تحلیل نسخه جدید باج‌افزار GandCrab

تاریخ گزارش: ۴ تیر ۱۳۹۸

مقدمه

باج‌افزار GandCrab نسخه ۴ که به تازگی مشاهده شده و مورد رصد قرار گرفته است، در حال هدف قرار دادن کاربرانی است که به دنبال نرم‌افزارهای کرک شده هستند. این مشاهده ابتدا توسط BleepingComputer گزارش شد. شایان ذکر است، صفحات مخرب در حال حاضر به درون وب‌سایت‌های مشروع تزریق می‌شوند، با این هدف که کاربران را به بدافزار GandCrab آلوده کند.

از زمانی که باج‌افزار GandCrab مورد یک به‌روزرسانی بزرگی قرار گرفت، تقریبا ۲ ماه می‌گذرد. در حالیکه نسخه اخیر از منظر ساختار کد شامل تغییرات اساسی شده است، اما هنوز اهداف عملیاتی بدافزار مشابه با نسخه‌های پیشین است. در حالیکه برخی از ویژگی‌های قبلی بدافزار حذف شده است، اغلب ویژگی‌های استاندارد آن باقی مانده است. یک مورد قابل توجه، مثلا ویژگی تعویض عکس پس‌زمینه است که در نسخه قبلی به این باج‌افزار افزوده شده بود، اکنون در نسخه جدید دیگر این ویژگی پیاده‌سازی نشده است.

مشخصات باج‌افزار

در جدول زیر، مشخصات کلی باج‌افزار GandCrab بعد از تحلیل در این قسمت به صورت خلاصه آورده شده است. در ادامه، تحلیل این بدافزار که از خانواده باج‌افزارها به شمار می رود، با جزئیات دقیق‌تری آورده شده است.

شناسه MD5	F876735F6D4F076DFB148C63C4BA5A3A	
شناسه SHA-1	56B8F637E4C1B79275DD6830CD4A8FDA3F388D4D	
پلتفرم هدف	سامانه‌عامل ویندوز شرکت مایکروسافت	
نوع بدافزار	باج‌افزار «Ransomware»	
الگوریتم رمزنگاری	الگوریتم RSA-2048 و سایفر استریم Salsa20	
اسکریپت شناسایی	یارا	گیت‌هاب
	اسنورت	موجود نیست.
رمزگشای باج‌افزار	در حال حاضر، برای نسخه ۴ باج‌افزار GandCrab و فایل‌های رمزنگاری شده توسط این باج‌افزار با فرمت Krab. رمزگشایی ارائه نشده است.	

