همه چیز درباره باج‌افزار

Cerber

شبکه گستر

عنوان سند: همه چیز درباره باج‌افزار Cerber

شناسه سند: SPT-A-0117-01

تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

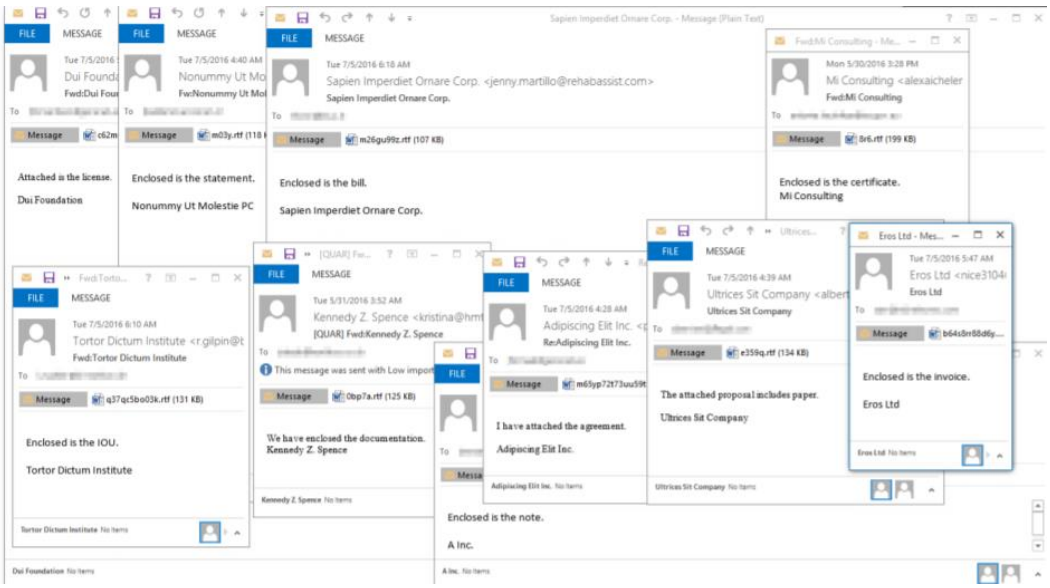
تاریخ تهیه: آذر ۱۳۹۵

در اواخر سال ۱۳۹۴، محققان خبر از کشف بدافزاری از نوع باج‌افزار دادند که عملکردی عجیب و در عین حال جالب در مقایسه با همنوعان خود داشت.

این باج‌افزار محتوا و نام فایل‌ها را رمزنگاری کرده و پسوند آنها را به ".cerber" تغییر می‌داد. موضوعی که سبب معروفیت این باج‌افزار به Cerber گردید.

> باج‌افزار یا Ransomware 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 اقدام به محدودسازی دسترسی کاربر به فایل‌ها می‌کنند موفقیت‌های بی‌مثالی را نصیب گردانندگان تبهکار خود کرده‌اند و بر اساس آمار، تعداد این باج‌افزارها بشدت در حال افزایش است. 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 بکاررفته در ساخت کلید است. هر چه تعداد این بیت‌ها بیشتر باشد شانس یافتن آن هم دشوارتر و در تعداد بیت بالا عملاً غیرممکن می‌شود.

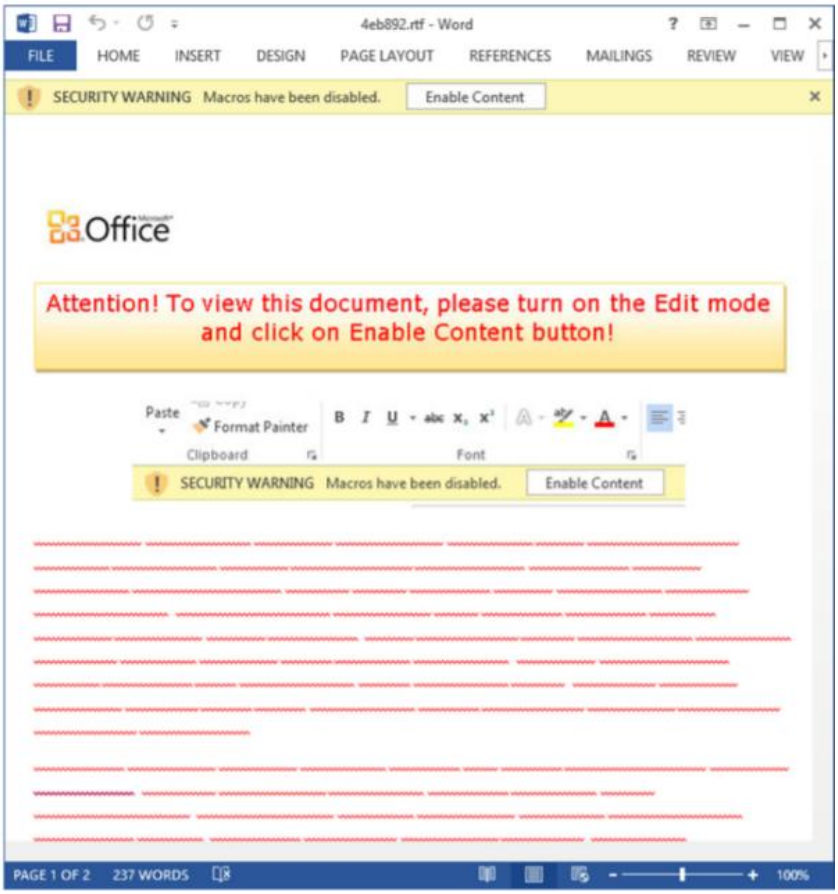
یکی از روش‌های مورد استفاده Cerber، نیز همانند بسیاری از همنوعان خود، استفاده از **ماکروهای آلوده** تزریق شده در فایل‌های Word یا Excel و انتشار آنها از طریق هرزنامه‌ها (Spam) است.



شکل ۱: نمونه‌هایی از هرزنامه‌های ناقل باج‌افزار Cerber

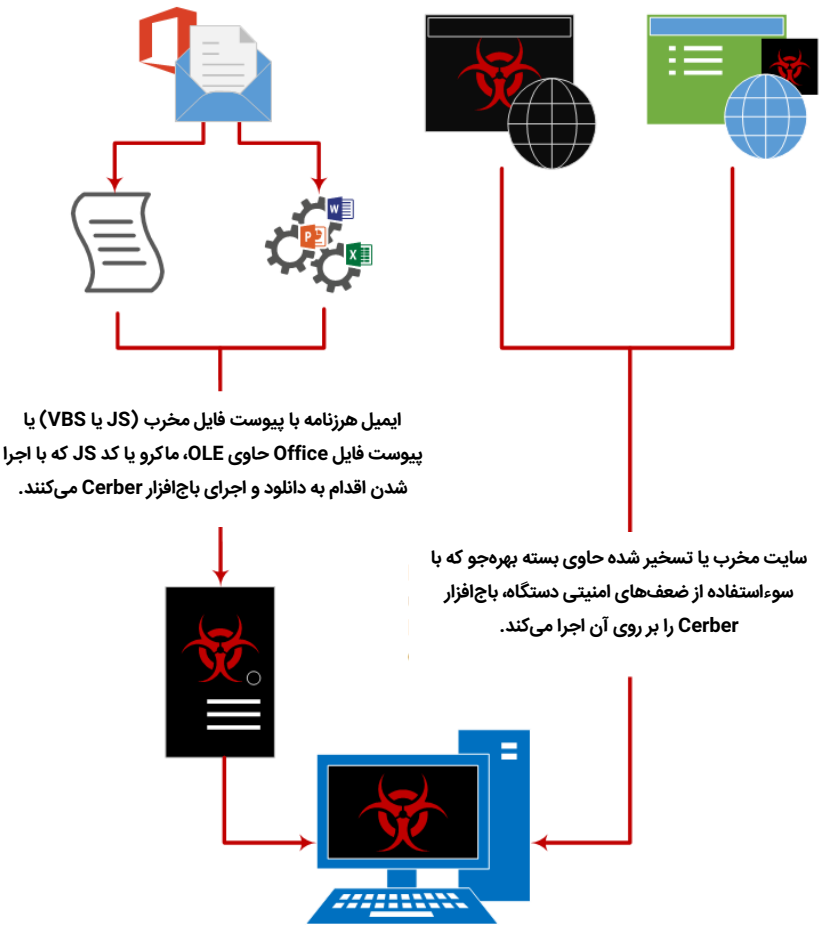
> ماکرو (Macro) نوعی برنامه است که حاوی فرامینی برای خودکارسازی برخی عملیات در نرم‌افزارهای کاربردی است. برنامه‌هایی همچون Word و Excel در مجموعه نرم‌افزارهای Office با فرامین ماکرو که با استفاده از VBA یا Visual Basic for Applications تهیه شده باشند، سازگار هستند. بدین روش و **با استفاده از قابلیت‌های ماکرو، می‌توان اقدامات مخربی، نظیر نصب بدافزار، را به اجرا در آورد.**

به‌صورت پیش‌فرض در زمان باز شدن فایل‌های حاوی ماکرو در مجموعه برنامه‌های Office، از کاربر خواسته می‌شود تا بخش ماکرو را فعال کند. گردانندگان Cerber با استفاده از روش‌های مهندسی اجتماعی کاربر را تشویق به فعال نمودن ماکر می‌کنند.



