باسمه تعالی

گزارش تحلیل باج افزار

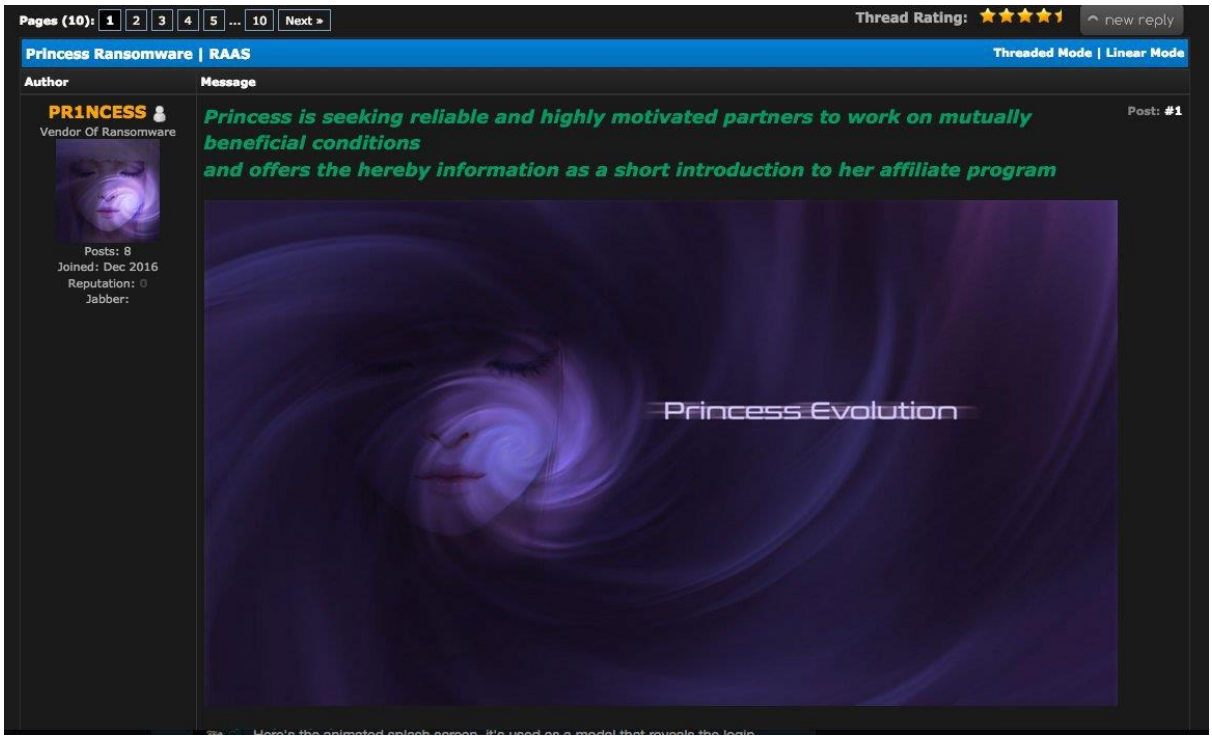
PrincessLocker ۳.۰

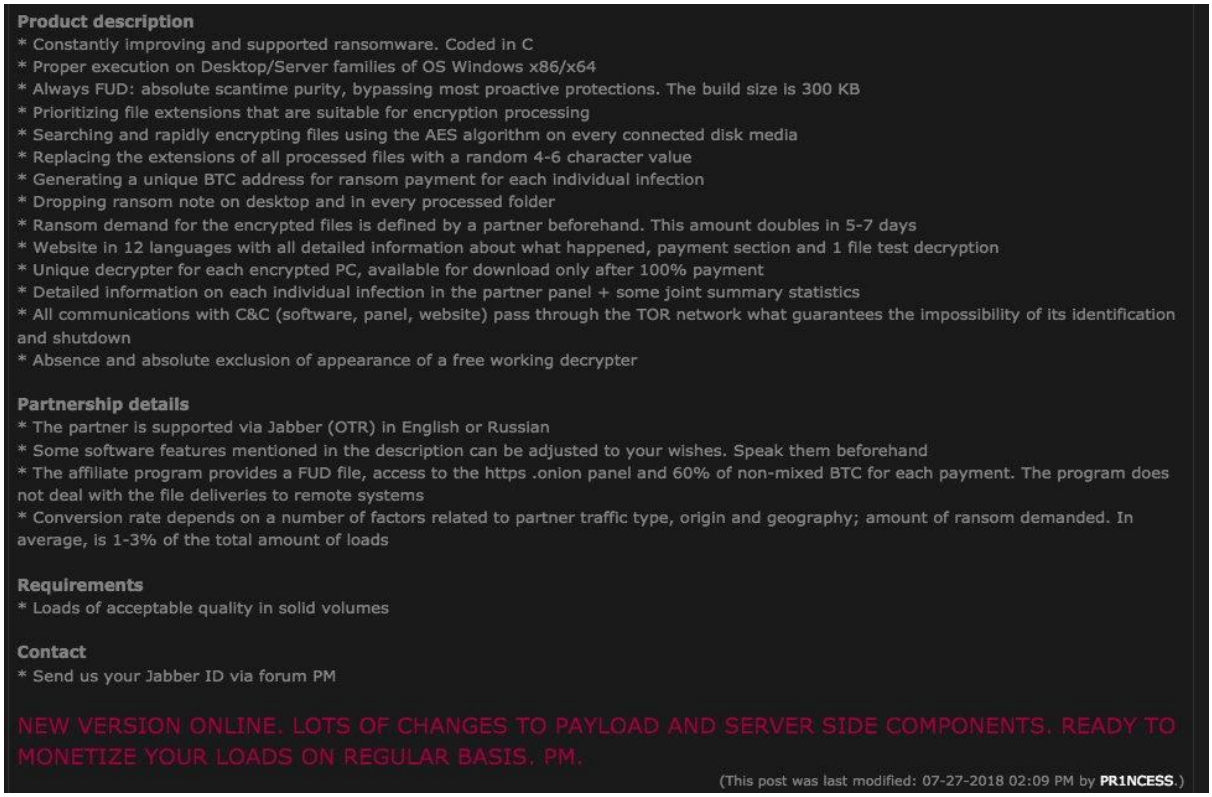
مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت باج افزار PrincessLocker خبر می‌دهد. طبق بررسی های صورت گرفته، باج افزار PrincessLocker در اواسط آگوست سال ۲۰۱۸ شروع به فعالیت کرده که این باج‌افزار نسخه سوم آن می‌باشد .

