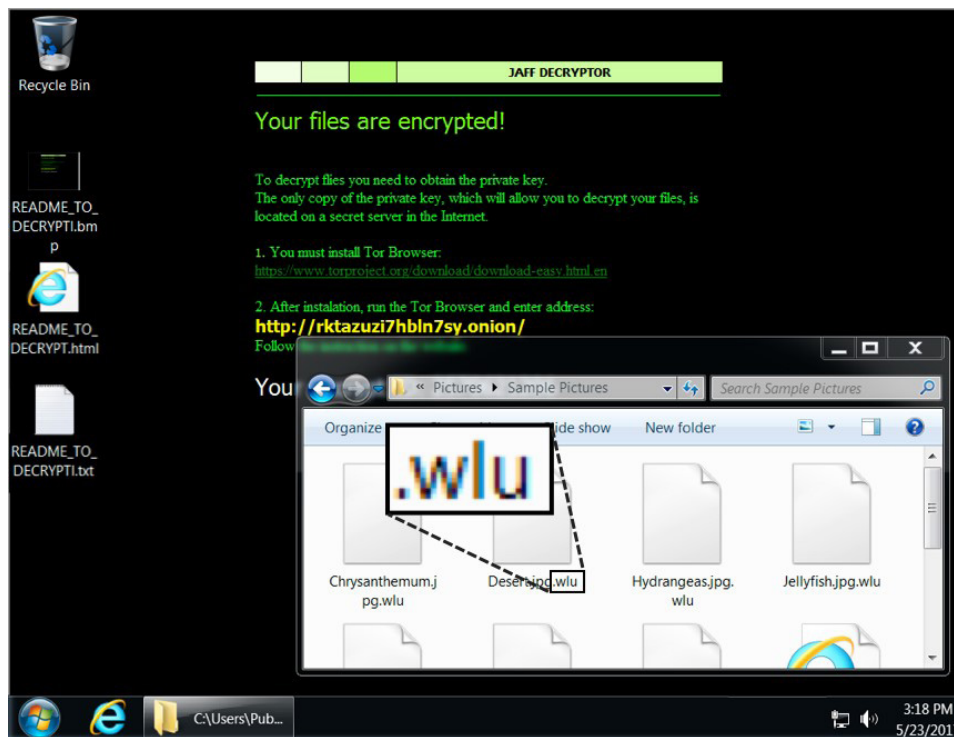


▲ شکل ۲: نمونه‌ای از تصویر نمایش داده شده توسط یک باج‌افزار قفل‌کننده صفحه

^۳ Rescue Disk

باج‌افزارهای رمزگذار فایل

در روش‌های پیشرفته‌تر، ممکن است باج‌افزار اقدام به رمز کردن فایل‌های کامپیوتر کند. این نوع بدافزارها به باج‌افزارهای رمزگذار فایل موسوم هستند. هدف از رمز کردن، محدود کردن دسترسی است؛ به نحوی 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 پیشرفته باج‌افزارها، در هنگام رمزنگاری، برای هر دستگاه یک کلید خصوصی^۴ منحصر به فرد تولید شده و نزد نویسنده باج‌افزار نگهداری 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.

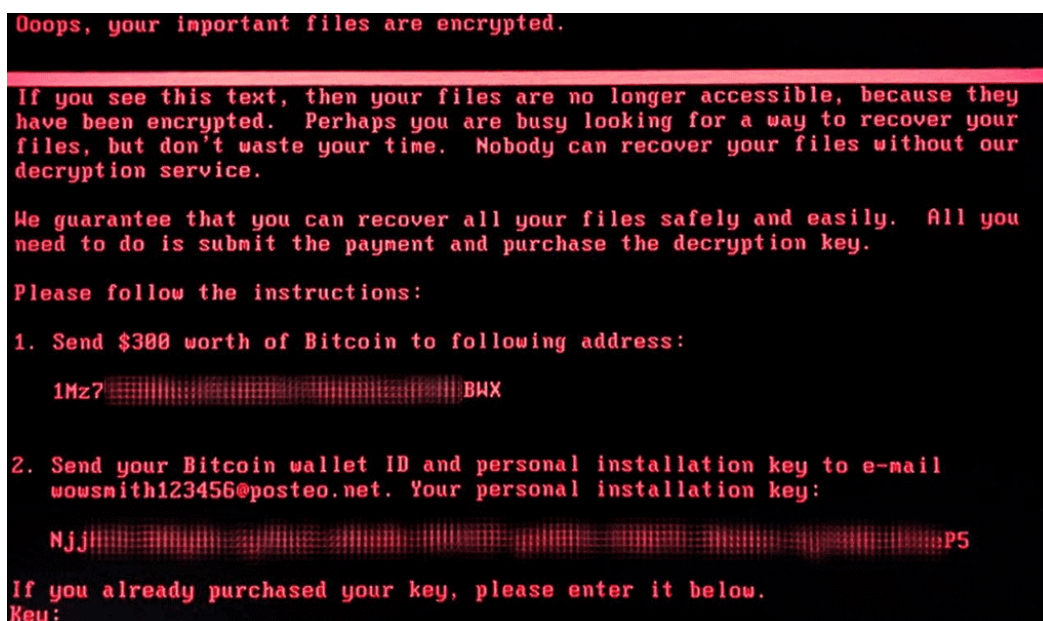


▲ شکل ۳: نمونه‌ای از یک باج‌افزار رمزگذار فایل که در زمان رمزنگاری پسوند wlu به انتهای نام فایل اضافه می‌کند

Decryption Key ^۴
Private Key ^۵

باج‌افزارهای کنترل‌کننده بخش راه‌انداز

بیش از دو سال است که نوع جدیدی از باج‌افزارها با روشی خاص اقدام به قطع کامل دسترسی کاربر به کامپیوتر می‌کنند. این باج‌افزارها با رمزگذاری بخش Master Boot Record دیسک سخت، کامپیوتر را غیرقابل راه‌اندازی می‌کنند. بخش Master Boot Record در قسمت‌های ابتدایی دیسک سخت ذخیره و نگهداری می‌شود. این بخش شامل اطلاعاتی درباره ساختار دیسک و برنامه‌ای که سیستم عامل را به اجرا در می‌آورد، می‌باشد. بدون یک Master Boot Record سالم و صحیح، کامپیوتر نمی‌داند که سیستم عامل بر روی کدام قسمت از دیسک سخت است و چگونه باید راه‌اندازی و اجرا شود. نخستین بار، باج‌افزار Petya با بکارگیری این روش توجه کارشناسان امنیتی را به خود جلب کرد. نویسنده این باج‌افزار پس از مدتی اقدام به استفاده همزمان از دو باج‌افزار Petya و Mischa به صورت ترکیبی نمود تا اگر به هر دلیلی امکان رونویسی بخش Master Boot Record فراهم نشد با استفاده از باج‌افزار Mischa فایل‌های قربانی رمزگذاری شود.