شکل ۲: نمونه‌ای از یک فایل Word حاوی ماکروی Cerber

گردانندگان Cerber استفاده از بسته‌های بهره‌جوی Rig، Neutrino و Magnitude را نیز در کارنامه خود دارند. این باج‌گیران با بکارگیری این بسته‌های بهره‌جو (Exploit Kit) از ضعف‌های امنیتی موجود بر روی دستگاه سوءاستفاده نموده و اقدام به آلوده نمودن آنها می‌کنند.

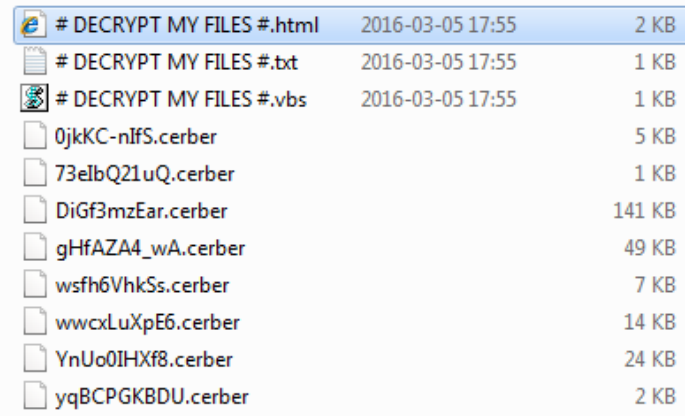


شکل ۳: روش آلوده شدن دستگاه به باج‌افزار Cerber

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

باج‌افزار Cerber، نه فقط محتوای پوشه‌های Map شده که فایل‌های موجود در پوشه‌های اشتراکی را که کاربر دستگاه آلوده شده به آنها دسترسی با حق نوشتن دارد نیز رمزنگاری می‌کند.

با پایان یافتن فرآیند رمزنگاری، سه فایل با پسوندهای TXT، HTML و VBS بر روی Desktop و هر پوشه‌ای که فایل‌های آن رمزنگاری شده‌اند کپی می‌شود.



شکل ۴: نمونه پوشه‌ای که فایل‌های آن توسط باج‌افزار Cerber رمزنگاری شده است.

این فایل‌ها حاوی دستورالعمل پرداخت باج هستند که به ۱۲ زبان ارائه شده‌اند.

شکل ۵: دستورالعمل پرداخت باج به ۱۲ زبان ارائه شده است.

در فایل VBS کدی از نوع مبدل "نوشته به صوت" قرار دارد و زمانی که کاربر این فایل را اجرا می‌کند پیامی صوتی پخش شده و در آن به‌صورت مکرر گفته می‌شود که فایل‌های کاربر رمز شده‌اند.

```
Set SAPI = CreateObject("SAPI.SpVoice")
SAPI.Speak "Attention! Attention! Attention!"
For i = 1 to 5
SAPI.Speak "Your documents, photos, databases and other important files have been encrypted!"
Next
```

شکل ۶: کد تبدیل متن به صوت در باج‌افزار Cerber

باج‌افزار Cerber فایل‌های دستگاه‌های با برخی زبان‌ها را که عمدتاً مربوط به کشورهای عضو اتحاد جماهیر شوروی سابق می‌شوند رمزنگاری نمی‌کند.

```
{
  "antiav": 1,
  "blacklist": {
    "countries": [
      "am",
      "az",
      "by",
      "ge",
      "kg",
      "kz",
      "md",
      "ru",
      "tm",
      "tj",
      "ua",
      "uz"
    ],
```

شکل ۷: فهرست دامنه کشورهایی که باج‌افزار Cerber بر روی آنها اجرا نمی‌شود.

"

با توجه به حجم تبلیغات برای این باج‌افزار به زبان روسی، احتمالاً باج‌افزار Cerber در کشور روسیه طراحی و ساخته شده است. به همین دلیل هم این باج‌افزار هیچ قربانی در کشورهای اتحاد جماهیر شوروی سابق (ارمنستان، آذربایجان، بلاروس، گرجستان، قزاقستان، قرقیزستان، تاجیکستان و...) نمی‌گیرد و آلودگی ایجاد نمی‌کند تا گرفتار قوانین مشترک بین این کشورها نشود.

"

بهره‌جویی از ضعف امنیتی روز صفر

در اوایل فرودین ۱۳۹۵، گونه‌ای جدید از باج‌افزار Cerber منتشر شد که از ضعفی امنیتی در نرم‌افزار Flash بهره‌جویی می‌کرد.

زمانی که کاربر، فایل Office آلوده به ماکروی مخرب را باز می‌کرد به صفحه‌ای اینترنتی هدایت می‌شد که در آن یک بسته بهره‌جو جاسازی شده بود.

بسته بهره‌جوی استفاده شده توسط گردانندگان Cerber مجهز به بهره‌جویی (Exploit) در نرم‌افزار Flash بود که ضعف امنیتی آن، ۱۹ فروردین توسط شرکت Adobe ترمیم شد. بنابراین حداقل در مدت حدود دو هفته Cerber از ضعفی امنیتی سوءاستفاده می‌کرده که هیچ اصلاحیه‌ای برای پوشش آن عرضه نشده بود. به این نوع ضعف‌های امنیتی روز صفر (Zero-day) اطلاق می‌شود.

نکته قابل توجه اینکه هر چند این ضعف امنیتی در تمامی نسخه‌های Flash وجود داشت اما ابزار نفوذ مذکور تنها نسخه‌های 20.0.0.306 و قبل از آن را در نرم‌افزار Flash هدف قرار می‌داده است.

> به نشان دادن توانایی بدافزار یا بهره‌جو ضعیف‌تر از آنچه که هست، اصطلاحاً تنزل رتبه (Degradation) گفته می‌شود.

روش‌های پیشرفته ضدتحلیل

در اردیبهشت سال ۱۳۹۵، منابع خبری، از انتشار گونه‌ای جدید از باج افزار Cerber خبر دادند که از روش‌های پیشرفته ضدتحلیل و فرار از سد نرم‌افزارها و تجهیزات امنیتی بهره می‌برد.

در گونه جدید، ماکروی تزریق شده در فایل پیوست هرزنامه ناقل باج‌افزار، یک فایل VBScript را از اینترنت دانلود کرده و آن را در مسیر %appdata% کپی می‌کرد. تفاوت این روش با گونه‌های قبلی در آن بود که بجای درج کدهای مخرب در ماکروی فایل پیوست، ماکرو تنها حاوی یک کد دانلود کننده فایل بود. این کار به‌منظور مسدود نشدن ایمیل در درگاه شبکه هدف – در نتیجه پویش شدن پیوست ایمیل توسط دیواره‌های آتش – انجام می‌گیرد.

همچنین فایل VBScript دانلود شده حاوی کدهایی بود که تحلیل عملکرد آن را تا حدودی دشوار می‌کرد. برخی از روش‌های ضدتحلیل استفاده شده در آن گونه به‌شرح زیر بود:

- معرفی چندین "متغیر" (Variable) که از آنها در کد اصلی استفاده نشده است.

- استفاده از یک "حلقه" (Loop) برای ایجاد تأخیر: این حلقه، مقدار یک متغیر را از ۱ به ۹۶۱۶۶۲۳۷ افزایش می‌دهد. هدف از این روش فریب دادن سیستم‌های تحلیلگر بدافزار است.

```
sUB G1JBxy()
dIM BKerOe8LabHJTs,VqZhdIc6W7w6,SctiZlFm
BKerOe8LabHJTs=96166237:VqZhdIc6W7w6=0:SctiZlFm=0
fOr VqZhdIc6W7w6=1 To BKerOe8LabHJTs
SctiZlFm=SctiZlFm+1
nExt
If SctiZlFm=BKerOe8LabHJTs ThEN
Timer_Function(4)
Resume_Execution
ElSE
End If
End suB
```

شکل ۸: کد حلقه ایجادکننده تأخیر

پیش از دانلود کد Cerber، فایل VBScript برقراری ارتباط را بررسی می‌کرد. برای این منظور فایل VBScript یک HTTP Range Request را به یک سایت بی‌خطر ارسال می‌کرد.

```
SUb PWJhDjTiG()
On erRoR ResuMe NEXt
Dim In2zhshWoHz,JGLHuujnF,JFp28ZXUxjN,BpIcCg13VNU
In2zhshWoHz="http://www.[redacted].com"
sEt JGLHuujnF=crEATEobjeCT("Microsoft.XMLHTTP")
JGLHuujnF.opEn "GET",In2zhshWoHz,0
JGLHuujnF.SeTreqUESthEADer Range,"bytes=96-"
JGLHuujnF.sEND()
If JGLHuujnF.StAtUStexT<>Partial Content ThEn KjntrflraAcmCup3q
EnD SuB
```

شکل ۹: کد بررسی‌کننده برقراری ارتباط

فایل VBScript بدنبال عبارت "Partial Content" در پاسخ دریافت شده می‌گشت؛ اگر پاسخ دریافت شده صحیح نمی‌بود، کد VBScript تابعی حاوی یک حلقه بی‌نهایت را فراخوانی می کرد. بدین ترتیب اجرا بدون برقراری اینترنت انجام نمی‌شد.

