باسمه تعالی

تحلیل فنی باج‌افزار

Sodinokibi

فهرست مطالب

۱. مقدمه :

در اوایل ماه آوریل سال ۲۰۱۹ میلادی، خبر انتشار باج‌افزاری قدرتمند به نام Sodinokibi در فضای سایبری منتشر شد. محققان امنیتی بدلیل رفتار مشابه این باج‌افزار در شیوه رمزگذاری فایل‌ها و همچنین تشابه در کد باج‌افزار، آن را بسیار شبیه به باج‌افزار GandCrab می‌دانند. حتی عده‌ای تیم توسعه دهنده این باج‌افزار را با باج‌افزار GandCrab یکسان می‌دانند و معتقدند که این دو باج‌افزار از یک خانواده هستند. باج‌افزار Sodinokibi به اسامی دیگری از جمله Sodin و Revil نیز شناخته می‌شود. در ادامه تحلیل یکی از جدیدترین نسخه‌های این باج‌افزار را مشاهده می‌کنید.

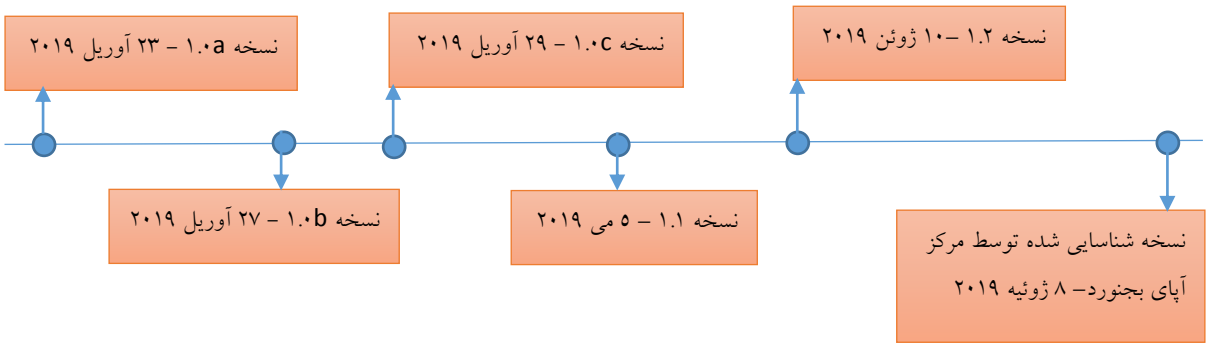
۲. مشخصات فایل اجرایی :

نام فایل	Update.exe zbetcheckin_tracker_update.exe
MD5	60e55e692c83d9d80da80f94241006c4
SHA-1	75b494bc7c6224593f31942bc822e47c32dfcf0b
SHA-256	a6c25e66ffad6d0b15c92bb70254c8599b87c69c6a9f1f12e210c6937c9cef3d
نوع فایل	Win32 EXE
اندازه فایل	٤٠٤ کیلوبایت

فایل اجرایی این باج‌افزار دارای ۸ بخش است :

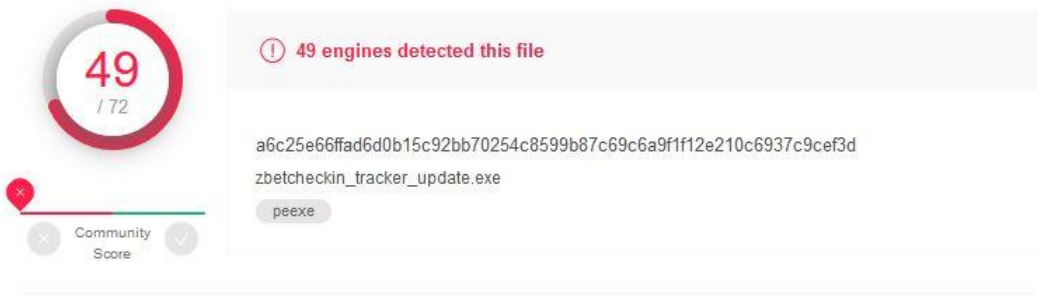
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٧٣	٤٠٩٦	١٥٧٠٠٥	١٥٧١٨٤
.rdata	٥.٠٩	١٦٣٨٤٠	٤٠٨٠٤	٤٠٩٦٠
.data	٣.٢٦	٢٠٤٨٠٠	٨٤٠٤٦٧٢	٧١٦٨
.text	٦	٨٦٠٩٧٩٢	١٨٢٣٦٠	١٨٢٧٨٤
.gibohol	٠	٨٧٩٤١١٢	١٠٢٤	١٠٢٤
.raxoduw	٠	٨٧٩٨٢٠٨	٦١٤٤	٢٥٦٠
.rsrc	٥.٠٩	٨٨٠٦٤٠٠	١١٩٨٤	١٢٢٨٨
.reloc	٦.٥٧	٨٨١٨٦٨٨	٨٤٣٢	٨٧٠٤

۳. شجره‌نامه



٤. میزان تهدید فایل باج‌افزار

درحال حاضر تعداد ٤٩ مورد از ۷۲ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.



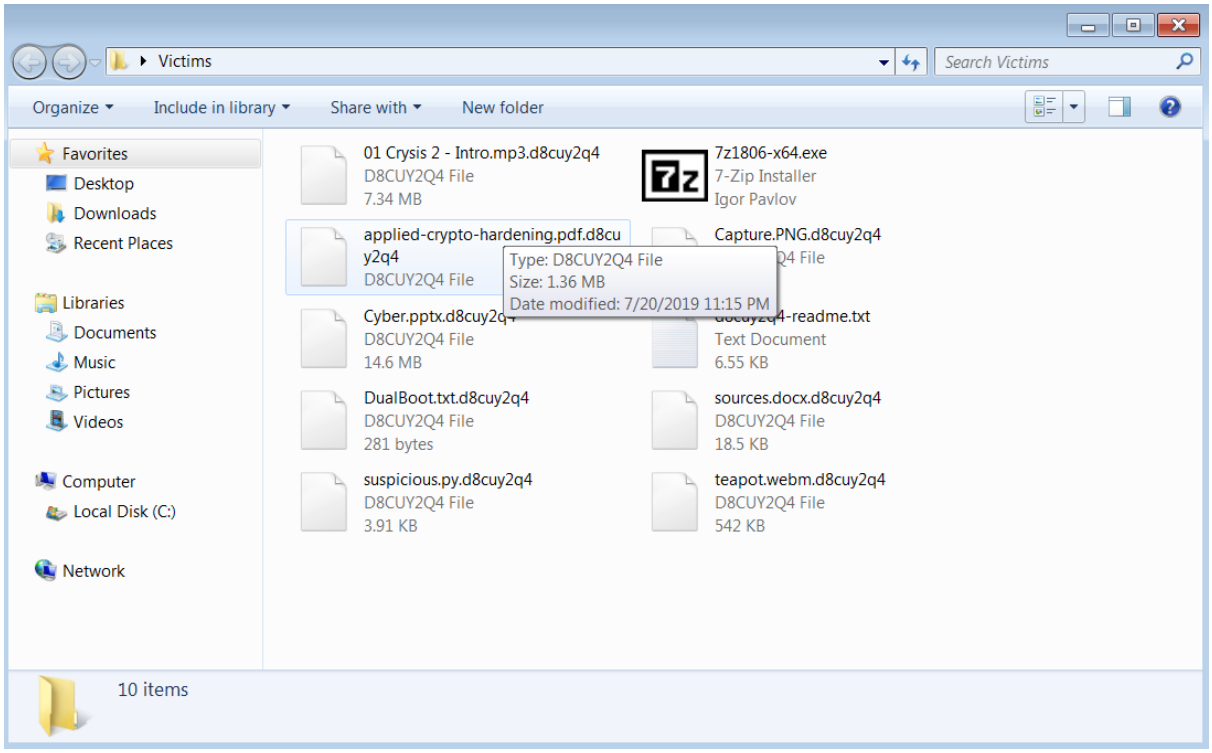
۵. تحلیل پویا

۵-۱ آناتومی حمله

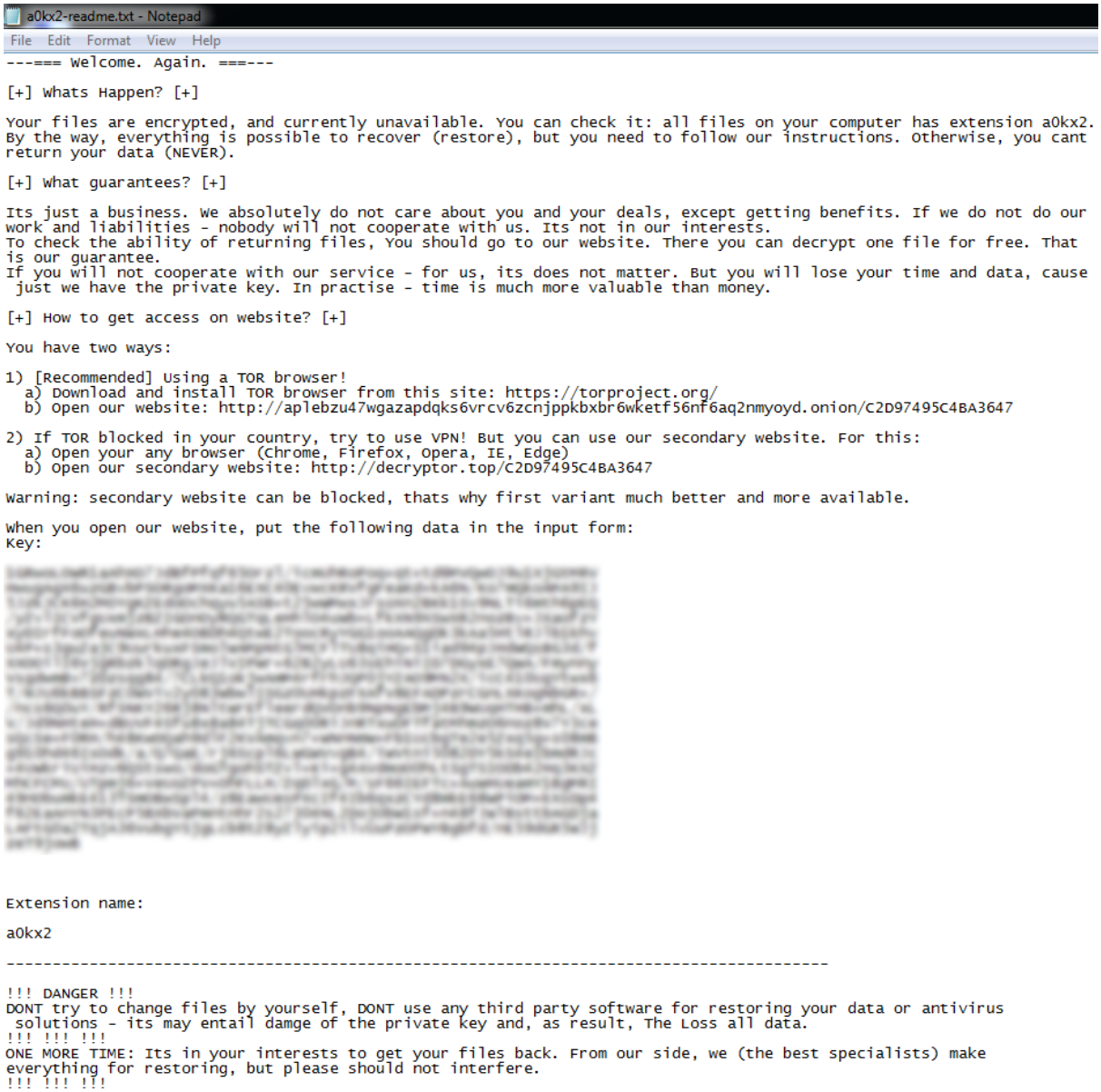
طبق بررسی‌های صورت گرفته، باج‌افزار Sodinokibi به محض شروع فعالیت در سیستم قربانی، دستورات زیر را در محیط خط فرمان ویندوز اجرا می‌کند:

حذف فضای VSS	vssadmin.exe Delete Shadows /All /Quiet
غیرفعال کردن قابلیت بازیابی فایل‌ها	bcdedit /set {default} recoveryenabled No
غیرفعال کردن پنجره Error Recovery هنگام بوت ویندوز	bcdedit /set {default} bootstatuspolicy ignoreallfailures

سپس شروع به جست و جو و رمزگذاری فایل‌های مورد نظر خود در سیستم قربانی می‌کند. فایل‌های سیستم قربانی پس از رمزگذاری، به شکل زیر تغییر پیدا می‌کنند:



پس از چند بار اجرا و بررسی‌های متوالی، متوجه شدیم پسوندی که به انتهای هر فایل اضافه می‌شود کاملاً تصادفی بوده و این پسوند به ابتدای فایل متنی پیغام باج‌خواهی باج‌افزار، اضافه می‌شود. این فایل درون هر پوشه حاوی فایل‌های رمزشده قرار می‌گیرد. این باج‌افزار قدرتمند، تمام فایل‌های موجود در سیستم قربانی با هر نام و پسوند، به غیر از فایل‌های سیستمی و فایل‌های اجرایی با پسوند exe. را رمزگذاری می‌کند. فایل متنی پیغام باج‌خواهی این باج‌افزار با عنوان readme.txt- (پسوند تصادفی) به صورت زیر می‌باشد:



a0kx2-readme.txt - Notepad

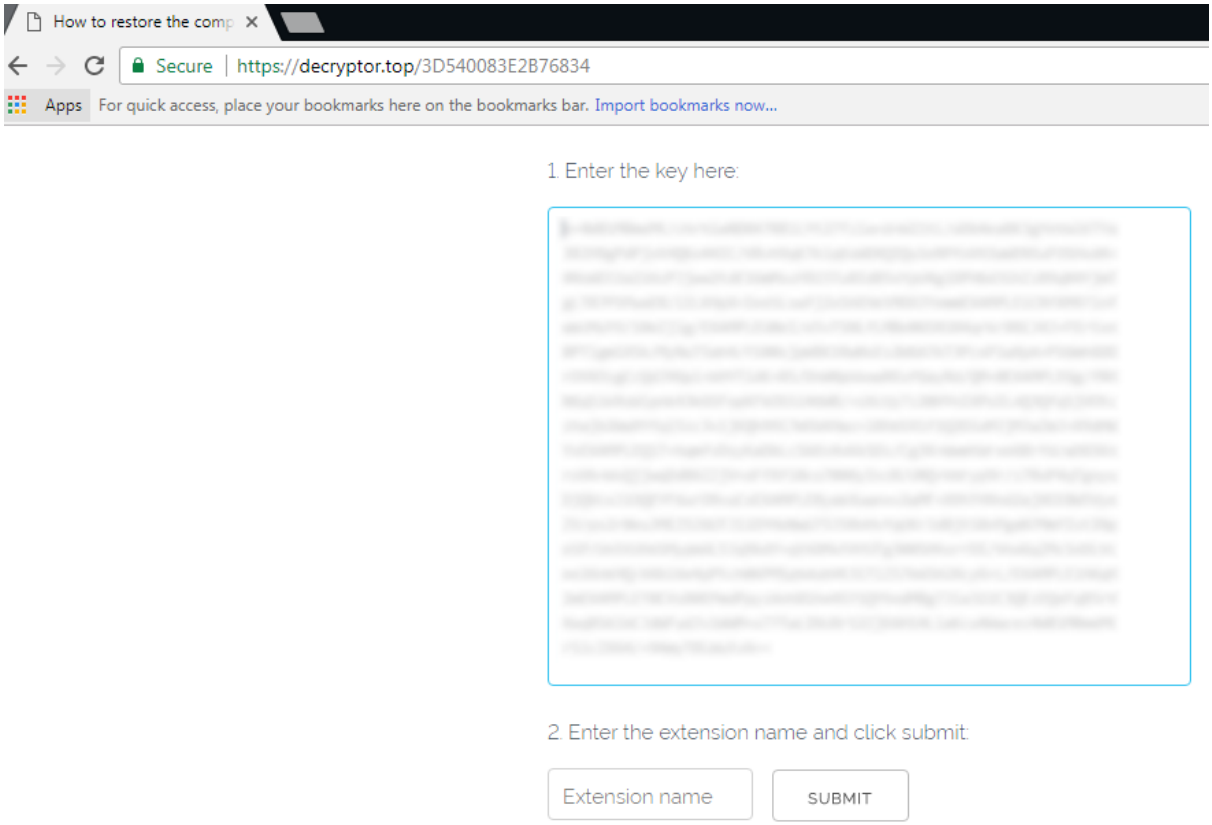
File Edit Format View Help

```
------ Welcome. Again. ------

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your computer has extension a0kx2.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant
return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our
work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That
is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause
 just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/C2D97495C4BA3647

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.top/C2D97495C4BA3647

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

[redacted]

Extension name:

a0kx2

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

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus
 solutions - its may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make
everything for restoring, but please should not interfere.
!!! !!! !!!
```

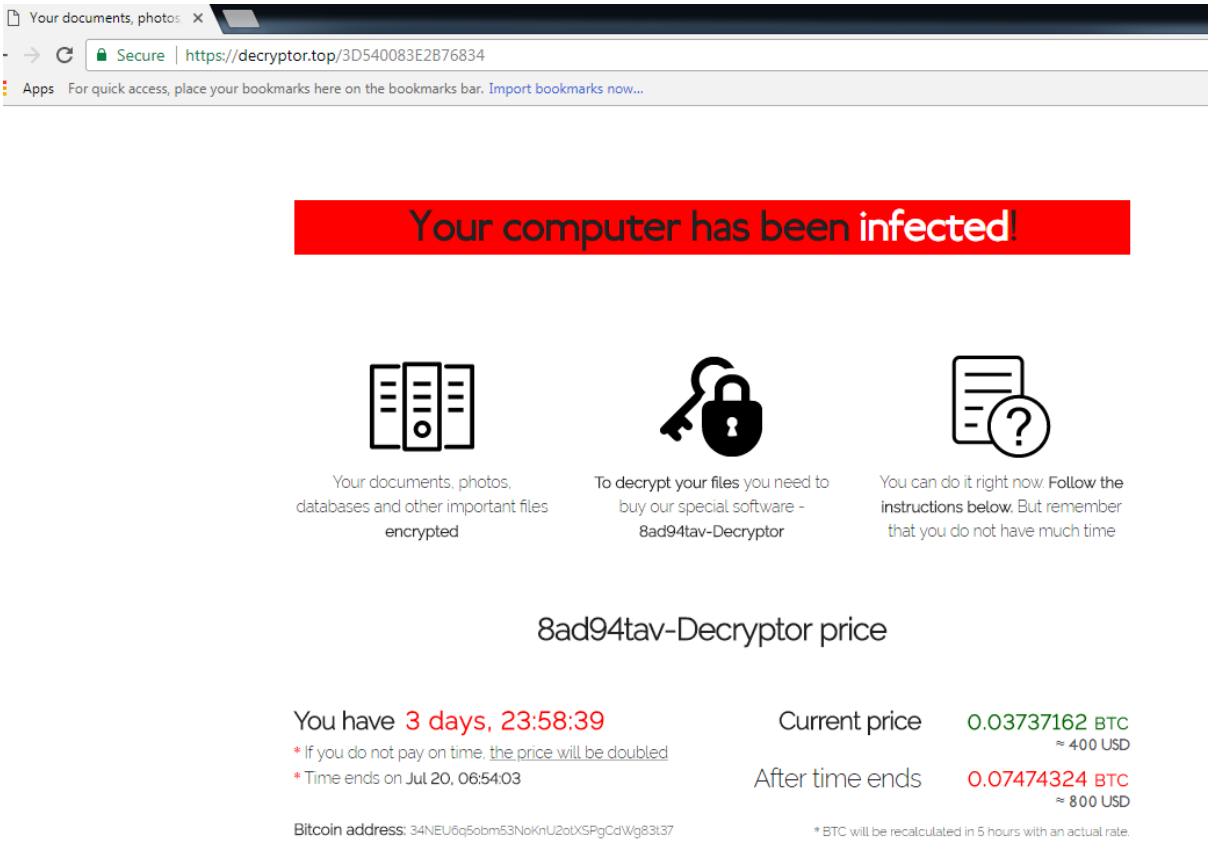
همانطور که در پیغام باج‌خواهی این باج‌افزار مشخص است، ابتدا به قربانی اطلاع داده شده که تمام فایل‌های موجود در سیستم رمزگذاری شده است و تنها راه بازیابی آن‌ها، انجام دستورالعمل‌های ارایه شده در پیغام باج‌خواهی می‌باشد. سپس عنوان شده است که جهت اعتماد و تضمین رمزگشایی فایل‌ها، قربانی باید از پرتال طراحی شده توسط مهاجم بازدید کند و در آنجا می‌تواند یک فایل را طبق قواعد ارایه شده به صورت رایگان رمزگشایی کند. آدرس این پرتال در ادامه پیغام قرار داده شده و دو راه ارتباطی نیز برای دسترسی به این وب‌سایت در نظر گرفته شده است. راه اول از طریق شبکه مخفی Tor می‌باشد. لینک دانلود مرورگر Tor نیز درون پیغام قرار داده شده است. در صورتی که قربانی موفق به دانلود یا بازکردن لینک موردنظر از طریق مرورگر Tor نشود باید از راه دوم یعنی استفاده از آدرس جایگزین و باز کردن آن از طریق مرورگرهای معمول مانند Mozilla، Chorme و ... اقدام نماید. در انتها نیز، کلید عمومی استفاده شده