(Genealogy: PrincessLocker > PrincessLocker ۲.۰ > PrincessLocker ۳.۰)

باج‌افزارPrincessLocker کاربران انگلیسی زبان را مورد هدف قرار می‌دهد اما این امر مانع از گسترش آن در سایر کشورها نمی‌شود. براساس گزارش TrendMicro، ظاهرا باج‌افزار مورد اشاره از طریق اکسپلویت کیت RIG منتشر می گردد. نکته قابل توجه در مورد این باج‌افزار RaaS بودن آن است. تصاویر زیر ویژگی‌های مختلفی که RaaS باید ارائه دهد شامل تقسیم درآمد، نحوه پشتیبانی، گزینه های پیکربندی و موارد دیگر را نشان می‌دهد.





Product description
* Constantly improving and supported ransomware. Coded in C
* Proper execution on Desktop/Server families of OS Windows x86/x64
* Always FUD: absolute scantime purity, bypassing most proactive protections. The build size is 300 KB
* Prioritizing file extensions that are suitable for encryption processing
* Searching and rapidly encrypting files using the AES algorithm on every connected disk media
* Replacing the extensions of all processed files with a random 4-6 character value
* Generating a unique BTC address for ransom payment for each individual infection
* Dropping ransom note on desktop and in every processed folder
* Ransom demand for the encrypted files is defined by a partner beforehand. This amount doubles in 5-7 days
* Website in 12 languages with all detailed information about what happened, payment section and 1 file test decryption
* Unique decrypter for each encrypted PC, available for download only after 100% payment
* Detailed information on each individual infection in the partner panel + some joint summary statistics
* All communications with C&C (software, panel, website) pass through the TOR network what guarantees the impossibility of its identification and shutdown
* Absence and absolute exclusion of appearance of a free working decrypter

Partnership details
* The partner is supported via Jabber (OTR) in English or Russian
* Some software features mentioned in the description can be adjusted to your wishes. Speak them beforehand
* The affiliate program provides a FUD file, access to the https .onion panel and 60% of non-mixed BTC for each payment. The program does not deal with the file deliveries to remote systems
* Conversion rate depends on a number of factors related to partner traffic type, origin and geography; amount of ransom demanded. In average, is 1-3% of the total amount of loads

Requirements
* Loads of acceptable quality in solid volumes

Contact
* Send us your Jabber ID via forum PM

NEW VERSION ONLINE. LOTS OF CHANGES TO PAYLOAD AND SERVER SIDE COMPONENTS. READY TO MONETIZE YOUR LOADS ON REGULAR BASIS. PM.

(This post was last modified: 07-27-2018 02:09 PM by PR1NCESS.)

مشخصات فایل اجرایی :

نام فایل	princess_ransom.exe
MD۵	acaeaf۱e۱ff۰b۰٤۳a۳۷d۲a۳e۳f۹f۳fbe
SHA-۱	٦٥٢٦١٣٠١٣d٣١٣٢٥a٠٩cd٤b١٣٤٧f٤٩eed١٥٠a٨١de
SHA-٢٥٦	١٤٠٨a٢٤b٧٤٩٤٩٩٢٢cc٦٥١٦٤eea٠٧٨٠٤٤٩c٢d٠٢bb٦١٢٣fd٩٩٢b٢٣٩٧f١٨٧٣afd٢١
اندازه فایل	٢٦٧.٥ KB
کامپایلر	Microsoft Visual C++ ٨

فایل اجرایی این باج افزار دارای پنج بخش است :

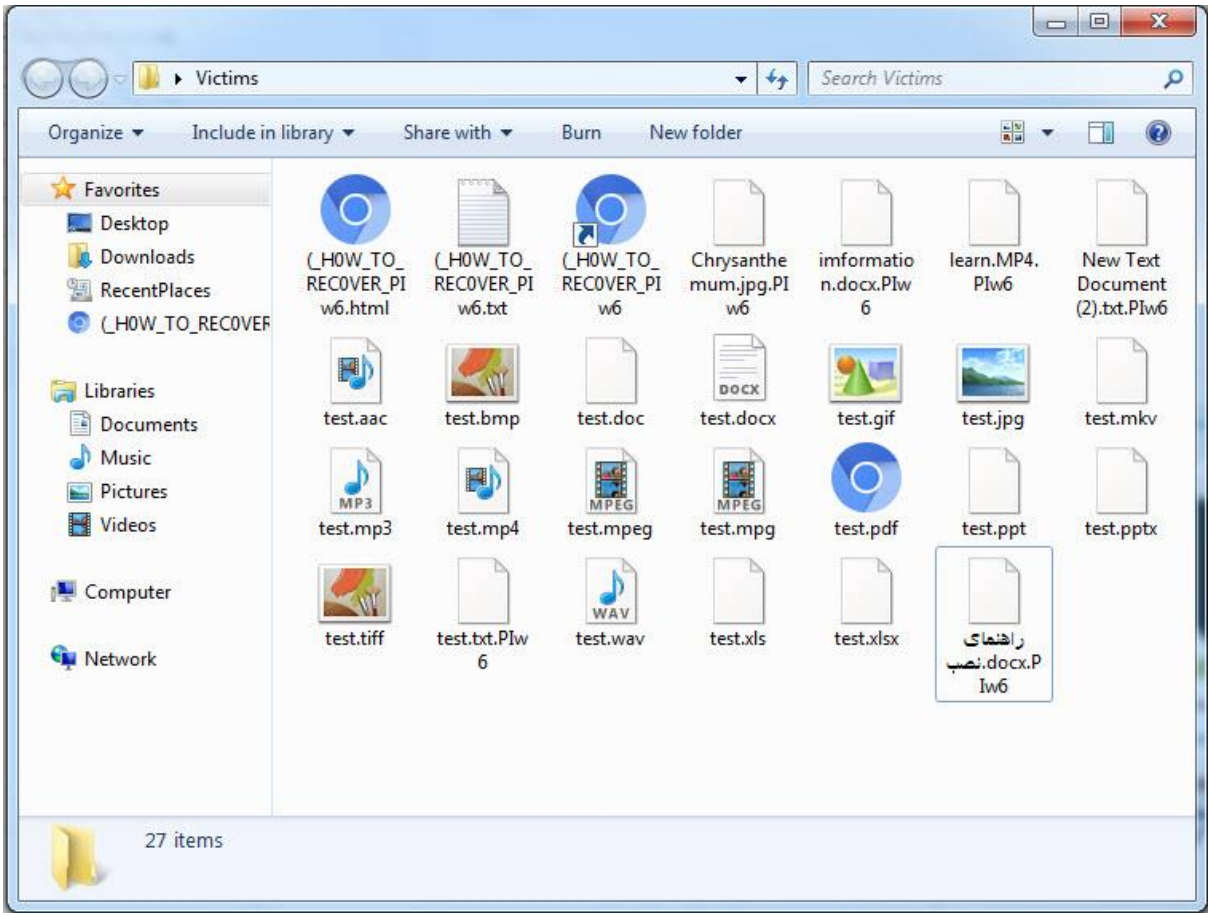
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٦٤	٤٠٩٦	٣٧٢٩٢	٣٧٣٧٦
.rdata	٥.٤١	٤٥٠٥٦	١٠٤٣٠	١٠٧٥٢
.data	٠.٧٢	٥٧٣٤٤	٢٩٣٥٢	١٨٤٣٢
.rsrc	٧.٨	٩٠١١٢	٢٢٧٧٢٤	١٩٩١٦٨
.reloc	٣.١١	٣١٩٤٨٨	٦٨٥٨	٧١٦٨