پس از آنکه فرآیند بررسی برقراری اینترنت به پایان می‌رسید، فایل VBScript یک HTTP Range Request دیگر را برای دریافت یک فایل JPG از نشانی زیر ارسال می‌کرد:

hxxp://bsprint[.]ro/images/karma-autumn/bg-footer-bottom.jpg?OblpcVG=

در بخش Range Header درخواست مقدار "bytes=11193-" آمده است. بر این اساس، سرور وب تنها آن بخش از فایل JPG را که آفست آنها از ۱۱,۱۹۳ شروع می‌شد باز می‌گرداند.

محتوای پاسخ دریافت شده با کلید "amfrshakf" و XOR می‌شد. شکل زیر بخشی از کد را که وظیفه این رمزگشایی را بر عهده دارد نشان می‌دهد.

```
fUnCtIoN Unskh2OTD(BIvsJOZgb,Y4ailNo)
DIm IoC9aQhsk4146,W7Iz6Qr135gRgpOhw,ELPROO2dwzUN,GKtrMNgvBtBxL1cQ,Iu4opE62JtdxTw8g,decryption_key(8)
decryption_key(0)=97
decryption_key(1)=109
decryption_key(2)=102
decryption_key(3)=114
decryption_key(4)=115
decryption_key(5)=104
decryption_key(6)=97
decryption_key(7)=107
decryption_key(8)=102
seT W7Iz6Qr135gRgpOhw =CrEaTeObJeCT("Scripting.FileSystemObject")
seT ELPROO2dwzUN=W7Iz6Qr135gRgpOhw.gETFiLE(BIvsJOZgb)
seT Iu4opE62JtdxTw8g=ELPROO2dwzUN.oPenAstexTSTrEAM(1,0)
seT GKtrMNgvBtBxL1cQ=W7Iz6Qr135gRgpOhw.cREAtETeXTFile(Y4ailNo,1,0)
IoC9aQhsk4146=0
dO unTIL Iu4opE62JtdxTw8g.aTENdOFSTREaM
IoC9aQhsk4146=(IoC9aQhsk4146+1)\9
GKtrMNgvBtBxL1cQ.wriTe Chr(XoR_Decryption(asc(Iu4opE62JtdxTw8g.rEad(1)),decryption_key(IoC9aQhsk4146)))
loOP
GKtrMNgvBtBxL1cQ.cLOsE
Iu4opE62JtdxTw8g.clOSE
enD funCtiOn

fUnCtioN XoR_Decryption(CJbuyqex412I,IlHYmSaEwjmr)
XoR_Decryption=(CJbuyqex412I aNd NoT IlHYmSaEwjmr)oR(noT CJbuyqex412I aNd IlHYmSaEwjmr)
ENd FUnCtIoN
```

شکل ۱۰: کد رمزگشایی پاسخ دریافت شده از سرور

عملکرد گونه جدید باج‌افزار Cerber تغییر چندانی نسبت به گونه‌های پیشین نداشت و همچون گونه‌های قبلی ".cerber" به انتهای فایل‌های رمز شده اضافه می‌شد.

> در این گونه شواهدی مبنی بر وجود بخش Spambot در باج‌افزار یافت شد. اما ساختار ناقص کد آن بیانگر این موضوع بود که Spambot حداقل در آن زمان در مراحل آزمایشی خود قرار داشت.
>
> Spambot دستگاه آلوده شده را تبدیل به یک ارسال‌کننده هرزنامه می‌کند.

قابلیت اجرای حملات DoS

در اوایل خرداد ماه گونه جدیدی از این باج‌افزار شناسایی شد که علاوه بر اینکه فایل‌های کامپیوتر آلوده شده را رمزگذاری می‌کرد، کامپیوتر را نیز به تسخیر گردانندگان شبکه‌های مخرب (Botnet) درآورده و در نقش یک ماشین مهاجم به همراه لشگری از این ماشین‌ها، علیه یک هدف خاص، برای اجرای حملاتی از نوع "از کاراندازی سرویس" یا Denial of Service – به اختصار DoS – مورد استفاده قرار می‌داد.

افزودن قابلیت حملات DoS به باج‌افزار، یک ایده خلاقانه ولی شیطانی بود. Cerber اولین باج افزاری بود که قابلیت انجام حملات DoS را نیز داشت. در نسخه‌های اولیه Cerber بخش حملات DoS در حالت آزمایشی بود ولی در این گونه، این بخش به بلوغ و تکامل رسیده و فعال شد.

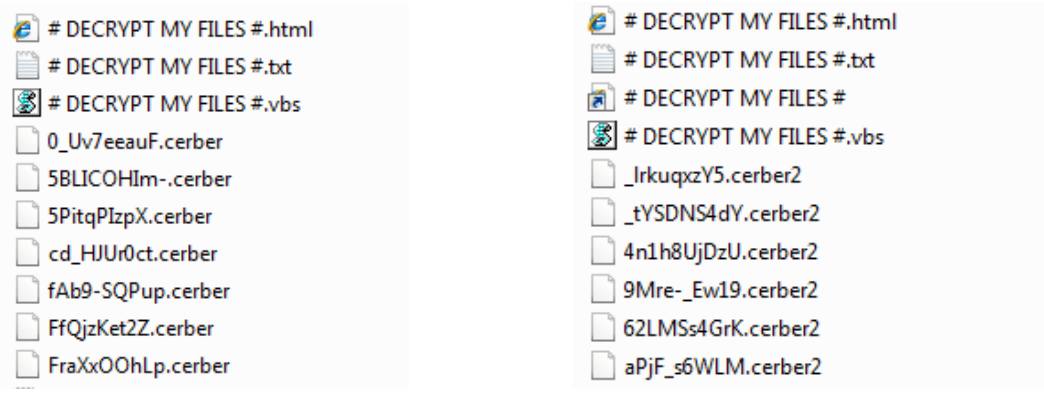
با افزوده شدن قابلیت ایجاد شبکه‌های مخرب Botnet به باج افزارها، انتظار می‌رود که میزان آلودگی به این نوع از بدافزارها با سرعت بیشتری رشد کند. در ضمن پاک کردن کامپیوتر از باج‌افزار، نیز تضمینی بر خارج شدن کامپیوتر از کنترل گردانندگان شبکه‌های مخرب نیست.

Cerber v2

در مرداد ماه ۱۳۹۵، گونه‌ای جدید از این باج‌افزار منتشر شد که به Cerber v2 معروف شد.

نسخه جدید تغییرات و بهبودهایی در ساختار و عملکرد خود داشت.

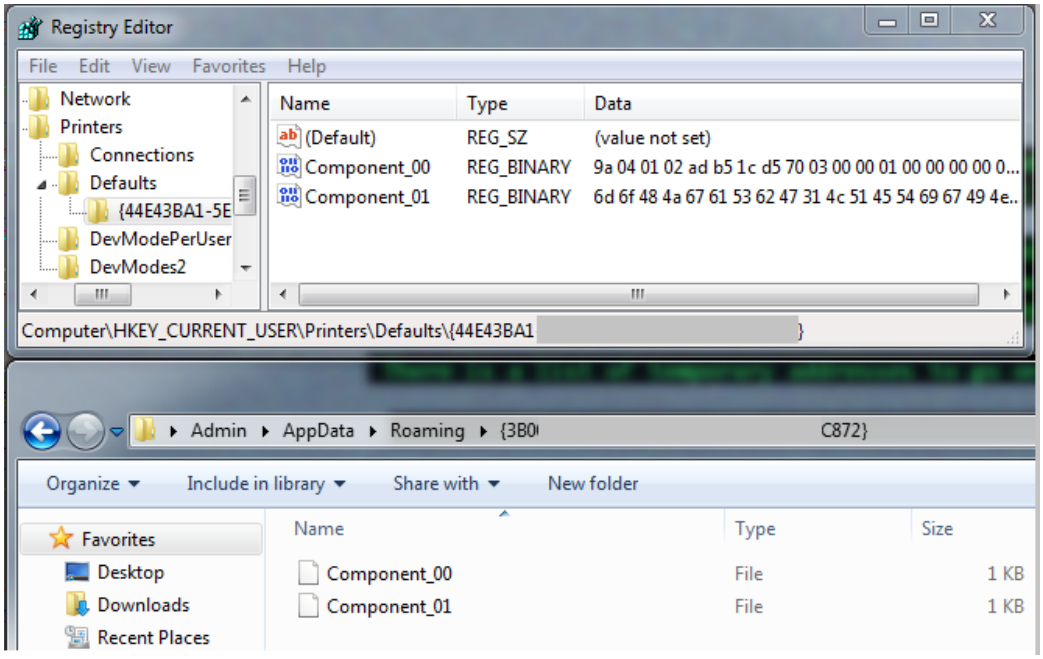
نخستین تغییر قابل توجه، تغییر پسوند فایل‌های رمز شده از ".cerber" در نسخه پیشین به ".cerber2" در نسخه جدید بود.



شکل ۱۱: تغییر پسوند فایل‌های رمز شده در نسخه ۲ باج‌افزار Cerber

نسخه جدید این باج‌افزار با استفاده از یک Packer جدید شناسایی شدن توسط ضدویروس را دشوارتر و تحلیل آن را سخت‌تر می‌کرد.

