بـررسـی و تـحـلـیـل

Dot Ransomware RaaS

شبکه گستر
شـرکت مهندسی شـبکه گسـتر

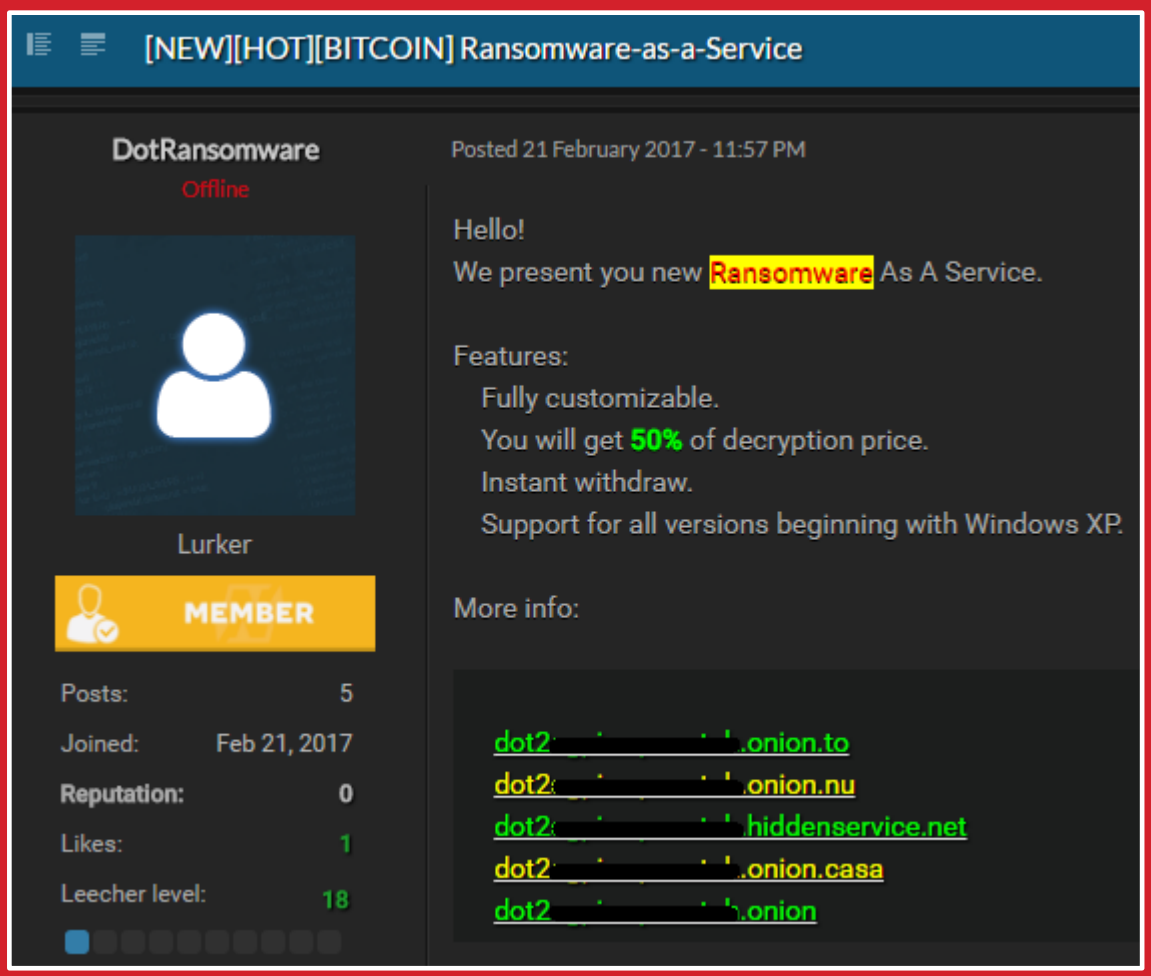
عنوان سند: بررسی و تحلیل Dot Ransomware RaaS
شناسه سند: SPT-A-0130-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ آخرین بازنگری: ۱۵ اسفند ۱۳۹۵ | شرح آخرین بازنگری: -

باج‌افزارهای رمزگذار را می‌توان یکی از مخرب‌ترین و همچنین رایج‌ترین تهدیدات دو سال اخیر قلمداد کرد. یکی از عوامل نگران‌کننده که انتظار می‌رود سبب افزایش انتشار و گسترش این نوع بدافزارها شود عرضه باج‌افزار در قالب خدماتی موسوم به Ransomware-as-a-Service – بـه اختصار RaaS – (باج‌افزار به‌عنوان خدمت) است.

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.

Dot Ransomware نمونه‌ای جدید از این خدمات است که عرضه آن هم اکنون در تالارهای گفتگوی اینترنتی تبهکاران سایبری تبلیغ می‌شود.

در این گزارش، ساختار بکار رفته و مکانیزم‌های استفاده شده در Dot Ransomware RaaS مورد بررسی و تحلیل قرار گرفته است.



شکل ۱: تبلیغ Dot Ranomware RaaS در تالارهای گفتگوی اینترنتی تبهکاران سایبری

باج‌افزار[1] گونه‌ای بدافزار است که از راه‌های مختلف دسترسی به فایل‌های کاربر را محدود ساخته و برای دسترسی مجدد، از او درخواست باج می‌کند.

در سال‌های اخیر آن دسته از باج‌افزارهایی که از طریق رمزنگاری[2] اقدام به محدودسازی دسترسی کاربر به فایل‌ها می‌کنند موفقیت‌های بی‌مثالی را نصیب صاحبان تبهکار خود نموده‌اند.