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار PrincessLocker ، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. فرآیند اجرای این باج افزار بسته به منابع سیستم قربانی به طور متوسط حدودا ۵ دقیقه تا اجرای کامل زمان می‌برد، پس از ورود به سیستم و بررسی محیط آن ، اقدام به رمزگذاری فایل ها با استفاده از الگوریتم رمزنگاری خود می کند. .فایل های زیر ، فایل های مورد هدف باج افزار می باشند :

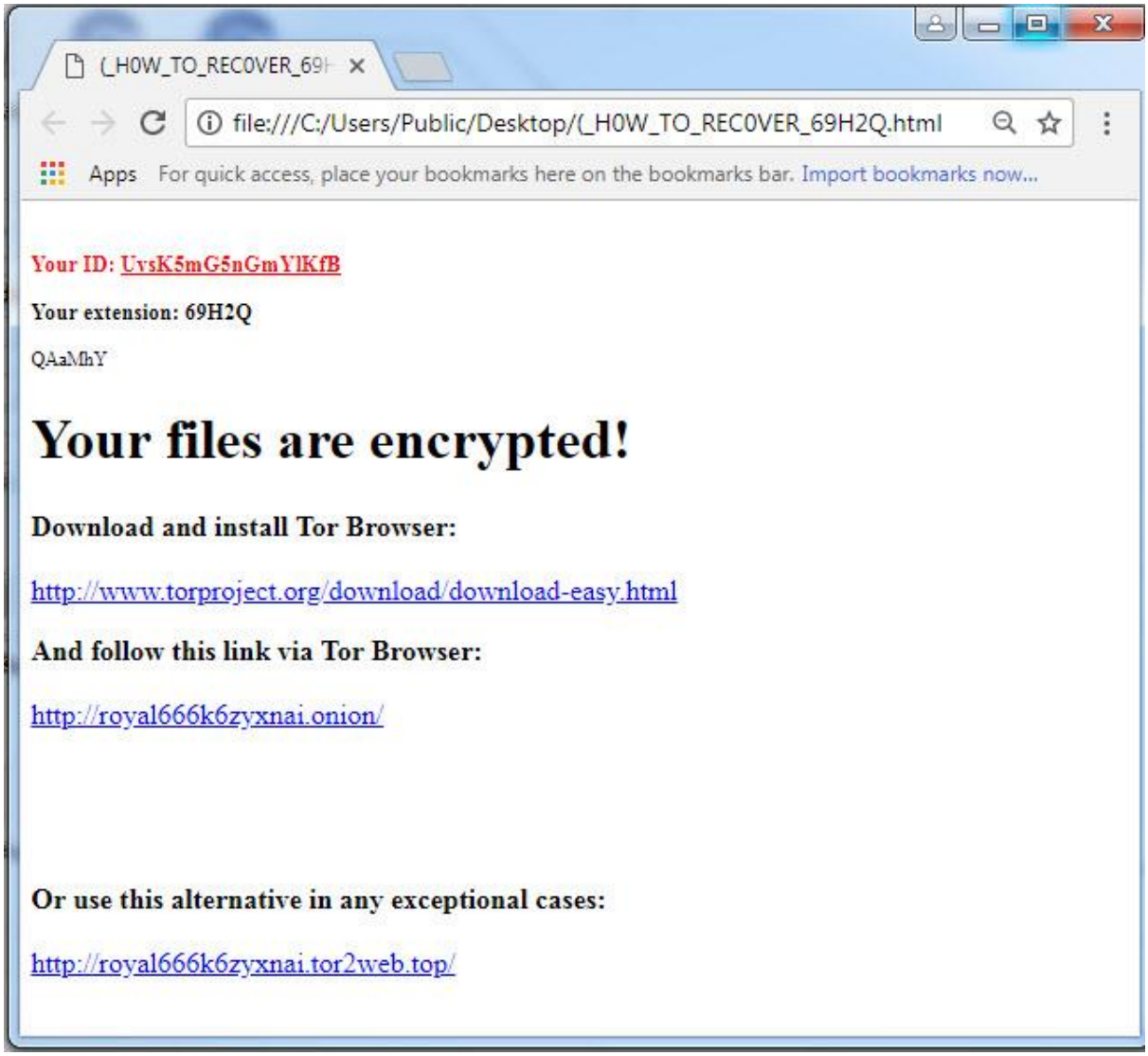
MS Office documents, OpenOffice, PDF, text files, databases, photos, music, video, image files, archives, etc

پس از اتمام رمزگذاری ، فایل های سیستم قربانی به شکل زیر تغییر پیدا می کنند :