در رمزگذاری و همچنین پسوند اضافه شده به انتهای فایل‌ها، درون پیغام قرار داده شده است که قربانی باید از آن‌ها پس از ورود موفقیت‌آمیز به پرتال مهاجم، استفاده نماید.

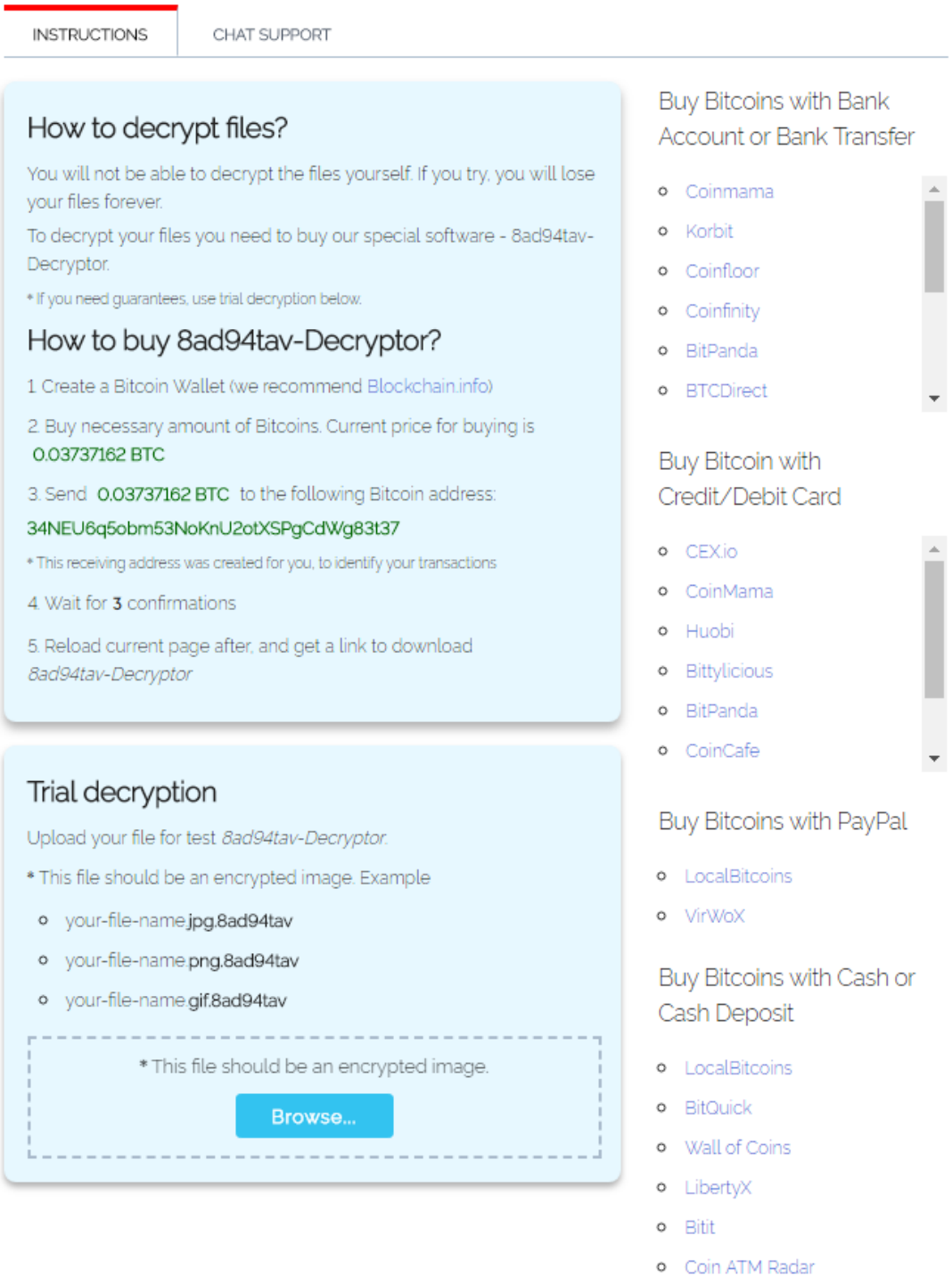
تصویر زیر، صفحه وب طراحی شده برای ارتباط با قربانیان و دستورالعمل ارایه شده در آن، جهت پرداخت باج را نشان می‌دهد:



پس از درج اطلاعات خواسته شده که همان کلید عمومی و پسوند عنوان شده در پیغام باج‌خواهی می‌باشند، قربانی با کلیک بر روی گزینه SUBMIT به صفحه زیر هدایت می‌شود:

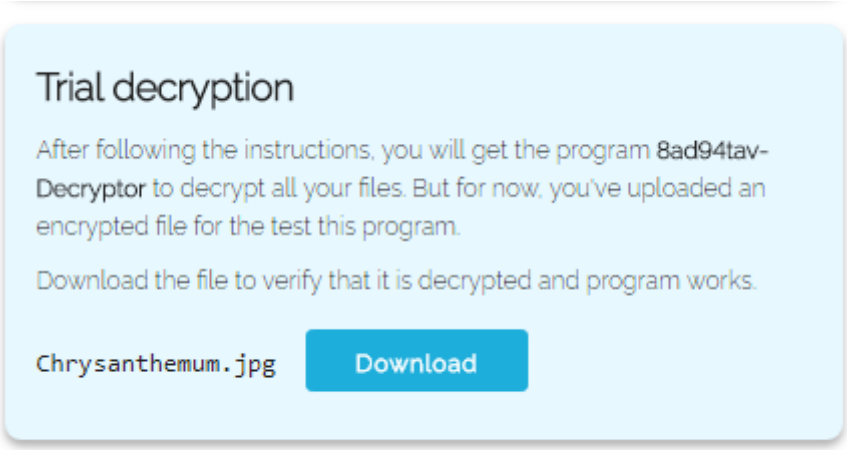


این صفحه، صفحه اصلی پرتال جهت راهنمایی قربانیان برای پرداخت باج می‌باشد. همانطور که قابل مشاهده است مبلغ ۰.۰۳۷بیت‌کوین معادل ٤۰۰ دلار برای رمزگشایی فایل‌ها در نظر گرفته شده است که قربانی باید آن را حداکثر در مدت زمان ٤ روز پرداخت نماید. در غیر این‌صورت، مبلغ باج به دوبرابر یعنی ۰.۰۷٤بیت‌کوین معادل ۸۰۰ دلار افزایش می‌یابد. آدرس کیف‌پول مهاجم نیز در زیر مهلت مشخص شده برای پرداخت هزینه رمزگشایی، قرار داده شده است.

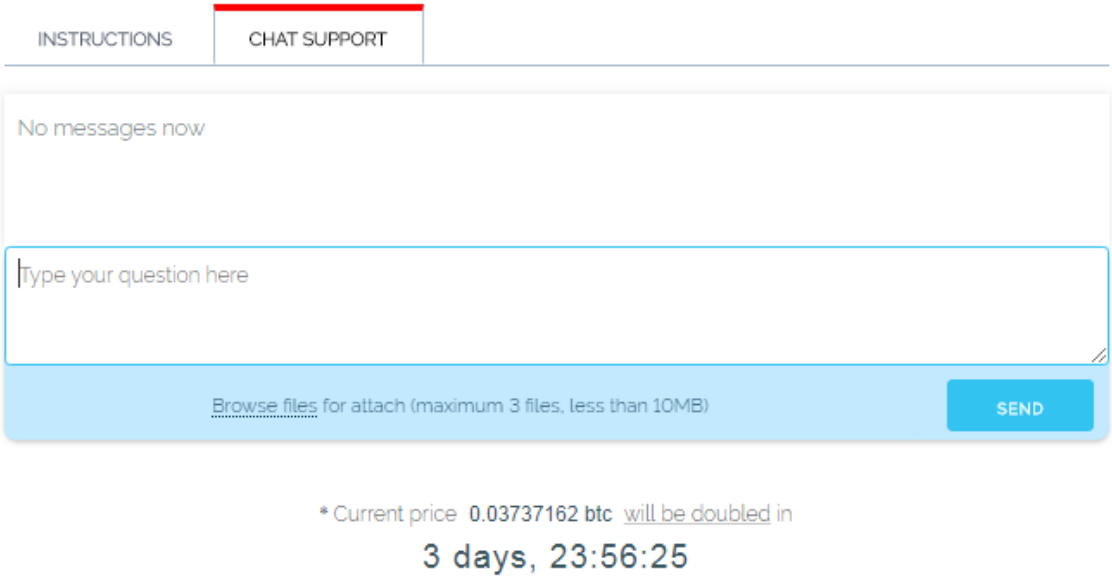


تصویر بالا، مربوط به ادامه محتوای پرتال می‌باشد. ستون سمت راست تصویر، روش‌های مختلف تهیه بیت‌کوین را نشان می‌دهد که برای راهنمایی قربانی قرار داده شده است. سمت چپ تصویر نیز، دستورالعمل رمزگشایی فایل‌ها، به طور کامل برای قربانی توضیح داده شده است. همچنین قسمتی برای رمزگشایی رایگان یک فایل، با پسوندهای jpg، png و gif در نظر گرفته شده است و قربانی با کلیک بر