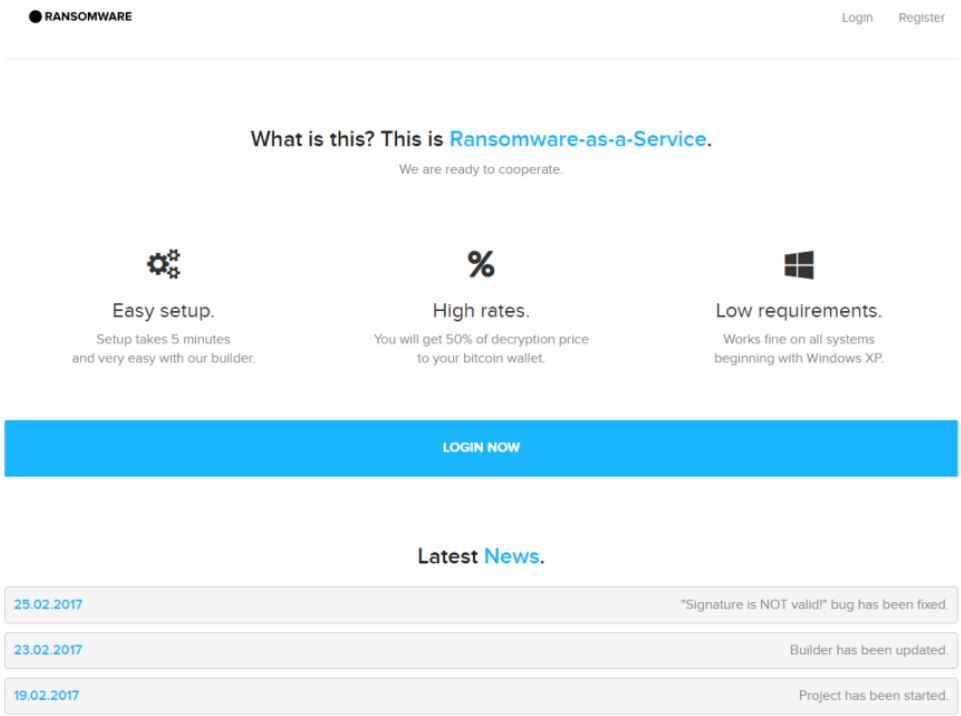
در این نوع محدودسازی، هدف از رمز کردن، تغییر ساختار فایل است؛ به‌نحوی که تنها با داشتن کلید رمزگشایی[3] بتوان به محتوای فایل دسترسی پیدا کرد. پیچیدگی و قدرت این کلیدها بر اساس تعداد بیت بکار رفته در کلید است. هر چه تعداد این بیت‌ها بیشتر باشد شانس یافتن آن هم دشوارتر و در تعداد بیت بالا عملاً غیرممکن می‌شود.

مدتی است که برخی نویسندگان ویروس، باج‌افزارهای خود را در قالب خدماتی موسوم به Ransomware-as-a-Service – به اختصار RaaS – به متقاضیان تبهکاری که معمولاً تخصص چندانی در زمینه ویروس‌نویسی و یا حتی برنامه‌نویسی ندارند اجاره می‌دهند. در این روش، متقاضی تنها وظیفه انتشار را بر عهده دارد.

الگوی پرداخت در خدمات RaaS باج‌افزار Dot Ransomware به‌صورت ۵۰/۵۰ است. بدان معنا که در صورت آلوده شدن یک دستگاه به باج‌افزار Dot Ransomware و پرداخت باج توسط قربانی نیمی از آن به نویسنده یا نویسندگان این باج‌افزار و نیمی دیگر – بر اساس ادعای این افراد – به متقاضی اجاره کننده که انتشار توسط او انجام شده می‌رسد.

پورتال Dot Ransomware RaaS

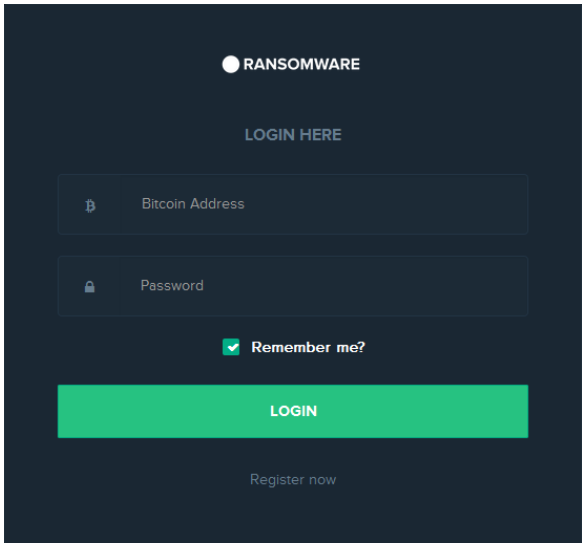
شکل ۲ صفحه ورود به پورتال Dot Ransomware را نشان می‌دهد.



شکل ۲: صفحه ورود به پورتال Dot Ranomware RaaS

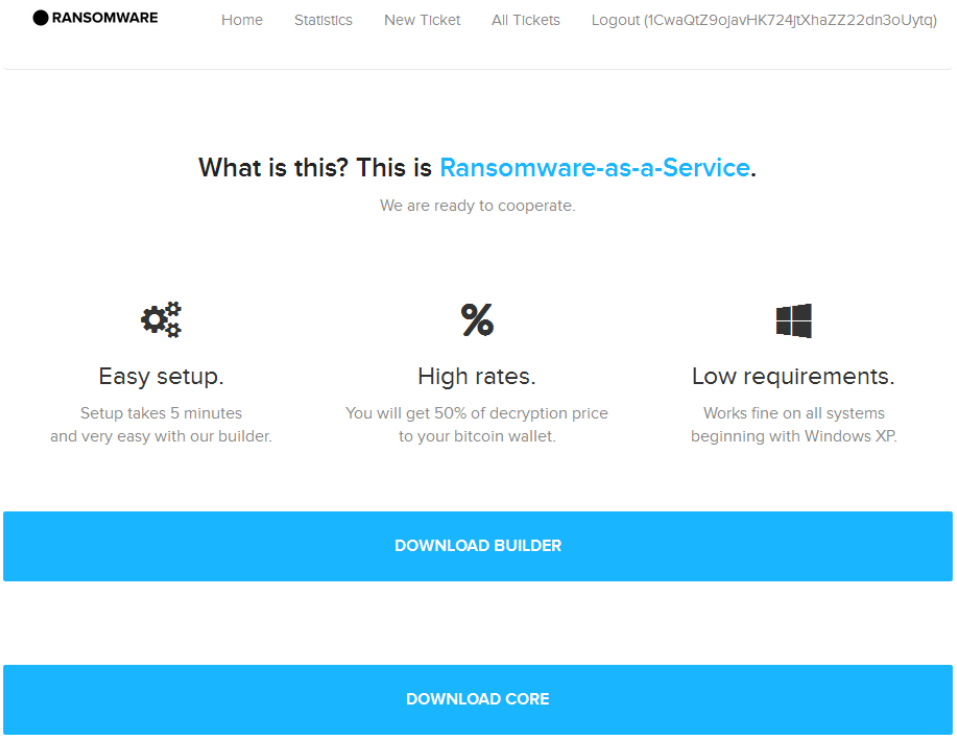
[1] Ransomware
[2] Encryption
[3] Decryption Key

برای شروع کافی است که متقاضی با یک حساب بیت‌کوین[۴] ثبت نام در سایت را انجام دهد.



