

باسمه تعالی

تحلیل فنی باج افزار

**Sodinokibi**

## فهرست مطالب

۱. مقدمه : ..... ۳
۲. مشخصات فایل اجرایی : ..... ۳
۳. شجره‌نامه ..... ۴
۴. میزان تهدید فایل باج‌افزار: ..... ۴
۵. تحلیل پویا ..... ۴
- ۵-۱ آناتومی حمله: ..... ۴
- ۵-۲ روش انتشار: ..... ۱۴
- ۵-۳ روش جلوگیری: ..... ۱۴
- ۶- تحلیل ایستا ..... ۱۵
- ۶-۱ تحلیل کد: ..... ۱۵
- ۶-۲ تحلیل ترافیک شبکه: ..... ۱۹
- ۶-۳ رمزگشایی: ..... ۲۳

## 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.

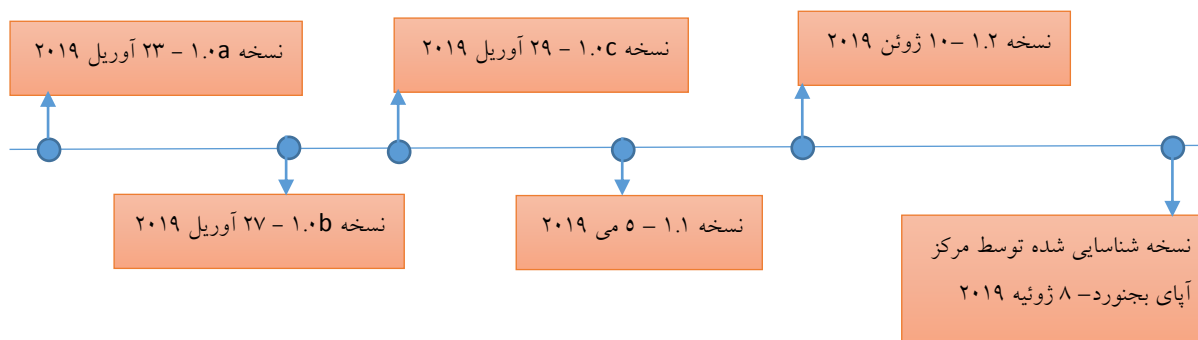
## ۲. مشخصات فایل اجرایی :

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

فایل اجرایی این باج‌افزار دارای ۸ بخش است :

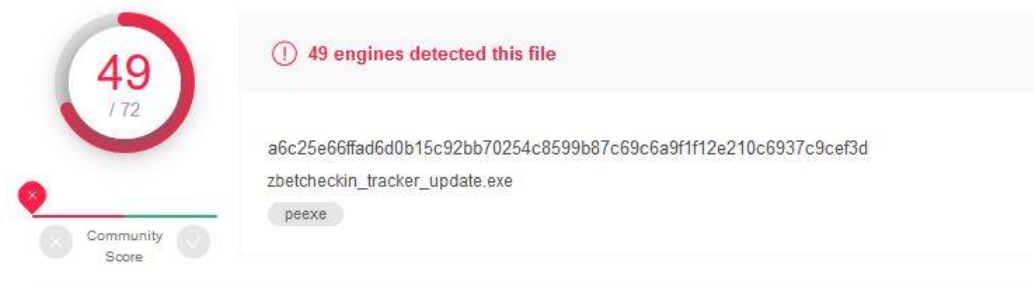
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۷۳	۴۰۹۶	۱۵۷۰۰۵	۱۵۷۱۸۴
.rdata	۵.۰۹	۱۶۳۸۴۰	۴۰۸۰۴	۴۰۹۶۰
.data	۳.۲۶	۲۰۴۸۰۰	۸۴۰۴۶۷۲	۷۱۶۸
.text	۶	۸۶۰۹۷۹۲	۱۸۲۳۶۰	۱۸۲۷۸۴
.gibohol	۰	۸۷۹۴۱۱۲	۱۰۲۴	۱۰۲۴
.raxoduw	۰	۸۷۹۸۲۰۸	۶۱۴۴	۲۵۶۰
.rsrc	۵.۰۹	۸۸۰۶۴۰۰	۱۱۹۸۴	۱۲۲۸۸
.reloc	۶.۵۷	۸۸۱۸۶۸۸	۸۴۳۲	۸۷۰۴

### ۳. شجره نامه



### ۴. میزان تهدید فایل باج افزار

در حال حاضر تعداد ۴۹ مورد از ۷۲ ضدباج افزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج افزار می باشند.



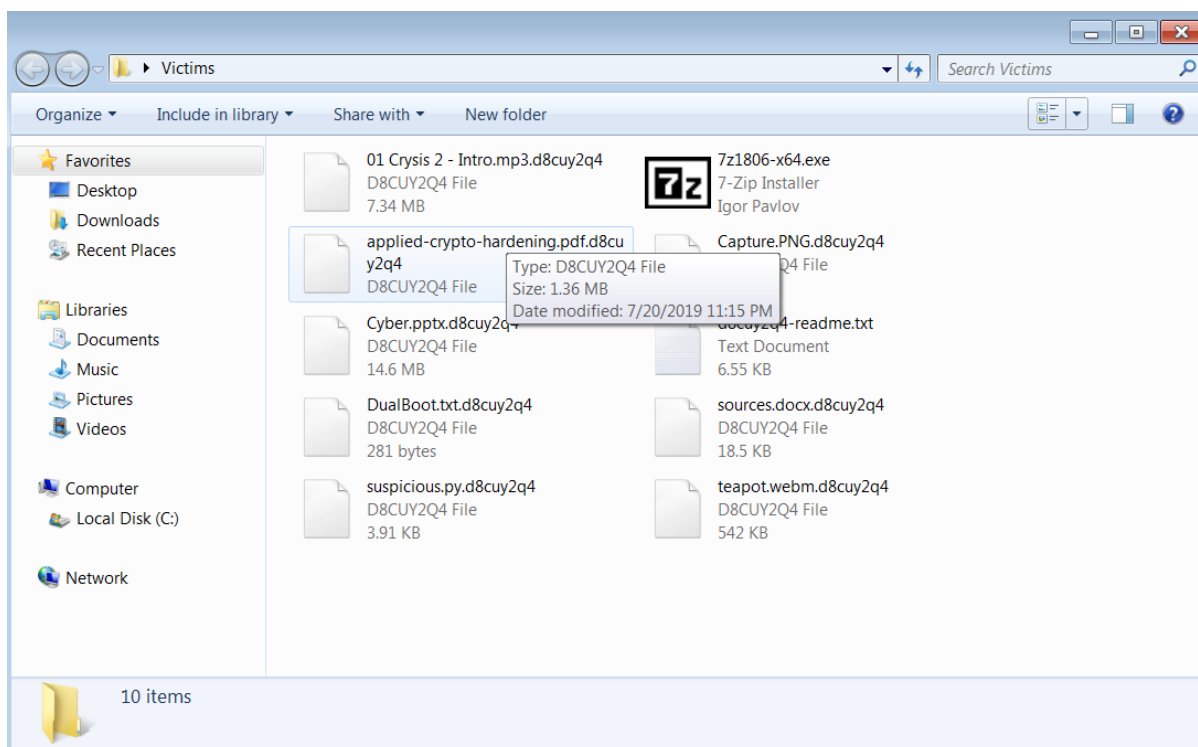
### ۵. تحلیل پویا

#### ۱-۵ آناتومی حمله

طبق بررسی های صورت گرفته، باج افزار Sodinokibi به محض شروع فعالیت در سیستم قربانی، دستورات زیر را در محیط خط فرمان ویندوز اجرا می کند:

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

سپس شروع به جست و جو و رمزگذاری فایل های مورد نظر خود در سیستم قربانی می کند. فایل های سیستم قربانی پس از رمزگذاری، به شکل زیر تغییر پیدا می کنند:



پس از چند بار اجرا و بررسی های متوالی، متوجه شدیم پسوندی که به انتهای هر فایل اضافه می شود کاملاً تصادفی بوده و این پسوند به ابتدای فایل متنی پیغام باج خواهی باج افزار، اضافه می شود. این فایل درون هر پوشه حاوی فایل های رمز شده قرار می گیرد. این باج افزار قدرتمند، تمام فایل های موجود در سیستم قربانی با هر نام و پسوند، به غیر از فایل های سیستمی و فایل های اجرایی با پسوند .exe. را رمزگذاری می کند. فایل متنی پیغام باج خواهی این باج افزار با عنوان readme.txt- (پسوند تصادفی) به صورت زیر می باشد:

```
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://ap1ebzu47wgazapdqks6vrcv6zcnjppkxbr6wketf56nf6aq2nmyoyd.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

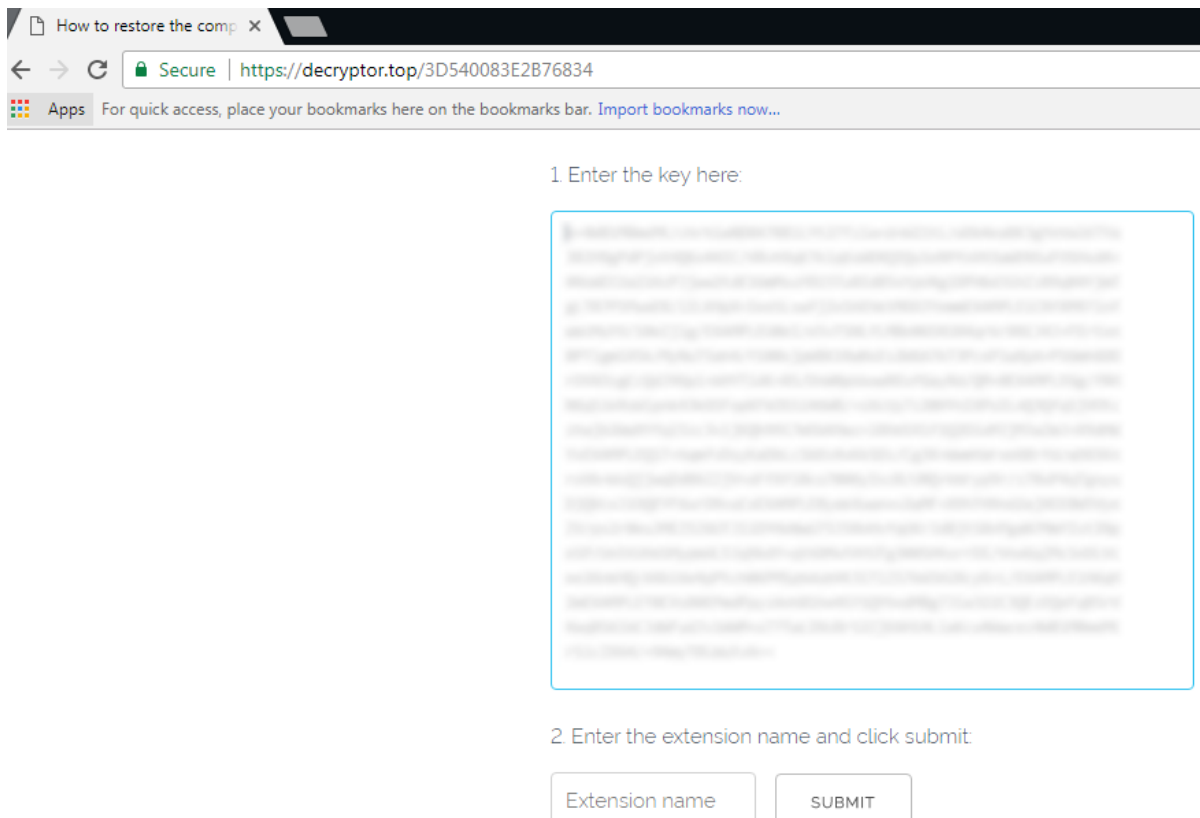
warning: secondary website can be blocked, thats why first variant much better and more available.
when you open our website, put the following data in the input form:
Key:
[Blurred Key]

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 damage 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.
!!! !!! !!!
```

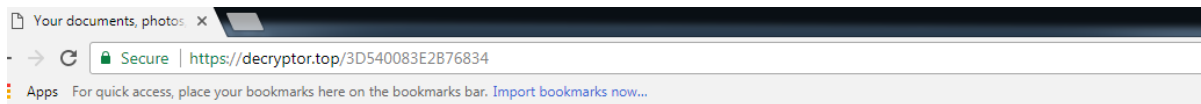
همانطور که در پیغام باج‌خواهی این باج‌افزار مشخص است، ابتدا به قربانی اطلاع داده شده که تمام فایل‌های موجود در سیستم رمزگذاری شده است و تنها راه بازیابی آن‌ها، انجام دستورالعمل‌های ارائه شده در پیغام باج‌خواهی می‌باشد. سپس عنوان شده است که جهت اعتماد و تضمین رمزگشایی فایل‌ها، قربانی باید از پرتال طراحی شده توسط مهاجم بازدید کند و در آنجا می‌تواند یک فایل را طبق قواعد ارائه 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، Chrome 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:



## Your computer has been infected!



Your documents, photos, databases and other important files encrypted



To decrypt your files you need to buy our special software - 8ad94tav-Decryptor



You can do it right now. Follow the instructions below. But remember that you do not have much time

### 8ad94tav-Decryptor price

You have **3 days, 23:58:39**

\* If you do not pay on time, the price will be doubled

\* Time ends on Jul 20, 06:54:03

Current price **0.03737162 BTC**  
≈ 400 USD

After time ends **0.07474324 BTC**  
≈ 800 USD

Bitcoin address: 34NEU6q5obm53NoknU2oXSPgCdWg83i37

\* BTC will be recalculated in 5 hours with an actual rate.