▲ شکل ۴: نمونه‌ای از پیام نمایش داده شده توسط یک باج‌افزار کنترل‌کننده بخش راه‌انداز در زمان بالا آمدن دستگاه آلوده

دلایل موفقیت باج افزارها

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

تکنیک‌های پیشرفته و نوآوری مستمر در باج افزارها

- گردانندگان باج افزارها از ترفندهای مهندسی اجتماعی^۱ ماهرانه، برای تشویق کاربر به اجرای باج افزار استفاده می‌کنند.
- ارائه خدمات "باج افزار به عنوان سرویس" که حتی تبهکاران با دانش کم برنامه‌نویسی را نیز قادر به استفاده از باج افزارهای پیشرفته می‌کند. در این روش صاحب باج افزار، فایل مخرب را به عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخذی شده از قربانی به نویسنده و بخشی دیگر به متقاضی می‌رسد.

ضعف‌های امنیتی سازمان‌ها

- نبود استراتژی صحیح تهیه نسخه پشتیبان
- عدم نصب مستمر اصلاحیه‌های امنیتی سیستم‌های عامل و نرم افزارها
- تخصیص نادرست سطح دسترسی به کاربران و پوشه‌های اشتراکی
- عدم آگاهی‌رسانی به کاربران در خصوص نحوه برخورد با ایمیل‌ها و فایل‌های مشکوک
- نبود سیستم‌های امنیتی نظیر پوشش‌های ویروس، دیوار آتش^۲، نفوذیاب^۳، کنترل‌کننده وب^۴، ضدهرزنامه^۵ و یا عدم پیکربندی صحیح آنها
- عدم تقسیم‌بندی شبکه‌ای سیستم‌های حساس و بااهمیت
- نبود سیاست‌های امنیتی جامع و صحیح؛ برای مثال مسدود نشدن ایمیل‌های با فایل پیوست حاوی ماکرو^۶
- اولویت‌بندی نادرست و چشم‌پوشی از الزامات امنیتی با بیان عباراتی نظیر "ما می‌دانیم این روش امن نیست، اما کارکنان ما باید کار کنند!"

عدم استفاده از فناوری پیشرفته حفاظتی در سازمان‌ها

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

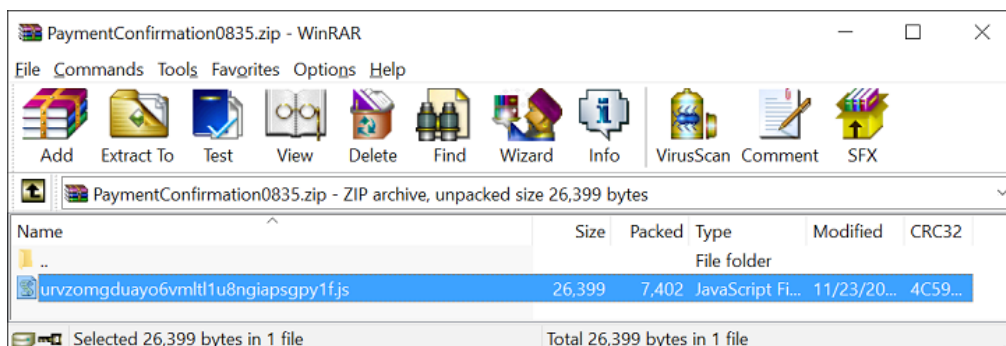
^۱ Social Engineering
^۲ Firewall
^۳ Intrusion Prevention
^۴ Web Control
^۵ AntiSpam
^۶ Macro

انتشار و آلوده‌سازی

انتشار از طریق هرزنامه

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. در اکثر حملات، پیوست این ایمیل‌ها (هرزنامه‌ها) معمولاً نقش داندوکننده^۳ 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، در نسخه‌هایی از باج‌افزار Petya، هرزنامه‌های ناقل آن در ظاهر رزومه فردی که متقاضی استخدام است به بخش منابع انسانی سازمان‌ها ارسال می‌شده است. پیوست ایمیل‌های ناقل باج‌افزار معمولاً یکی از موارد زیر است:

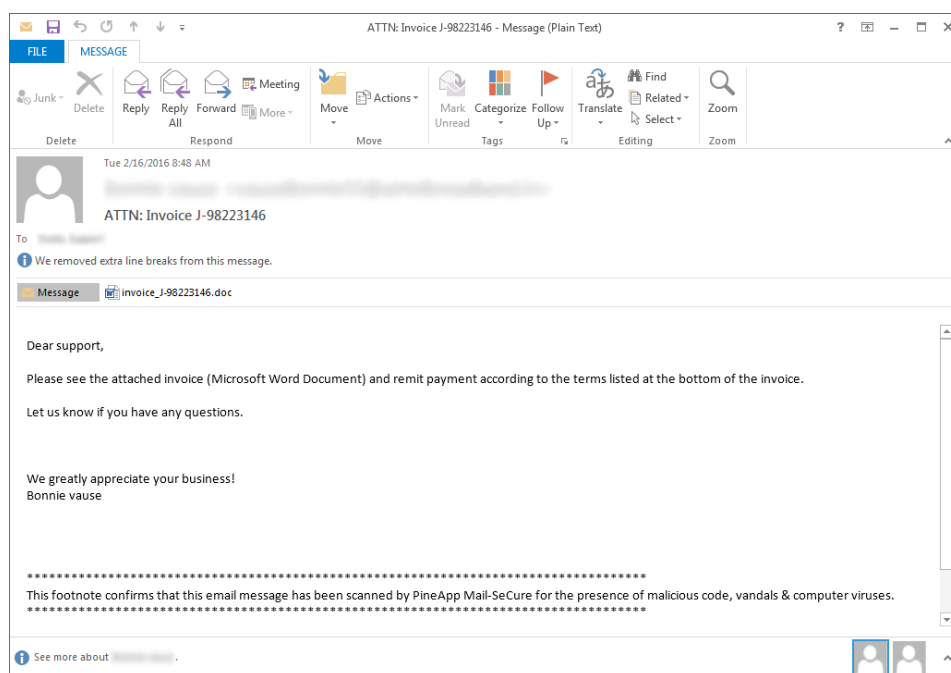
- فایل‌های مرتبط با نرم‌افزار Office نظیر DOC و PPT - در این فایل‌ها از بخش VBA - Visual Basic for Applications - که به ماکرو معروف است سواستفاده می‌شود. به این نوع فایل‌ها، ماکروی مخرب اطلاق می‌شود.
 - HTA - فایل‌های HTA، قابلیت اجرا شدن بر روی مرورگر - فارغ از محدودیت‌های امنیتی لحاظ شده در آن مرورگر - را دارا هستند.
 - JS - این فایل‌ها، حاوی کدهای JavaScript هستند.
 - VBS - این نوع فایل‌ها، حاوی کدهای VB Script هستند.
 - JSE - این فایل‌ها که می‌توانند حاوی اسکریپت باشند برای محافظت کدگذاری شده‌اند.
 - WSF - 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 - این فایل‌ها می‌توانند حاوی کدهای HTML و زبان‌های اسکریپت‌نویسی باشند.
 - LNK - فایل‌های LNK میانبری برای اجرای یک برنامه یا فایل هستند. برخی نویسندگان باج‌افزار از این نوع فایل برای اجرای کد مخرب باج‌افزار از طریق پروسه‌های مجازی نظیر Windows PowerShell استفاده می‌کنند.
- توضیح اینکه در اکثر نمونه‌ها فایل‌های مذکور به صورت فشرده شده به هرزنامه پیوست می‌شوند.