روی گزینه Browse، می تواند یک فایل رمز شده با این پسوندها را از درون سیستم خود انتخاب و بارگذاری کرده و به صورت رایگان رمزگشایی نماید. پس از رمزگشایی، مطابق تصویر زیر، قربانی قادر به دانلود فایل رمزگشایی شده می‌باشد:



قابلیت گفتگو با مهاجمین نیز درون این پرتال گنجانده شده است تا قربانیان از طریق آن بتوانند با مهاجمین ارتباط برقرار کنند. تصویر زیر مربوط به این قسمت می‌باشد:



همزمان با اتمام رمزگذاری فایل‌ها، صفحه نمایش سیستم قربانی، به شکل زیر تغییر پیدا می‌کند:

این باج‌افزار، پس از پایان کار خود، همچنان به صورت فعال در سیستم قربانی باقی می‌ماند.

تغییرات رجیستری ایجاد شده توسط باج‌افزار در طول فعالیت در سیستم قربانی نیز، به صورت زیر می‌باشد:

کلید اضافه شده:

HKLM\SOFTWARE\recfg

مقادیر اضافه شده:

HKLM\SOFTWARE\recfg\sub_key: F1 2B E9 99 C6 4C EC 5C 02 C9 21 B7 CE E1 08 0F 40 19 88 12 E0 4C D7 9A C3 4C AD DA C6 E8 FC 54

HKLM\SOFTWARE\recfg\pk_key: 73 52 0C 89 EB 77 AA 00 66 BD 78 3E B0 14 AB B0 04 EA 93 DD B7 C2 B3 AE 43 81 A0 2C E5 9F 72 02

HKLM\SOFTWARE\recfg\sk_key: 78 3D 8B 21 30 07 6E 93 C8 81 F8 30 40 11 75 DF EF 03 50 99 E5 B2 78 F5 C1 98 14 A4 F4 23 9F 1F 63 91 3E 51 38 96 3C 11 7A 3D 31 A8 95 C4 F0 6B F1 0B C8 42 CD 22 0A 40 A6 72 CE AD AE 4E 47 12 56 4F 34 21 9D 82 32 DA 0D 67 23 AC 2D 0B 6D 76 08 40 1C D1 ED 41 59 B2

HKLM\SOFTWARE\recfg\0_key: 24 92 3E 16 B0 D1 4D 09 D3 EF 03 4D 91 2C D3 F1 31 E8 A6 F5 06 8C A6 81 CD 8A 14 4D 96 E7 60 1E 5B CE 13 C9 1B EA FB 0C E3 E8 F3 0B 0F CE E5 13 15 0E E1 A2 84 84 88 03 44 D2 63 03 D9 86 8B 0E B7 29 75 25 BA F9 BF 26 C2 4C E2 89 E0 12 3B AD E1 64 74 01 89 3F A9 CA

HKLM\SOFTWARE\recfg\rnd_ext: ".1r6yk2"

HKLM\SOFTWARE\recfg\stat: ED 6A C2 09 97 8F 6F 63 FC 85 6F 4D 39 05 88 3E 19 DE 08 E9 14 CE 24 5F B4 4E 53 3C 80 78 77 25 86 5C BE 76 AF 12 A1 00 25 B7 0E 4B C1 5F 89 8A 5A C6 91 44 01 DE A4 5D AA B7 A8 8A 5A 6E 69 F4 47 56 50 39 CC C1 0B BF CE 76 54 E0 C8 60 87 C6 62 6B F3 FC DB 5E 4D D7 B5 52 B7 A1 14 3E B1 F8 31 F5 8C ED 27 1F D0 D4 A4 AE 19 57 6A CC A9 F7 F8 BC 72 7F 34 D5 E5 EC 3F 6E 26 83 7D 07 9C 48 15 8A 11 D7 7F 3E B3 15 D7 F8 C4 D1 46 7B 35 C7 60 AE 6A 0E 63 32 8D 3D 67 53 D1 05 86 CF A1 07 DD 6F 62 DA D0 97 BD 4D B4 5C 93 CC 2A ED 7F 36 B5 C2 2B D6 A4 98 1B 0E 9A 6D 72 8F 23 E0 BA C8 A0 F7 30 DD BF E5 C8 83 28 32 40 7C 45 B9 B4 F1 94 04 C5 4E 80 BA F4 CE 68 B9 C0 90 01 55 33 25 7B 60 A1 20 D2 89 26 6B 71 35 BE B0 E4 B4 D4 C9 2F 03 C3 CE C2 53 74 2A D4 B9 6E 8E 8B 3F 35 B6 20 CF 6F 7C 88 92 4D 9D 47 FF 60 EA 91 71 ED D7 CB 20 17 FC 42 DA C7 89 B4 FF 8D 50 58 F3 E9 DE 51 74 15 56 95 A6 25 C4 FF B9 A0 4D 2C 7E E0 93 51 8C 86 BD EF 4A 2F F6 24 5A DD 3B 35 73 57 F5 C8 9B 0A B9 83 3D C9 61 00 9D 58 05 4B C1 9A 37 34 6A DC 88 70 8F 7C EE F3 90 39 BD DC 3D A0 7C 53 94 B2 41 67 FC CC 6A C8 62 3F FA 7B 11 5A 8C F8 E8 5A 01 F0 00 F9 D9 D5 7A 25 ED 39 C1 DC AD F6 D0 4E 7C 6D C3 D0 25 E0 47 63 D9 C6 10 87 70 23 AC 4B 5A 47 17 E5 25 02 E4 82 5A 14 9F D9 31 53 26 7A D0 BE 81 4F 31 C8 50 F4 50 BB 92 8F 6D A2 42 93 B7 51 8E 4F 78 B7 4F E5 C8 A8 20 31 F6 6E B3 89 52 8E 3D 85 51 26 FF B4 D3 82 C0 05 C4 8B BB 9F 5A DA F1 27 3B 27 E4 EC F9 21 2C 5E D4 41 8F 5B E1 C4 4C 4E 94 60 EF 81 75 57 EE 92 6C 5F 12 FE 14 54 32 85 B7 7A 91 2F 9E A2 F1 0A 05 81 C5 84 9D DC 10 62 13 66 5F 70 92 CB 3E C4 36 17 4D 73 F1 2A A0 B6 6B 5A 89 72 4C 14 F1 62 AB AF 3A BA DF DA 05 10 A7 B9 23 7A B8 9D 42 EE 58 CB 9E DB C6 1B 62 53 C6 AF 55 3D 1D 04 34 06 F4 E3 27 F5 AF 00 02 04 05 05 AA E6 8B 3C F1 DF 51 55 B5 3C 4F 85 C3 3A B7 DF 6F 76 1B 81 14 23 9D AD 09 F5 78 42 F4 7D 55 2D 4B AB D0 CE AA 7F 29 A8 C1 5F A5 7A 7D 16 92 1F 46 78 32 59 23 43 87 D0 A3 62 85 E3 1F D9 B5 A6 72 59 15 36 78 78 57 EB E5 D1 A0 AA 24 DF D1 F6 C1 55 59 0B D0 BC DE 67 6F BE 17 BD 00 F4 D4 F8 0C 00 D4 D9 B3 4C DD 33 3B 8F DC 1E 5D 97 55 97 88 22 C6 DF 02 7A 4F D0 9E EE 19 81 C6 B8 AF D3 A3 14 74 33 D3 10 18 E6 7D B9 F3 F3 97 BD C4 B0 40 02 C6 2F C8 52 6C DA 63 F9 BD 9C D3 5E C3 90 16 79 22 2E F7 B8 90 95 0C FB D6 78 D0 2E 6F AE 47 FB 10 A6 EF 95 31 F7 1F 77 1B 56 AF F1 C2 7D EE F3 E7 1F AA BB DE 19 68 A6 28 0A BF 60 84 C2 87 0F 87 CD ED 62 05 16 77 D7 27 86 67 66 A4 4E E7 6E 01 0F 7E 98 78 29 47 66 D0 CF CA 5D 57 10 00 84 9B 3E 86 95 68 F1 86 9C 0D 21 61 08 A7 4F 25 AA 90 CB 3E AD 55 99 5A 8D B6 C6 19 C4 3D E6 AE 65 3E D7 15 89 BB 5C 54 89 1B A6 91 F6 9E AF 09 B4 ED 4B 9F 91 4A F8 A0 6E B4 66 23 92 2A

HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Program Files\Common Files\system\wab32res.dll,-10100: "Contacts"

HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\eHome\ehepgres.dll,-304: "Public Recorded TV"

HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\system32\MCTRes.dll,-200005: "Websites for United States"

HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\System32\ieframe.dll,-12385: "Favorites Bar"

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\HO-PREG\Qrfxgbc\1.rkr: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF D0 6A 48 0A D9 3A D5 01 00 00 00 00

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\UB-CERT\Desktop\1.exe: "1.exe"

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\UB-CERT\Desktop\1.exe: "1.exe"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Program Files\Common Files\system\wab32res.dll,-10100: "Contacts"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\eHome\ehepgres.dll,-304: "Public Recorded TV"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\system32\MCTRes.dll,-200005: "Websites for United States"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\System32\ieframe.dll,-12385: "Favorites Bar"

کلیدهایی که مقادیر آن‌ها تغییر پیدا کرده است:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter

HKLM\SYSTEM\ControlSet001\Control\ProductOptions\ProductPolicy

HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Enter)

HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Leave)

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Control Panel\Desktop\Wallpaper

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{7P5N40RS-N0SO-4OSP-874N-P0S2R0O9SN8R}\Ertfubg 1.8.3\i5_ertfubg_1.8.3_orgn1_jva32_k64_fep_ova_i5\ertfubg.rkr

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation\LastAction

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation\ActionId

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx

۵-۲ روش انتشار:

براساس اخبار منتشر شده، نسخه‌های اولیه این باج‌افزار، با بهره‌گیری از آسیب‌پذیری CVE-2018-8453 به سیستم قربانی نفوذ می‌کردند. این آسیب‌پذیری که در گروه آسیب‌پذیری‌های روز صفرم ویندوز قرار دارد، سطح دسترسی مهاجم را به سطح مدیر در سیستم‌عامل میزبان افزایش می‌دهد. بنابراین، مهاجم با نفوذ موفقیت‌آمیز می‌تواند تمام اختیار سیستم میزبان را به دست آورد.