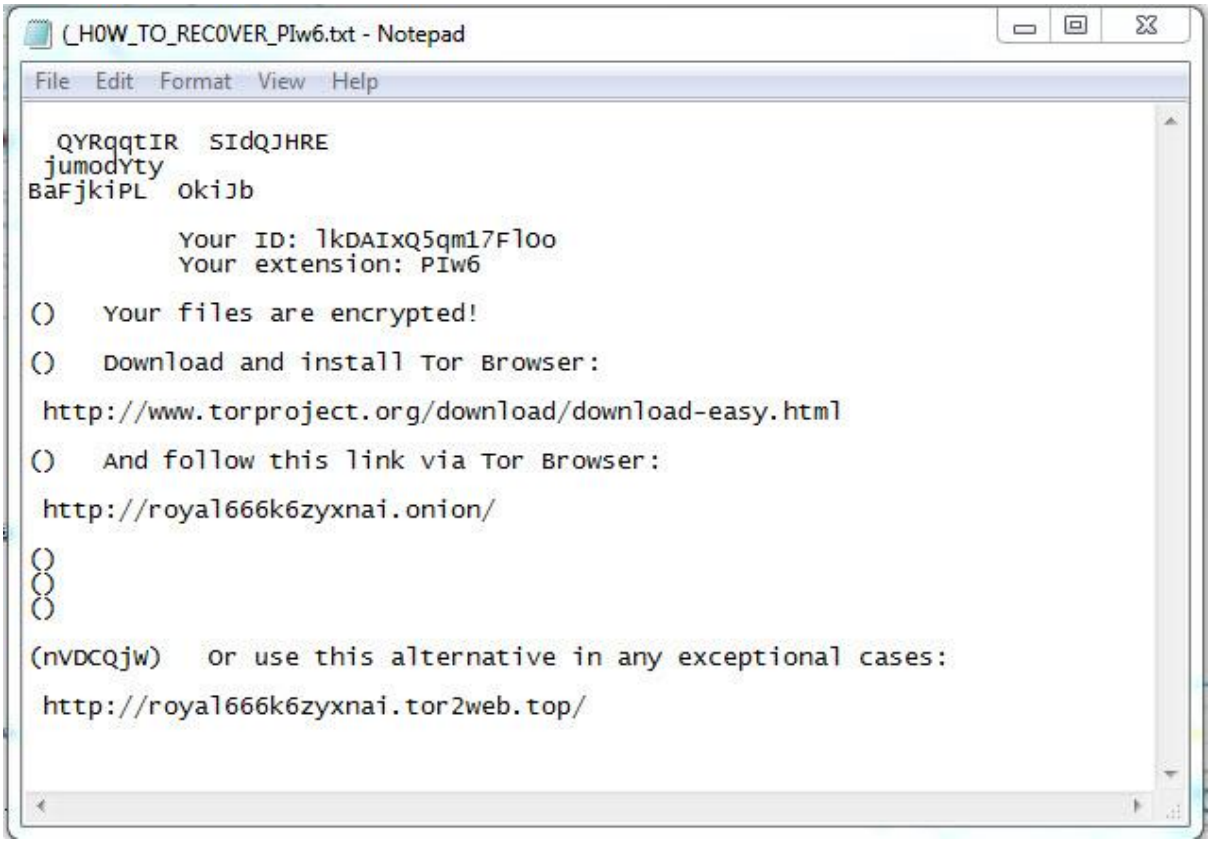
باج‌افزار PrincessLocker پس از اتمام رمزگذاری، پسوندی تصادفی را به انتهای فایل‌ها اضافه می‌کند، به عنوان مثال : ٦٩H٢Q، PIw٦ ... , . همانطور که در تصویر مشاهده می‌کنید این باج‌افزار فایل‌های فاقد محتوا را رمزگزاری نمی‌کند .

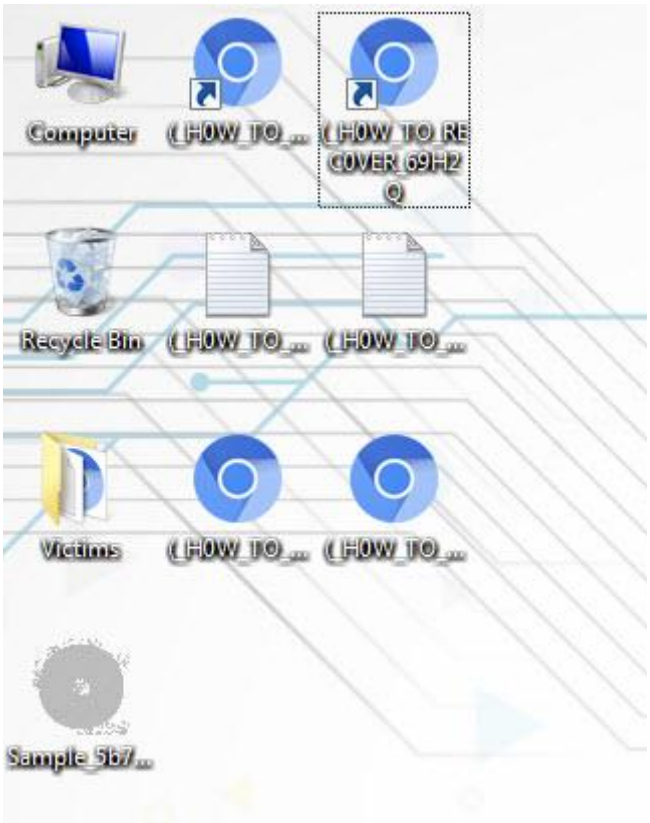
حال پیغام باج خواهی باج افزاربه صورت پنجره ای تحت عنوان H٠W_TO_REC٠VER_PIw٦.html بـرای قربانی نمایش داده می شود:



در این پیغام مهاجم از قربانی می‌خواهد که جهت برقراری ارتباط و تعیین مبلغ باج مرورگر Tor را دانلـود و به آدرس httproyal٦٦٦k٦zyxnai.onion یا httproyal٦٦٦k٦zyxnai.tor٢web.top مراجعه نماید.