▲ شکل ۵: نمونه فایل مخرب JS که در یک فایل ZIP با عنوان جذاب فشرده شده است

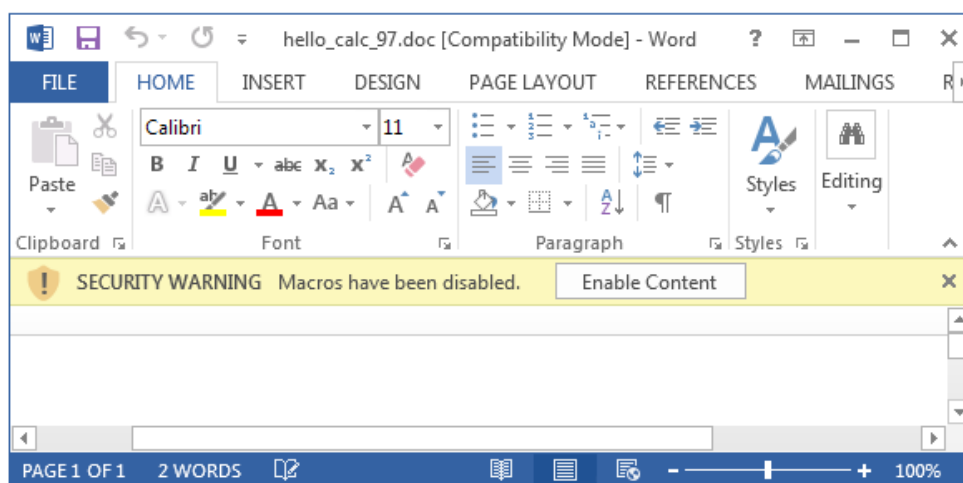
^۳ Downloader

شکل ۶، نمونه‌ای از هرزنامه ناقل یک باج‌افزار با پیوست فایل Word را نمایش می‌دهد.



▲ شکل ۶: نمونه هرزنامه ارسال شده توسط گردانندگان باج‌افزار Locky

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



▲ شکل ۷: نمونه فایل Word حاوی ماکرو

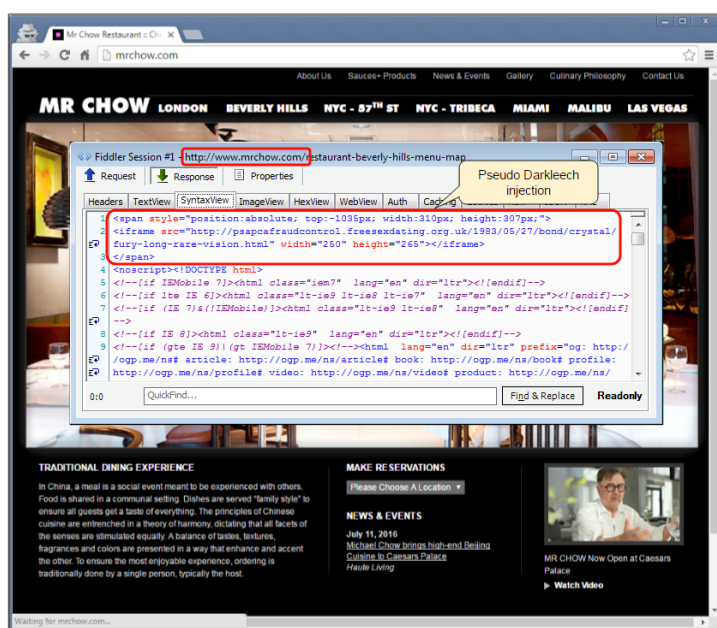
با کلیک کاربر بر روی Enable Content، بخش ماکرو فعال شده و پس از دانلود شدن فایل مخرب باج‌افزار بر روی دستگاه کاربر اجرا می‌شود.

بهره‌جویی از آسیب‌پذیری امنیتی

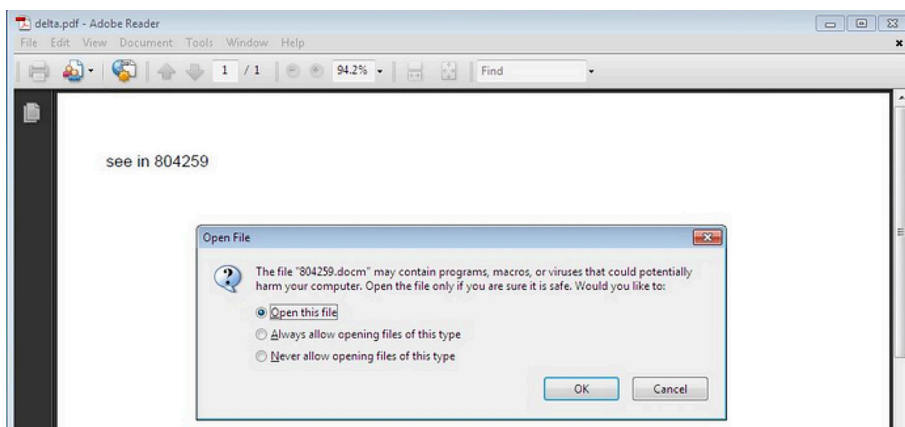
روش دیگر انتشار، سواستفاده از آسیب‌پذیری^{۱۳} سیستم عامل یا هر یک از نرم‌افزارهای نصب شده بر روی دستگاه کاربر با هدف اجرای خودکار فایل مخرب باج‌افزار بدون نیاز به دخالت کاربر است. بدین‌منظور، مهاجمان با بکارگیری روش‌های مهندسی اجتماعی کاربر را تشویق به باز نمودن یک فایل حاوی بهره‌جو یا هدایت او به سایت‌های مخرب یا سایت‌های تسخیر شده حاوی بسته بهره‌جو می‌کنند.

در نمونه‌های متعددی سایت‌های پربیننده مجاز نیز به تسخیر هرکجا در آمده و در زمان مراجعه کاربر به این سایت‌ها دستگاه آسیب‌پذیر او به باج‌افزار آلوده شده است.