طبق گزارش آزمایشگاه کسپرسکی، این باج‌افزار از آسیب‌پذیری CVE-2019-2725 برای بهره‌گیری از آن در نرم‌افزار Oracle WebLogic که توسط شرکت اوراکل ارایه شده است نیز استفاده می‌کند. اجرای موفقیت‌آمیز این آسیب‌پذیری، به مهاجمین این امکان را می‌دهد تا یک فایل راه‌انداز را درون سرور آپلود کنند و از طریق آن، فایل اصلی باج‌افزار در سیستم نصب شود. وصله‌های امنیتی برای این آسیب‌پذیری ارایه شده است، اما در اواخر ماه ژوئن مجدداً یک آسیب‌پذیری مشابه با شناسه CVE-2019-2729 منتشر شد.

روش‌های متداول دیگری که در نسخه‌های جدیدتر این باج‌افزار استفاده شده است، استفاده از اسناد آفیس آلوده به کد باج‌افزار می‌باشد که در قالب ایمیل ارسال می‌شوند. همچنین گزارشاتی مبنی بر انتشار باج‌افزار Sodinokibi از طریق حمله Brute Force بر روی پروتکل RDP نیز به ثبت رسیده است.

۵-۳ روش جلوگیری:

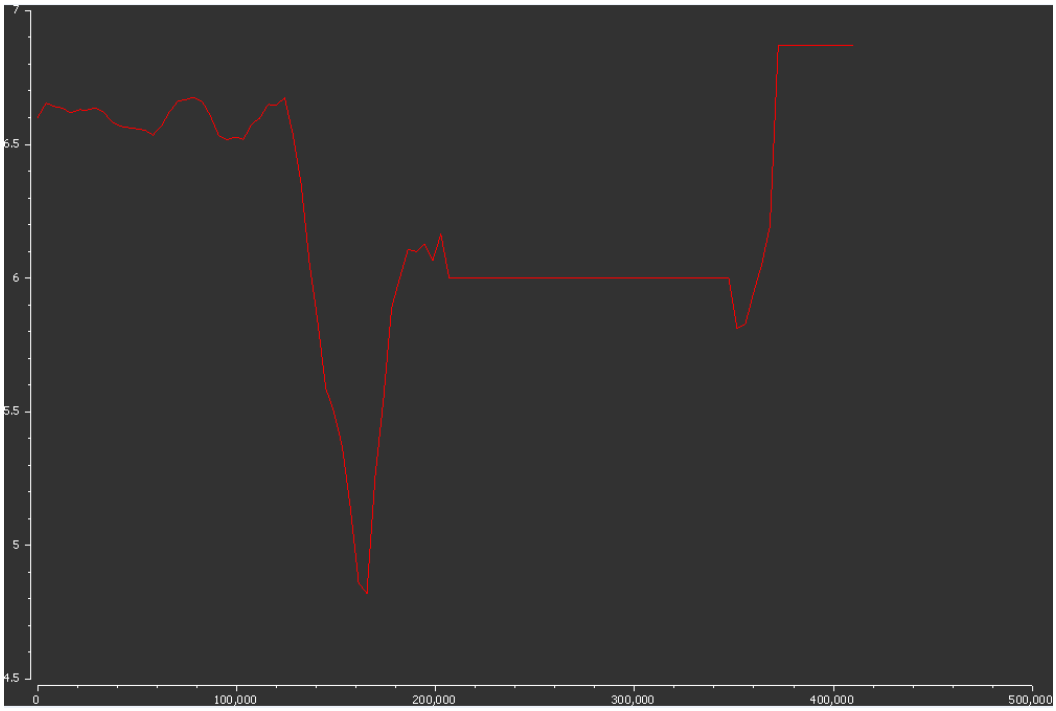
با توجه به روش‌های نفوذ و انتشار این باج‌افزار، اکیداً توصیه می‌کنیم که سیستم‌عامل‌های خود، مخصوصاً نسخه‌های نصب بر روی سرورها را با وصله‌های امنیتی ارایه شده برای آسیب‌پذیری‌های ذکر شده در بالا، به روز رسانی کنید.

همچنین توصیه می‌شود اقدامات مربوط به امن‌سازی RDP را به طور کامل بر روی سیستم‌های خود انجام دهید و نرم‌افزارهای امنیتی نصب شده درون سیستم عامل خود نظیر آنتی ویروس را، به طور مداوم به روز رسانی کنید.

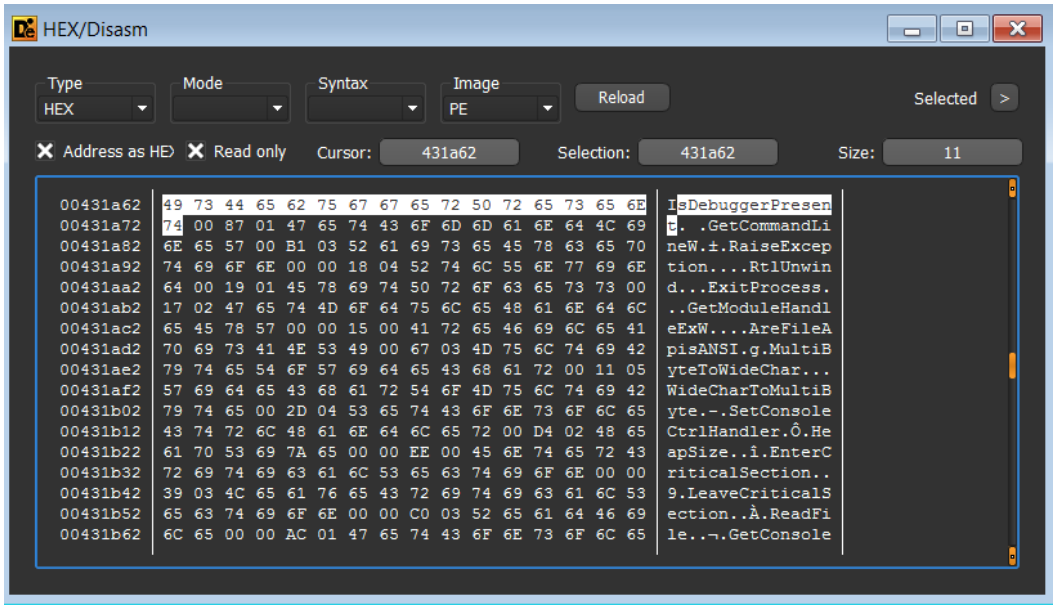
٦. تحلیل ایستا

٦-١ تحلیل کد

آنتروپی بالای نمونه فایل تحلیل شده در آزمایشگاه نشان می‌دهد که در کدنویسی این باج‌افزار به شدت از تکنیک‌های مبهم‌سازی (Obfuscation) استفاده شده است.



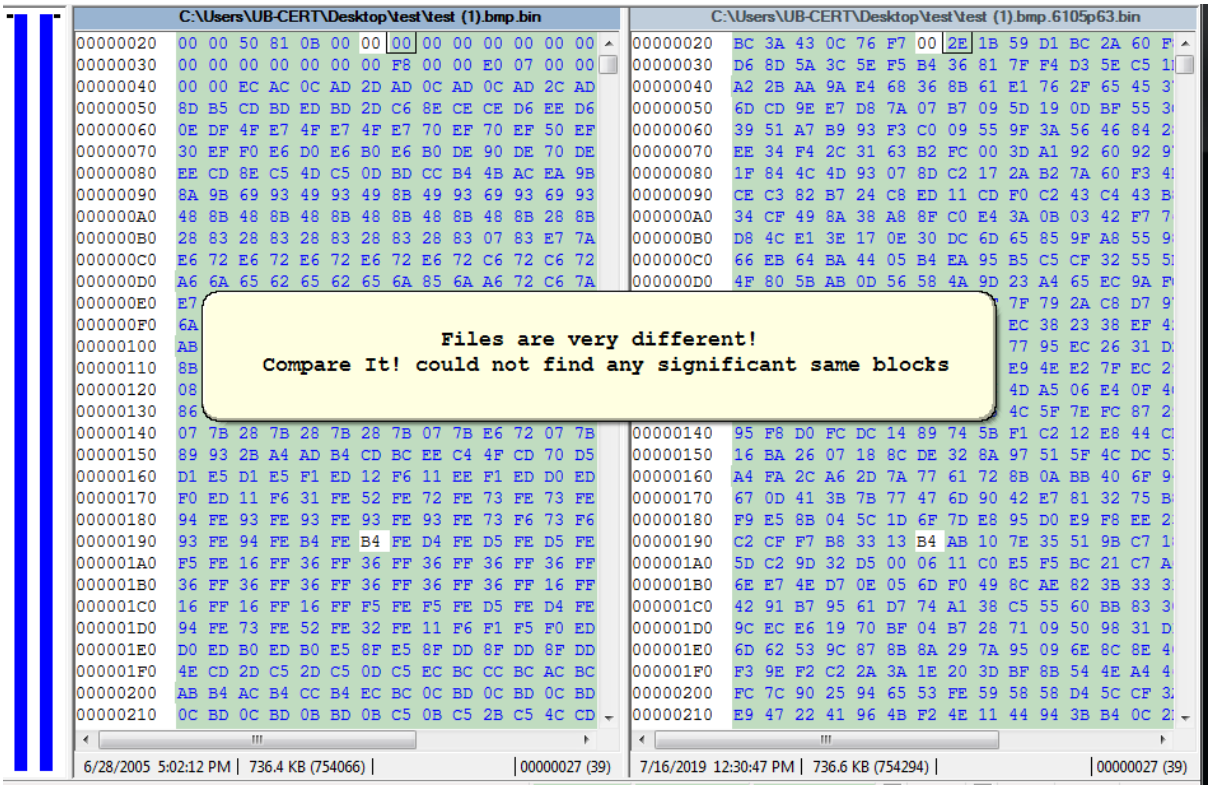
بررسی‌ها بر روی فایل اجرایی این باج‌افزار نشان می‌دهد که توسعه‌دهندگان آن برای جلوگیری تحلیل کد توسط تحلیلگران بدافزار، از تکنیک‌های ضد مهندسی معکوس نیز استفاده کرده‌اند. حضور تابع IsDebuggerPresent گواهی بر این مسأله است:

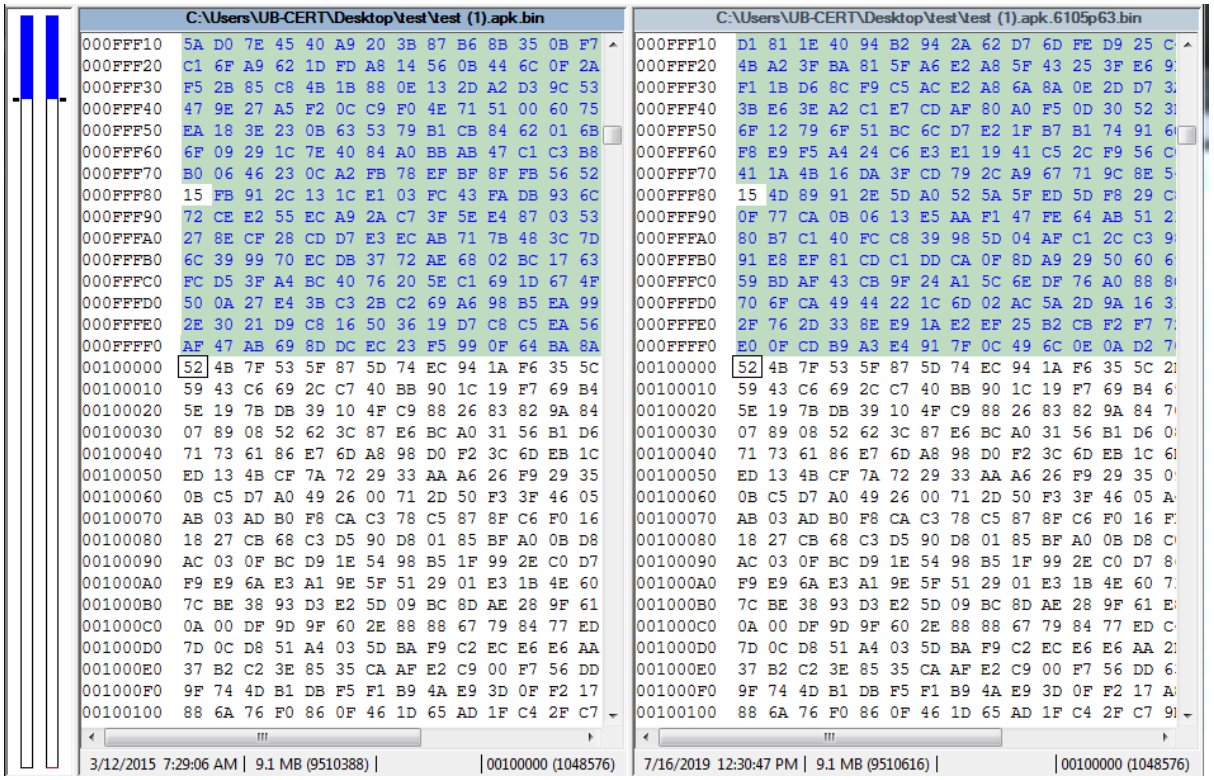


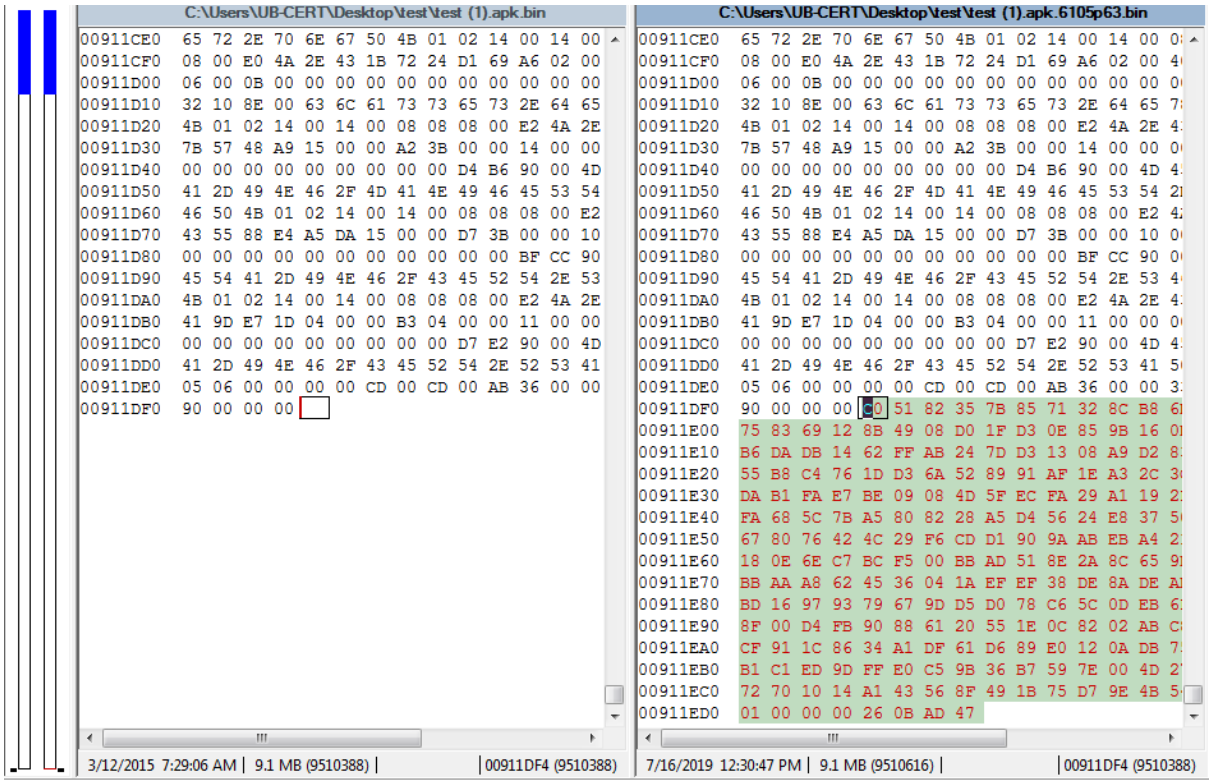
باج‌افزار Sodinokibi، از کتابخانه‌ای به نام winhttp.dll برای ارسال و دریافت درخواست‌های http بهره می‌برد. این کتابخانه در لیست سیاه قرار دارد.

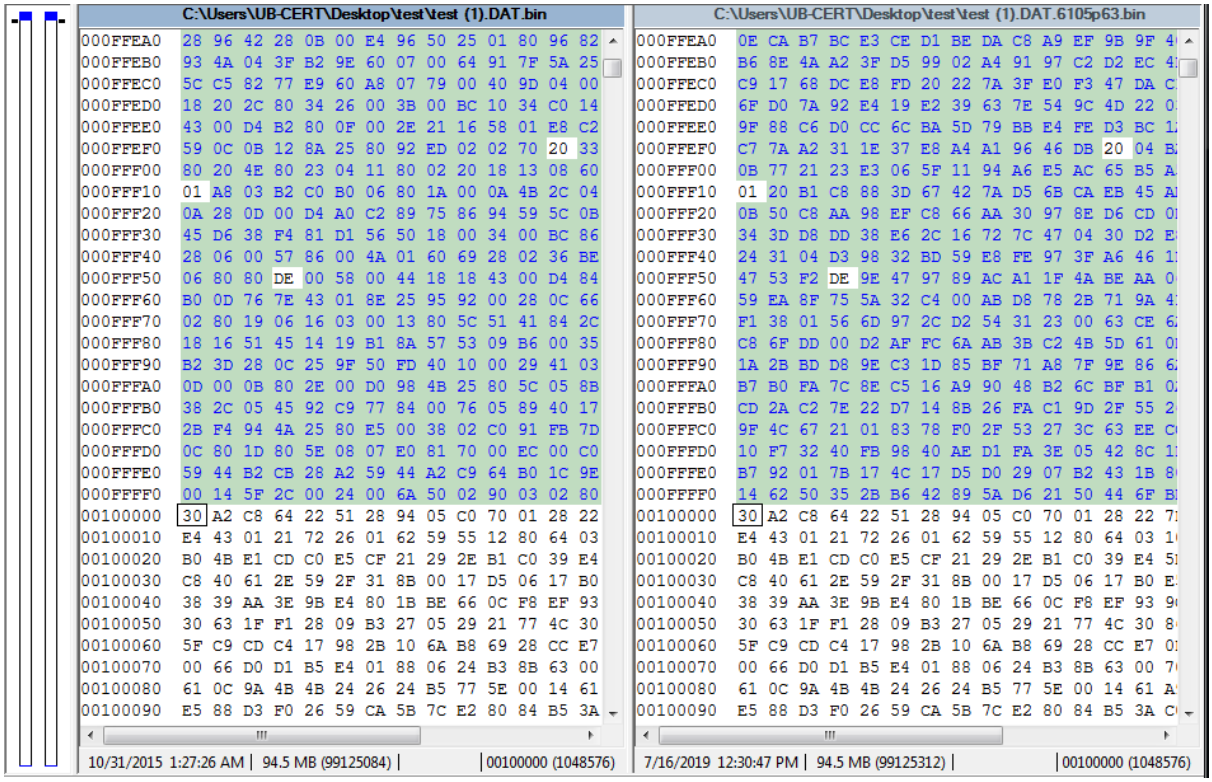
library (3)	blacklist (1)	type (1)	imports (112)	description
winhttp.dll	x	implicit	5	Windows HTTP Services
kernel32.dll	-	implicit	94	Windows NT BASE API Client DLL
advapi32.dll	-	implicit	13	Advanced Windows 32 Base API