البته این پیغام ، تنها پیغام باج خواهی باج افزار نیست، پیغامی مشابه با فرمت txt در دسکتاپ قربانی ظـاهر می شود. در تصویر زیر می توانید این پیغام را مشاهده کنید :

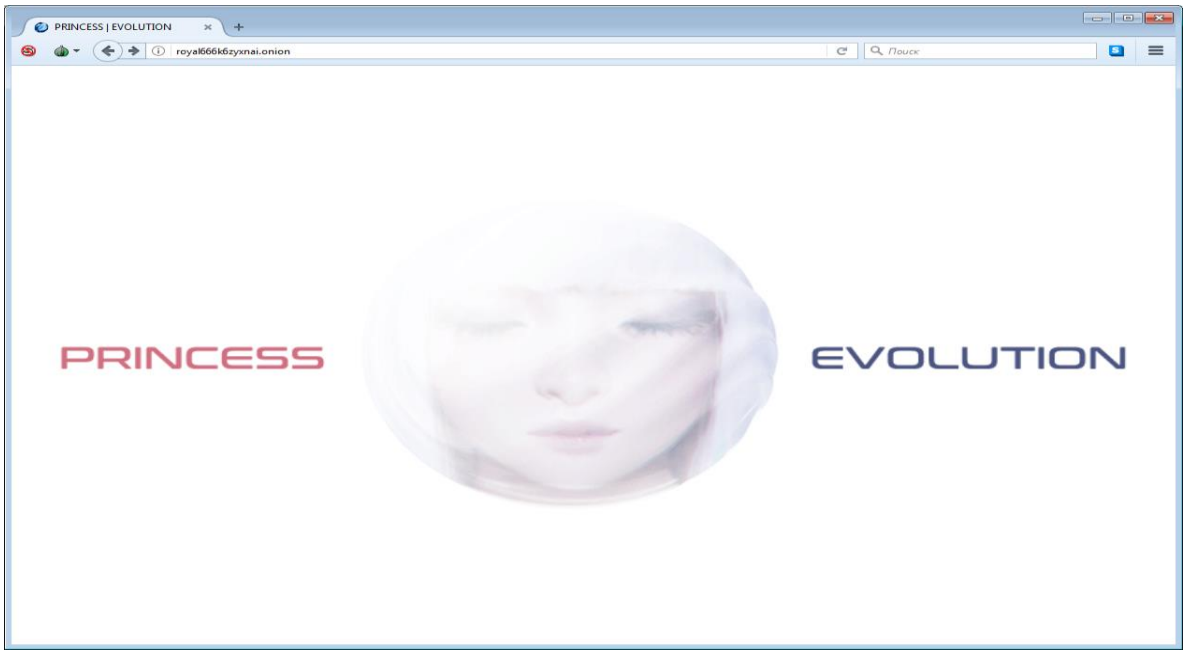


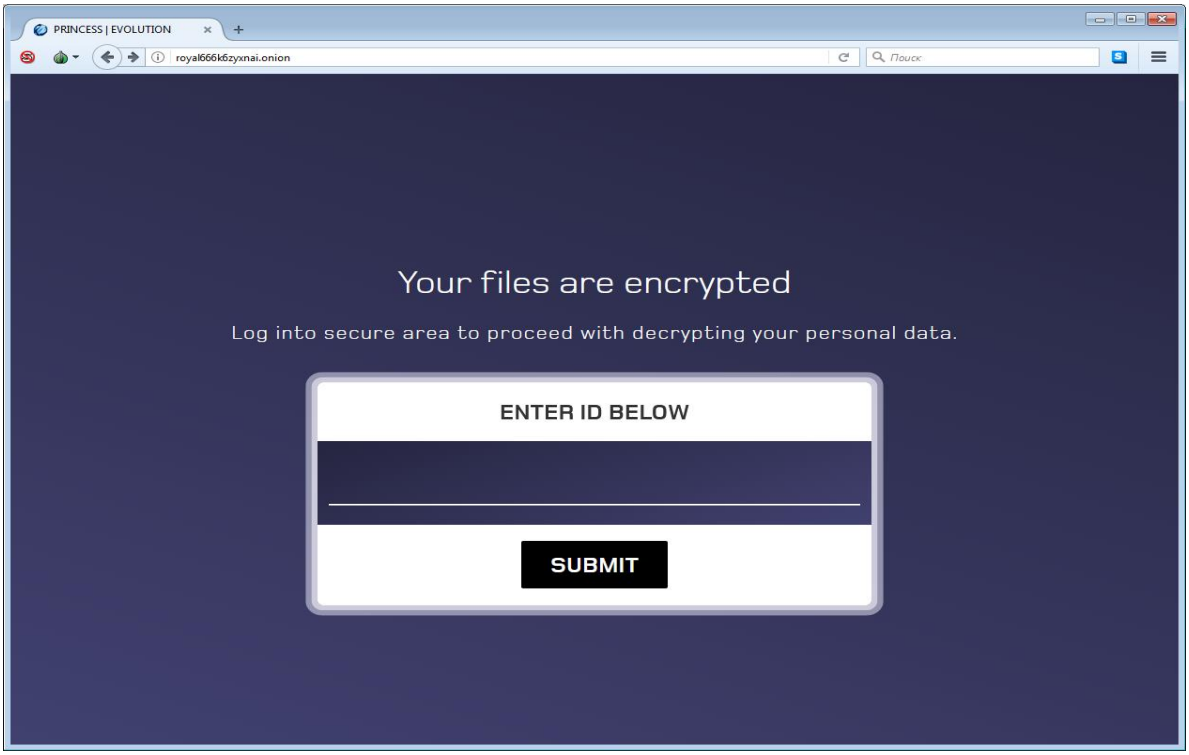


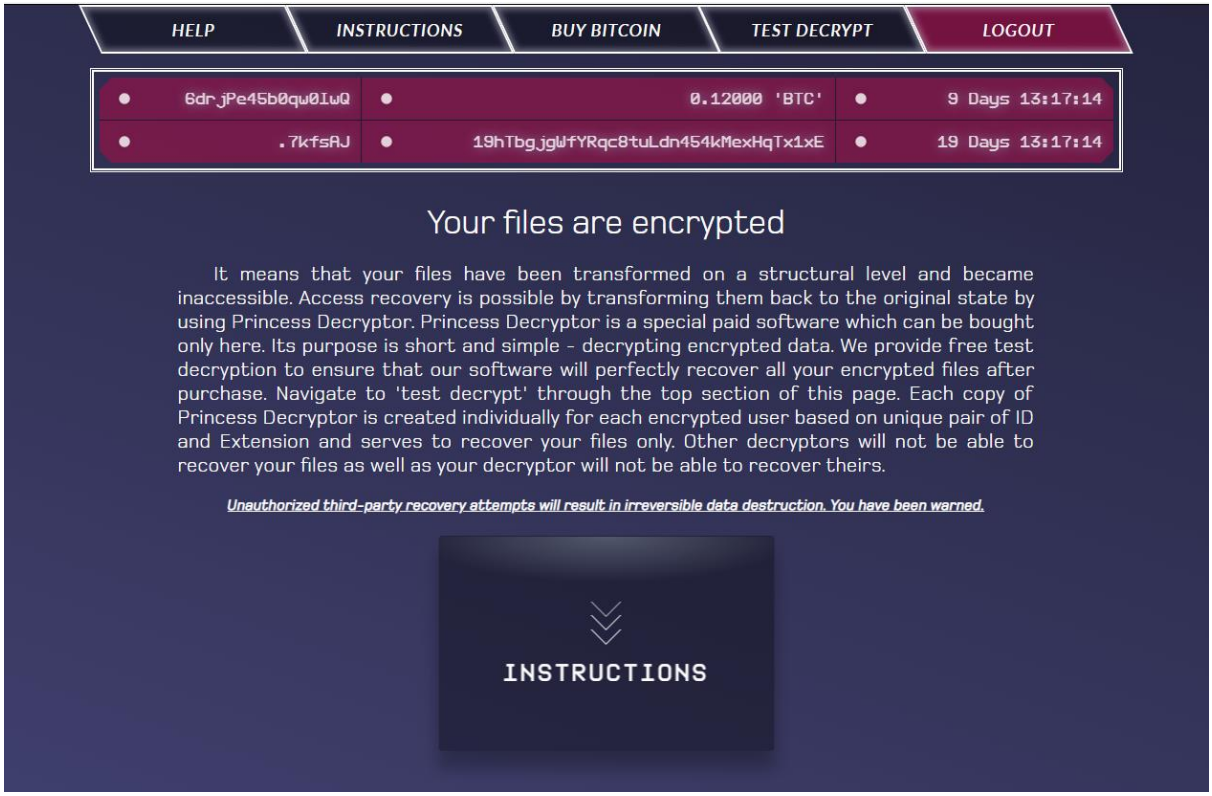
آیکون باج‌افزار PrincessLocker به صورت زیر می‌باشد .