شکل ۳: ثبت نام در پورتال Dot Ranomware RaaS

با ورود به سیستم، دو فایل با نام‌های core.exe و DotRansomwareBuilder.exe به متقاضی ارائه می‌شود.



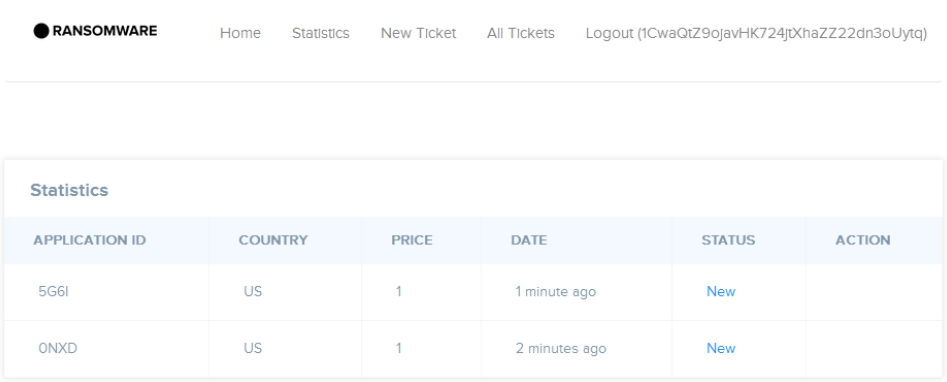
شکل ۴: بخش دانلود فایل در پورتال Dot Ransomware

برای رهگیری تعداد و وضعیت آلودگی‌ها، یک صفحه آماری نیز برای متقاضی قابل دسترس است. Dot Ransomware RaaS آن دسته از آلودگی‌هایی را موفق می‌داند که قربانی حداقل یکبار به سایت اشاره شده در اطلاعیه باج‌گیری[۵] مراجعه کرده باشد.

---

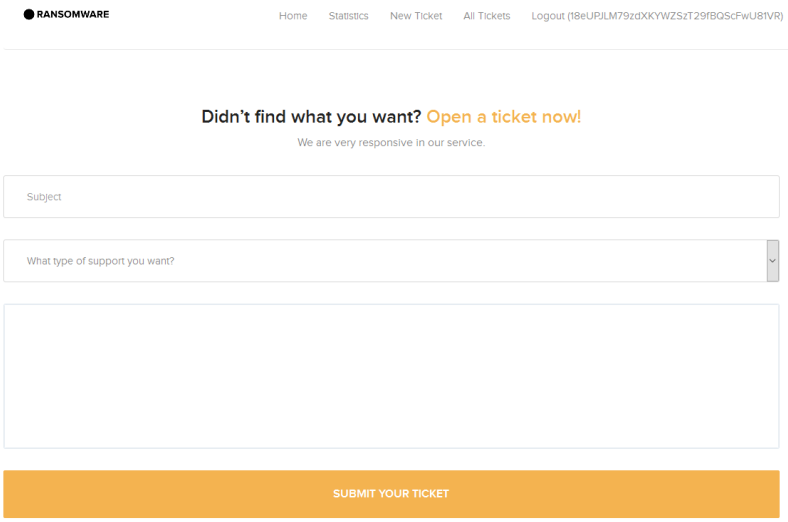
[۴] Bitcoin

[۵] Ransom Note



شکل ۵: آمار آلودگی‌ها به Dot Ransomware در پورتال متقاضی

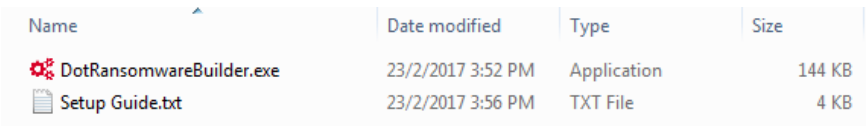
همچنین در پورتال Dot Ransomware بخشی نیز برای دریافت پشتیبانی در نظر گرفته شده است.