این صفحه، صفحه اصلی پرتال جهت راهنمایی قربانیان برای پرداخت باج می باشد. همانطور که قابل مشاهده است مبلغ ۰.۰۳۷ بیت کوین معادل ۴۰۰ دلار برای رمزگشایی فایل ها در نظر گرفته شده است که قربانی باید آن را حداکثر در مدت زمان ۴ روز پرداخت نماید. در غیر این صورت، مبلغ باج به دو برابر یعنی ۰.۰۷۴ بیت کوین معادل ۸۰۰ دلار افزایش می یابد. آدرس کیف پول مهاجم نیز در زیر مهلت مشخص شده برای پرداخت هزینه رمزگشایی، قرار داده شده است.



## How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

To decrypt your files you need to buy our special software - 8ad94tav-Decryptor.

\* If you need guarantees, use trial decryption below.

## How to buy 8ad94tav-Decryptor?

- 1 Create a Bitcoin Wallet (we recommend [Blockchain.info](#))
  - 2 Buy necessary amount of Bitcoins. Current price for buying is **0.03737162 BTC**
  3. Send **0.03737162 BTC** to the following Bitcoin address:  
**34NEU6q5obm53NoKnU2otXSPgCdWg83t37**
- \* This receiving address was created for you, to identify your transactions
- 4 Wait for **3** confirmations
  - 5 Reload current page after, and get a link to download *8ad94tav-Decryptor*

## Trial decryption

Upload your file for test *8ad94tav-Decryptor*.

\* This file should be an encrypted image. Example

- o your-file-name.jpg.8ad94tav
- o your-file-name.png.8ad94tav
- o your-file-name.gif.8ad94tav

\* This file should be an encrypted image.

Browse...

## Buy Bitcoins with Bank Account or Bank Transfer

- o [Coinmama](#)
- o [Korbit](#)
- o [Coinfloor](#)
- o [Coinfinity](#)
- o [BitPanda](#)
- o [BTCDirect](#)

## Buy Bitcoin with Credit/Debit Card

- o [CEX.io](#)
- o [CoinMama](#)
- o [Huobi](#)
- o [Bittylicious](#)
- o [BitPanda](#)
- o [CoinCafe](#)

## Buy Bitcoins with PayPal

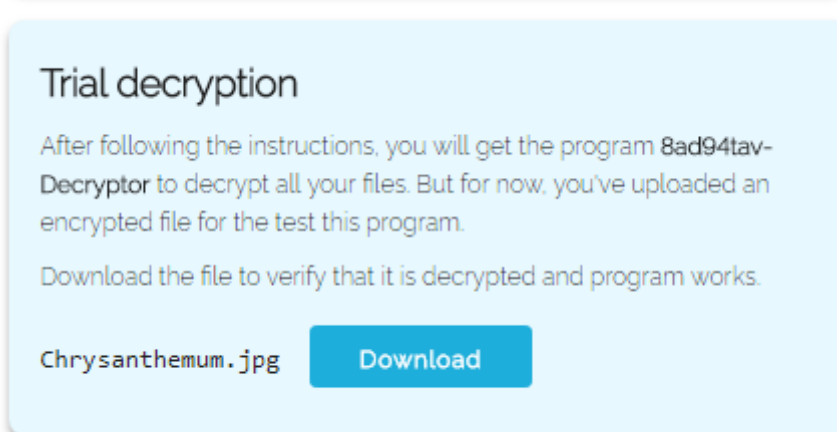
- o [LocalBitcoins](#)
- o [VirWoX](#)

## Buy Bitcoins with Cash or Cash Deposit

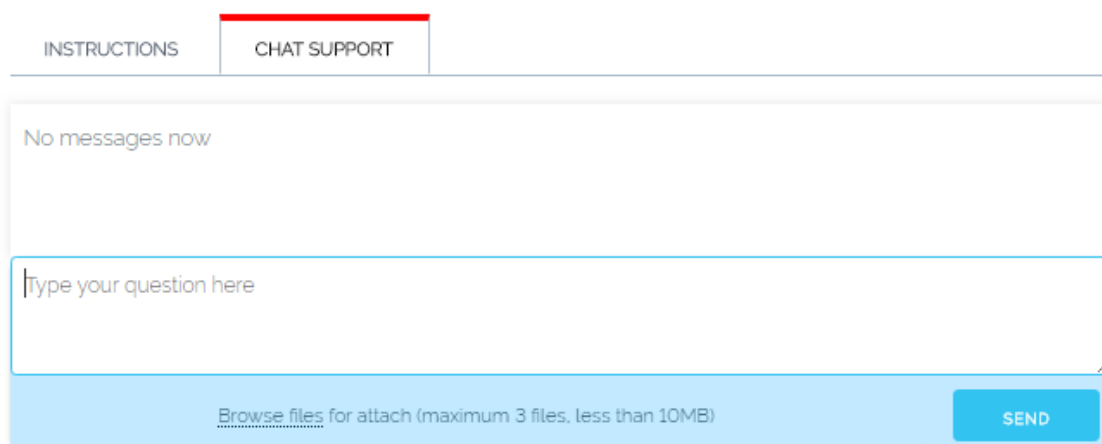
- o [LocalBitcoins](#)
- o [BitQuick](#)
- o [Wall of Coins](#)
- o [LibertyX](#)
- o [Bitit](#)
- o [Coin ATM Radar](#)

تصویر بالا، مربوط به ادامه محتوای پرتال می باشد. ستون سمت راست تصویر، روش های مختلف تهیه بیت کوین را نشان می دهد که برای راهنمایی قربانی قرار داده شده است. سمت چپ تصویر نیز، دستورالعمل رمزگشایی فایل ها، به طور کامل برای قربانی توضیح داده شده است. همچنین قسمتی برای رمزگشایی رایگان یک فایل، با پسوندهای png, jpg, 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 می باشد:



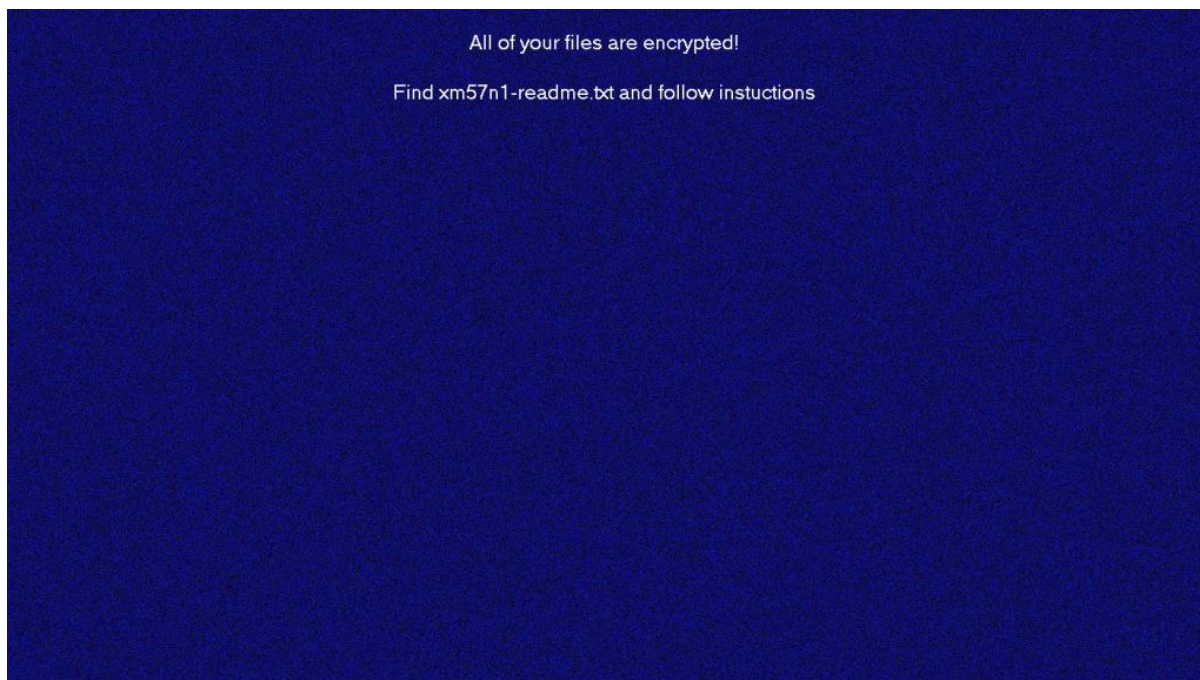
قابلیت گفتگو با مهاجمین نیز درون این پرتال گنجانده شده است تا قربانیان از طریق آن بتوانند با مهاجمین ارتباط برقرار کنند. تصویر زیر مربوط به این قسمت می باشد:



\* Current price 0.03737162 btc will be doubled in

3 days, 23:56:25

همزمان با اتمام رمزگذاری فایل ها، صفحه نمایش سیستم قربانی، به شکل زیر تغییر پیدا می کند:



این باج افزار، پس از پایان کار خود، همچنان به صورت فعال در سیستم قربانی باقی می ماند. تغییرات رجیستری ایجاد شده توسط باج افزار در طول فعالیت در سیستم قربانی نیز، به صورت زیر می باشد:

```
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\ehereg.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 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\ehereg.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-P0S2R009SN8R}\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

## ۲-۵ 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 ارائه 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 ارائه 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 گزارشی مبنی بر انتشار باج‌افزار Sodinokibi از طریق حمله Brute Force بر روی پروتکل RDP نیز به ثبت رسیده است.

## ۳-۵ روش جلوگیری:

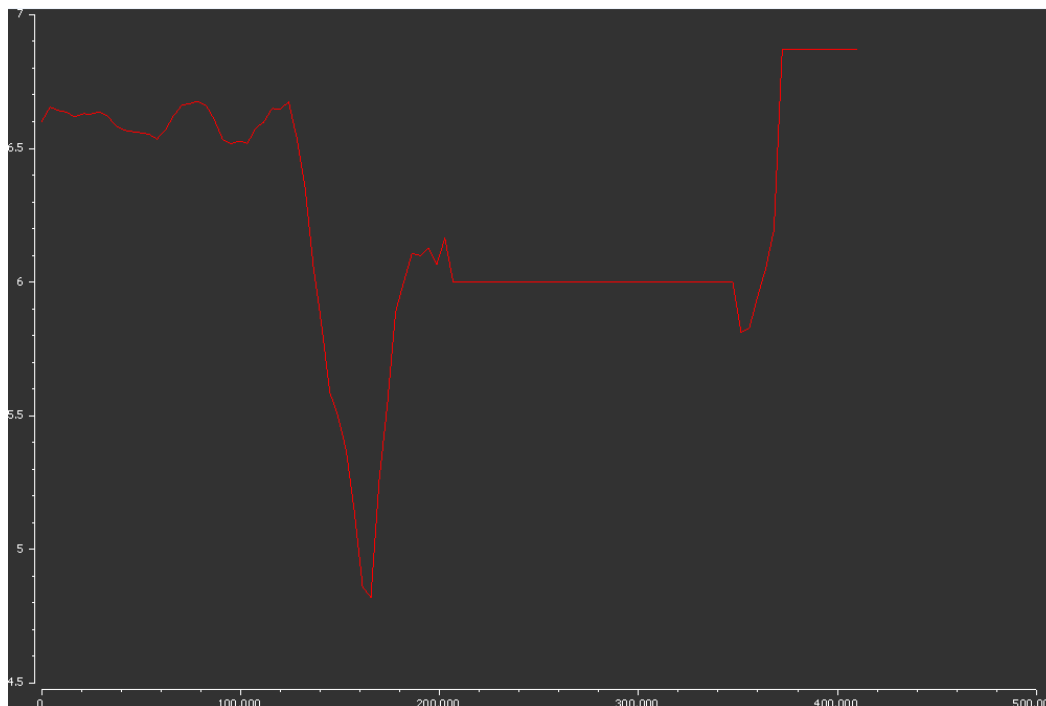
با توجه به روش‌های نفوذ و انتشار این باج‌افزار، اکیداً توصیه می‌کنیم که سیستم‌عامل‌های خود، مخصوصاً نسخه‌های نصب بر روی سرورها را با وصله‌های امنیتی ارائه شده برای آسیب‌پذیری‌های ذکر شده در بالا، به روز رسانی کنید.

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.

## ۶. تحلیل ایستا

### ۶-۱ 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 از تحلیل کد توسط تحلیلگران بدافزار، از تکنیک‌های ضد مهندسی معکوس نیز استفاده کرده‌اند. حضور تابع `IsDebuggerPresent` گواهی بر این مسأله است:

```

00431a62 49 73 44 65 62 75 67 67 65 72 50 72 65 73 65 6E IsDebuggerPresen
00431a72 74 00 87 01 47 65 74 43 6F 6D 6D 61 6E 64 4C 69
00431a82 6E 65 57 00 B1 03 52 61 69 73 65 45 78 63 65 70
00431a92 74 69 6F 6E 00 00 18 04 52 74 6C 55 6E 77 69 6E
00431aa2 64 00 19 01 45 78 69 74 50 72 6F 63 65 73 73 00
00431ab2 17 02 47 65 74 4D 6F 64 75 6C 65 48 61 6E 64 6C
00431ac2 65 45 78 57 00 00 15 00 41 72 65 46 69 6C 65 41
00431ad2 70 69 73 41 4E 53 49 00 67 03 4D 75 6C 74 69 42
00431ae2 79 74 65 54 6F 57 69 64 65 43 68 61 72 00 11 05
00431af2 57 69 64 65 43 68 61 72 54 6F 4D 75 6C 74 69 42
00431b02 79 74 65 00 2D 04 53 65 74 43 6F 6E 73 6F 6C 65
00431b12 43 74 72 6C 48 61 6E 64 6C 65 72 00 D4 02 48 65
00431b22 61 70 53 69 7A 65 00 00 EE 00 45 6E 74 65 72 43
00431b32 72 69 74 69 63 61 6C 53 65 63 74 69 6F 6E 00 00
00431b42 39 03 4C 65 61 76 65 43 72 69 74 69 63 61 6C 53
00431b52 65 63 74 69 6F 6E 00 00 C0 03 52 65 61 64 46 69
00431b62 6C 65 00 00 AC 01 47 65 74 43 6F 6E 73 6F 6C 65
  
```

باج افزار 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 رمز شده 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 ۲۲۸ بایت اضافه می‌کند. تصاویر زیر، مقایسه چند نمونه فایل سالم با نمونه رمز شده آن‌ها را نشان می‌دهد:

The screenshot displays a file comparison interface. On the left, the file 'C:\Users\UB-CERT\Desktop\test\test (1).bmp.bin' is open, showing a hex dump starting with '00 00 50 81 0B 00 00 00'. On the right, the file 'C:\Users\UB-CERT\Desktop\test\test (1).bmp.6105p63.bin' is open, showing a hex dump starting with 'BC 3A 43 0C 76 F7 00 2E'. A yellow dialog box in the center of the comparison area contains the text: 'Files are very different! Compare It! could not find any significant same blocks'. The status bar at the bottom shows the file sizes and positions: 736.4 KB (754066) for the left file and 736.6 KB (754294) for the right file.



C:\Users\UB-CERT\Desktop\Vest\Vest (1).apk.bin	C:\Users\UB-CERT\Desktop\Vest\Vest (1).apk.6105p63.bin
000FFF10 5A D0 7E 45 40 A9 20 3B 87 B6 8B 35 0B F7	000FFF10 D1 81 1E 40 94 B2 94 2A 62 D7 6D FE D9 25 C
000FFF20 C1 6F A9 62 1D FD A8 14 56 0B 44 6C 0F 2A	000FFF20 4B A2 3F BA 81 5F A6 E2 A8 5F 43 25 3F E6 9
000FFF30 F5 2B 85 C8 4B 1B 88 0E 13 2D A2 D3 9C 53	000FFF30 F1 1B D6 8C F9 C5 AC E2 A8 6A 8A 0E 2D D7 3
000FFF40 47 9E 27 A5 F2 0C C9 F0 4E 71 51 00 60 75	000FFF40 3B E6 3E A2 C1 E7 CD AF 80 A0 F5 0D 30 52 3
000FFF50 EA 18 3E 23 0B 63 53 79 B1 CB 84 62 01 6B	000FFF50 6F 12 79 6F 51 BC 6C D7 E2 1F B7 B1 74 91 6
000FFF60 6F 09 29 1C 7E 40 84 A0 BB AB 47 C1 C3 B8	000FFF60 F8 E9 F5 A4 24 C6 E3 E1 19 41 C5 2C F9 56 C
000FFF70 B0 06 46 23 0C A2 FB 78 EF BF 8F FB 56 52	000FFF70 41 1A 4B 16 DA 3F CD 79 2C A9 67 71 9C 8E 5
000FFF80 15 FB 91 2C 13 1C E1 03 FC 43 FA DB 93 6C	000FFF80 15 4D 89 91 2E 5D A0 52 5A 5F ED 5D F8 29 C
000FFF90 72 CE E2 55 EC A9 2A C7 3F 5E E4 87 03 53	000FFF90 0F 77 CA 0B 06 13 E5 AA F1 47 FE 64 AB 51 2
000FFFA0 27 8E CF 28 CD D7 E3 EC AB 71 7B 48 3C 7D	000FFFA0 80 B7 C1 40 FC C8 39 98 5D 04 AF C1 2C C3 9
000FFFB0 6C 39 99 70 EC DB 37 72 AE 68 02 BC 17 63	000FFFB0 91 E8 EF 81 CD C1 DD CA 0F 8D A9 29 50 60 6
000FFFC0 FC D5 3F A4 BC 40 76 20 5E C1 69 1D 67 4F	000FFFC0 59 BD AF 43 CB 9F 2A 41 5C 6E DF 76 A0 88 8
000FFFD0 50 0A 27 E4 3B C3 2B C2 69 A6 98 B5 EA 99	000FFFD0 70 6F CA 49 44 22 1C 6D 02 AC 5A 2D 9A 16 3
000FFFE0 2E 30 21 D9 C8 16 50 36 19 D7 C8 C5 EA 56	000FFFE0 2F 76 2D 33 8E E9 1A E2 EF 25 B2 CB F2 7
000FFFF0 AF 47 AB 69 8D DC EC 23 F5 99 0F 64 BA 8A	000FFFF0 E0 0F CD B9 A3 E4 91 7F 0C 49 6C 0E 0A D2 7
00100000 52 4B 7F 53 5F 87 5D 74 EC 94 1A F6 35 5C	00100000 52 4B 7F 53 5F 87 5D 74 EC 94 1A F6 35 5C 2
00100010 59 43 C6 69 2C C7 40 BB 90 1C 19 F7 69 B4	00100010 59 43 C6 69 2C C7 40 BB 90 1C 19 F7 69 B4 6
00100020 5E 19 7B DB 39 10 4F C9 88 26 83 82 9A 84	00100020 5E 19 7B DB 39 10 4F C9 88 26 83 82 9A 84 7
00100030 07 89 08 52 62 3C 87 E6 BC A0 31 56 B1 D6	00100030 07 89 08 52 62 3C 87 E6 BC A0 31 56 B1 D6 0
00100040 71 73 61 86 E7 6D A8 98 D0 F2 3C 6D EB 1C	00100040 71 73 61 86 E7 6D A8 98 D0 F2 3C 6D EB 1C 6
00100050 ED 13 4B CF 7A 72 29 33 AA A6 26 F9 29 35	00100050 ED 13 4B CF 7A 72 29 33 AA A6 26 F9 29 35 0