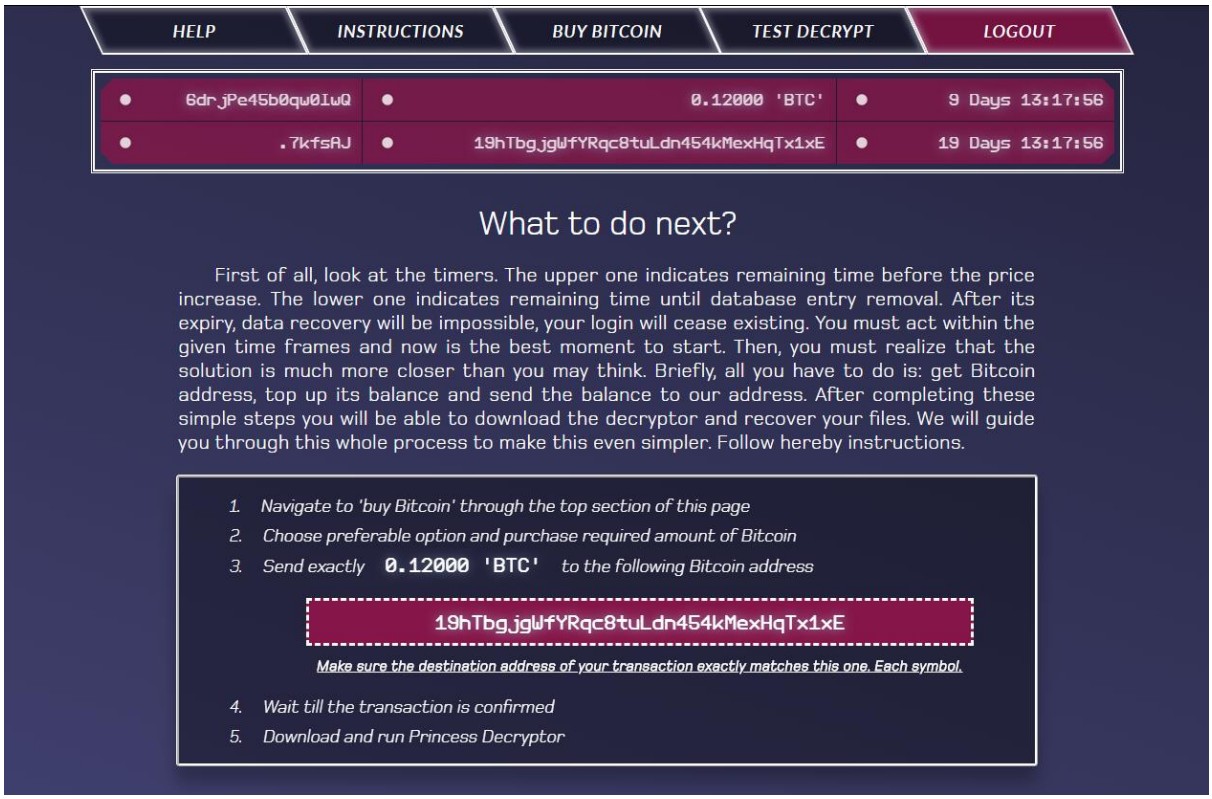
-

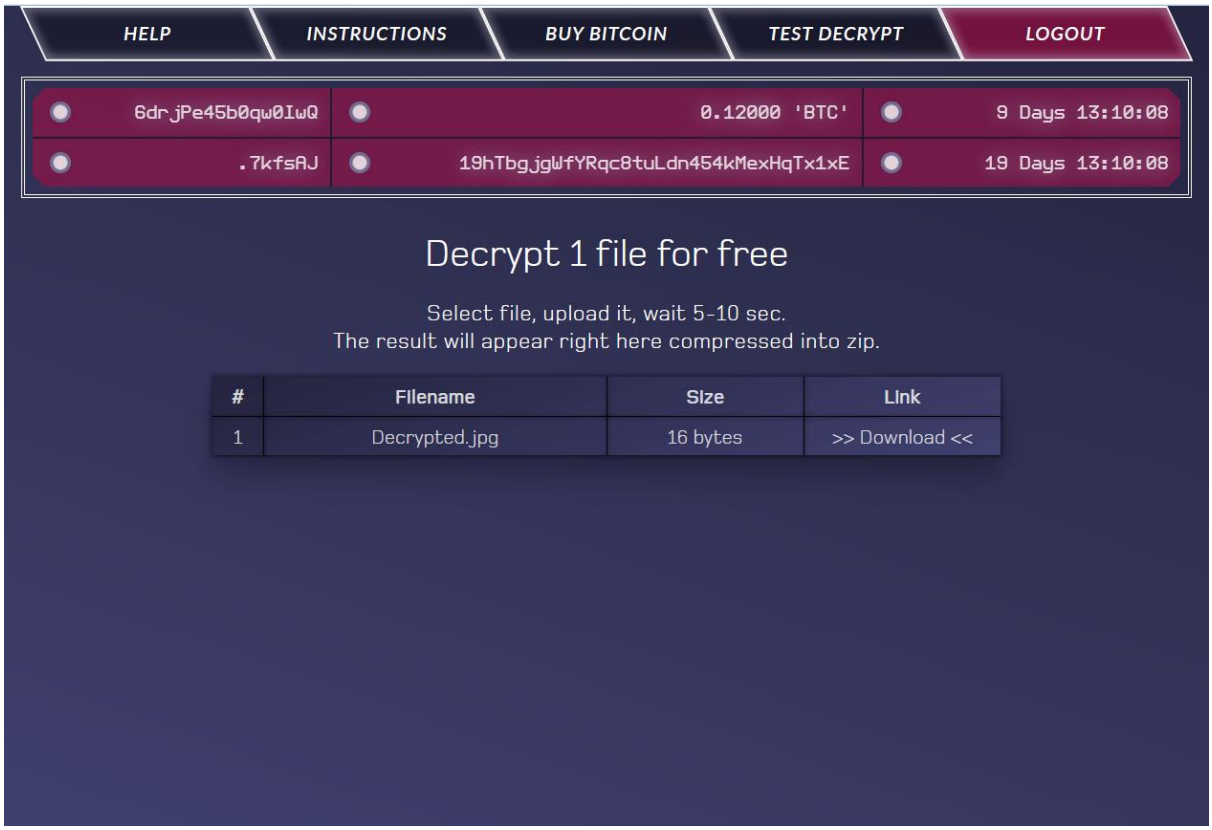
تصاویر مربوط به صفحه پرداخت باج می باشند :