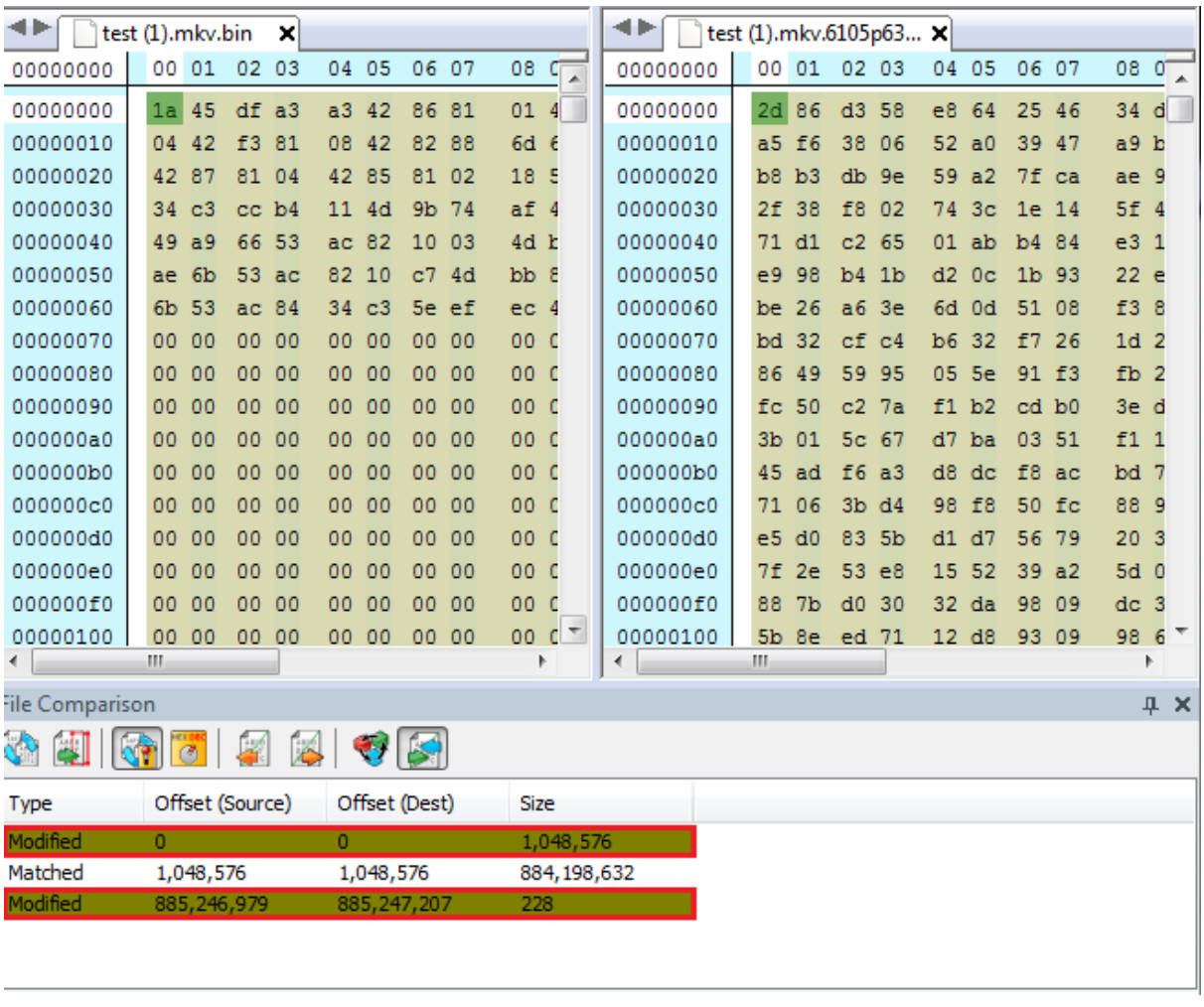
بررسی نمونه فایل‌های رمزشده با نمونه سالم آن‌ها نشان می‌دهد که این باج‌افزار، از الگویی مشابه با باج‌افزار GandCrab جهت رمزگشایی فایل‌های مورد نظر خود بهره می‌برد. Sodinokibi نیز همانند GandCrab فقط یک مگابایت اول هر فایل را رمزگذاری می‌کند و به انتهای آن‌ها ۲۲۸بایت اضافه می‌کند. تصاویر زیر، مقایسه چند نمونه فایل سالم با نمونه رمز شده آن‌ها را نشان می‌دهد:




C:\Users\UB-CERT\Desktop\test\test (1).apk.bin
C:\Users\UB-CERT\Desktop\test\test (1).apk.6105p63.bin
3/12/2015 7:29:06 AM | 9.1 MB (9510388) | 00100000 (1048576)
7/16/2019 12:30:47 PM | 9.1 MB (9510616) | 00100000 (1048576)


C:\Users\UB-CERT\Desktop\test\test (1).apk.bin
C:\Users\UB-CERT\Desktop\test\test (1).apk.6105p63.bin
3/12/2015 7:29:06 AM | 9.1 MB (9510388) | 00911DF4 (9510388)
7/16/2019 12:30:47 PM | 9.1 MB (9510616) | 00911DF4 (9510388)


C:\Users\UB-CERT\Desktop\test\test (1).DAT.bin
C:\Users\UB-CERT\Desktop\test\test (1).DAT.6105p63.bin
10/31/2015 1:27:26 AM | 94.5 MB (99125084) | 00100000 (1048576)
7/16/2019 12:30:47 PM | 94.5 MB (99125312) | 00100000 (1048576)


test (1).mkv.bin
test (1).mkv.6105p63...
File Comparison
Type | Offset (Source) | Offset (Dest) | Size
Modified | 0 | 0 | 1,048,576
Matched | 1,048,576 | 1,048,576 | 884,198,632
Modified | 885,246,979 | 885,247,207 | 228

۲-۶ تحلیل ترافیک شبکه:

با بررسی‌های صورت گرفته بر روی ترافیک ضبط شده در حین فعالیت باج‌افزار Sodinokibi مشخص گردید که این باج‌افزار با تعداد بسیار زیادی آدرس آی‌پی و دامنه ارتباط برقرار می‌کند. احتمالا از الگوریتم تولید دامنه تصادفی (DGA) در کد خود بهره برده است. باج‌افزارها از این ترفند برای عدم شناسایی آدرس اصلی سرور فرمان و کنترل خود، استفاده می‌کنند. تقریبا تمام ترافیک شبکه این باج‌افزار بر روی پورت 443 قرار دارد و ارتباطات آن از طریق پروتکل TCP برقرار می‌گردد.

لیست آی‌پی های شناسایی شده :	لیست درخواست‌های DNS :
148.251.11.181	*90nguyentuan.com*
78.142.209.221	*a-zpaperwork.eu*
50.97.149.92	*advancedeyecare.com*
46.243.156.72	*agendatwentytwenty.com*
197.221.14.44	*alattekniksipil.com*
46.30.215.77	*alene.co*
209.182.203.153	*alharsunindo.com*
67.20.76.129	*alisodentalcare.com*
178.63.89.23	*alnectus.com*
87.98.154.146	*andreaskildegaard.dk*
210.245.90.240	*annida.it*
77.104.162.69	*aquacheck.co.za*
95.216.117.200	*arearugcleaningnyc.com*
150.95.54.240	*astrographic.com*
96.127.180.186	*atma.nl*
198.46.89.70	*atrgroup.it*
46.30.215.168	*avisioninthedesert.com*
5.152.193.244	*banukumbak.com*
74.208.236.75	*baptistdistinctives.org*
52.174.40.218	*bayshoreelite.com*
198.71.233.104	*beauty-traveller.com*
81.19.215.5	*belinda.af*
35.228.55.150	*belofloripa.be*
194.30.35.117	*benchbiz.com*
46.105.57.169	*berdonllp.com*
104.31.84.195	*biketruck.de*
104.31.85.195	*block-optic.com*
95.143.172.245	*blucamp.com*
91.195.240.87	*bluelakevision.com*
185.26.156.167	*bmw-i-pure-impulse.com*
69.89.31.228	*bonitabeachassociation.com*
46.30.215.111	*bourchier.org*
166.62.112.193	*brinkdoepke.eu*
198.50.129.250	*brownswoodblog.com*
192.163.232.100	*bruut.online*
69.164.206.96	*bundan.com*
104.27.165.36	*buzzneakers.com*
104.27.164.36	*bychowo.pl*
185.199.220.28	*cainlaw-okc.com*
141.138.169.215	*carmel-york.com*
192.0.78.151	*carsten.sparen-it.de*
192.0.78.245	*cascinarosa33.it*
51.68.89.43	*ceocenters.com*
184.173.96.66	*ciga-france.fr*
192.145.232.92	*citiscapes-art.com*
103.23.22.248	*citydogslife.com*
103.74.54.152	*cookinn.nl*