بر خلاف نسخه قبلی که اطلاعات بدافزار در محضرخانه (Registry) ذخیره می شدند، در نسخه دوم این باج‌افزار پس از پایان رمزنگاری، اطلاعاتی همچون کلید عمومی بر روی دیسک سخت دستگاه قربانی ذخیره می‌شد.



شکل ۱۲: تغییر محل ذخیره‌سازی اطلاعات باج‌افزار در نسخه ۲

همچنین عنصری (Tag) با عنوان rc4_key_size به تنظیمات این باج‌افزار اضافه شده بود. مقدار تخصیص داده شده به این عنصر، پیش‌تر در زمان اجرا در نظر گرفته می‌شد. همچنین طول کلید رمزنگاری RSA (rsa_key_size) نیز افزایش یافته بود.

```
"network":1,
"new_extension":".cerber",
"max_block_size":2,
"max_blocks":5,
"min_file_size":6,
"multithread":1,
"rsa_key_size":576
},
```

```
"network":1,
"new_extension":".cerber2",
"max_block_size":2,
"max_blocks":5,
"min_file_size":6,
"multithread":1,
"rc4_key_size":256,
"rsa_key_size":880
},
```

شکل ۱۳: افزایش طول کلید رمزنگاری در نسخه ۲ باج‌افزار Cerber

در نسخه جدید فهرست سیاهی (Black List) که شامل نام تعدادی از شرکت‌های ضدویروس است به باج‌افزار افزوده شده بود.

```
"av_blacklist":
    ["arcabit","arcavir","avast software","bitdefender","bitdefender agent","bullguard
    ltd","bullguard software","ca","emsisoft anti-malware","escan","eset","etrust ez
    armor","f-secure","g data","kaspersky lab","lavasoft","trustport"],
```

شکل ۱۴: فهرست سیاهی از شرکت‌های ضدویروس

برخی برنامه‌ها دارای مکانیزمی برای قفل کردن فایل باز شده به‌منظور جلوگیری از دسترسی سایر برنامه‌ها به فایل و حفظ یکپارچگی آن هستند. نسخه پیشین Cerber پروسه‌های زیر را که دارای چنین مکانیزمی بودند متوقف می‌کرد.

```
"close_process":
    ["outlook.exe","steam.exe","thebat.exe","thebat64.exe","thunderbird.exe","winword.exe"],
```

شکل ۱۵: پروسه‌هایی که در نسخه اول باج‌افزار Cerber توسط آن متوقف می‌شدند.

این فهرست در نسخه دوم Cerber بسیار کامل‌تر شده بود.

```
"close_process":["excel.exe","infopath.exe","msaccess.exe","mspub.exe","onenote.exe"
,"outlook.exe","powerpnt.exe","steam.exe","sqlservr.exe","thebat.exe","thebat64.exe"
,"thunderbird.exe","visio.exe","winword.exe","wordpad.exe"],
```

شکل ۱۶: فهرست پروسه‌هایی که در نسخه دوم باج‌افزار Cerber توسط آن متوقف می‌شدند.

در نسخه جدید عنصری با عنوان wallpaper اضافه شد که یک تصویر پس‌زمینه برای Desktop کامپیوتر آلوده شده ایجاد می‌کرد. این عنصر شامل متغیرهایی است که در زمان اجرا به‌روز شده و بر روی Desktop درج می‌شوند.

```
"wallpaper":
{
    "background":0,"color":65280,"size":12,"text":" Your documents, photos,
    databases and other important files have been encrypted!

    If you understand all importance of the situation then we propose to you
    to go directly to your personal page where you will receive the complete
    instructions and guarantees to restore your files.

    There is a list of temporary addresses to go on your personal page below:

    ------------------------------------------------------------------------

    1.  http://{TOR}.{SITE_1}/{PC_ID}

    2.  http://{TOR}.{SITE_2}/{PC_ID}

    3.  http://{TOR}.{SITE_3}/{PC_ID}

    4.  http://{TOR}.{SITE_4}/{PC_ID}

    5.  http://{TOR}.{SITE_5}/{PC_ID}

    6.  http://{TOR}.onion/{PC_ID} (TOR) "
},
```

شکل ۱۷: کد بخش wallpaper در نسخه ۲ باج‌افزار Cerber

”

Cerber یکی از کامل‌ترین بدافزارها از لحاظ توانایی شناسایی ماشین‌های مجازی و عدم اجرا شدن بر روی آنها محسوب می‌شد.

تحلیلگران ویروس عمدتاً از ماشین‌های مجازی برای تحلیل یک بدافزار استفاده می‌کنند.

“

باج‌افزار Cerber قادر است که بسترهای مجازی‌سازی معروفی نظیر Parallel، QEMU، VMware و VBox را شناسایی کند. یکی از جالب‌ترین تکنیک‌ها که در هر دو نسخه این باج‌افزار مورد استفاده قرار گرفته بود بررسی مسیر HKLM\SYSTEM\CurrentControlSet\Enum\PCIدر محضرخانه است.

```
51          PUSH ECX                    pHandle = 0022F9E0
68 19010200 PUSH 20119                  Access = KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS|KEY_NOTIFY|20100
33FF        XOR EDI,EDI
57          PUSH EDI                    Reserved = 0
50          PUSH EAX                    Subkey = "SYSTEM\\CurrentControlSet\\Enum\\PCI"
68 02000080 PUSH 80000002               hKey = HKEY_LOCAL_MACHINE
FF15 00404100 CALL DWORD PTR DS:[<&ADVAPI32.RegOpenKey RegOpenKeyExW
```

شکل ۱۸: کد شناسایی‌کننده بستر مجازی‌سازی در باج‌افزار Cerber

هر زیرکلید در این مسیر نمایانگر اتصال یک PCI-bus با قالب زیر است:

VEN_XXXX&DEV_XXXX&SUBSYS_XXXXXXXX&REV_XX

که در آن VEN مشخص‌کننده Vendor ID است.

جدول زیر، Vendor ID برخی از بسترهای مجازی‌سازی را نشان می‌دهد.

Vendor	Vendor ID
VMware	0x15AD
VBox	0x80EE
Parallel	0x1AB8

”

در صورتی که Cerber وجود ماشین‌مجازی را تشخیص دهد اجرای خود را متوقف می‌کند.

“

باج‌افزار به‌عنوان سرویس

در اواخر مرداد ماه دو شرکت امنیتی Check Point Software و IntSight Cyber Intelligence یک گزارش تحلیلی درباره باج‌افزار Cerber و کسب و کار آن به‌عنوان یک سرویس نرم‌افزاری (Ransomware-as-a-Service) منتشر کردند.

در این گزارش ۶۰ صفحه‌ای با عنوان CerberRing آمده که به‌طور متوسط باج افزار Cerber روزانه به هشت متقاضی به‌صورت سرویس نرم افزاری اجاره داده می‌شود و در طی یک ماه توانسته ۱۵۰ هزار کامپیوتر را در ۲۰۱ کشور آلوده سازد. از این میزان دستگاه آلوده، تبهکاران سایبری توانسته‌اند حدود ۲۰۰ هزار دلار به‌صورت باج پرداختی از سوی قربانیان، درآمد کسب کنند که ۴۰ درصد از آن به‌عنوان هزینه سرویس نرم‌افزاری به سازنده اصلی باج‌افزار Cerber تعلق می‌گیرد. بدین ترتیب برآورد می‌شود که سازندگان Cerber سالانه نزدیک به یک میلیون دلار درآمد داشته باشند.

این ارقام درآمدی در حال اتفاق می‌افتد که طبق تخمین صورت گرفته، تنها ۰/۳ درصد از قربانیان حاضر به پرداخت باج درخواست شده به میزان یک "بیت کوین" (Bitcoin) معادل حدود ۷۰۰ دلار می‌شوند.

> برآورد می‌شود که سازندگان Cerber سالانه بیش از یک میلیون دلار درآمد داشته باشند.

باج‌افزار Cerber با داشتن چندین مرکز کنترل و فرماندهی (Command & Control) مجزا و مستقل و همچنین داشتن کنسول مدیریت باج‌افزار به ۱۲ زبان رایج دنیا، امکانات زیادی برای کسانی که مایل به اجاره این باج‌افزار هستند، فراهم می‌آورد.

باج جمع‌آوری شده از هر مستاجر Cerber به یک حساب کاربری جداگانه Bitcoin ریخته می‌شود. ولی در پایان مدت اجاره، همه باج‌ها از چند حساب کاربری مختلف عبور داده می‌شود تا کاملاً ردپاهای تبهکاران پاک شود. سپس به میزان ۴۰ درصد به نویسندگان باج‌افزار و ۶۰ درصد به مستاجر باج‌افزار، باج تقسیم و پرداخت می‌شود.