شکل ۶: صفحه درخواست پشتیبانی در پورتال Dot Ransomware RaaS

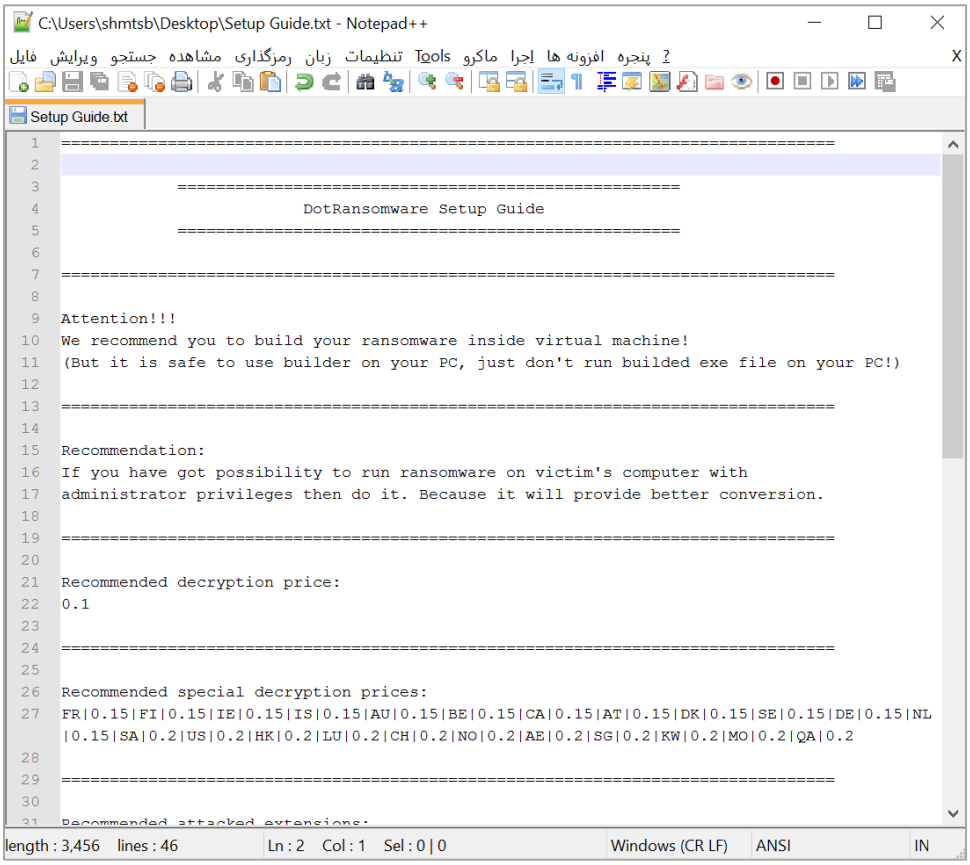
ساخت نمونه باج‌افزار

به همراه DotRansomwareBuilder فایلی با نام Setup Guide.txt نیز ارائه می‌شود.



شکل ۷: فایل‌های DotRansomwareBuilder و Setup Guide در پورتال متقاضی

Setup Guide حاوی توصیه‌ها و پیشنهادهایی به متقاضی است.

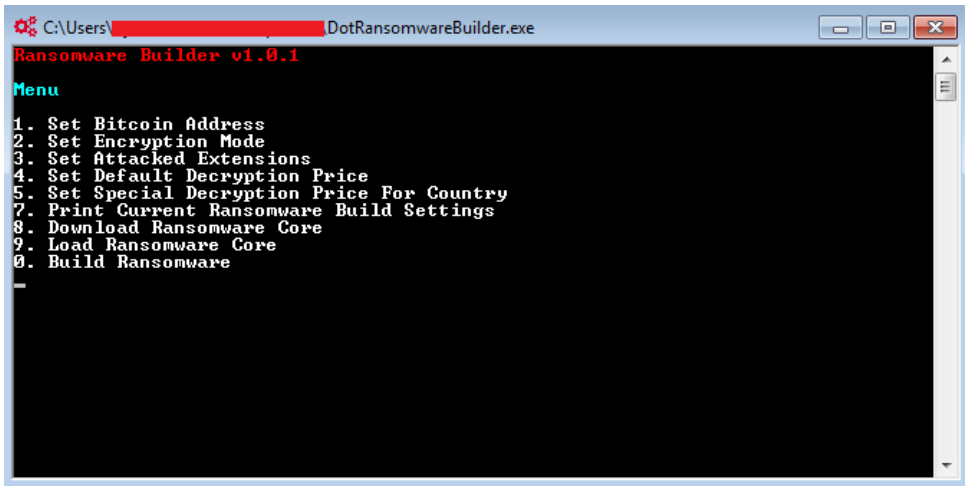


شکل ۸: فایل Setup Guide

برای مثال در بخشی از آن در خصوص قیمت‌گذاری مقدار باج برای کشورهای مختلف، موارد زیر توصیه شده است.

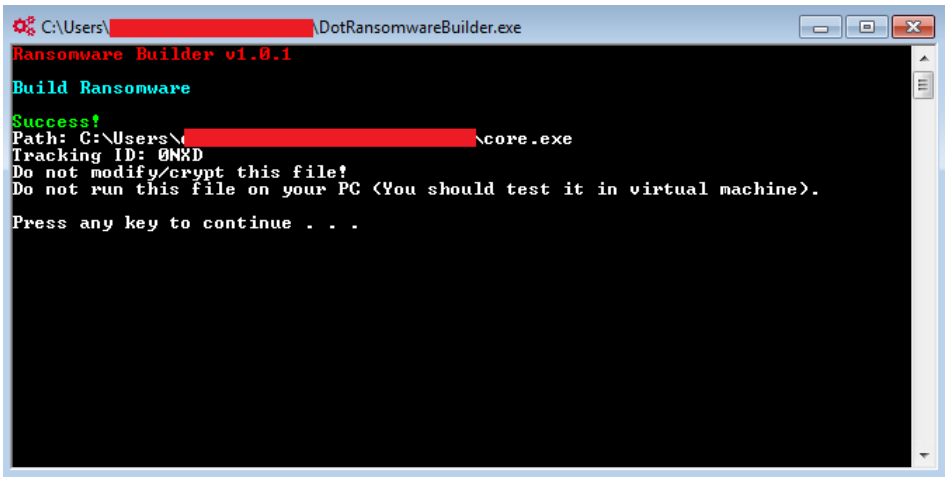
```
FR|0.15|FI|0.15|IE|0.15|IS|0.15|AU|0.15|BE|0.15|CA|0.15|AT|0.15|DK|0.15|SE|0.15|DE|0.15|NL|
0.15|SA|0.2|US|0.2|HK|0.2|LU|0.2|CH|0.2|NO|0.2|AE|0.2|SG|0.2|KW|0.2|MO|0.2|QA|0.2
```

با اجرای DotRansomwareBuilder.exe پنجره خط فرمانی مشابه شکل ۹ ظاهر شده و متقاضی می‌تواند تنظیمات مورد نظر خود را از طریق آن تعیین کند.