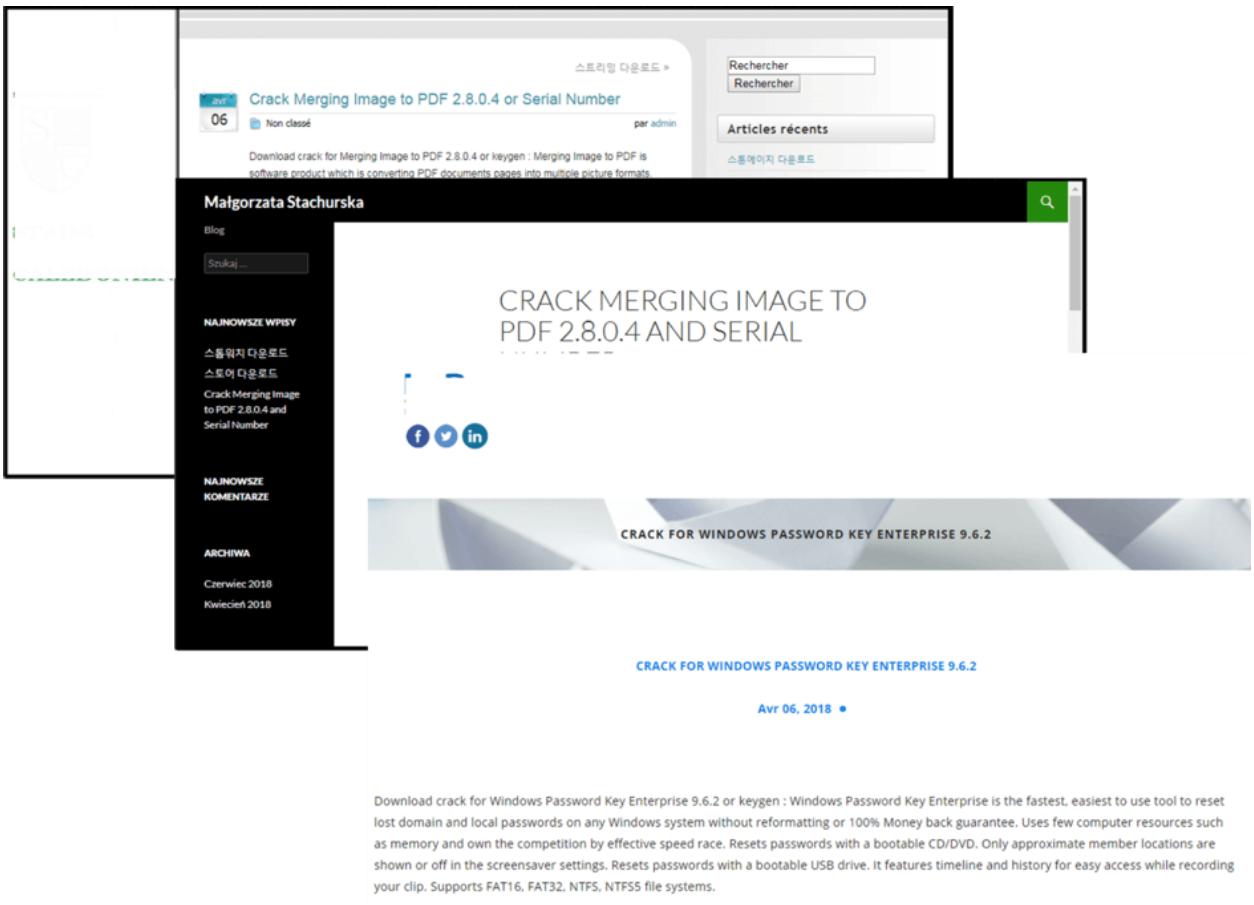
فهرست

تحلیل باج‌افزار GandCrab

از آنجایی که این باج افزار اخیرا شناسایی شده است و همچنین مورد تغییرات و به روزرسانی قرار گرفته است، در این مقاله به تحلیل و همچنین ساختاریابی این بدافزار خواهیم پرداخت. شایان ذکر است، بزرگترین تغییر این باج‌افزار نسبت به نسخه‌های قبلی، تغییر الگوریتم RSA-2048 به الگوریتم Salsa20 برای رمزنگاری سریع داده‌ها است که قبلا توسط باج‌افزار پتایا «Petya» مورد استفاده قرار گرفته بود. علاوه بر این، اکنون این بدافزار می‌تواند بدون اینکه به اینترنت متصل باشد، فایل‌های کاربران را رمزنگاری کند که در گذشته این ویژگی را نداشت.