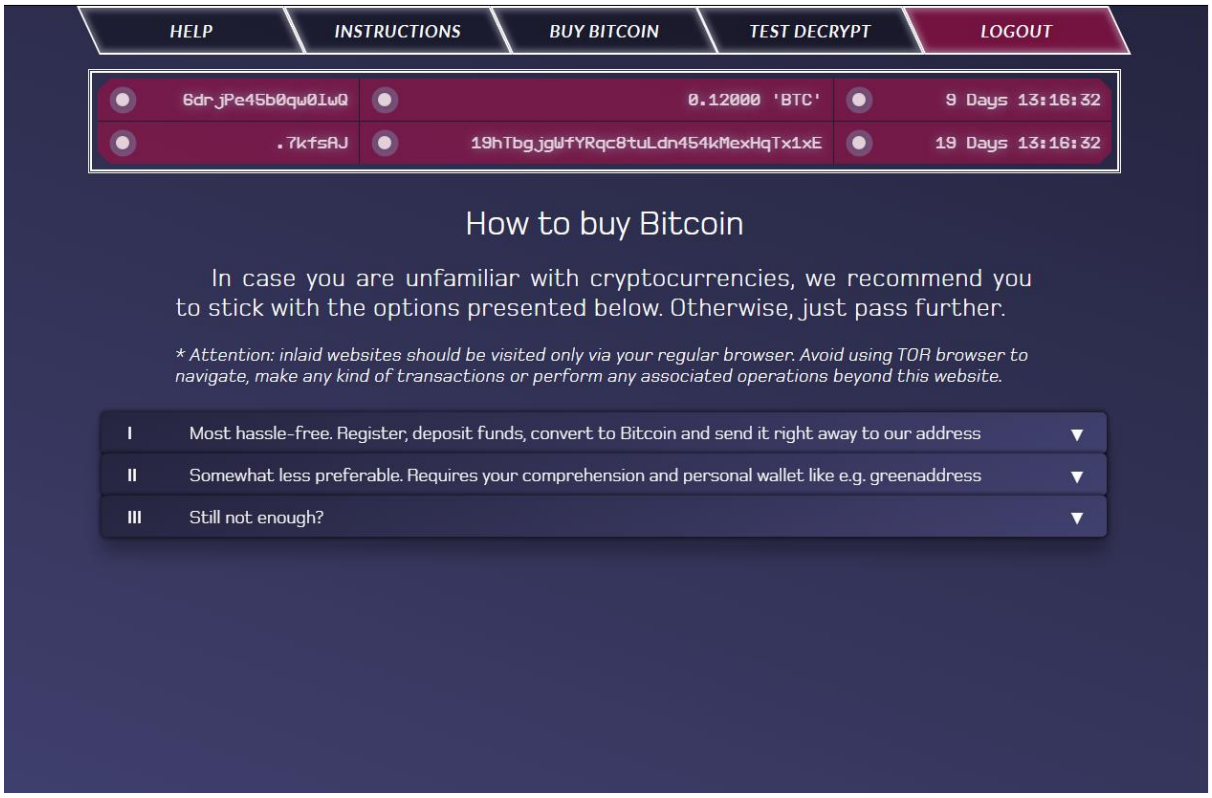


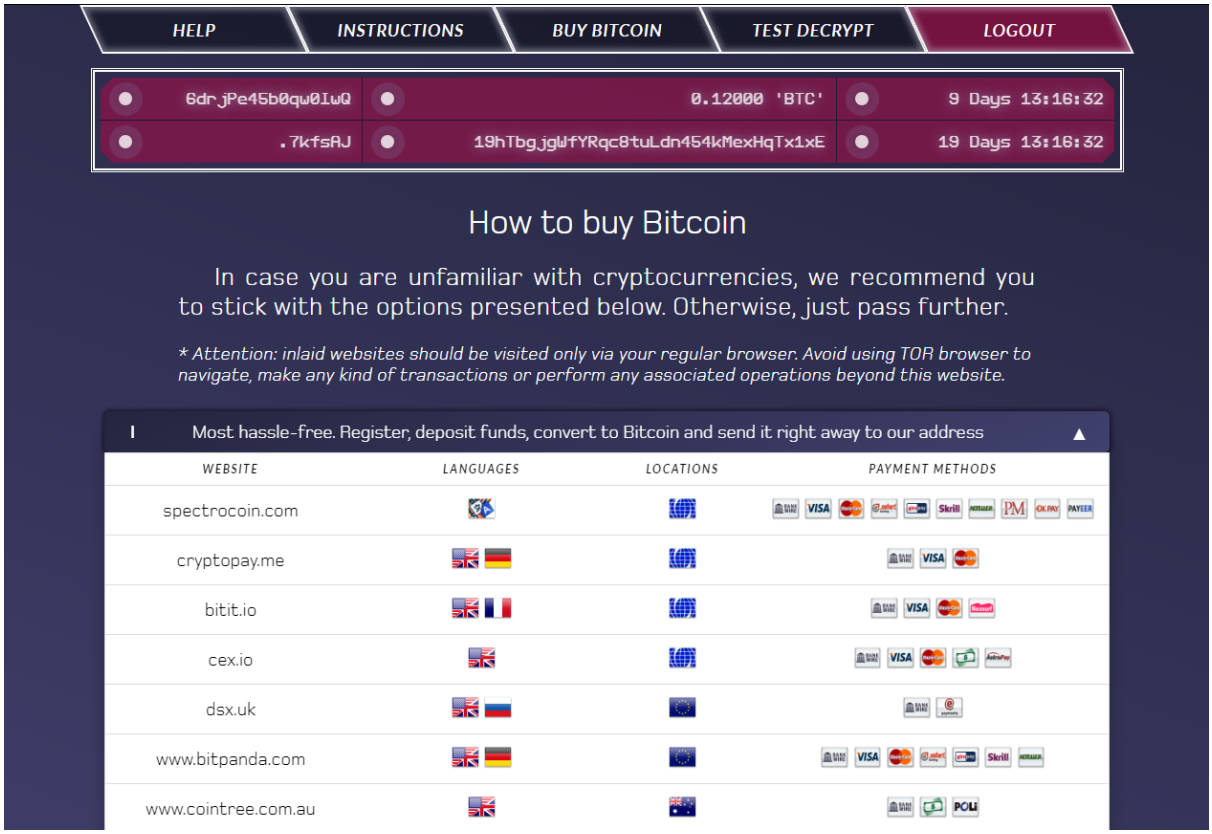



HELP
INSTRUCTIONS
BUY BITCOIN
TEST DECRYPT
LOGOUT
6drjPe45b0qw0IwQ
0.12000 'BTC'
9 Days 13:17:14
.7kfsAJ
19hTbgjgWfYRqc8tuLdn454kMexHqTx1xE
19 Days 13:17:14
Your files are encrypted
It means that your files have been transformed on a structural level and became inaccessible. Access recovery is possible by transforming them back to the original state by using Princess Decryptor. Princess Decryptor is a special paid software which can be bought only here. Its purpose is short and simple - decrypting encrypted data. We provide free test decryption to ensure that our software will perfectly recover all your encrypted files after purchase. Navigate to 'test decrypt' through the top section of this page. Each copy of Princess Decryptor is created individually for each encrypted user based on unique pair of ID and Extension and serves to recover your files only. Other decryptors will not be able to recover your files as well as your decryptor will not be able to recover theirs.
Unauthorized third-party recovery attempts will result in irreversible data destruction. You have been warned.
INSTRUCTIONS


HELP
INSTRUCTIONS
BUY BITCOIN
TEST DECRYPT
LOGOUT
6drjPe45b0qw0IwQ
0.12000 'BTC'
9 Days 13:17:56
.7kfsAJ
19hTbgjgWfYRqc8tuLdn454kMexHqTx1xE
19 Days 13:17:56
What to do next?
First of all, look at the timers. The upper one indicates remaining time before the price increase. The lower one indicates remaining time until database entry removal. After its expiry, data recovery will be impossible, your login will cease existing. You must act within the given time frames and now is the best moment to start. Then, you must realize that the solution is much more closer than you may think. Briefly, all you have to do is: get Bitcoin address, top up its balance and send the balance to our address. After completing these simple steps you will be able to download the decryptor and recover your files. We will guide you through this whole process to make this even simpler. Follow hereby instructions.