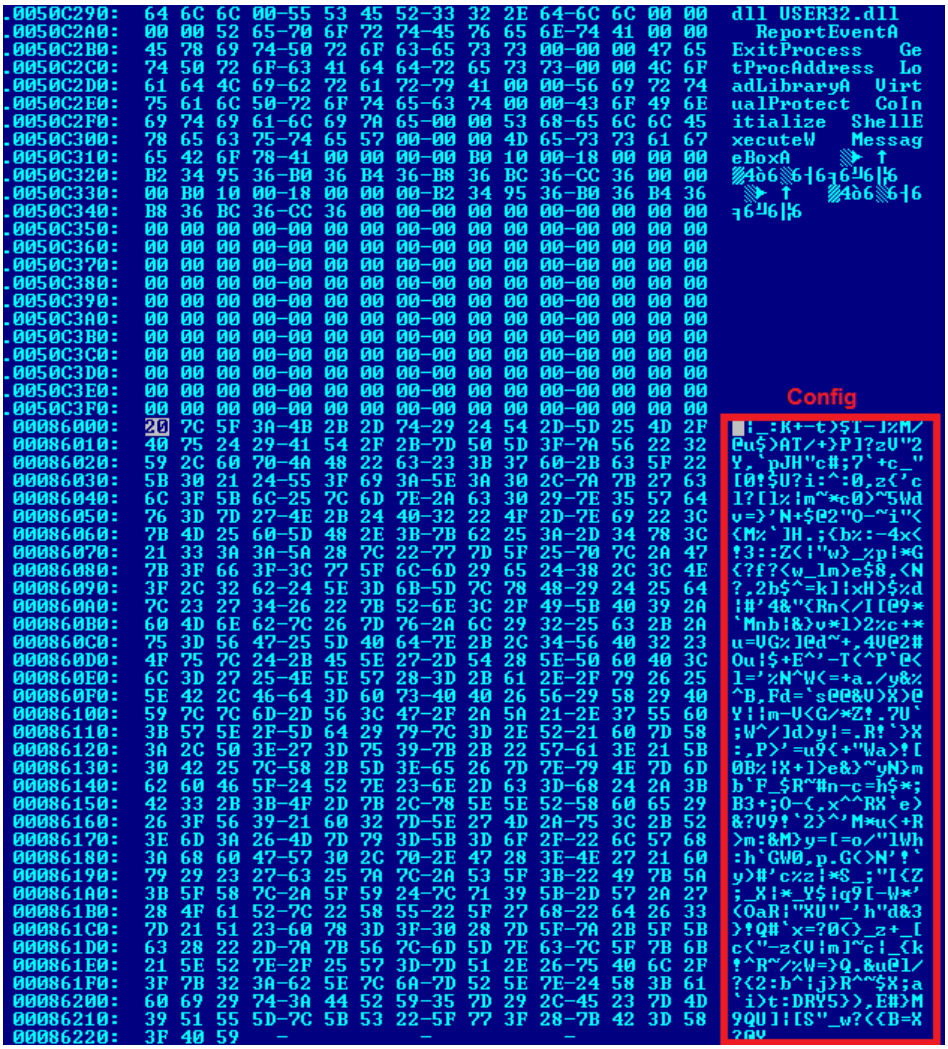
شکل ۹: منوی DotRansomwareBuilder.exe

پس از پیکربندی موفقیت‌آمیز، نمونه‌ای از باج‌افزار DotRansomwareBuilder با یک Track ID (شناسه ردیابی) منحصربه‌فرد ایجاد می‌شود. این Track ID شناسه اختصاص یافته به نمونه ساخته شده است.



شکل ۱۰: اعلام ساخت موفقیت‌آمیز نمونه باج‌افزار از طریق DotRansomwareBuilder.exe

تنظیمات تعیین شده به‌صورت رمز شده در کد مخرب باج‌افزار درج می‌شود.



شکل ۱۱: تنظیمات رمزگذاری شده در نمونه ساخته شده

جدول ۱ این تنظیمات را نمایش می‌دهد.

متغیر	توضیحات
appID (Tracking ID)	شناسه ردیابی که به ازای هر نمونه اجاره داده شده منحصربه‌فرد است.
bitcoinAddress	نشانی بیت‌کوین متقاضی
defaultPrice	مبلغ پیش‌فرض اخاذی که یک بیت‌کوین است. در صورتی که متقاضی مقداری تعیین نکرده باشد، این مبلغ در نظر گرفته خواهد شد.
partEncryption	با فعال بودن این گزینه تنها ٤ مگابایت ابتدایی فایل رمزگذاری می‌شود. این گزینه به صورت True / False (صحیح / نادرست) ذخیره می‌شود.
extensions	پسوندهای هدف قرار گرفته شده توسط متقاضی در این قسمت مشخص می‌شوند.
countries	کشورهای با مبلغ اخاذی شده خاص در این قسمت تعیین می‌شوند.
prices	مبلغ اخاذی به ازای کشورهای خاص تعیین شده توسط متقاضی در این قسمت مشخص می‌شود.

جدول ۱: تنظیمات درج شده در فایل نمونه ساخته شده

حفاظت از حقوق صاحبان باج‌افزار!

در صورت اجرا شدن فایل بر روی دستگاه قربانی، پس از رمزگشایی تنظیمات، نشانی URL که قربانی برای پرداخت باج به آن هدایت می شود (unlock26ozqwoyfv) نیز رمزگشایی می‌شود. این نشانی URL، توسط نویسنده یا نویسندگان Dot Ransomware در کد تزریق شده است. برای اطمینان یافتن از اینکه نشانی URL تغییر نکرده باشد، درهم ساز[۶] SHA256 آن محاسبه شده و با مقدار درون کد مقایسه می‌شود.

این کار برای اطمینان یافتن از انجام فرآیند پرداخت در صفحه طراحی شده توسط نویسنده یا نویسندگان باج‌افزار و جلوگیری از دور زدن این افراد توسط متقاضی صورت می‌پذیرد! تنها در آن صورت است که احتمالاً متقاضی تکثیرکننده باج‌افزار سهم خود را دریافت خواهد کرد.

```
Address  Hex dump                                         ASCII
004F0AE8 62 62 39 36 61 65 61 31 30 66 33 33 61 64 35 38 bb96aea10f33ad58
004F0AF8 37 38 62 65 39 62 32 30 65 33 66 66 61 31 35 36 78be9b20e3ffa156
004F0B08 62 64 63 39 66 31 66 30 64 62 66 66 65 39 36 33 bdc9f1f0dbffe963
004F0B18 30 61 35 30 37 30 30 63 65 34 37 65 64 38 39 61 0a50700ce47ed89a
```

شکل ۱۲: مقدار درهم‌ساز SHA256 تزریق شده در کد

همین کار برای کلید عمومی RSA-4096 درون فایل نیز انجام می‌شود. هدف، اطمینان حاصل شدن از توانایی رمزگشایی فایل از طریق کلید خصوصی میزبانی شده بر روی سرور فرماندهی[۷] است.

در صورت برابر نبودن مقادیر درهم‌سازها، باج‌افزار اجرای خود را متوقف می‌کند.