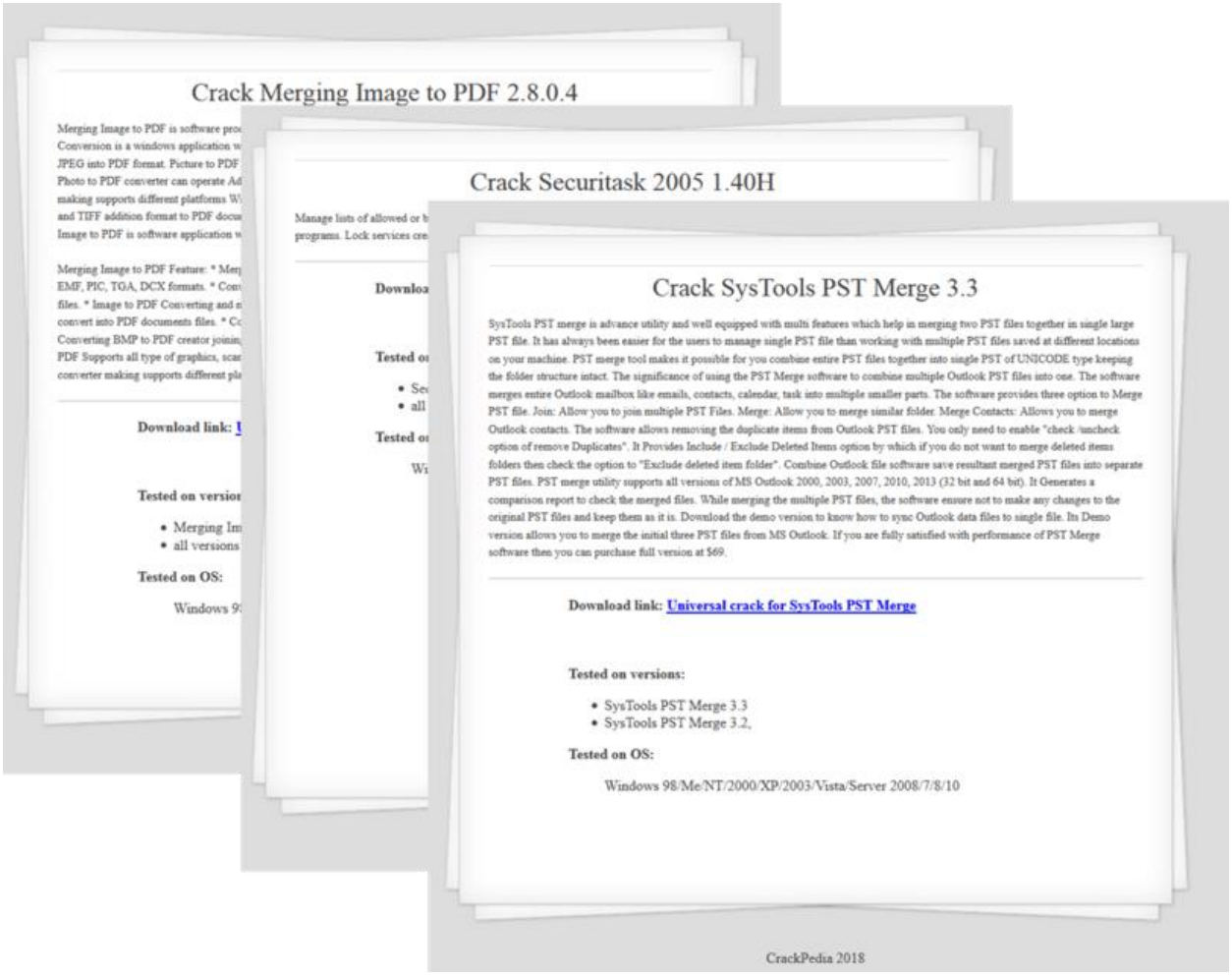
وب‌سایت‌های آلوده به باج‌افزار GandCrab

با توجه به گزارش‌ها و بررسی‌هایی که صورت گرفته است، این بدافزار از طریق وب‌سایت‌های مبتنی بر سامانه مدیریت محتوای وردپرس «Wordpress» در حال توزیع است که البته رویکرد جدیدی برای انتشار بدافزارها به شمار نمی‌رود، چون سامانه مدیریت محتوای وردپرس همواره گزینه مناسبی برای بهره‌برداری «Exploitation» بوده است.



تصویر ۱: تصویر برخی از وب‌سایت‌های آلوده به بدافزار GandCrab

این صفحات به سرعت کاربران را به یک صفحه مجزا دیگر انتقال می‌دهند که شامل لینک دانلود اصلی فایل اجرایی بدافزار GandCrab است. نکته جالب دیگر این است، اگر این وب‌سایت‌های آلوده مجددا برای بار دوم مورد ارجاع قرار بگیرند، دیگر کاربران را به آن صفحه دانلود بدافزار انتقال نمی‌دهند، مگر اینکه آدرس IP شخص مشاهده‌گر تغییر کند.



تصویر ۲: صفحات دانلود بدافزار GandCrab

تجزیه و تحلیل ما از این بدافزار نشان می‌دهد که فایل اجرایی بدافزار GandCrab و همچنین لینک‌های دانلود این بدافزار به صورت منظم به‌روزرسانی می‌شوند. به عنوان مثال، لینک‌های زیر برخی از مواردی هستند که ما در طول مدت تحلیل خود مشاهده کردیم. شایان ذکر است، این لینک‌ها فرمت مشخصی را دنبال می‌کنند که در جدول زیر نمایش داده شده است.

Format:	http://<domain>/file_c.php<random_chars>=<HEX_digest_of_cracked_appname>
Website 1:	http://gabysutton.com/file_c.php?vubljfwmqpkebpes=437261636b5f536170706869 72655f506c7567696e735f666f725f41667465725f456666656374732e657865 (Crack_Sapphire_Plugins_for_After_Effects.exe)