بهره‌جو، مجموعه‌ کدهایی است که سواستفاده از ضعف‌های امنیتی نرم‌افزارهای نصب شده بر روی کامپیوتر را ممکن می‌سازد. برخی از ضعف‌های امنیتی، مهاجم را قادر به اجرای از راه دور کد مخرب بر روی دستگاه حاوی نرم‌افزار آسیب‌پذیر می‌کنند.



▲ شکل ۸: نمونه‌ای از یک سایت حاوی بسته بهره‌جو



▲ شکل ۹: نمونه‌ای از یک فایل PDF حاوی بهره‌جو

^{۱۳} Vulnerability

اتصال از طریق پودمان RDP

پودمان Remote Desktop Protocol - به اختصار RDP - قابلیت در سیستم عامل Windows است که امکان اتصال از راه دور کاربران تعیین شده را به دستگاه فراهم می‌کند.

علاوه بر مدیران شبکه که از این پودمان برای اتصال به سرورها و ایستگاه‌های کاری سازمان استفاده می‌کنند، در بسیاری از سازمان‌های کوچک و متوسط نیز از RDP برای برقرار نمودن ارتباط از راه دور پیمانکاران حوزه IT، به سرورهایی همچون حقوق و دستمزد، اتوماسیون اداری و غیره استفاده می‌شود.

تبهکاران سایبری از ابزارهایی همچون Shodan برای شناسایی سرورهای با درگاه RDP باز بر روی اینترنت استفاده کرده و در ادامه با بکارگیری ابزارهایی نظیر NLBrute اقدام به اجرای حملات موسوم به Brute Force می‌کنند. هدف از اجرای حملات Brute Force رخنه به دستگاه از طریق پودمانی خاص - در اینجا RDP - با بکارگیری ترکیبی از نام‌های کاربری و رمزهای عبور رایج است. بنابراین در صورتی که دسترسی به پودمان RDP از طریق کاربری با رمز عبور ساده و غیرپیچیده باز شده باشد مهاجمان نیز به راحتی امکان اتصال به دستگاه را خواهند داشت.

در صورت برقرار شدن اتصال، مهاجمان نرم‌افزاری را بر روی سرور اجرا کرده و از آن برای دست‌درازی به تنظیمات و سرویس‌های نرم‌افزارهای ضدبافزار، پشتیبان‌گیری و پایگاه داده نصب شده بر روی آن استفاده می‌کنند. در ادامه نیز فایل مخرب باج‌افزار را دریافت کرده و بر روی سرور به اجرا در می‌آورند.

در طی دو سال گذشته گزارش‌های متعددی از آلودگی سرورهای حساس سازمان‌ها به باج‌افزار از طریق پودمان RDP به شرکت مهندسی شبکه گستر واصل شده است. مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر) نیز به کرات در خصوص حملات باج‌افزاری به این پودمان در سطح کشور هشدار داده است. با این حال در گزارشی که این مرکز در اردیبهشت ماه امسال منتشر کرد از عدم اعمال حفاظت کافی در خصوص پودمان RDP در برخی سازمان‌ها و شرکت‌ها خبر داد. به گفته ماهر قربانیان حملات مبتنی بر RDP معمولاً مراکزی هستند که برای ایجاد دسترسی به‌منظور دریافت پشتیبانی برای نرم‌افزارهای اتوماسیون از این پودمان استفاده می‌کنند. در گزارش ماهر اشاره شده که خسارت ناشی از این حملات، بدون احتساب مبالغ احتمالی باج پرداخت شده توسط بعضی از قربانیان، به طور میانگین حدود نهمصد میلیون ریال برای هر رخداد بوده است.



هشدار: احتمال آلودگی به باج‌افزار از طریق RDP

به اطلاع می‌رساند در هفته‌های اخیر، گزارشات متعددی از حمله باج‌افزارها به سرورهای ویندوزی ازجمله چندین سامانه بیمارستانی در کشور واصل شده است که خسارات جبران‌ناپذیری به بار آورده است. بررسی‌های فنی نشان داده که در بسیاری از این حملات، مهاجمین با سوء استفاده از دسترسی به سرویس دسترسی از راه دور در سیستم‌عامل ویندوز که مبتنی بر پروتکل RDP است، وارد شده، آنتی ویروس نصب شده را غیرفعال می‌کنند و با انتقال فایل باج‌افزار، اقدام به رمزگشایی فایل‌های سرور می‌نمایند. حتی در مواردی، مشاهده شده است که مهاجمین، با صرف زمان کافی و پس از کسب شناخت و انجام انواع دیگری از سوء استفاده‌های ممکن، زمان و الگوی انجام پشتیبان‌گیری از اطلاعات را نیز شناسایی کرده و موفق به انجام حملات باج‌افزاری بی‌نص شدند.

در این حملات، مهاجم با سوء استفاده از نسخه‌های آسیب‌پذیر سرویس Remote Desktop، رمز عبور ضعیف، تنظیمات ناقص یا بی‌احتیاطی در حفاظت از رمز عبور، وارد سرورها می‌شوند. به منظور جلوگیری از وقوع این حملات لازم است که تا حد امکان، نسبت به مسدود نمودن سرویس‌های غیر ضروری Remote Desktop بر روی سرورهای در دسترس از طریق شبکه اینترنت اقدام نمود و در صورت ضرورت و غیرقابل اجتناب بودن (ارائه این امکان در بستر اینترنت، به دقت موارد زیر را رعایت نمود. همچنین یادآور می‌شود که فعال بودن دسترسی Remote Desktop به صورت حفاظت نشده در سطح اینترنت، سرور و داده‌های شما را جداً در معرض خطر قرار خواهد داد.

۱. به‌روزرسانی مداوم سیستم‌عامل و هوشیاری از احتمال رخداد حملات جدید و شناسایی آسیب‌پذیری‌های جدید.
۲. انجام منظم و سخت‌گیرانه پشتیبان‌گیری از اطلاعات بر روی تعداد کافی از رسانه‌های ذخیره‌سازی اطلاعات و آزمایش نسخ پشتیبان پس از

نوشته



تاریخ ایجاد: ۱۱ مرداد ۱۳۹۶

دسته‌ها

اخبار

▲ شکل ۱۰: نمونه‌ای از هشدار مرکز ماهر در خصوص سواستفاده گردانندگان باج‌افزار از پودمان RDP

رمزگذاری و اخذی

پس از آلوده شدن اولیه از طریق هرنامه 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 رمزگذاری را دریافت می‌کند.
- فایل‌های پرترافیک و استفاده را - که بسته به باج‌افزار، فهرست آن می‌تواند متفاوت باشد - بر روی سیستم، حافظه‌های جاشدنی^{۱۴} متصل به آن و پوشه‌های به اشتراک گذاشته شده که کاربر دستگاه آلوده به آنها دسترسی دارد رمزگذاری می‌کند. معمولاً در حین رمزگذاری پسوندی خاص به فایل‌های رمز شده الصاق می‌شود.
- در برخی نمونه‌ها، بخش Master Boot Record دستگاه نیز رونویسی یا رمزگذاری می‌شود. با این کار عملاً دستگاه غیرقابل راه‌اندازی می‌شود.
- سیستم‌های پشتیبان‌گیری سیستم عامل Windows، نظیر Shadow Copy معمولاً حذف می‌شوند تا امکان برگرداندن داده‌ها فراهم نشود.
- پیامی موسوم به اطلاعیه باج‌گیری^{۱۵} نشان داده شده و در آن نحوه پرداخت باج شرح داده می‌شود. معمولاً باج باید به صورت ارز رمز^{۱۶} پرداخت شود.
- در برخی موارد، باج‌افزار خود را حذف کرده و فایل‌های رمزگذاری شده و اطلاعیه باج‌گیری را بر روی سیستم باقی می‌گذارد.