00100060 0B C5 D7 A0 49 26 00 71 2D 50 F3 3F 46 05	00100060 0B C5 D7 A0 49 26 00 71 2D 50 F3 3F 46 05 A
00100070 AB 03 AD B0 F8 CA C3 78 C5 87 8F C6 F0 16	00100070 AB 03 AD B0 F8 CA C3 78 C5 87 8F C6 F0 16 F
00100080 18 27 CB 68 C3 D5 90 D8 01 85 BF A0 0B D8	00100080 18 27 CB 68 C3 D5 90 D8 01 85 BF A0 0B D8 C
00100090 AC 03 0F BC D9 1E 54 98 B5 1F 99 2E C0 D7	00100090 AC 03 0F BC D9 1E 54 98 B5 1F 99 2E C0 D7 8
001000A0 F9 E9 6A E3 A1 9E 5F 51 29 01 E3 1B 4E 60	001000A0 F9 E9 6A E3 A1 9E 5F 51 29 01 E3 1B 4E 60 7
001000B0 7C BE 38 93 D3 E2 5D 09 BC 8D AE 28 9F 61	001000B0 7C BE 38 93 D3 E2 5D 09 BC 8D AE 28 9F 61 E
001000C0 0A 00 DF 9D 9F 60 2E 88 88 67 79 84 77 ED	001000C0 0A 00 DF 9D 9F 60 2E 88 88 67 79 84 77 ED C
001000D0 7D 0C D8 51 A4 03 5D BA F9 C2 EC E6 E6 AA 2	001000D0 7D 0C D8 51 A4 03 5D BA F9 C2 EC E6 E6 AA 2
001000E0 37 B2 C2 3E 85 35 CA AF E2 C9 00 F7 56 DD	001000E0 37 B2 C2 3E 85 35 CA AF E2 C9 00 F7 56 DD 6
001000F0 9F 74 4D B1 DB F5 F1 B9 4A E9 3D 0F F2 17	001000F0 9F 74 4D B1 DB F5 F1 B9 4A E9 3D 0F F2 17 A
00100100 88 6A 76 F0 86 0F 46 1D 65 AD 1F C4 2F C7	00100100 88 6A 76 F0 86 0F 46 1D 65 AD 1F C4 2F C7 9

C:\Users\UB-CERT\Desktop\Vest\Vest (1).apk.bin	C:\Users\UB-CERT\Desktop\Vest\Vest (1).apk.6105p63.bin
00911CE0 65 72 2E 70 6E 67 50 4B 01 02 14 00 14 00	00911CE0 65 72 2E 70 6E 67 50 4B 01 02 14 00 14 00 0
00911CF0 08 00 E0 4A 2E 43 1B 72 24 D1 69 A6 02 00 00	00911CF0 08 00 E0 4A 2E 43 1B 72 24 D1 69 A6 02 00 00 4
00911D00 06 00 0B 00 00 00 00 00 00 00 00 00 00 00	00911D00 06 00 0B 00 00 00 00 00 00 00 00 00 00 00 0
00911D10 32 10 8E 00 63 6C 61 73 73 65 73 2E 64 65	00911D10 32 10 8E 00 63 6C 61 73 73 65 73 2E 64 65 7
00911D20 4B 01 02 14 00 14 00 08 08 08 00 E2 4A 2E 4	00911D20 4B 01 02 14 00 14 00 08 08 08 00 E2 4A 2E 4
00911D30 7B 57 48 A9 15 00 00 A2 3B 00 00 14 00 00 00	00911D30 7B 57 48 A9 15 00 00 A2 3B 00 00 14 00 00 00 0
00911D40 00 00 00 00 00 00 00 00 00 D4 B6 90 00 4D	00911D40 00 00 00 00 00 00 00 00 D4 B6 90 00 4D 4
00911D50 41 2D 49 4E 46 2F 4D 41 4E 49 46 45 53 54	00911D50 41 2D 49 4E 46 2F 4D 41 4E 49 46 45 53 54 2
00911D60 46 50 4B 01 02 14 00 14 00 08 08 08 00 E2 4	00911D60 46 50 4B 01 02 14 00 14 00 08 08 08 00 E2 4
00911D70 43 55 88 E4 A5 DA 15 00 00 D7 3B 00 00 10 00	00911D70 43 55 88 E4 A5 DA 15 00 00 D7 3B 00 00 10 00 0
00911D80 00 00 00 00 00 00 00 00 00 00 BF CC 90	00911D80 00 00 00 00 00 00 00 00 00 BF CC 90 0
00911D90 45 54 41 2D 49 4E 46 2F 43 45 52 54 2E 53 4	00911D90 45 54 41 2D 49 4E 46 2F 43 45 52 54 2E 53 4
00911DA0 4B 01 02 14 00 14 00 08 08 08 00 E2 4A 2E 4	00911DA0 4B 01 02 14 00 14 00 08 08 08 00 E2 4A 2E 4
00911DB0 41 9D E7 1D 04 00 00 B3 04 00 00 11 00 00 00	00911DB0 41 9D E7 1D 04 00 00 B3 04 00 00 11 00 00 00 0
00911DC0 00 00 00 00 00 00 00 00 00 00 D7 E2 90 00 4D 4	00911DC0 00 00 00 00 00 00 00 00 00 D7 E2 90 00 4D 4
00911DD0 41 2D 49 4E 46 2F 43 45 52 54 2E 52 53 41 50	00911DD0 41 2D 49 4E 46 2F 43 45 52 54 2E 52 53 41 50
00911DE0 05 06 00 00 00 00 CD 00 CD 00 AB 36 00 00 00	00911DE0 05 06 00 00 00 00 CD 00 CD 00 AB 36 00 00 00 3
00911DF0 90 00 00 00 00 51 82 35 7B 85 71 32 8C B8 6	00911DF0 90 00 00 00 00 51 82 35 7B 85 71 32 8C B8 6
00911E00 75 83 69 12 8B 49 08 D0 1F D3 0E 85 9B 16 00	00911E00 75 83 69 12 8B 49 08 D0 1F D3 0E 85 9B 16 00 0
00911E10 B6 DA DB 14 62 FF AB 24 7D D3 13 08 A9 D2 8	00911E10 B6 DA DB 14 62 FF AB 24 7D D3 13 08 A9 D2 8
00911E20 55 B8 C4 76 1D D3 6A 52 89 91 AF 1E A3 2C 3	00911E20 55 B8 C4 76 1D D3 6A 52 89 91 AF 1E A3 2C 3
00911E30 DA B1 FA E7 BE 09 08 4D 5F EC FA 29 A1 19 2	00911E30 DA B1 FA E7 BE 09 08 4D 5F EC FA 29 A1 19 2
00911E40 FA 68 5C 7B A5 80 82 28 A5 D4 56 24 E8 37 5	00911E40 FA 68 5C 7B A5 80 82 28 A5 D4 56 24 E8 37 5
00911E50 67 80 76 42 4C 29 F6 CD D1 90 9A AB EB A4 2	00911E50 67 80 76 42 4C 29 F6 CD D1 90 9A AB EB A4 2
00911E60 18 0E 6E C7 BC F5 00 BB AD 51 8E 2A 8C 65 9	00911E60 18 0E 6E C7 BC F5 00 BB AD 51 8E 2A 8C 65 9
00911E70 BB AA A8 62 45 36 04 1A EF EF 38 DE 8A DE A	00911E70 BB AA A8 62 45 36 04 1A EF EF 38 DE 8A DE A
00911E80 BD 16 97 93 79 67 9D D5 D0 78 C6 5C 0D EB 6	00911E80 BD 16 97 93 79 67 9D D5 D0 78 C6 5C 0D EB 6
00911E90 8F 00 D4 FB 90 88 61 20 55 1E 0C 82 02 AB C	00911E90 8F 00 D4 FB 90 88 61 20 55 1E 0C 82 02 AB C