---

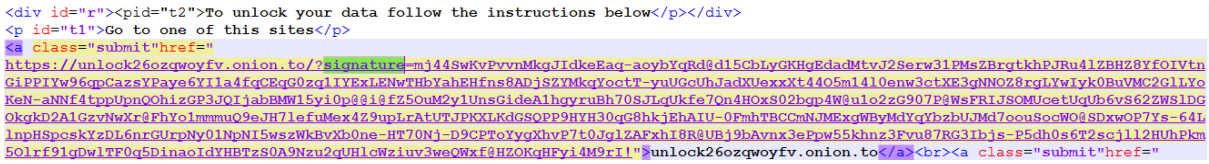
۶ Hash

۷ Command and Control – C&C – C2

ایجاد امضاء

رمزگذاری داده‌های کاربر بدون اتصال به سرور فرماندهی انجام می‌شود. مزیت این روش آن است که ترافیک مشکوک کمتری در سطح شبکه ایجاد شده و حتی در صورت عدم اتصال دستگاه به اینترنت، رمزگذاری همچنان انجام می‌شود.

اما در عین حال باید راهی برای متمایز کردن هر دستگاه آلوده شده با دستگاه‌های آلوده دیگر فراهم باشد تا در صورت پرداخت باج توسط قربانی، عملیات رمزگشایی تنها برای آن دستگاه انجام شود. بدین منظور برای هر آلودگی یک امضای منحصربه‌فرد تولید شده و به لینکی که قربانی را به سایت نویسنده یا نویسندگان Dot Ransomware هدایت می‌کند الصاق می‌شود.



شکل ۱۳: نمونه‌ای از امضای الصاق شده به نشانی URL

جدول ۲ حاوی مواردی است که امضای ساخته شده شامل آنها می‌شود.

جزء تشکیل‌دهنده امضا	توضیحات
key{38 bytes }	مقداری که به‌صورت تصادفی ایجاد شده و برای رمزگذاری از آن استفاده می‌شود.
iv{8 bytes}	مقداری که به‌صورت تصادفی ایجاد شده و از آن به عنوان بردار اولیه[۸] استفاده می‌شود.
bitcoinAddress	نشانی بیت‌کوین متقاضی
appID(TrackingID)	شناسه ردیابی که به ازای هر نمونه اجاره داده شده منحصربه‌فرد است.
country	کشوری که دستگاه آلوده شده در آن قرار دارد
price	مبلغ اخاذی تعیین شده توسط متقاضی
partEncryption	رمزگذاری تنها ٤ مگابایت ابتدایی فایل (True / False – صحیح / نادرست)
uniqueExtension {3 char}	سه شناسه تصادفی که در قالب زیر پسوند فایل‌های رمز شده می‌شود. locked-{uniqueExtension}

جدول ۲: اجزای تشکیل‌دهنده امضای دستگاه آلوده شده

پس از جمع‌آوری تمامی داده‌های مورد نیاز، امضا با یک کلید عمومی RSA-4096 که در کد تزریق شده رمزگذاری می‌شود. برخی نویسه‌های امضای ایجاد شده به‌صورت زیر جایگزین می‌شوند.

- + → @
- / → _
- = → !

[۸] Initialization Vector

رمزگذاری فایل‌های قربانی

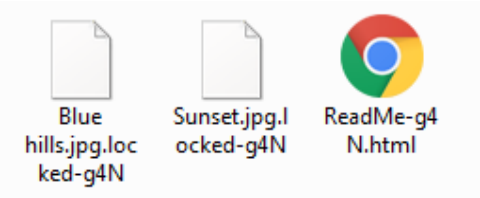
Dot Ransomware فایل‌های با پسوندهای تعیین شده بر روی دستگاه قربانی را با الگوریتم Blowfish رمزگذاری می‌کند. Blowfish یک الگوریتم کلید متقارن[۹] است. در الگوریتم‌های متقارن، کلید رمزگذاری و رمزگشایی یکسان یا بسیار مشابه است. این کلید در باج‌افزار Dot Ransomware یک مقدار ۳۸ بایتی تصادفی است.

همچنین ۸ بایت نیز به‌صورت تصادفی به‌عنوان بردار اولیه ایجاد شده و مورد استفاده قرار می‌گیرد. هدف از استفاده از بردار اولیه با مقداری تصادفی، دشوار نمودن رمزگشایی از طریق بررسی چندین نمونه رمز شده با یک کلید یکسان است.

نویسنده یا نویسندگان Dot Ransomware کلید Blowfish را نیز با الگوریتم RSA-4096 رمزگذاری می‌کنند. RSA-4096 یک کلید رمزنگاری نامتقارن است. در این نوع رمزنگاری، از دو کلید عمومی[۱۰] و خصوصی[۱۱] به‌ترتیب برای رمزگذاری و رمزگشایی استفاده می‌شود. بنابراین برای رمزگشایی فایل‌های رمز شده توسط Dot Ransomware به کلید خصوصی نیز نیاز است.

پسوند فایل های رمز شده به صورت قالب زیر تغییر می‌کند:

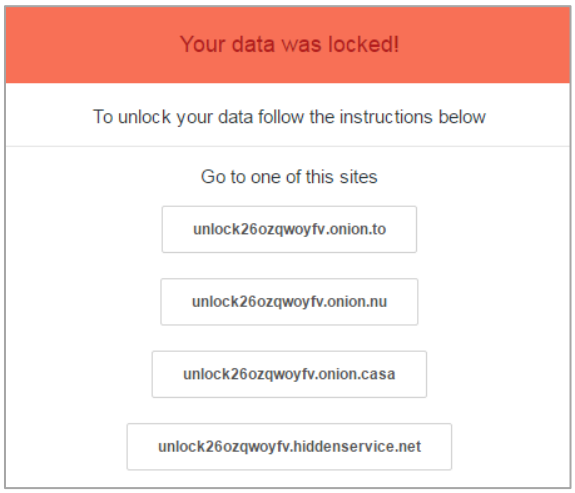
- .locked-{3 random char}



شکل ۱۴: فایل‌های رمز شده توسط Dot Ransomware

پس از رمزگذاری، باج‌افزار فایل ReadMe-{3char}.html را که حاوی اطلاعیه باج‌گیری است و در مسیر %Temp% ذخیره شده باز می‌کند. نسخه‌ای از این فایل در هر پوشه‌ای که حداقل یک فایل آن رمزگذاری شده است نیز کپی می‌شود.