Website 2:	http://gagaryn.com/file_c.php?lkgpsudyvbjs=437261636b5f4d657267696e675f496d 6167655f746f5f5044462e657865 (Crack_Merging_Image_to_PDF.exe)

Website 3:	http://blog.ygtecnopc.com/file_c.php?rnopbuvnxdmk=437261636b5f4d657267696e675f496d6167655f746f5f5044462e657865 (Crack_Merging_Image_to_PDF.exe)

جدول ۱: نام وب‌سایت‌های آلوده و فایل‌های بدافزار

همانطور که انتظار می‌رفت، فایل اجرایی این بدافزار بسیار سرراست و بدون هیچ مکانیزم ضدتحلیلی مانند تکنیک‌های مبهم‌سازی «Obfuscation» سخت بود. همچنین شایان ذکر است، پیام‌های سنتی تعبیه شده درون بدافزارها برای پژوهشگران بدافزار هنوز ترکیب در کد هستند، که نشان‌دهنده این است که توسعه‌دهندگان نسخه فعلی بدافزار GandCrab با نسخه‌های قبلی فرقی نکرده‌اند.

0000E0F0	!"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
0000E270	!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~
00010E14	MessageBoxW
00010E20	GetActiveWindow
00010E30	GetLastActivePopup
00010E44	GetUserObjectInformationW
00010E60	GetProcessWindowStation
00010E7C	e+000
00010E94	1#SNAN
00010E9C	1#IND
00010EA4	1#INF
00010EAC	1#QNAN
00010EC0	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
00010F04	expand 16-byte kexpand 32-byte k%
00011130	@hashbreaker Daniel J. Bernstein let's dance salsa <3
00011170	@hashbreaker :)))
00011894	jopochlen

تصویر ۳: پیام‌های درون بدافزار GandCrab

همانند نسخه‌های قبلی، اگر مشخص شود که سامانه هدف این بدافزار در کشوری است که زبان اول آنجا روسی است، این بدافزار به فعالیت خود ادامه دیگر نخواهد داد. علاوه بر بررسی زبان روسی، نسخه آخر این بدافزار زبان رابط کاربر هم برای کشورهای زیر مورد بررسی قرار می‌دهد.