بی‌استفاده شدن ابزار رمزگشایی در مدتی کوتاه

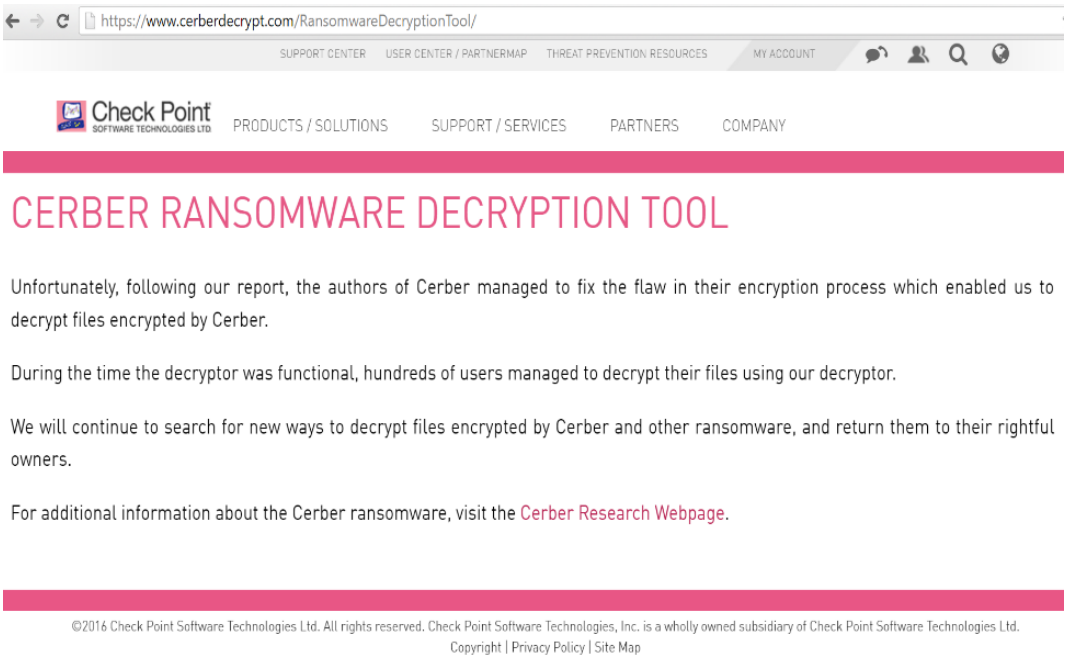
همزمان با انتشار گزارش مذکور، شرکت Check Point Software ابزاری را برای رمزگشایی باج‌افزار Cerber ارائه کرد.

این ابزار با بهره‌گیری از یک ضعف امنیتی در باج افزار Cerber کلید خصوصی رمزنگاری را شناسایی و از طریق آن اقدام به رمزگشایی فایل‌های رمز شده با این باج افزار می‌کرد.

در زمان عرضه این ابزار، شرکت Check Point اعلام کرد که با استفاده از ابزار این شرکت می‌توان فایل‌های رمز شده با نسخه‌های ۱ و ۲ باج‌افزار Cerber را به حالت اولیه بازگرداند.

برای این منظور قربانیان این باج‌افزار با مراجعه به سایت CerberDecrypt.com و آپلود یک فایل با پسوند ".cerber" یا ".cerber2" با حجم ۱ مگابایت یا کمتر، کلید خصوصی رمزگشایی و ابزاری برای بازگرداندن فایل‌ها را دریافت می‌کردند.

در پی انتشار گزارش شرکت Check Point که در آن به‌طور مفصل به بررسی این باج‌افزار پرداخته شده بود، نویسندگان باج‌افزار Cerber نیز اقدام به ترمیم ضعفی که ابزار این شرکت با بهره‌گیری از آن موفق به رمزگشایی فایل‌ها می‌شد کرده و نسخه جدیدی از این باج‌افزار را ارائه کردند.



شکل ۱۹: توضیحات سایت CerberDecrypt.com پس از ترمیم شدن آسیب‌پذیری Cerber توسط نویسندگان این باج‌افزار

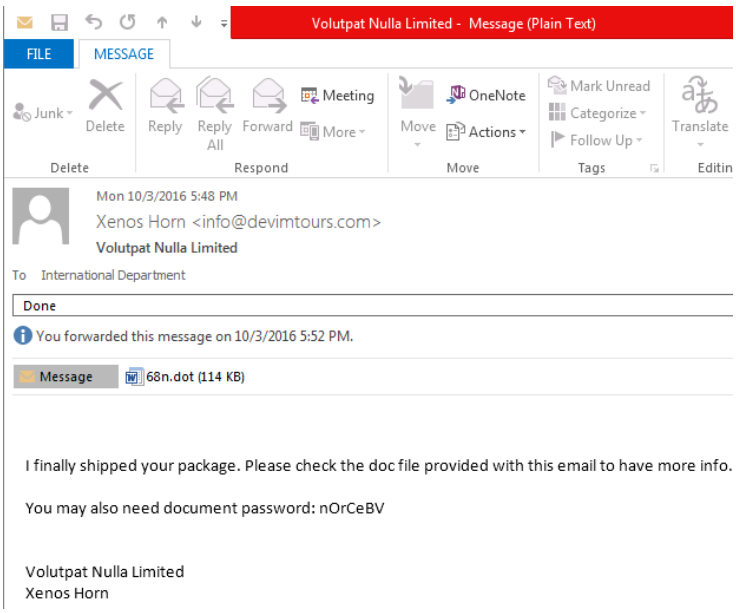
در گونه جدید پسوند فایل‌های رمز شده به cerber3. تغییر داده می‌شد.

> "
>
> این اقدام گردانندگان Cerber یک بار دیگر ثابت کرد تبهکاران سایبری همواره در حال رفع نواقص و افزودن امکانات جدید در برنامه‌های مخرب خود هستند. لذا پیشگیری همیشه بهتر از درمان است.
>
> "

انتشار باج‌افزار از طریق پیوست‌های رمز شده

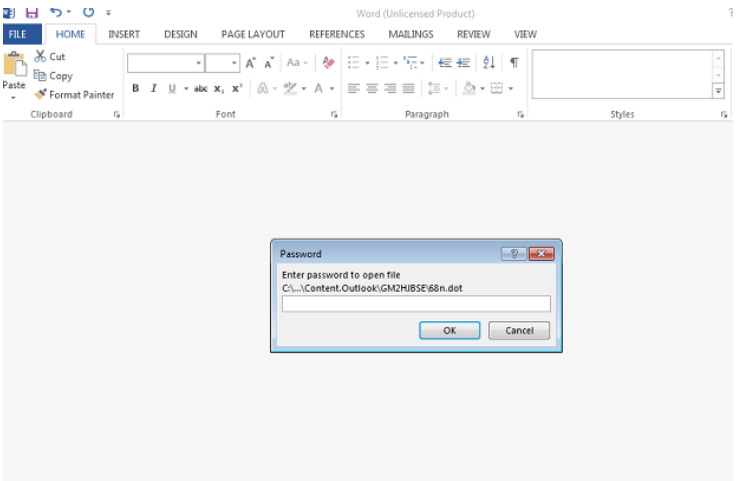
در آبان ۱۳۹۵، شرکت McAfee از ظهور گونه جدیدی از بدافزارهای ماکرویی خبر داد که در آن کاربر برای باز کردن فایل آلوده پیوست شده به ایمیل باید از گذرواژه درج شده در متن ایمیل استفاده می‌کرد. این کار سبب پویش نشدن فایل در زمان عبور از درگاه‌های شبکه‌ای مجهز به دیواره آتش و ضدویروس می‌شود.

با نگاهی به یکی از ایمیل‌های گونه جدید مشخص می‌شود که پیوست ایمیل، فایلی با پسوند dot و با نامی تصادفی است. در متن ایمیل هم به گذرواژه‌ای برای باز کردن فایل اشاره شده است.



شکل ۲۰: نمونه‌ای از هرزنامه حاوی فایل رمز شده

در این صورت در زمان باز کردن فایل از کاربر خواسته می‌شود که گذرواژه صحیح را وارد کند. در غیراینصورت فایل باز نخواهد شد.



شکل ۲۱: درخواست گذرواژه در زمان باز شدن پیوست هرزنامه

زمانی که کاربر گذرواژه صحیح را وارد کند از کاربر خواسته می‌شود که بر روی دگمه Enable Content کلیک کند. با این کار ماکروی ویروسی تزریق شده در درون فایل اجرا شده و با برقراری ارتباط با سرور فرماندهی مهاجمان، یک فایل VBScript را دریافت نموده و با نامی تصادفی در مسیر %appdata% ذخیره می‌کند.