▲ شکل ۱۱: داده‌نمایی از مراحل کار باج‌افزارهای رمزگذار

^{۱۴} Removable Storage

^{۱۵} Ransom Note

^{۱۶} Cryptocurrency

چند نمونه شاخص

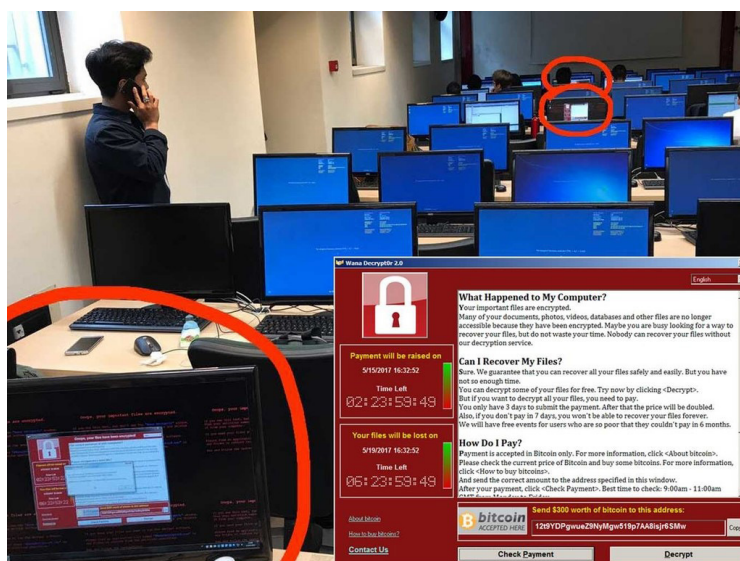
WannaCry

۲۲ اردیبهشت ماه ۱۳۹۶، منابع متعدد از انتشار گسترده باج‌افزار جدیدی با عنوان WannaCry خبر دادند. باج‌افزاری که با خاصیت کرم گونه و با بهره‌جویی از یک ضعف امنیتی در بخش SMB سیستم عامل Windows از روی نخستین دستگاه آلوده شده، به سرعت خود را در سطح شبکه و اینترنت تکثیر می‌کرد.

ماجرای آسیب‌پذیری مورد استفاده WannaCry به انتشار اسناد محرمانه‌ای باز می‌گردد که در جریان آن فایل‌های سرقت شده از یک گروه نفوذگر حرفه‌ای با نام Equation که وابستگی اثبات شده‌ای به "سازمان امنیت ملی" دولت آمریکا (NSA) دارد توسط گروه Shadow Brokers بر روی اینترنت به اشتراک گذاشته شدند. در بین این فایل‌ها، بهره‌جوایی به چشم می‌خورد که از یک ضعف امنیتی روز صفر^{۱۷} در بخش SMB سیستم عامل Windows که به EternalBlue موسوم شد سواستفاده می‌کردند. یک ماه پیش از درز این اطلاعات شرکت مایکروسافت اقدام به عرضه اصلاحیه‌ای با شناسه MS17-010 به منظور ترمیم آسیب‌پذیری مذکور نموده بود. نویسنده یا نویسندگان WannaCry نیز با استفاده از بهره‌جویی این آسیب‌پذیری باج‌افزار خود را به کرمی بسیار مخرب تبدیل کرده بودند.

تنها در انگلیس، آلودگی تعداد زیادی از بیمارستان‌های این کشور به این باج افزار سبب تعطیلی برخی از بخش‌های این مراکز درمانی شد. در آن زمان، مرکز اصلی سلامت لندن به نام Barts Health به بیماران توصیه کرد که بیماران به مراکز درمانی دیگری مراجعه کنند. برخی دیگر از مراکز درمانی این کشور نیز مجبور به ترخیص زود هنگام بیماران و محدود کردن خدمات رادیولوژی خود شدند. حتی یکی از بیمارستان‌ها تصمیم گرفت تا بخش اورژانس خود را تعطیل کرده و فقط به موارد حیاتی رسیدگی کند. در مدتی کوتاه، بیش از ۳۵۰ هزار دستگاه در ۲۰۰ کشور جهان به این باج‌افزار گرفتار شدند. به گزارش شرکت مهندسی شبکه گستر، در ایران نیز، تعداد قابل توجهی از سیستم‌ها به این باج‌افزار مخرب آلوده شدند.

اصلی‌ترین راهکار در پیشگیری از آلوده شدن به این باج‌افزار اطمینان از نصب بودن اصلاحیه MS17-010 و بکارگیری نرم‌افزار ضدویروس مناسب و به‌روز است.