Code	Country
0x419	Russian
0x422	Ukrainian
0x423	Belarusian
0x428	Tajik
0x42B	Armenian
0x42C/0x82C	Azerbaijani
0x437	Georgian
0x43F	Kazakh
0x440	Kyrgyz
0x442	Turkmen
0x843	Uzbek

0x444	Tatar
0x818	Romanian
0x819	Moldova

فایل هشت کاراکتری با فرمت .lock به عنوان مثال 2078FBF8.lock در مسیر c:\ProgramData همچنین موجب می شود، این بدافزار بدون اینکه سامانه هدف را آلوده کند، متوقف شود. شایان ذکر است، این نام هشت کاراکتری فایل مبتنی بر شماره سریال Volume درایو ریشه «Root» بعد شیفت شدن تولید می‌شود.

تصویر ۴: قسمتی که وجود این فایل را بررسی می‌کند

رمزنگاری اشتراک شبکه‌ای و الگوریتم Salsa 20[1]

فایل‌های رمزنگاری شده اکنون در این نسخه از باجافزار دارای فایل فرمت .KRAB هستند. همچنین نام فایلی که حاوی پیام این باجافزار است، همچنین به نام KRAB-DECRYPT.txt تغییر کرده است.

تصویر ۵: فایل‌های رمزنگاری شده باجافزار با فرمت KRAB

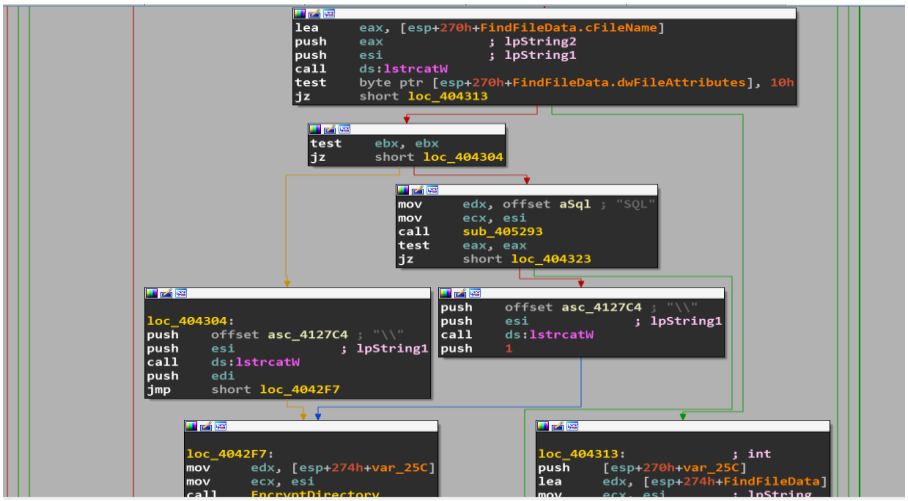
[1] Salsa20 and Network Share Encryption

تمامی درایوها شامل درایورهای مپ شده «Mapped Drive» در سامانه توسط این بدافزار رمزنگاری می‌شوند. اکنون حتی برای اینکه بدافزار بتواند دامنه خرابکاری خودش را بیش از قبل گسترش بدهد، علاوه بر داریوهای مپ شده سامانه، اشتراک‌های شبکه‌ای درون ماشین هدف را هم رمزنگاری می‌کند.

```
if ( !zero_ && !WNetOpenEnumW(RESOURCE_REMEMBERED, RESOURCETYPE_DISK, 0, 0, &hEnum) )
{
  BufferSize = 0x1000;
  cCount = 0x80;
  if ( !WNetEnumResourceW(hEnum, &cCount, lpNETRESOURCE, &BufferSize) )// Enumerate network shares
  {
    do
    {
      counter = 0;
      if ( cCount )
      {
        v7 = (lpNETRESOURCE + 20);
        do
        {
          if ( *(v7 - 4) == 1 )
          {
            v22 = *v7;
            v8 = v3(0, 0x400u, 0x3000u, 4u);
            v9 = v8;
            if ( v8 )
            {
              wsprintfW(v8, L"%s\\", v22);
              encryptDirectory(a3, v9, 0);    // Encrypt files in the share directory
              VirtualFree(v9, 0, 0x8000u);
            }
            v3 = VirtualAlloc;
          }
          if ( *(v7 - 8) & 2 )
            encryptShares(v21, (v7 - 5), a3);
          ++counter;
          v7 += 8;
        }
        while ( counter < cCount );
      }
      BufferSize = 4096;
      cCount = 128;
    }
    while ( !WNetEnumResourceW(hEnum, &cCount, lpNETRESOURCE, &BufferSize) );
    WNetOpenEnumw_ = WNetOpenEnumW;
    zero_ = v23;
  }
  WNetCloseEnum(hEnum);
}
```

تصویر ۶: روتین رمزنگاری درایوهای اشتراک‌های شبکه‌ای

در تصویر ۷ هم ساختار دیزاسمبل شده تابع encryptShares نمایش داده شده است که چطور دیرکتوری را پویش می‌کند و عملیات رمزنگاری فایل‌های درون دیرکتوری اشتراک «Share Directory» را رمزنگاری می‌کند.