کدهای ماکرو و VBScript هر دو به‌شدت مبهم‌سازی شده‌اند. پس از رمزگشایی، VBScript یک کد مخرب رمز شده با پسوند jop را دانلود می‌کند. در مرحله بعد فایل توسط یک عملیات ساده XOR، رمزگشایی می‌شود. اما کد رمزگشایی شده خود نیز مبهم‌سازی شده است.

```
diM EQjWxPFs
funCTIon Sa8nWD(F1)
Sa8nWD=Asc(F1)
ENd fUNCtIon
FUnCTIon TadKPeb(A9hHYc1P,D2)
diM KapI2QaX,UkMQQ99,LW,Mn1Gt,KwR97wR(5)
KwR97wR(5)=53
KwR97wR(3)=50
KwR97wR(4)=54
KwR97wR(1)=115
KwR97wR(2)=118
KwR97wR(0)=121
seT KapI2QaX=CReATeObject(Vzv("3C321D381F25063F087F293803343C281C250A3C203305340C25", "Qo"))
SEt UkMQQ99=KapI2QaX.GETfilE(A9hHYc1P)
sEt Mn1Gt=UkMQQ99.OpENAsTeXtstrEAm(7208-7207,3149-3149)
SeT LW=KapI2QaX.CREatEtexTFiLE(D2,2615-2614,4792-4792)
dO unTIl Mn1Gt.ATeNdOFstream
LW.WrITE JEDSs(YH(Sa8nWD(Mn1Gt.REaD(9024-9023)),KwR97wR(0)))
```

شکل ۲۲: بخشی از کد مبهم‌سازی شده فایل VBScript

در این گونه، الگوریتم مبهم‌سازی همیشه یکسان نیست. محققان شرکت McAfee، در گونه بررسی شده محتوا را از طریق یک اسکریپت Python از حالت مبهم‌سازی شده خارج کردند.

```
import os
import sys
Inputstr1 = sys.argv[1]
Inputstr2 = sys.argv[2]
Lenstr1 = len(Inputstr1)/2
Lenstr2 = len(Inputstr2)
Index = 0
Decrypted_String = ""
while (Index < Lenstr1):
    temp3 = int((Inputstr1[(2 * Index)] + (Inputstr1[(2 * Index) + 1])),16) ^ ord(Inputstr2[(Index + 1) % Lenstr2])
    Decrypted_String = Decrypted_String + chr(temp3)
    Index = Index + 1
print Decrypted_String
```

شکل ۲۳: اسکریپت رمزگشایی فایل مبهم‌سازی شده

با این کار کدهای مخرب بیشتری از جمله نشانی‌های سرور فرماندهی نمایان می‌شوند.

```
"http://csir.bdx6.siteinternet.com/kls.doc"
"http://www.ldlogistic.it/kls.doc"
```

شکل ۲۴: سایت‌های فرماندهی فایل VBScript

نویسندگان حرفه‌ای بدافزارها از تکنیک‌های مختلفی برای به تأخیر انداختن اجرای کدهای مخرب فایل استفاده می‌کنند. هدف از این کار فرار از سد قرنطینه‌های امنی است که رفتار پروسه‌ها را در مدتی کوتاه بررسی می‌کنند. این کارها معمولاً از روش‌هایی همچون Sleep Call و Stalling انجام می‌شود. اما در گونه جدید تاخیر از طریق اجرای فرمان ping 8.8.8.8 -n 250 > nul که در آن سرور DNS شرکت Google برای ۲۵۰ بار Ping می‌شود صورت می‌پذیرد.

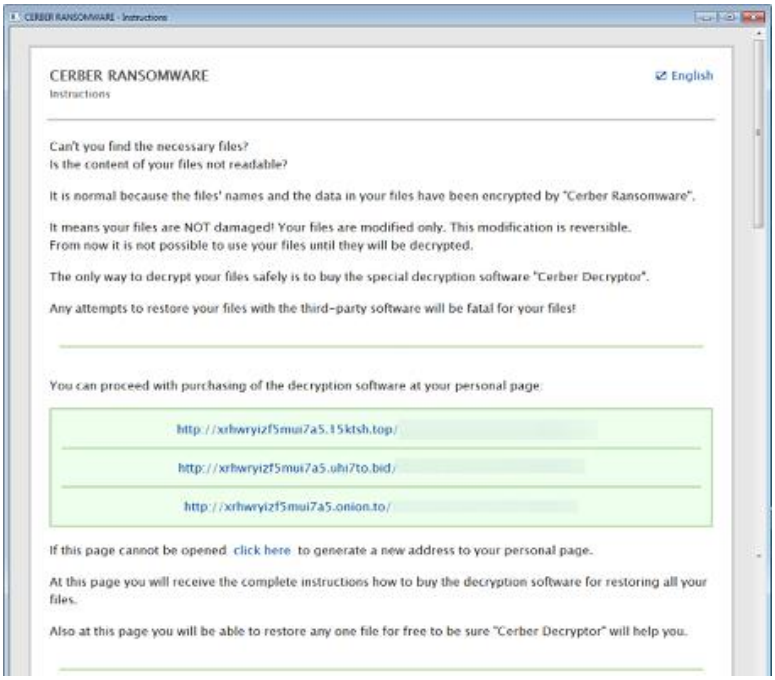
شکل ۲۵: ایجاد تأخیر با استفاده از فرمان Ping

در نهایت فایل نصب باج‌افزار Cerber شروع به اجرا می‌کند.

فایل‌های بانک داده؛ هدف جدید Cerber

باز هم در آبان ۱۳۹۵، شرکت امنیتی McAfee از انتشار گونه‌ای جدید از باج‌افزار معروف و مخرب Cerber خبر داد که تغییرات عمده‌ای نسبت به نسخه‌های پیشین خود داشت. نخستین تغییر در نسخه جدید مربوط به پسوند فایل‌های رمزشده بود. در نسخه‌های پیشین این باج‌افزار یکی از دو عبارت "cerber" یا "#cerber" که در آن # نمایانگر شماره نسخه باج‌افزار بود به‌عنوان پسوند به فایل‌های رمزشده الصاق می‌شد. حال آنکه از آن نسخه به بعد بجای این عبارات در هر آلودگی چهار نویسه به‌صورت تصادفی ایجاد می‌شود.

تغییر دوم مربوط به دستورالعمل پرداخت باج است. نسخه جدید، دستورالعمل را در قالبی شکیل‌تر و با طراحی حرفه‌ای‌تر نمایش می‌دهد. عاملی که ممکن است سبب اطمینان بیشتر قربانی به بازگشت فایل‌ها در صورت پرداخت باج شود.



شکل ۲۶: دستورالعمل پرداخت باج در نسخه‌های جدید باج‌افزار Cerber

آخرین و با اهمیت‌ترین تغییر، هدف قرار گرفتن فایل‌های بانک داده (Database) در نسخه جدید بود. با توجه به اینکه امکان دست‌درازی به فایل در زمان استفاده شدن از آن توسط یک برنامه فراهم نیست، نسخه‌های جدید Cerber ابتدا پروسه پایگاه داده را متوقف کرده و سپس اقدام به رمزنگاری فایل‌های بانک داده می‌کنند.


```
"close_process":{
   "close_process":1,
   "process":[
      "msftesql.exe",
      "sqlagent.exe",
      "sqlbrowser.exe",
      "sqlservr.exe",
      "sqlwriter.exe",
      "oracle.exe",
      "ocssd.exe",
      "dbsnmp.exe",
      "synctime.exe",
      "mydesktopqos.exe",
      "agntsvc.exeisqlplussvc.exe",
      "xfssvccon.exe",
      "mydesktopservice.exe",
      "ocautoupds.exe",
      "agntsvc.exeagntsvc.exe",
      "agntsvc.exeencsvc.exe",
      "firefoxconfig.exe",
      "tbirdconfig.exe",
      "ocomm.exe",
      "mysqld.exe",
      "mysqld-nt.exe",
      "mysqld-opt.exe",
      "dbeng50.exe",
      "sqbcoreservice.exe"
   ]
```


شکل ۲۷: فهرست پروسه‌های پایگاه داده که توسط باج‌افزار Cerber متوقف می‌شوند.

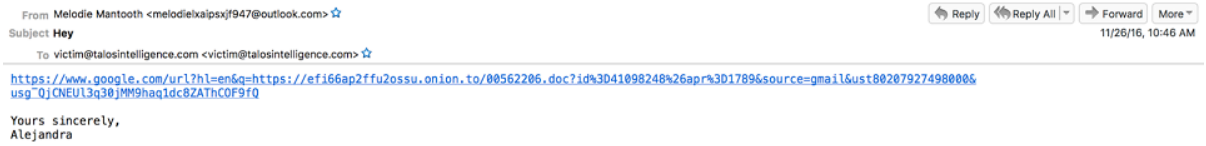
فایل پیکربندی نسخه‌های جدید باج‌افزار Cerber فهرست بلندبالایی از پسوندها را از جمله فایل‌های بانک داده نرم‌افزارهای Microsoft Access، Oracle، MySQL و SQL Server Agent و همچنین فایل‌های مرتبط با برنامه‌های حسابداری، حقوق و دستمزد و سامانه‌های بیمارستانی را در خود دارد.

رویکرد جدید گردانندگان باج‌افزار Cerber نقطه عطفی در تاریخ این باج‌افزار محسوب می‌شد. چرا که در نسخه جدید بر باج‌گیری از کسب‌وکارها و سازمان‌ها تمرکز بیشتری صورت گرفته بود.

البته رمزنگاری فایل‌های بانک داده منحصر به باج‌افزار Cerber نیست. در نیمه نخست سال ۲۰۱۶ باج‌افزارهای crypJOKER، SURPRISE، PowerWare و Emper نیز پسوند فایل‌های مرتبط با بانک‌های داده را به فهرست اهداف خود اضافه کردند.