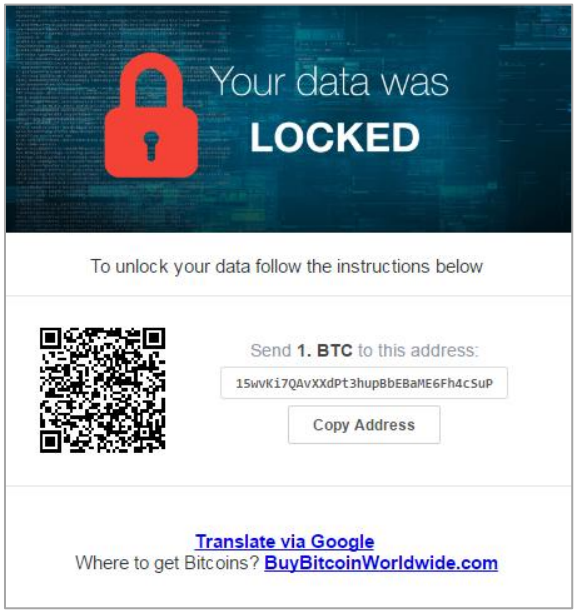
در ReadMe-{3char}.html از کاربر خواسته می‌شود به سایت باج‌افزار از طریق لینکی که در آن امضای دستگاه آلوده شده نیز مشخص شده است مراجعه کند.



شکل ۱۵: محتوای فایل ReadMe-{3char}.html

[۹] Symmetric-key
[۱۰] Public Key
[۱۱] Private Key

تنها گزینه‌ای که قربانی با مراجعه به سایت با آن مواجه می شود پرداخت باج است.



شکل ۱۶: محتوای فایل ReadMe-{3char}.html

نتیجه‌گیری

گرچه عرضه باج‌افزار در قالب خدمات RaaS در ابتدای راه خود قرار دارد اما تردیدی نیست که این رویکرد سبب افزایش هرچه بیشتر تعداد باج‌افزارها، به‌عنوان یکی از مخرب‌ترین تهدیدات چند سال اخیر خواهد شد. به‌خصوص آنکه در این روش متقاضی بدون نیاز به سرمایه و دانش برنامه‌نویسی می‌تواند به این تهدیدات مخرب دست یابد.

آنچه که سازمان‌ها باید در نظر بگیرند رعایت اقدامات پیشگیرانه در نبرد با این تهدیدات است.

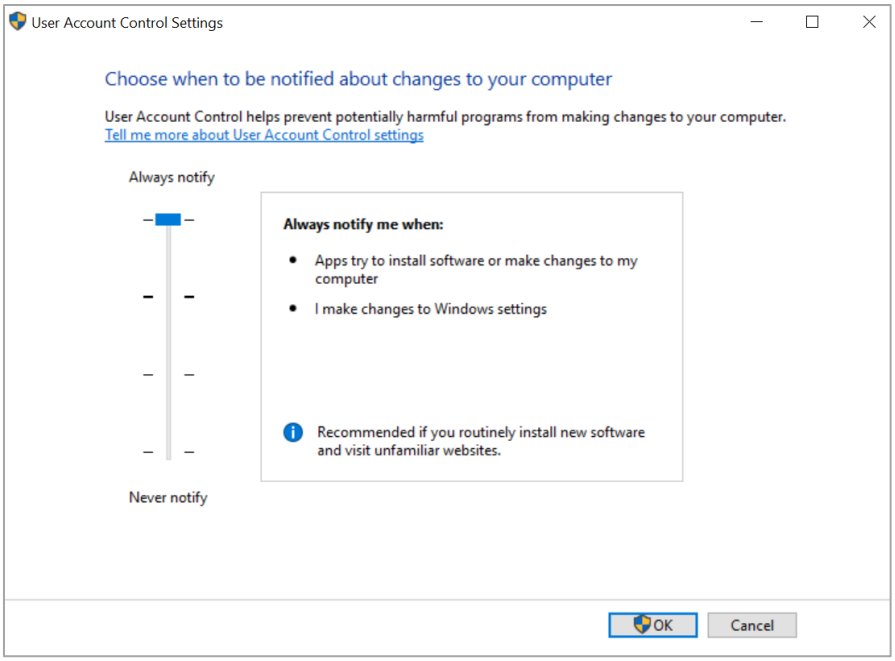
۱ تهیه نسخه پشتیبان

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

۲ 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 حالت Always notify me قرار داده شود.



شکل ۱۷: تنظیمات بخش User Account Control

برای اعمال این پیکربندی بر روی تمامی دستگاه‌های سازمان از طریق Group Policy می‌توان از این راهنما استفاده کرد.