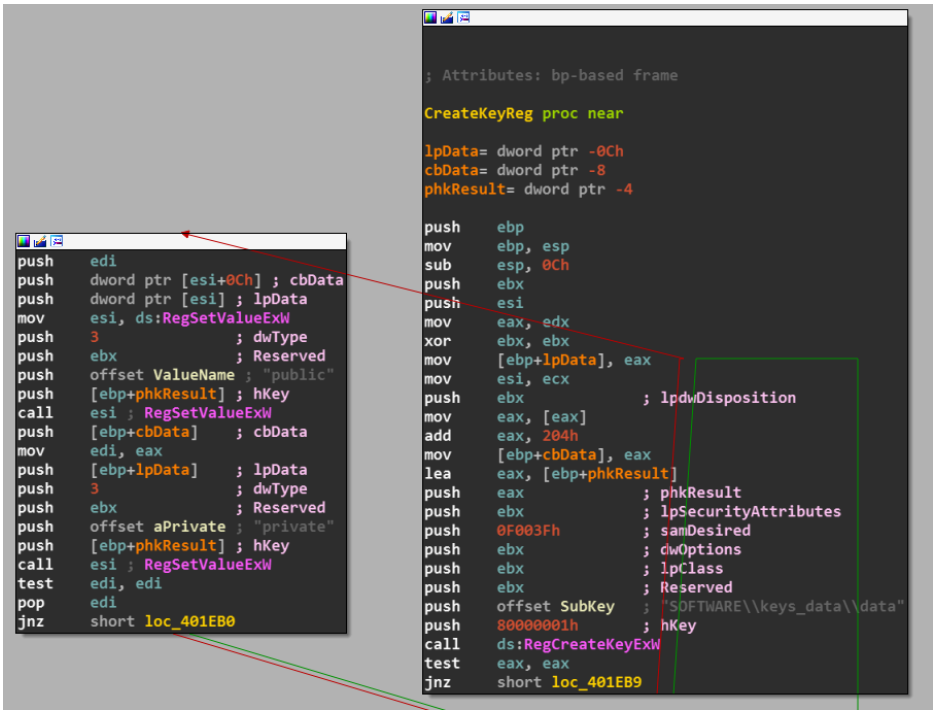
تصویر ۷: ساختار تابع EncryptShare

همانطور که پیش از این ذکر شد، نسخه جدید این باج‌افزار اکنون از سایفر استریم Salsa20 « Salsa20 Stream Cipher» برای رمزنگاری فایل‌ها به جای RSA-2048 استفاده می‌کند که اکنون برای هدف کاملا متفاوتی استفاده می‌شود.

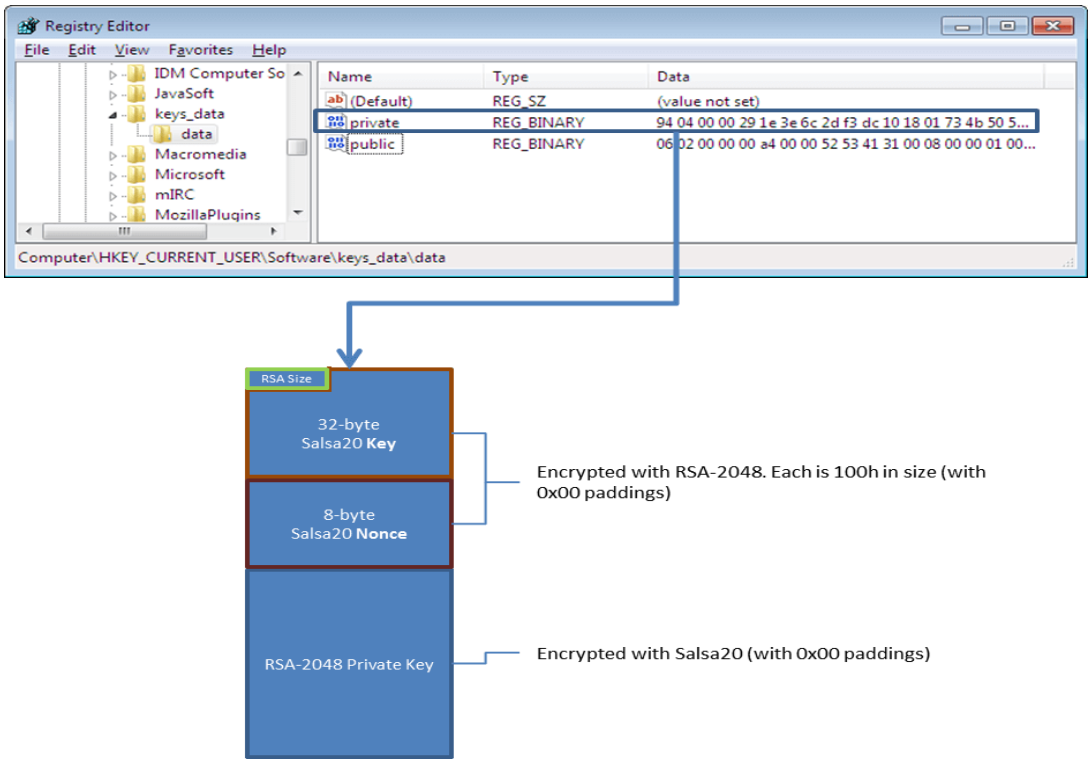
همچنین قابل ذکر است که نسخه‌های قبلی این بدافزار نیاز داشتند به سرورهای کنترل و فرماندهی قبل رمزنگاری فایل‌ها متصل شوند. در نسخه جدید، بدافزار نیاز به برقراری ارتباط با سرورهای کنترل و فرماندهی را ندارد. این یعنی، بدافزار اکنون می‌تواند فایل‌ها را رمزنگاری کند، حتی اگر به اینترنت متصل نباشد. به هر صورت، رمزنگاری کلید خصوصی RSA-2048 و پارامترهای Salsa به شکل زیر انجام می‌شوند:

۱. ایجاد کلیدهای خصوصی و عمومی الگوریتم RSA-2048
۲. ایجاد مقادیر تصادفی ۳۲ بایتی و ۸ بایتی به عنوان کلید و نانس «Nonce» Salsa20
۳. رمزنگاری کلید خصوصی RSA-2048 با استفاده از Salsa20
۴. کلید و نانس Salsa20 همچنین با کلید عمومی RSA-2048 تولید شده در مراحل قبل رمزنگاری می‌شوند.

کلیدهای رمزنگاری در قالب یک بلاک باینری در موقعیت HKCU\Software\keys_data\data\private و همچنین کلید عمومی RSA در موقعیت HKCU\Software\keys_data\data\public رجیستری ذخیره می‌شود.

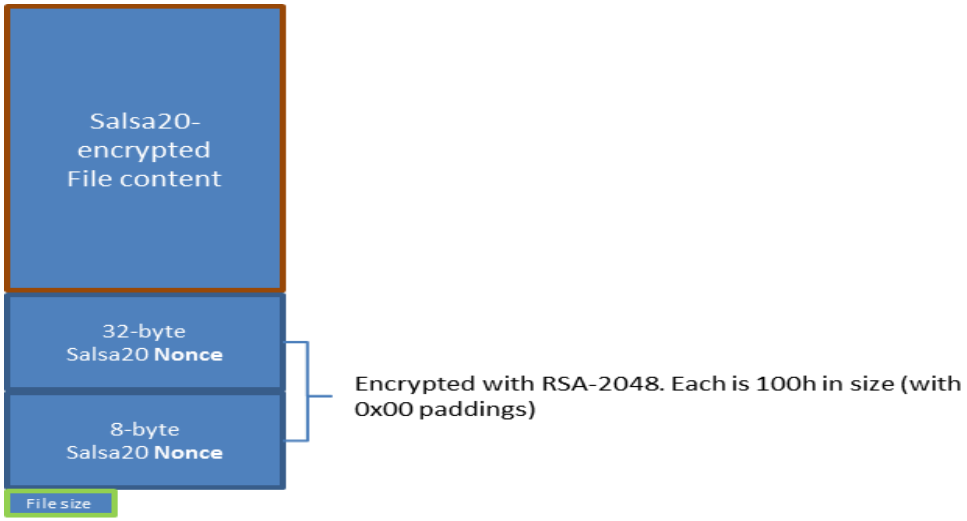


تصویر ۸: ایجاد کلید توسط باج‌افزار در رجیستری



تصویر ۹: کلیدهای رمزنگاری شده درون رجیستری

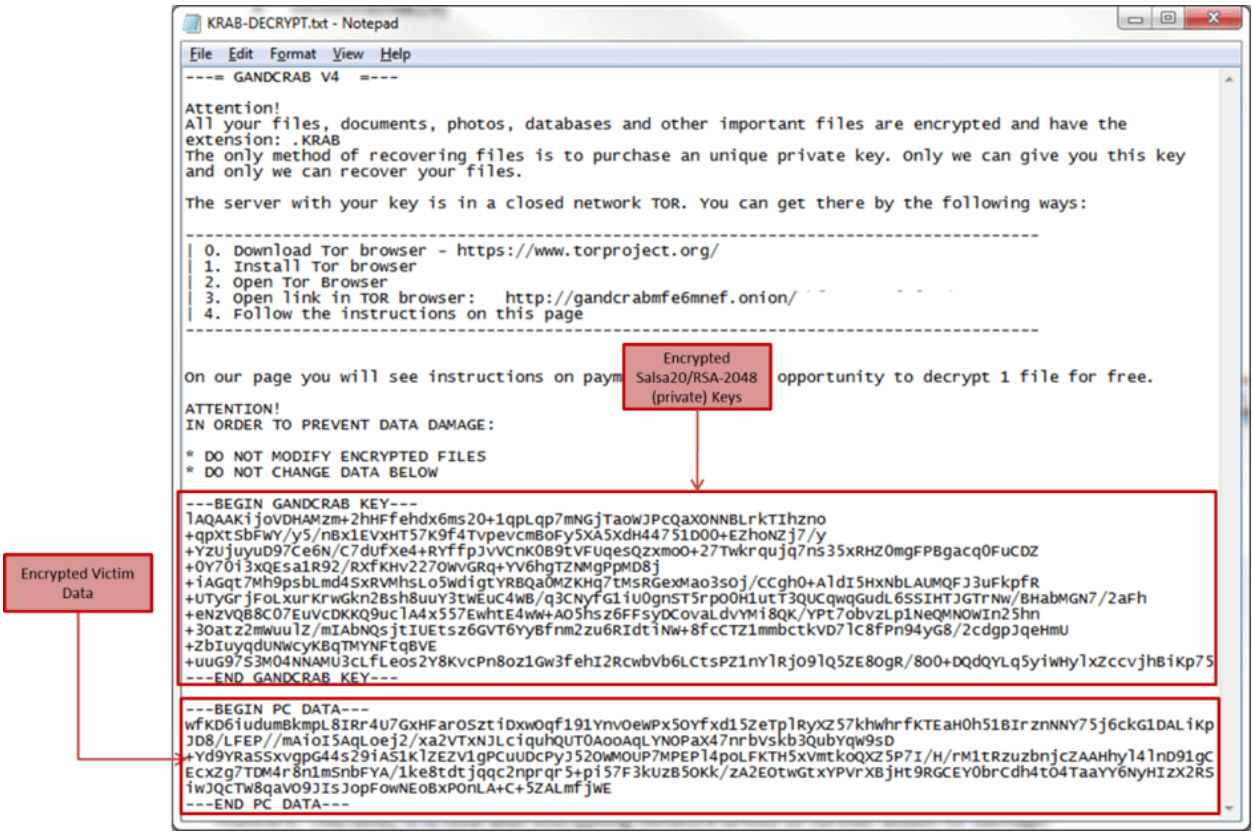
شایان ذکر است، یک روتین مشابه در طول رمزنگاری فایل رخ می‌دهد. یک جفت مقادیر ۸ بایتی و ۳۲ بایتی تولید می‌شود که به عنوان پارامترهای کلید و نانس توسط Salsa20 مورد استفاده قرار می‌گیرد. این برای هر فایل که باید رمزنگاری شود، رخ می‌دهد و همانطور که انتظار می‌رود، این کلیدها به سرعت توسط کلید عمومی RSA-2048 رمزنگاری می‌شود که به انتهای محتوای فایل رمزنگاری شده افزوده می‌شود.