▲ شکل ۱۲: آلودگی به باج‌افزار WannaCry در یک دانشگاه

Zero-day^{۱۷}

Petya

در اواخر سال ۱۳۹۴، یکی از شرکت‌های ضدویروس از انتشار باج‌افزار جدیدی به نام Petya در بین سازمان‌های آلمانی خبر داد که اقدام به رمزگذاری بخش MBR دیسک سخت کرده و با این روش کامپیوتر را غیرقابل راه‌اندازی می‌کرد. از آن زمان تا کنون نسخه‌های متعددی از این باج‌افزار منتشر شده است. در بسیاری از نسخه‌های Petya، پس از رمزگذاری MBR، اطلاعیه باجگیری در قالب یک تصویر جمجمه که با حروف ASCII ساخته شده، نمایش داده می‌شود. رنگ جمجمه در برخی نسخه‌های این باج‌افزار تغییر کرده است. فردی با شناسه Janus خود را به‌عنوان نویسنده و صاحب این باج‌افزار معرفی کرده است. او تا اکتبر سال ۲۰۱۶ میلادی سایت Janus Cybercrime را اداره می‌کرد و در این سایت Petya را به عنوان باج‌افزار به‌عنوان سرویس اجاره می‌داد. بنابراین احتمال اینکه افرادی نسخه‌های منحصربه‌فرد از این باج‌افزار را در اختیار داشته باشند دور از ذهن نیست. در ششم تیر ماه ۱۳۹۶، نسخه جدیدی از Petya با بهره‌جویی از آسیب‌پذیری بخش SMB و بکارگیری چندین روش اجرای از راه دور کد، خاصیت کرم‌گونه به خود گرفت و در عرض چند ساعت سازمان‌ها و شرکت‌های متعددی را، ابتدا در اوکراین و سپس در کشورهای دیگر عمدتاً در اروپا به خود آلوده کرد. هر چند که برخی شرکت‌های ضدویروس بر این باورند که نسخه ششم تیر ماه باج‌افزار مذکور بدافزاری متفاوت و مستقل از Petya بوده و بر همین اساس آن را NotPetya نامگذاری کرده‌اند. بررسی برخی محققان نشان می‌دهد که در نسخه ششم تیر ماه روشی برای نگهداری نسخه اصلی MBR دستگاه آلوده شده - که این باج‌افزار آن را با MBR خود جایگزین می‌کند - در نظر گرفته نشده و ممکن است داشتن کلید رمزگشایی هم نتواند کمکی به قربانی کند. حتی برخی این نظریه را نیز مطرح کرده‌اند که بکارگیری این باج‌افزار صرفاً برای مخفی ساختن حمایت یک دولت از اجرای حمله سایبری بر ضد کشور اوکراین بوده باشد. اگر چه در مدتی بسیار کوتاه دامنه آلودگی‌ها از اوکراین به بسیاری از کشورهای دیگر گسترش پیدا کرد.



▲ شکل ۱۳: آلودگی گسترده سیستم‌ها به باج‌افزار Petya در ششم تیر ماه ۹۶

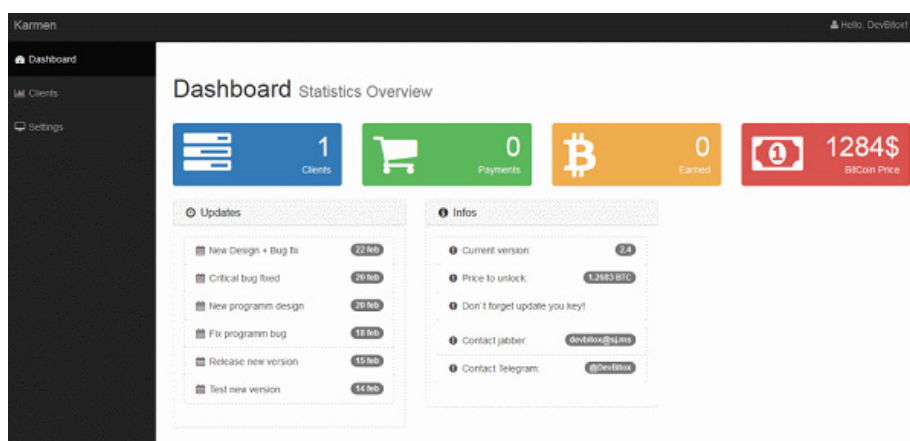
Karmen

Karmen از جمله باج‌افزارهایی است که در قالب خدمات "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service) - به اختصار RaaS - ارائه شده است.

در RaaS، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخذی شده از قربانی به نویسنده و بخشی دیگر به متقاضی می‌رسد.

باج‌افزار Karmen بر پایه HiddenTear که یک پروژه کد باز^{۱۸} است توسط یک نفوذگر روسی زبان با نام DevBitox و با مشارکت یک برنامه‌نویس آلمانی در قالب RaaS توسعه داده شده است.

با خرید عضویت سرویس Karmen با قیمت ۱۷۵ دلار، یک دسترسی تحت وب به پورتال آن فراهم می‌شود و پرداخت‌کننده می‌تواند نسخه‌ای سفارشی شده از Karmen را ایجاد و دریافت کند.



▲ شکل ۱۴: پورتال RaaS باج‌افزار Karmen

با آلوده شدن دستگاه به Karmen، فایل‌های کاربر رمزگذاری شده و در پنجره‌ای ضمن اطلاع‌رسانی، به قربانی هشدار داده می‌شود که در صورت دست‌درازی به فرآیند رمزگذاری، ممکن است فایل‌ها برای همیشه از دست بروند. باج‌افزار Karmen مجهز به قابلیت‌های ضد ماشین مجازی و ضد قرنطینه امن^{۱۹} بوده و در صورت شناسایی هر یک از این بسترها اجرای خود را متوقف می‌کند.

سازندگان Karmen ادعا می‌کنند که این باج‌افزار توسط اکثر محصولات ضدویروس قابل شناسایی نیست. این در حالی است که باج‌افزارهای مبتنی بر Hidden Tear از جمله Karmen بخوبی توسط بسیاری از محصولات ضدویروس شناسایی و متوقف می‌شوند.

خوشبختانه فایل‌های رمز شده توسط باج‌افزار Karmen بدون نیاز به پرداخت باج قابل رمزگشایی هستند.

Open Source ^{۱۸}
Anti-Sandbox ^{۱۹}

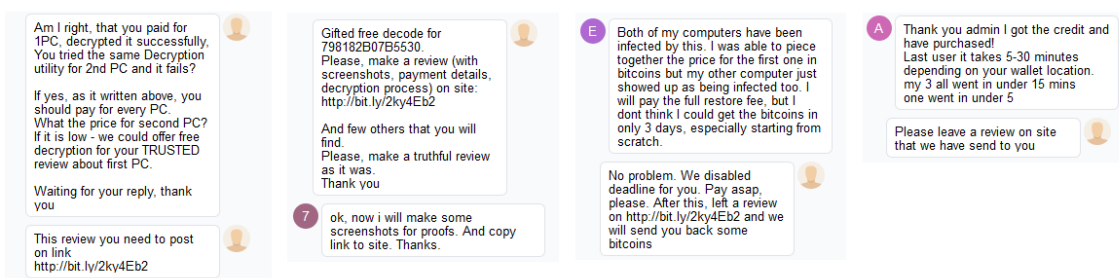
Spora

از جمله خدمات ارائه شده توسط تبهکاران صاحب باج‌افزار Spora پورتال ویژه‌ای است که قربانیان می‌توانند از طریق شناسه آلودگی درج شده در اطلاعیه باج‌گیری به آن متصل شوند. پورتالی که علاوه بر امکانات منحصر به فرد خود مجهز به بخشی برای گفتگوی زنده قربانیان با صاحبان باج‌افزار Spora است.

محققان گروه MalwareHunter موفق شده‌اند تا با تغییر شناسه یک نمونه آلودگی، به پورتال چندین قربانی این باج‌افزار متصل شده و ارتباطات بین این قربانیان و صاحبان Spora را رصد کنند.