00911EA0 CF 91 1C 86 34 A1 DF 61 D6 89 E0 12 0A DB 7	00911EA0 CF 91 1C 86 34 A1 DF 61 D6 89 E0 12 0A DB 7
00911EB0 B1 C1 ED 9D FF E0 C5 9B 36 B7 59 7E 00 4D 2	00911EB0 B1 C1 ED 9D FF E0 C5 9B 36 B7 59 7E 00 4D 2
00911EC0 72 70 10 14 A1 43 56 8F 49 1B 75 D7 9E 4B 5	00911EC0 72 70 10 14 A1 43 56 8F 49 1B 75 D7 9E 4B 5
00911ED0 01 00 00 00 26 0B AD 47	00911ED0 01 00 00 00 26 0B AD 47

C:\Users\UB-CERT\Desktop\test\test (1).DAT.bin																C:\Users\UB-CERT\Desktop\test\test (1).DAT.6105p63.bin															
000FFFEA0	28	96	42	28	0B	00	E4	96	50	25	01	80	96	82	000FFFEA0	0E	CA	B7	BC	E3	CE	D1	BE	DA	C8	A9	EF	9B	9F	4	
000FFFE80	93	4A	04	3F	B2	9E	60	07	00	64	91	7F	5A	25	000FFFE80	B6	8E	4A	A2	3F	D5	99	02	A4	91	97	C2	D2	EC	4	
000FFFE60	5C	C5	82	77	E9	60	A8	07	79	00	40	9D	04	00	000FFFE60	C9	17	68	DC	E8	FD	20	22	7A	3F	E0	F3	47	DA	C	
000FFFE40	18	20	2C	80	34	26	00	3B	00	BC	10	34	C0	14	000FFFE40	6F	D0	7A	92	E4	19	E2	39	63	7E	54	9C	4D	22	0	
000FFFE20	43	00	D4	B2	80	0F	00	2E	21	16	58	01	E8	C2	000FFFE20	9F	88	C6	D0	CC	6C	BA	5D	79	BB	E4	FE	D3	BC	1	
000FFF00	80	20	4E	80	23	04	11	80	02	20	18	13	08	60	000FFF00	0B	77	21	23	E3	06	5F	11	94	A6	E5	AC	65	B5	A	
000FFF10	01	A8	03	B2	C0	B0	06	80	1A	00	0A	4B	2C	04	000FFF10	01	20	B1	C8	88	3D	67	42	7A	D5	6B	CA	EB	45	A	
000FFF20	0A	28	0D	00	D4	A0	C2	89	75	86	94	59	5C	0B	000FFF20	0B	50	C8	AA	98	EF	C8	66	AA	30	97	8E	D6	CD	0	
000FFF30	45	D6	38	F4	81	D1	56	50	18	00	34	00	BC	86	000FFF30	34	3D	D8	DD	38	E6	2C	16	72	7C	47	04	30	D2	E	
000FFF40	28	06	00	57	86	00	4A	01	60	69	28	02	36	BE	000FFF40	24	31	04	D3	98	32	BD	59	E8	FE	97	3F	A6	46	1	
000FFF50	06	80	80	DE	00	58	00	44	18	18	43	00	D4	84	000FFF50	47	53	F2	DE	9E	47	97	89	AC	A1	1F	4A	BE	AA	0	
000FFF60	B0	0D	76	7E	43	01	8E	25	95	92	00	28	0C	66	000FFF60	59	EA	8F	75	5A	32	C4	00	AB	D8	78	2B	71	9A	4	
000FFF70	02	80	19	06	16	03	00	13	80	5C	51	41	84	2C	000FFF70	F1	38	01	56	6D	97	2C	D2	54	31	23	00	63	CE	6	
000FFF80	18	16	51	45	14	19	B1	8A	57	53	09	B6	00	35	000FFF80	C8	6F	DD	00	D2	AF	FC	6A	AB	3B	C2	4B	5D	61	0	
000FFF90	B2	3D	28	0C	25	9F	50	FD	40	10	00	29	41	03	000FFF90	1A	2B	BD	D8	9E	C3	1D	85	BF	71	A8	7F	9E	86	6	
000FFFA0	0D	00	0B	80	2E	00	D0	98	4B	25	80	5C	05	8B	000FFFA0	B7	B0	FA	7C	8E	C5	16	A9	90	48	B2	6C	BF	B1	0	
000FFFAB0	38	2C	05	45	92	C9	77	84	00	76	05	89	40	17	000FFFAB0	CD	2A	C2	7E	22	D7	14	8B	26	FA	C1	9D	2F	55	2	
000FFFAC0	2B	F4	94	4A	25	80	E5	00	38	02	C0	91	FB	7D	000FFFAC0	9F	4C	67	21	01	83	78	F0	2F	53	27	3C	EE	C		
000FFFD0	0C	80	1D	80	5E	08	07	E0	81	70	00	EC	00	00	000FFFD0	10	F7	32	40	FB	98	40	AE	D1	FA	3E	05	42	83	1	
000FFFE0	59	44	B2	CB	28	A2	59	44	A2	C9	64	B0	1C	9E	000FFFE0	B7	92	01	7B	17	4C	17	D5	D0	29	07	B2	43	1B	8	
000FFFE20	00	14	5F	2C	00	24	00	6A	50	02	90	03	02	80	000FFFE20	14	62	50	35	2B	B6	42	89	5A	D6	21	50	44	6F	B	
001000000	30	A2	C8	64	22	51	28	94	05	C0	70	01	28	22	001000000	30	A2	C8	64	22	51	28	94	05	C0	70	01	28	22	7	
001000010	E4	43	01	21	72	26	01	62	59	55	12	80	64	03	001000010	E4	43	01	21	72	26	01	62	59	55	12	80	64	03	1	
001000020	B0	4B	E1	CD	C0	E5	CF	21	29	2E	B1	C0	39	E4	001000020	B0	4B	E1	CD	C0	E5	CF	21	29	2E	B1	C0	39	E4	5	
001000030	C8	40	61	2E	59	2F	31	8B	00	17	D5	06	17	B0	001000030	C8	40	61	2E	59	2F	31	8B	00	17	D5	06	17	B0	E	
001000040	38	39	AA	3E	9B	E4	80	1B	BE	66	0C	F8	EF	93	001000040	38	39	AA	3E	9B	E4	80	1B	BE	66	0C	F8	EF	93	9	
001000050	30	63	1F	F1	28	09	B3	27	05	29	21	77	4C	30	001000050	30	63	1F	F1	28	09	B3	27	05	29	21	77	4C	30	8	
001000060	5F	C9	CD	C4	17	98	2B	10	6A	B8	69	28	CC	E7	001000060	5F	C9	CD	C4	17	98	2B	10	6A	B8	69	28	CC	E7	0	
001000070	00	66	D0	D1	B5	E4	01	88	06	24	B3	8B	63	00	001000070	00	66	D0	D1	B5	E4	01	88	06	24	B3	8B	63	00	7	
001000080	61	0C	9A	4B	4B	24	26	24	B5	77	5E	00	14	61	001000080	61	0C	9A	4B	4B	24	26	24	B5	77	5E	00	14	61	A	
001000090	E5	88	D3	F0	26	59	CA	5B	7C	E2	80	84	B5	3A	001000090	E5	88	D3	F0	26	59	CA	5B	7C	E2	80	84	B5	3A	C	

10/31/2015 1:27:26 AM | 94.5 MB (99125084) | 001000000 (1048576) | 7/16/2019 12:30:47 PM | 94.5 MB (99125312) | 001000000 (1048576)

test (1).mkv.bin																test (1).mkv.6105p63...															
00000000	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	00000000	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D		