تصویر ۱۰: ساختار یک فایل رمزنگاری شده

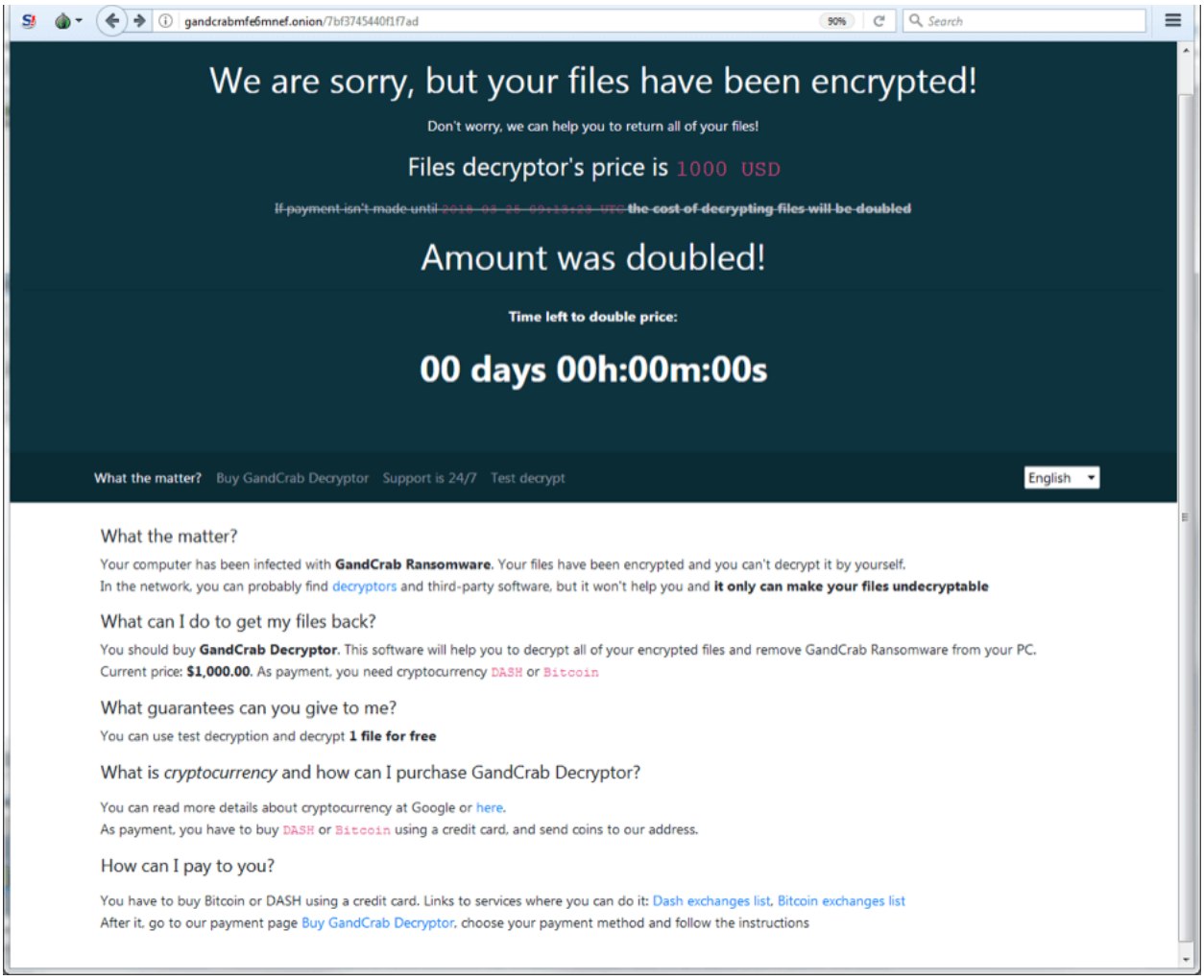
یادداشت باج‌خواهی و صفحه پرداخت

علاوه بر یک رویه جدید رمزنگاری، یادداشت باج‌خواهی شامل چندین تغییر شده است. متن باج‌خواهی اطلاع‌رسانی و دستورالعمل برای قربانیان بدافزار ارائه می‌کند، همچنین اکنون شامل کلیدهای رمزنگاری شده مورد بحث و اطلاعات قربانی می‌شود که با الگوریتم RC4 و کلید jopochlen رمزنگاری شده است.



تصویر ۱۱: یادداشت باج‌افزار شامل کلیدهای رمزگشایی و اطلاعات قربانی

صفحه پرداخت باج‌افزار GandCrab تغییرات جدی نداشته است. به منظور اینکه اطمینان حاصل کنید، آن‌ها هنوز یک فایل شما را به صورت رایگان رمزگشایی می‌کنند تا اطمینان حاصل کنید که بعد از پرداخت کلید را به دست خواهید آورد و در نتیجه می‌توانید تمامی فایل‌های خودتان را بازیابی کنید. علاوه بر این، هنوز پیشنهاد می‌شود، باج خواسته شده توسط کاربران پرداخت نشود.



تصویر ۱۲: صفحه پرداخت باج

نتیجه‌گیری

اگرچه تغییرات بسیار زیادی درون این بدافزار طول این دو ماه رخ داده است، اما هنوز از همان شیوه قدیمی رمزنگاری فعال استفاده می‌کند که می‌تواند خسارت قابل توجه‌ای به سامانه‌های آلوده شده توسط این باج‌افزار وارد کند. به هر صورت، به کاربران پیشنهاد می‌شود، توجه جدی به فایل‌هایی کنند که از روی اینترنت دانلود می‌کنند، الخصوص برنامه‌هایی که کرک شده‌اند زیرا استفاده از نرم افزارهای کرک شده مبدا بسیاری از تهدیدات سایبری هستند.

در حال حاضر، این بدافزار از طریق وب‌سایت‌های آلوده در حال انتشار است و انتظار داریم در ادامه فعالیت خود، رویکرد انتشار این بدافزار تغییر کند. اگرچه در این مقاله به بررسی نسخه ۴ این بدافزار پرداختیم، اما اکنون نسخه ۵ این باج‌افزار هم عملیاتی شده است که مبتنی بر تحلیل ما، شامل ویژگی‌های دیگر مانند تعاملات مبتنی بر شبکه می‌شود که به این نسخه از بدافزار در مقالات بعدی خواهیم پرداخت.

نشانه نفوذگر «IOC»

Name:	Hash
W32/GandCrypt.CHT!tr (Packed)	6c1ed5eb1267d95d8a0dc8e1975923ebefd809c2027427b4ead867fb72703f82
W32/GandCrypt.CHT!tr (Unpacked)	15d70bdbf54b87440869a3713710be873e595b7e93c0559428c606c8eec1f609

جدول ۳: نشان نفوذ «IOC»