آنچه که مشخص است صاحبان این باج‌افزار توجه‌ای خاص به پشتیبانی از مشتریان یا بهتر بگوییم قربانیان خود دارند. صاحبان Spora پشتیبانی را به دو زبان انگلیسی و روسی ارائه کرده و به سئوالات و ابهامات مشتریان عصبانی در نهایت ادب و احترام و با صرف زمان کافی پاسخ می‌دهند.

در خصوص قربانیانی که قادر به پرداخت باج در فرصت تعیین شده نیستند صاحبان Spora با ملایمت و خوشرویی این مهلت را برای این قشر از مشتریان خود یا تمدید کرده یا به طور کامل غیرفعال می‌کنند.



شکل ۱۵: نمونه هایی از گفتگوی گردانندگان باج‌افزار Spora با قربانیان خود

همچنین صاحبان Spora به آن دسته از قربانیانی که تجربشان را از کیفیت پشتیبانی این باج‌افزار در تالار گفتگوی اینترنتی سایت Bleeping Computer که به بررسی باج‌افزارها شهرت دارد به اشتراک بگذارند تخفیف رمزگشایی و یا حتی امکان رمزگشایی رایگان ارائه می‌دهند.

در طی چند سال گذشته نمونه‌هایی از باج‌افزارها بوده‌اند که حتی در صورت پرداخت باج توسط قربانی عملیات رمزگشایی را انجام نمی‌دادند. برای اینگونه باج‌افزارهای کلاهبردار که از ابتدا قصد برگرداندن اطلاعات قربانی را ندارند و فقط سعی در گرفتن پول از قربانی دارند، از اصطلاح Ranscam که خلاصه شده Ransome Scam است، استفاده می‌شود. به نظر می‌رسد هدف صاحبان Spora از این پیشنهاد، اطمینان خاطر دادن به قربانیان خود در خصوص رمزگشایی شدن فایل‌ها با پرداخت باج بوده باشد. گروه MalwareHunter پشتیبانی صاحبان Spora را از بخش پشتیبانی بسیاری از شرکت‌های فناوری کاربرپسندتر و کمک‌کننده‌تر توصیف کرده است.

صاحبان این باج‌افزار خدمات خود را در قالب بسته‌های "بازگردانی کامل"، "مصونیت در برابر حملات آتی باج‌افزار"، "حذف باج‌افزار" و "بازگردانی فقط فایل" به قربانیان خود ارائه می‌دهند.

بررسی‌های انجام شده نشان می‌دهد که در صورت خرید بسته "مصونیت در برابر حملات آتی باج‌افزار" ابزاری در اختیار کاربر قرار می‌گیرد که با اجرای آن در مسیر %AppData% فایل‌ها با شماره سریال Volume دستگاه ایجاد می‌شود.

PooleZoor

در اواسط تابستان ۱۳۹۷، منابع مختلف از شناسایی باج‌افزاری خبر داده‌اند که پس از رمزگذاری فایل‌های کاربر با الگوریتم AES به آنها پسوند poolezoor را الصاق می‌کرد. این باج‌افزار بر پایه پروژه کد باز HiddenTear توسعه داده شده است. نکته جالب در خصوص باج‌افزار PooleZoor، درج یک جمله انگلیسی و دو جمله فارسی با نویسه‌های انگلیسی در اطلاعیه باج‌گیری آن با نام READ_me_for_encrypted_Files.txt است.

```
public void messageCreator()
{
    string userName = Environment.UserName;
    string str = "C:\\Users\\";
    string str2 = "\\Desktop\\READ_me_for_encrypted_Files.txt";
    string path = str + userName + str2;
    string[] contents = new string[]
    {
        "Files has been encrypted with PooleZoor",
        "Ba pardakht 10,000,000 Riyal File hay khod ra bazgardanid",
        "In Pool sarf omre kheyriye khahad shod"
    };
    File.WriteAllLines(path, contents);
}
```

▲ شکل ۱۶: کد نمایش دهنده اطلاعیه باج‌گیری در باج‌افزار PooleZoor

در بخشی از کد این باج‌افزار نیز به رمز عبور "Amir12345" اشاره شده است.

```
public void startAction()
{
    string userName = Environment.UserName;
    string str = "C:\\Users\\";
    string password = "Amir12345";
    string str2 = "\\Desktop\\";
    string location = str + userName + str2;
    this.encryptDirectory(location, password);
    this.messageCreator();
    Application.Exit();
}
```

▲ شکل ۱۷: اشاره به رمز عبور "Amir12345" در باج‌افزار PooleZoor

برخی منابع، وبلاگ <http://ransomware-poolzoor.blogspot.com> را که دیگر در سامانه Blogger قابل دسترس نیست به نویسنده یا نویسندگان این باج‌افزار نسبت داده‌اند. شکل زیر تصویری از این وبلاگ را پیش از حذف شدن نمایش می‌دهد:

The screenshot shows a blog post titled "Ransomware Poolzoor" dated Tuesday, August 7, 2018. The main text in Persian reads: "برای اینکه مارو حمایت بکنید مبلغ یک میلیون تومان به ما پرداخت و برای ما ارسال کنید و در جواب ایمیل شما ما Decryptor را در اختیار شما قرار می‌دهیم. نحوه پرداخت: ورود به لینک: <http://sep.shapaarak.cf> تصویر پرداخت خود را در زیر این پست به همراه آدرس ایمیل خود برای ما ارسال نمایید." The post is attributed to "Sales Ransomware" and has one comment. A sidebar on the right contains "About Me" (Sales Ransomware) and "Blog Archive" (2018: 3 posts, August: 2 posts, July: 1 post). At the bottom of the post, there is a small image of a document with text.

▲ شکل ۱۸: وبلاگ منتسب به نویسنده یا نویسندگان باج‌افزار PooleZoor

متن درج شده در وبلاگ به شرح زیر است:

برای اینکه مارو حمایت بکنید مبلغ یک میلیون تومان به ما پرداخت و برای ما ارسال کنید و در جواب ایمیل شما ما Decryptor را در اختیار شما قرار می دهیم.

نحوه پرداخت:

ورود به لینک: <http://sep.shapaarak.cf/>

تصویر پرداخت خود را در زیر این پست به همراه ادرس ایمیل خود برای ما ارسال نمائید.

نشانی استفاده شده در متن مذکور، سایتی فیشینگ^{۲۰} است که هدف آن کلاهبرداری و سرقت اطلاعات بانکی کاربر است. بنابراین در صورت مراجعه قربانی به سایت مذکور و وارد کردن اطلاعات کارت بانکی در آن نه فقط ابزار رمزگشایی در اختیار او قرار نمی‌گیرد که تمام اطلاعات بانکی وارد شده نیز در خدمت نویسنده یا نویسندگان PooleZoor قرار خواهد گرفت. PooleZoor، تنها یک نمونه از باج‌افزارهایی است که هدف آنها بطور خاص کاربران ایرانی است. این باج‌افزارها معمولاً با عنوان "باج‌افزار فارسی" شناخته می‌شوند.