curtsdiscountguns.com	178.208.33.134
deduktia.fi	87.254.25.84
dentalcircle.com	104.28.12.75
dentallabor-luenen.de	104.28.13.75
devus.de	217.182.126.186
direitapernambuco.com	109.73.237.93
dnqa.co.uk	185.2.4.123
domaine-des-pothiers.com	185.197.130.80
dreamvoiceclub.org	77.111.240.99
edrickennedymacfoy.com	162.241.217.111
egpu.fr	188.226.138.70
elex.is	70.40.217.80
elliemaccreative.wordpress.com	31.217.192.232
endlessrealms.net	74.80.196.90
enews-qca.com	178.249.187.226
epicjapanart.com	141.138.169.208
etgdogz.de	166.62.110.90
four-ways.com	212.49.100.165
frameмyballs.com	104.28.2.98
fsbforsale.com	104.28.3.98
fskhjalmar.se	185.15.78.186
go.labibini.ch	45.79.176.253
goeppinger-teppichreinigung.de	109.237.132.56
goodboyscustom.com	67.227.229.191
gosouldeep.com	45.76.155.31
guohedd.com	54.175.148.58
holocine.de	212.97.132.137
hostaletdelsindians.es	82.94.246.8
innovationgames-brabant.nl	79.137.39.123
irizar.com	185.197.128.45
janellrardon.com	87.230.47.47
jeanmonti.com	46.32.254.147
johnstonmingmanning.com	104.18.41.218
jollity.hu	104.18.40.218
kafkacare.com	217.160.0.95
kellengatton.com	104.25.215.14
ketomealprep.academy	104.25.214.14
kosten-vochtbestrijding.be	185.5.53.18
lagschools.ng	139.162.238.239
letsstopsmoking.co.uk	104.18.52.134
louiedager.com	104.18.53.134
lovcase.com	75.127.74.35
lyricalduniya.com	104.31.83.217
magnetvisual.com	104.31.82.217
manzel.tn	92.222.234.4
mariajosediazdemera.com	5.157.84.183
mayprogulka.ru	104.24.104.251
mensemetgesigte.co.za	104.24.105.251
michal-s.co.il	198.54.115.43
mieleshopping.it	185.33.54.16
molinum.pt	104.164.238.122
mslp.org	109.237.212.70
napisat-pismo-gubernatoru.ru	217.160.0.66
nationnewsroom.com	185.197.130.219
neolaiamedispa.com	134.119.253.108
nexstagefinancial.com	167.99.54.169
onesynergyinternational.com	94.23.87.17
onlinemarketingsurgery.co.uk	104.31.77.205
opticahubertruiz.com	104.31.76.205
p-ride.live	185.103.16.188
perfectgrin.com	89.184.74.152
photographycreativity.co.uk	159.65.213.163
pilotgreen.com	188.165.129.145

placermonticello.com	104.18.57.174
pokemonturkiye.com	104.18.56.174
precisetemp.com	109.199.121.217
primemarineengineering.com	213.186.33.19
projektparkiet.pl	192.0.78.13
prometeyagro.com.ua	192.0.78.12
putzen-reinigen.com	103.27.206.14
pxsrl.it	139.162.224.28
qandmmusiccenter.com	37.97.209.126
racefietsenblog.nl	172.96.187.244
rattanwarehouse.co.uk	64.91.251.150
renehartman.nl	3.94.148.248
ronaldhendriks.nl	77.240.183.196
satoblog.org	149.255.59.10
schlagbohrmaschinetests.com	149.126.4.47
sellthewrightway.com	217.160.0.117
shortsalemap.com	37.97.189.11
skinkeeper.li	81.19.159.86
so-sage.fr	162.241.217.186
stabilisateur.fr	83.223.101.76
stanleyqualitysystems.com	69.87.221.76
stressreliefadvice.com	104.31.65.66
studionumerik.fr	104.31.64.66
subyard.com	45.32.222.156
sytzedevries.com	206.189.227.79
tanatek.com	89.234.180.47
tbalp.co.uk	104.248.116.172
thestudio.academy	37.128.144.114
thisprettyhair.com	138.201.182.133
tilldeeke.de	192.81.213.222
topautoinsurers.net	69.168.78.206
topvijesti.net	91.106.198.231
tothebackofthemoon.com	173.236.197.54
transifer.fr	77.72.1.86
triavlete.com	195.182.210.188
tweedekansenloket.nl	162.144.26.133
ultimatelifesource.com	207.180.243.156
wyreforest.net	104.27.187.170
yournextshoes.com	104.27.186.170
zdrowieszczecin.pl	104.27.139.197
zorgboerderijravensbosch.nl	104.27.138.197
	77.72.0.150
	217.70.186.111
	178.32.149.185
	162.144.17.96
	66.228.32.51
	104.18.61.24
	104.18.60.24
	159.65.212.229
	92.51.181.23

تصاویر زیر، بخشی از ترافیک ضبط شده این باج‌افزار را نشان می‌دهد.

Name	Local address	Local...	Remote address	Remote ...	Proto...	State
1.exe (3256)	WIN-LQOUEMDES...	49741	WIN-LQOUEMDESN0	8888	TCP	Establish...
1.exe (3256)	WIN-LQOUEMDES...	49759	96.127.180.186	443	TCP	SYN sent
1.exe (3256)	WIN-LQOUEMDES...	49760	192.145.232.92	443	TCP	Establish...
Fiddler.exe (3236)	WIN-LQOUEMDES...	8888			TCP	Listen
Fiddler.exe (3236)	WIN-LQOUEMDES...	8888	WIN-LQOUEMDESN0	49741	TCP	Establish...
Fiddler.exe (3236)	WIN-LQOUEMDES...	49742	13.107.4.50	80	TCP	Establish...
lsass.exe (504)	WIN-LQOUEMDES...	49155			TCP	Listen
lsass.exe (504)	WIN-LQOUEMDES...	49155			TCP6	Listen
services.exe (496)	WIN-LQOUEMDES...	49156			TCP	Listen
services.exe (496)	WIN-LQOUEMDES...	49156			TCP6	Listen

Capture Window | DNS Hex View

Time	Domain Requested	DNS Returned
13:52:47	egpu.fr	FOUND
13:52:47	egpu.fr	FOUND
13:52:48	onlinemarketingsurgery.co.uk	FOUND
13:52:48	onlinemarketingsurgery.co.uk	FOUND
13:52:48	napisat-pismo-gubernatoru.ru	FOUND
13:52:48	napisat-pismo-gubernatoru.ru	FOUND
13:52:49	holocine.de	FOUND
13:52:49	holocine.de	FOUND
13:52:50	mayprogulka.ru	FOUND
13:52:50	mayprogulka.ru	FOUND
13:52:50	advancedeyecare.com	FOUND

درخواست‌های DNS

File Edit Rules Tools View Help

Replay | Go | Stream | Decode | Keep: All sessions | Any Process | Find | Save | Browse | Clear Cache

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process
1	200	HTTP	Tunnel to	www.gstatic.com:443	0			chrome:...
2	200	HTTP	www.download.windowsupdate.com	/msdownload/update/v3/static/trustedr/en...	914	public,m...	application/...	1:3256

درخواست http باج‌افزار

1035	185.766469	192.168.29.128	166.62.110.90	TCP	54 49688 → 443 [ACK] Seq=59 Ack=2 Win=64240 Len=0
1036	185.766630	192.168.29.128	166.62.110.90	TCP	54 49688 → 443 [FIN, ACK] Seq=59 Ack=2 Win=64240 Len=0
1037	185.766891	166.62.110.90	192.168.29.128	TCP	60 443 → 49688 [ACK] Seq=2 Ack=60 Win=64239 Len=0
1040	185.947680	192.168.29.128	104.18.41.218	TCP	66 49689 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1041	186.086202	104.18.41.218	192.168.29.128	TCP	60 443 → 49689 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1042	186.086237	192.168.29.128	104.18.41.218	TCP	54 49689 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1043	186.086666	192.168.29.128	104.18.41.218	TLSv1	175 Client Hello
1044	186.086799	104.18.41.218	192.168.29.128	TCP	60 443 → 49689 [ACK] Seq=1 Ack=122 Win=64240 Len=0
1046	186.238734	104.18.41.218	192.168.29.128	TLSv1	1454 Server Hello
1047	186.248328	104.18.41.218	192.168.29.128	TCP	1454 443 → 49689 [PSH, ACK] Seq=1401 Ack=122 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
1048	186.248367	192.168.29.128	104.18.41.218	TCP	54 49689 → 443 [ACK] Seq=122 Ack=2801 Win=64240 Len=0
1049	186.250228	104.18.41.218	192.168.29.128	TCP	1454 443 → 49689 [PSH, ACK] Seq=2801 Ack=122 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
1050	186.256205	104.18.41.218	192.168.29.128	TLSv1	1088 Certificate, Server Key Exchange, Server Hello Done
1051	186.256236	192.168.29.128	104.18.41.218	TCP	54 49689 → 443 [ACK] Seq=122 Ack=5235 Win=64240 Len=0
1052	186.262849	192.168.29.128	104.18.41.218	TLSv1	188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1053	186.263027	104.18.41.218	192.168.29.128	TCP	60 443 → 49689 [ACK] Seq=5235 Ack=256 Win=64240 Len=0
1054	186.398398	104.18.41.218	192.168.29.128	TLSv1	113 Change Cipher Spec, Encrypted Handshake Message
1055	186.459237	192.168.29.128	104.18.41.218	TLSv1	363 Application Data
1056	186.459317	192.168.29.128	104.18.41.218	TLSv1	987 Application Data
1057	186.459437	104.18.41.218	192.168.29.128	TCP	60 443 → 49689 [ACK] Seq=5294 Ack=565 Win=64240 Len=0
1058	186.459438	104.18.41.218	192.168.29.128	TCP	60 443 → 49689 [ACK] Seq=5294 Ack=1498 Win=64240 Len=0
1063	190.049407	104.18.41.218	192.168.29.128	TLSv1	1451 Application Data
1064	190.049882	192.168.29.128	104.18.41.218	TCP	54 49689 → 443 [RST, ACK] Seq=1498 Ack=6691 Win=0 Len=0
1067	190.388011	192.168.29.128	89.234.180.47	TCP	66 49690 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1068	190.527210	89.234.180.47	192.168.29.128	TCP	60 443 → 49690 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1069	190.527252	192.168.29.128	89.234.180.47	TCP	54 49690 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1070	190.527852	192.168.29.128	89.234.180.47	TLSv1	165 Client Hello

۳-۶ رمزگشایی:

تاکنون، هیچ‌گونه ابزاری جهت رمزگشایی این باج‌افزار ارایه نشده است.