00000000	1a	45	df	a3	a3	42	86	81	01	4					00000000	2d	86	d3	58	e8	64	25	46	34	d						
00000010	04	42	f3	81	08	42	82	88	6d	6					00000010	a5	f6	38	06	52	a0	39	47	a9	b						
00000020	42	87	81	04	42	85	81	02	18	5					00000020	b8	b3	db	9e	59	a2	7f	ca	ae	9						
00000030	34	c3	cc	b4	11	4d	9b	74	af	4					00000030	2f	38	f8	02	74	3c	1e	14	5f	4						
00000040	49	a9	66	53	ac	82	10	03	4d	b					00000040	71	d1	c2	65	01	ab	b4	84	e3	1						
00000050	ae	6b	53	ac	82	10	c7	4d	bb	8					00000050	e9	98	b4	1b	d2	0c	1b	93	22	e						
00000060	6b	53	ac	84	34	c3	5e	ef	ec	4					00000060	be	26	a6	3e	6d	0d	51	08	f3	8						
00000070	00	00	00	00	00	00	00	00	00	0					00000070	bd	32	cf	c4	b6	32	f7	26	1d	2						
00000080	00	00	00	00	00	00	00	00	00	0					00000080	86	49	59	95	05	5e	91	f3	fb	2						
00000090	00	00	00	00	00	00	00	00	00	0					00000090	fc	50	c2	7a	f1	b2	cd	b0	3e	d						
000000a0	00	00	00	00	00	00	00	00	00	0					000000a0	3b	01	5c	67	d7	ba	03	51	f1	1						
000000b0	00	00	00	00	00	00	00	00	00	0					000000b0	45	ad	f6	a3	d8	dc	f8	ac	bd	7						
000000c0	00	00	00	00	00	00	00	00	00	0					000000c0	71	06	3b	d4	98	f8	50	fc	88	9						
000000d0	00	00	00	00	00	00	00	00	00	0					000000d0	e5	d0	83	5b	d1	d7	56	79	20	3						
000000e0	00	00	00	00	00	00	00	00	00	0					000000e0	7f	2e	53	e8	15	52	39	a2	5d	0						
000000f0	00	00	00	00	00	00	00	00	00	0					000000f0	88	7b	d0	30	32	da	98	09	dc	3						
00000100	00	00	00	00	00	00	00	00	00	0					00000100	5b	8e	ed	71	12	d8	93	09	98	6						

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

## ۶-۲ 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. احتمالاً 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. تقریباً تمام ترافیک شبکه این باج‌افزار بر روی پورت 443 قرار دارد و ارتباطات آن از طریق پروتکل TCP برقرار می‌گردد.

لیست درخواست‌های DNS :

90nguyentuan.com  
a-zpaperwork.eu  
advancedeyecare.com  
agendatwentytwenty.com  
alattekniksipil.com  
alene.co  
alharsunindo.com  
alisodentalcare.com  
alnectus.com  
andreaskildegaard.dk  
annida.it  
aquacheck.co.za  
arearugcleaningnyc.com  
astrographic.com  
atma.nl  
atrgroup.it  
avisioninthedesert.com  
banukumbak.com  
baptistdistinctives.org  
bayshoreelite.com  
beauty-traveller.com  
belinda.af  
belofloripa.be  
benchbiz.com  
berdonllp.com  
biketruck.de  
block-optic.com  
blucamp.com  
bluelakevision.com  
bmw-i-pure-impulse.com  
bonitabeachassociation.com  
bourchier.org  
brinkdoepke.eu  
brownswoodblog.com  
bruut.online  
bundan.com  
buzzneakers.com  
bychowo.pl  
cainlaw-okc.com  
carmel-york.com  
carsten.sparen-it.de  
cascinarosa33.it  
ceocenters.com  
ciga-france.fr  
citiscapes-art.com  
citydogslife.com  
cookinn.nl

لیست آی‌پی‌های شناسایی شده :

148.251.11.181  
78.142.209.221  
50.97.149.92  
46.243.156.72  
197.221.14.44  
46.30.215.77  
209.182.203.153  
67.20.76.129  
178.63.89.23  
87.98.154.146  
210.245.90.240  
77.104.162.69  
95.216.117.200  
150.95.54.240  
96.127.180.186  
198.46.89.70  
46.30.215.168  
5.152.193.244  
74.208.236.75  
52.174.40.218  
198.71.233.104  
81.19.215.5  
35.228.55.150  
194.30.35.117  
46.105.57.169  
104.31.84.195  
104.31.85.195  
95.143.172.245  
91.195.240.87  
185.26.156.167  
69.89.31.228  
46.30.215.111  
166.62.112.193  
198.50.129.250  
192.163.232.100  
69.164.206.96  
104.27.165.36  
104.27.164.36  
185.199.220.28  
141.138.169.215  
192.0.78.151  
192.0.78.245  
51.68.89.43  
184.173.96.66  
192.145.232.92  
103.23.22.248  
103.74.54.152

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



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

Name	Local address	Local...	Remote address	Remote ...	Proto...	State
1.exe (3256)	WIN-LQOUEMDES...	49741	WIN-LQOUEMDESNO	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-LQOUEMDESNO	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
svchost.exe (1016)	WIN-LQOUEMDES...	3702			UDP	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-gubematoru.ru	FOUND
13:52:48	napisat-pismo-gubematoru.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

درخواست های  
DNS

File Edit Rules Tools View Help

Replay X 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 باج افزار

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.