^{۲۰} Phishing

راه‌های پیشگیری و مقابله

۱ تهیه نسخه پشتیبان

از اطلاعات سازمانی به صورت 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 استفاده از فناوری‌های حفاظتی پیشرفته

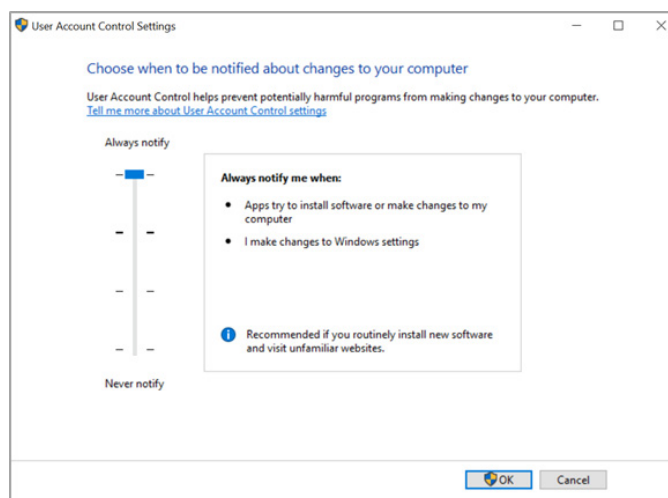
استفاده از ضدویروس قدرتمند و به‌روز جهت مقابله با انواع باج‌افزارها لازم و ضروری است. اما در کنار آن می‌بایست از راهکارها و محصولات نفوذیاب، ضدهرزنامه، کنترل‌کننده وب و دیوار آتش نیز بهره گرفت. همچنین برخی محصولات امنیتی نظیر McAfee و Bitdefender دارای راهکارهایی ویژه و خاص برای شناسایی و مقابله با باج‌افزارها هستند.

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

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

۴ محدود کردن سطح دسترسی

همه کاربران، حتی مدیر سیستم می‌بایست با حداقل سطح دسترسی مورد نیاز به هر سیستم وارد شوند. 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. همچنین توصیه می‌شود بخش User Account Control Settings در Windows بر روی حالت Always notify me قرار داده شود.



▲ شکل ۱۹: تنظیمات بخش User Account Control

۵ غیرفعال کردن بخش ماکرو در نرم‌افزار Office

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. غیرفعال کردن این قابلیت، از طریق Group Policy نیز ممکن است. همچنین توصیه می‌شود ایمیل‌های دارای پیوست ماکرو در همان درگاه شبکه مسدود شوند. بدین منظور می‌توان از تجهیزات دیواره آتش مجهز به چنین قابلیت‌هایی بهره گرفت.



در اتاق خبر شبکه گستر بخوانید... ◀

۶ پیگیربندی صحیح قابلیت Dynamic Data Exchange در نرم‌افزار Office

نرم‌افزار Microsoft Office چندین روش انتقال و به اشتراک گذاری اطلاعات میان برنامه‌ها را ارائه می‌دهد. یکی از این روش‌ها Dynamic Data Exchange - DDE - به اختصار DDE - است. DDE پودمانی متشکل از مجموعه‌ای از پیام‌ها و راهنماهاست. این پودمان راهکاری برای به اشتراک گذاری داده‌ها و استفاده از حافظه‌ای مشترک برای تبادل داده‌ها میان چندین برنامه است. از حدود چند ماه قبل چندین گروه از مهاجمان سایبری دست به اجرای حملاتی زده‌اند که در آنها در قالب فایل‌هایی همچون Word از پودمان مجاز DDE سواستفاده شده و فایل مخرب بر روی دستگاه قربانی اجرا می‌شود. توصیه می‌شود تنظیمات امنیتی مناسب در خصوص این پودمان اعمال گردد.



در اتاق خبر شبکه گستر بخوانید... ◀

۷ پیکربندی صحیح پودمان RDP

همانطور که اشاره شد در سال‌های اخیر، مهاجمان برای انجام فعالیت‌های مخربی همچون انتشار انواع بدافزارها از جمله باج‌افزارها به‌طور گسترده‌ای از پودمان RDP بهره گرفته‌اند. با پیکربندی دقیق این پودمان سازمان را از گزند این تهدیدات حفاظت کنید.



در اتاق خبر شبکه گستر بخوانید... ◀

۸ نمایش پسوند فایل‌ها

به‌صورت پیش‌فرض در سیستم عامل Windows پسوند فایل‌ها نمایش داده نمی‌شود. این بدان معناست که کاربر می‌بایست به نشان فایل اعتماد کند. موضوعی که سبب استفاده برخی ویروس‌نویسان از فایل‌های دو پسوندی برای فریب کاربران می‌شود. 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.

۹ به‌روز بودن در خصوص روش‌های جدید باج‌گیران

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

۱۰ 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 داده‌نمایی‌های شرکت مهندسی شبکه گستر که در نشانی www.shabakeh.net/infographic قابل دسترس است استفاده نمایید.

فهرست منابع

- <https://newsroom.shabakeh.net/18625/wannacry-analysis.html>
- <https://newsroom.shabakeh.net/18668/honda-wannacry-attack.html>
- <https://newsroom.shabakeh.net/17512/chimera-decryption-keys-leaked-by-rival-gang.html>
- <https://newsroom.shabakeh.net/18681/petya-analysis.html>
- <https://newsroom.shabakeh.net/18703/petya-master-decryption-keys-published.html>
- <https://newsroom.shabakeh.net/18124/petya-goldeneye.html>
- <https://newsroom.shabakeh.net/19749/hardening-rdp.html>
- <https://newsroom.shabakeh.net/19222/dde-attacks.html>
- <https://newsroom.shabakeh.net/19147/locky-ransomware-exploits-dde.html>
- <https://newsroom.shabakeh.net/19265/securing-office-macros.html>
- <https://newsroom.shabakeh.net/18477/karmen-ransomware-as-a-service.html>
- <https://newsroom.shabakeh.net/18224/spora-ransomware.html>
- <https://newsroom.shabakeh.net/18295/spora-with-excellent-customer-service.html>
- <https://www.certcc.ir/news/12389>
- <https://www.certcc.ir/news/82>

شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده

است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان 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 نرم افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) 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 با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان 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 بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که 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 پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه 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.



ISO 9001:2008

Cert No 9150.C528

شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

گروه فروش

sales@shabakeh.net | داخلی ۱ ۴۲۰۵۲

گروه پشتیبانی

support@shabakeh.net | داخلی ۲ ۴۲۰۵۲

تارنمای شرکت

www.shabakeh.net

خدمات پس از فروش و پشتیبانی

my.shabakeh.net

مرکز آموزش

events.shabakeh.net

اتاق خبر

newsroom.shabakeh.net