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

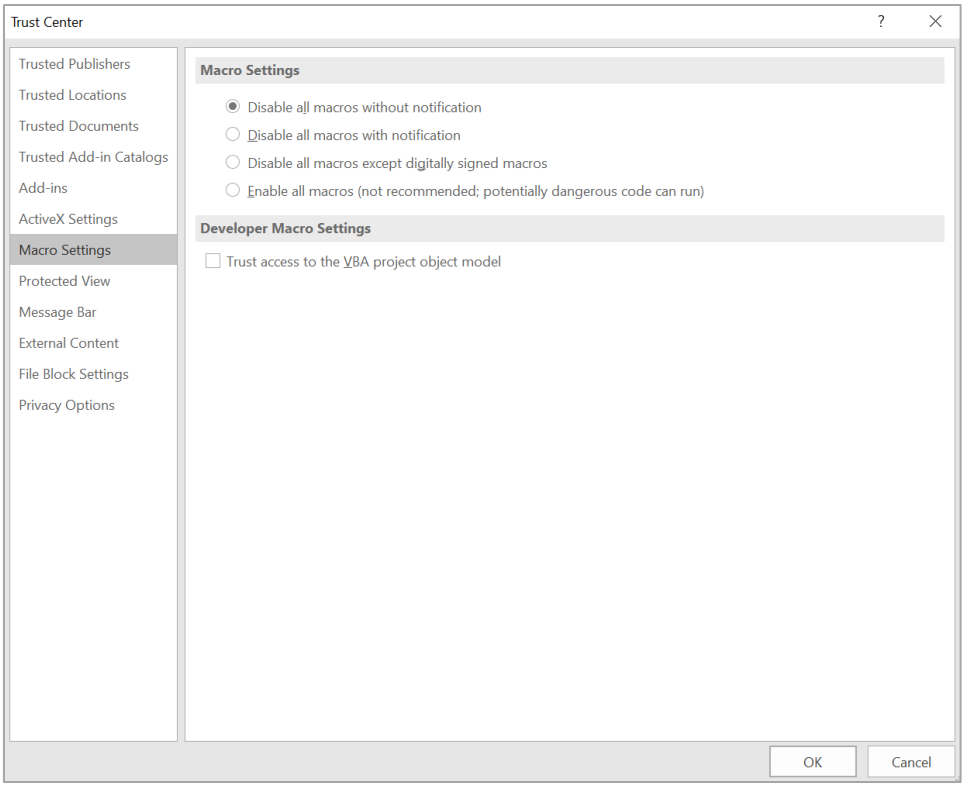
بسیاری از بهره‌جویی‌ها از طریق سوءاستفاده از ضعف‌های امنیتی نرم‌افزارهای پرکاربردی نظیر Adobe Flash، Office و مرورگرها صورت می‌پذیرد. هر چه زودتر اصلاحیه نصب شود آسیب کمتری متوجه سازمان می‌شود.

٤ استفاده از فناوری‌های حفاظتی پیشرفته

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

۵ غیرفعال کردن بخش ماکرو

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



شکل ۱۸: تنظیمات امنیتی بخش ماکرو در نرم‌افزار Office

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

همچنین توصیه می‌شود ایمیل‌های دارای پیوست ماکرو در همان درگاه شبکه مسدود شوند. بدین منظور می‌توان از تجهیزات دیواره آتش مجهز به این قابلیت بهره گرفت.

۶ احتیاط در زمان باز کردن ایمیل‌ها

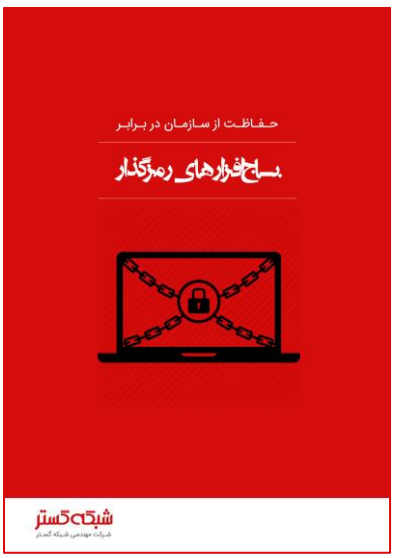
آموزش و راهنمایی کاربران سازمان به صرف‌نظر کردن از فایل‌های حتی کمی مشکوک و باز نکردن آنها می‌تواند نقشی مؤثر در پیشگیری از اجرا شدن پیوست‌های مخرب داشته باشد. برای این منظور می‌توانید از این داده‌نمایی‌ها استفاده کنید.

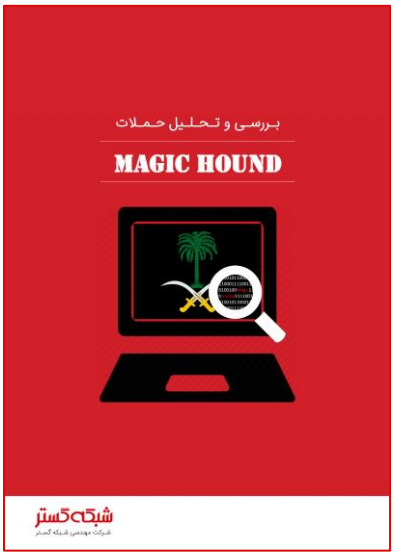
۷ به روز بودن در خصوص روش‌های جدید باج‌گیران

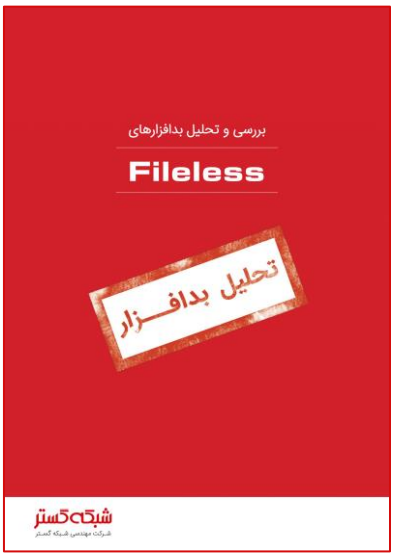
نویسندگان باج‌افزار دائماً در حال تغییر و تکامل روش‌های خود هستند. با مرور اخبار و حضور در دوره‌های آگاهی‌رسانی شرکت مهندسی شبکه گستر، از آخرین روش‌های مورد استفاده مهاجمان آگاه شده و سیاست‌ها پیشگرانه لازم را اعمال کنید.

منابع

- http://newsroom.shabakeh.net/17607/cerber-as-a-service.html
- https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/sophos-ransomware-protection.aspx
- http://newsroom.shabakeh.net/18240/satan-ransomware-as-a-service.html
- https://blog.fortinet.com/2017/03/02/dot-ransomware-yet-another-commission-based-ransomware-as-a-service
- https://www.bleepingcomputer.com/news/security/new-raas-portal-preparing-to-spread-unlock26-ransomware/







شبکه گستر

شرکت مهندسی شبـکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولیـن شـرکت ایـرانـی است کـه در زمینه نرم‌افزارهای ضـدویـروس فعـالیت تخصصی و متمـرکـزی را آغـاز کـرد. در ابتـدا، همکـاری مشتـرکی بیـن شرکت مهندسی شبـکه گستـر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International در ایران، بـه تـدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

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

در سـال ۱۳۸۴ شـرکت مهندسی شبـکه گستر مـوفـق بـه کسب نـمـایـنـدگی رسمـی و انحصـاری شـرکت آلمانی Astaro، سـازنـده محصولات "مـدیریت یکپـارچـه تهـدیـدات" (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 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، راه‌اندازی 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.

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