بهره‌گیری نسخه 5 باج‌افزار Cerber از Google و Tor2Web

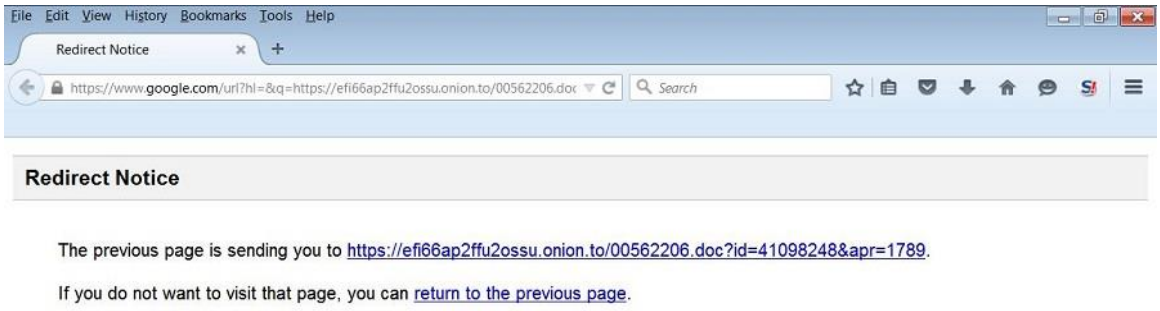
در آذر ۱۳۹۵، گردانندگان Cerber نسخه جدید دیگری از این باج‌افزار را عرضه کردند. در نسخه جدید، به شناسه 5.0.1، با سوءاستفاده از قابلیت تغییر مسیر نشانی وب Google و سرویس Tor2Web Proxy باج‌افزار Cerber که بر روی شبکه Tor میزبانی می‌شود دانلود شده و سپس بر روی دستگاه قربانی اجرا می‌شود.


From Melodie Mantooth <melodielxaipsxjf947@outlook.com>
Subject Hey
To victim@talosintelligence.com <victim@talosintelligence.com>
Reply Reply All Forward More
11/26/16, 10:46 AM
https://www.google.com/url?hl=en&q=https://efi66ap2ffu2ossu.onion.to/00562206.doc?id%3D41098248%26apr%3D1789&source=gmail&ust=802079274980008usg=QjCNEUl3q30jMM9haq1dc8ZAThCOF9fQ
Yours sincerely,
Alejandra

شکل ۲۸: نمونه‌ای از هرزنامه ناقل نسخه ۵ باج‌افزار Cerber

نشانی URL درج شده در متن هرزنامه از قابلیت تغییر مسیر نشانی وب (URL Redirection) بر روی سایت Google به‌منظور برقراری ارتباط با سرور حاوی فایل مخرب دانلودکننده باج‌افزار که در حقیقت بر روی شبکه Tor میزبانی می‌شود استفاده می‌کند.

استفاده از دامنه onion.to در اولین تغییر مسیر، مهاجم را قادر می‌سازد تا بدون نصب هر گونه نرم‌افزار Tor Client بر روی سیستم قربانی، از سرویس Tor2Web Proxy که از طریق یک پیشکار (Proxy) واسط امکان دسترسی به منابع موجود بر روی شبکه Tor را از روی اینترنت ممکن می‌سازد دستگاه را به شبکه Tor متصل کند.

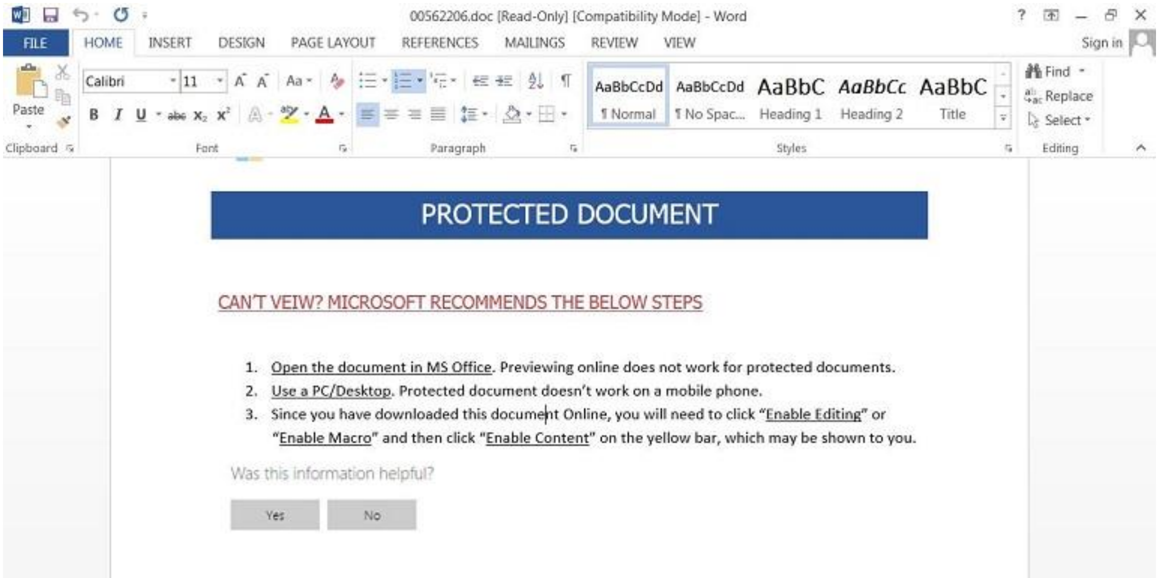

File Edit View History Bookmarks Tools Help
Redirect Notice
https://www.google.com/url?hl=&q=https://efi66ap2ffu2ossu.onion.to/00562206.doc
Search
Redirect Notice
The previous page is sending you to https://efi66ap2ffu2ossu.onion.to/00562206.doc?id=41098248&apr=1789.
If you do not want to visit that page, you can return to the previous page.

شکل ۲۹: سوءاستفاده از قابلیت تغییر مسیر نشانی وب در نسخه ۵ باج‌افزار Cerber

این نخستین بار نیست که مهاجمان از قابلیت Google Redirection سوءاستفاده می‌کنند. نمونه‌هایی از این روش پیش‌تر در بهره‌جوهایی نظیر Nuclear نیز دیده شده بود.

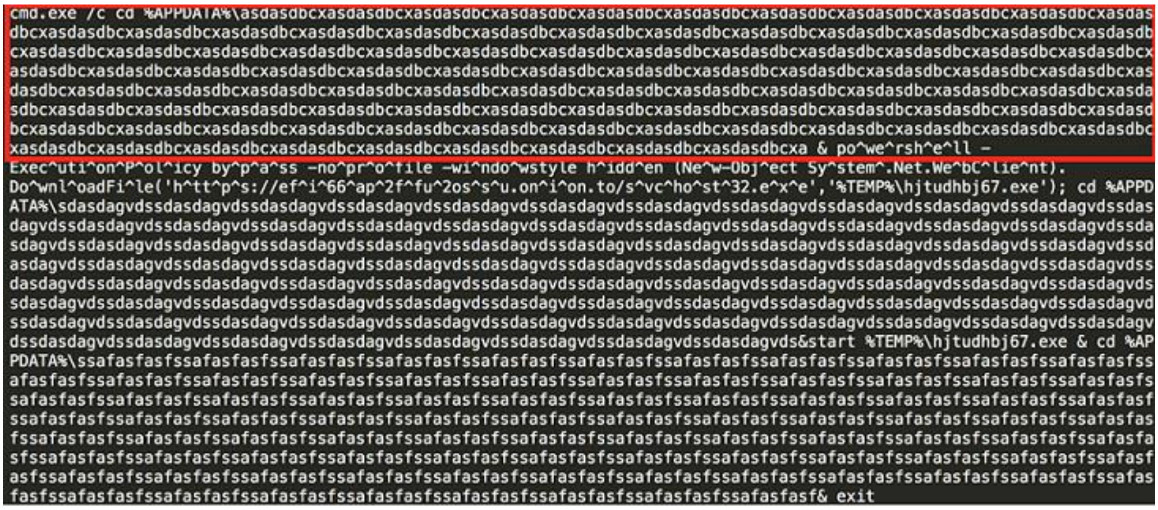
بر خلاف فایل‌های مخرب میزبانی شده در اینترنت – چه بر روی سایت‌های مجاز تسخیر شده و چه بر روی سرورهای فرماندهی مهاجمان – که معمولاً در مدتی کوتاه یا توسط صاحبان سایت حذف می‌شوند یا دسترسی به آنها از طریق نرم‌افزارها و سخت‌افزارهای امنیتی مسدود می‌شود، فایل‌های مخرب بر روی سرورهای متصل به شبکه Tor شانس بسیار بیشتری برای بقای طولانی مدت دارند. ضمن اینکه این معماری، گردانندگان بدافزار را قادر می‌سازد تا زنجیره ارتباطات را به سرعت و به آسانی به عنوان تلاشی برای فرار از سد فناوری‌های فهرست سیاه تغییر دهند.

به محض انتقال، یک فایل Word حاوی ماکروی مخرب بر روی دستگاه قربانی دانلود می‌شود. نقش این فایل دانلود کردن بدافزار (Downloader) است.



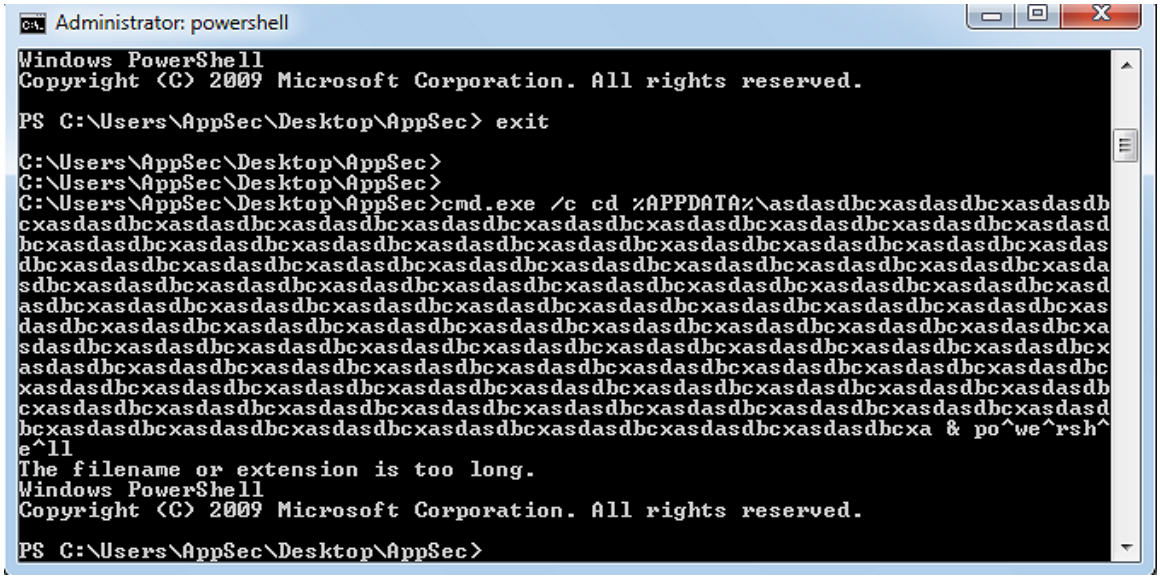
شکل ۳۰: نمونه‌ای از فایل Word حاوی ماکروی دانلود کننده نسخه ۵ باج‌افزار Cerber

در صورت باز شدن فایل توسط کاربر و فعال شدن بخش ماکرو، دانلودکننده با استفاده از Windows Command Processor پروسه Powershell را اجرا کرده و فایل اجرایی Cerber را دانلود و اجرا می‌کند. در کدنویسی ماکرو از روش‌های مبهم‌سازی استفاده شده است.



شکل ۳۱: ماکروی مبهم‌سازی شده در نسخه ۵ باج‌افزار Cerber

در بخشی از کد مذکور به مسیری اشاره شده که تعداد نویسه‌های نام پوشه ذکر شده در آن مسیر بیشتر از مقدار مجاز است؛ موضوعی که سبب می‌شود که از اجرای کد مبهم‌سازی شده به آسانی گذر شود.



شکل ۳۲: نحوه عبور از بخش مبهم سازی در نسخه ۵ باج‌افزار Cerber

فایل اجرایی Cerber پس از دانلود شدن در مسیر %TEMP% ذخیره شده و پس از اجرا اقدام به رمزنگاری اطلاعات کاربر می‌کند. در این نسخه – 5.0.1 – به پسوند فایل‌های رمز شده عبارت ab4c یا چهار نویسه تصادفی الصاق می‌شود.

راه‌های پیشگیری و مقابله

برای ایمن ماندن از گزند باج‌افزار Cerber، 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 بعنوان 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 Cerber 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 طریقGroup 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 Macroپیامی 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. بدین منظور 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.

پیوست ۱ – پسوندهای هدف باج‌افزار Cerber

```
.accdb,.mdb,.mdf,.dbf,.vpd,.sdf,.sqlitedb,.sqlite3,.sqlite,.sql,.sdb,.doc,.docx,.o
dt,.xls,.xlsx,.ods,.ppt,.pptx,.odp,.pst,.dbx,.wab,.tbk,.pps,.ppsx,.pdf,.jpg,.tif,.
pub,.one,.rtf,.csv,.docm,.xlsm,.pptm,.ppsm,.xlsb,.dot,.dotx,.dotm,.xlt,.xltx,.xltm
,.pot,.potx,.potm,.xps,.wps,.xla,.xlam,.erbsql,.sqlite-shm,.sqlite-wal,.litesql,.n
df,.ost,.pab,.oab,.contact,.jnt,.mapimail,.msg,.prf,.rar,.txt,.xml,.zip,.1cd,.3ds,
.3g2,.3gp,.7z,.7zip,.aoi,.asf,.asp,.aspx,.asx,.avi,.bak,.cer,.cfg,.class,.config,.
css,.dds,.dwg,.dxf,.flf,.flv,.html,.idx,.js,.key,.kwm,.laccdb,.ldf,.lit,.m3u,.mbx,
.md,.mid,.mlb,.mov,.mp3,.mp4,.mpg,.obj,.pages,.php,.psd,.pwm,.rm,.safe,.sav,.save,
.srt,.swf,.thm,.vob,.wav,.wma,.wmv,.3dm,.aac,.ai,.arw,.c,.cdr,.cls,.cpi,.cpp,.cs,.
db3,.drw,.dxb,.eps,.fla,.flac,.fxg,.java,.m,.m4v,.max,.pcd,.pct,.pl,.ppam,.ps,.psp
image,.r3d,.rw2,.sldm,.sldx,.svg,.tga,.xlm,.xlr,.xlw,.act,.adp,.al,.bkp,.blend,.cd
f,.cdx,.cgm,.cr2,.crt,.dac,.dcr,.ddd,.design,.dtd,.fdb,.fff,.fpx,.h,.iif,.indd,.jp
eg,.mos,.nd,.nsd,.nsf,.nsg,.nsh,.odc,.oil,.pas,.pat,.pef,.pfx,.ptx,.qbb,.qbm,.sas7
bdat,.say,.st4,.st6,.stc,.sxc,.sxw,.tlg,.wad,.xlk,.aiff,.bin,.bmp,.cmt,.dat,.dit,.
edb,.flvv,.gif,.groups,.hdd,.hpp,.m2ts,.m4p,.mkv,.mpeg,.nvram,.ogg,.pdb,.pif,.png,
.qed,.qcow,.qcow2,.rvt,.st7,.stm,.vbox,.vdi,.vhd,.vhdx,.vmdk,.vmsd,.vmx,.vmxf,.3fr
,.3pr,.ab4,.accde,.accdr,.accdt,.ach,.acr,.adb,.ads,.agdl,.ait,.apj,.asm,.awg,.bac
k,.backup,.backupdb,.bank,.bay,.bdb,.bgt,.bik,.bpw,.cdr3,.cdr4,.cdr5,.cdr6,.cdrw,.
ce1,.ce2,.cib,.craw,.crw,.csh,.csl,.db_journal,.dc2,.dcs,.ddoc,.ddrw,.der,.des,.dg
c,.djvu,.dng,.drf,.dxg,.eml,.erf,.exf,.ffd,.fh,.fhd,.gray,.grey,.gry,.hbk,.ibank,.
ibd,.ibz,.iiq,.incpas,.jpe,.kc2,.kdbx,.kdc,.kpdx,.lua,.mdc,.mef,.mfw,.mmw,.mny,.mo
neywell,.mrw,.myd,.ndd,.nef,.nk2,.nop,.nrw,.ns2,.ns3,.ns4,.nwb,.nx2,.nxl,.nyf,.odb
,.odf,.odg,.odm,.orf,.otg,.oth,.otp,.ots,.ott,.p12,.p7b,.p7c,.pdd,.mts,.plus_muhd,
.plc,.psafe3,.py,.qba,.qbr,.qbw,.qbx,.qby,.raf,.rat,.raw,.rdb,.rwl,.rwz,.s3db,.sd0
,.sda,.sr2,.srf,.srw,.st5,.st8,.std,.sti,.stw,.stx,.sxd,.sxg,.sxi,.sxm,.tex,.walle
t,.wb2,.wpd,.x11,.x3f,.xis,.ycbcra,.yuv,.mab,.json,.msf,.jar,.cdb,.srb,.abd,.qtb,.
cfn,.info,.info_,.flb,.def,.atb,.tbn,.tbb,.tlx,.pml,.pmo,.pnx,.pnc,.pmi,.pmm,.lck,
.pm!,.pmr,.usr,.pnd,.pmj,.pm,.lock,.srs,.pbf,.omg,.wmf,.sh,.war,.ascx,.k2p,.apk,.a
sset,.bsa,.d3dbsp,.das,.forge,.iwi,.lbf,.litemod,.ltx,.m4a,.re4,.slm,.tiff,.upk,.x
xx,.money,.cash,.private,.cry,.vsd,.tax,.gbr,.dgn,.stl,.gho,.ma,.acc,.db
```

پیوست ۲ – ارتباطات باج‌افزار Cerber

- **hxxp://ipinfo.io/json**
- **hxxp://freegeoip.net/json/**
- **hxxp://ip-api.com/json**
- **hxxp://www.ldlogistic.it/kls.doc**
- **hxxp://csir.bdx6.siteinternet.com/kls.doc**
- **87.98.128.0/19: 6891**
- **85.93.0.0/18: 6892**
- **31.184.234.0/23:6892**
- **81.93.0.0/19: 6892**
- **31.184.232.0/21:6892**

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 (تولید کننده 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 – 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، 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.

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