1. Navigate to 'buy Bitcoin' through the top section of this page
2. Choose preferable option and purchase required amount of Bitcoin
3. Send exactly 0.12000 'BTC' to the following Bitcoin address
19hTbgjgWfYRqc8tuLdn454kMexHqTx1xE
Make sure the destination address of your transaction exactly matches this one. Each symbol.
4. Wait till the transaction is confirmed
5. Download and run Princess Decryptor


HELP
INSTRUCTIONS
BUY BITCOIN
TEST DECRYPT
LOGOUT
6drjPe45b0qw0IwQ
0.12000 'BTC'
9 Days 13:10:08
.7kfsAJ
19hTbgjgWfYRqc8tuLdn454kMexHqTx1xE
19 Days 13:10:08
Decrypt 1 file for free
Select file, upload it, wait 5-10 sec.
The result will appear right here compressed into zip.
Filename Size Link
1 Decrypted.jpg 16 bytes >> Download <<


HELP
INSTRUCTIONS
BUY BITCOIN
TEST DECRYPT
LOGOUT
6drjPe45b0qw0IwQ
0.12000 'BTC'
9 Days 13:16:32
.7kfsAJ
19hTbgjgWfYRqc8tuLdn454kMexHqTx1xE
19 Days 13:16:32
How to buy Bitcoin
In case you are unfamiliar with cryptocurrencies, we recommend you to stick with the options presented below. Otherwise, just pass further.
* Attention: inlaid websites should be visited only via your regular browser. Avoid using TOR browser to navigate, make any kind of transactions or perform any associated operations beyond this website.
I Most hassle-free. Register, deposit funds, convert to Bitcoin and send it right away to our address
II Somewhat less preferable. Requires your comprehension and personal wallet like e.g. greenaddress
III Still not enough?



در صفحات نخستین کاربر پس از ورود به سایت و وارد کردن شناسه اختصاصی می‌تواند یک فایل را به عنوان نمونه رمزگشایی کند، و در دیگر صفحه‌ها اطلاعاتی در مورد نحوه خرید بیت‌کوین، مبلغ باج و .. نمایش داده شده است .

Summary	
Address	19hTbgjgWfYRqc8tuLdn454kMexHqTx1xE
Hash 160	5f67d8ff95b3f4a08733bca62350260689ef343e

Transactions	
No. Transactions	1
Total Received	0.00012 BTC
Final Balance	0.00012 BTC

همانطور که قابل ملاحظه است این باج‌افزار تاکنون یک تراکنش مالی داشته است .

تحلیل ایستا:

با بررسی بیشتر کد های باج افزار به نتایج زیر دست یافتیم :

همانطور که گفته شد باج افزار پس از نفوذ به سیستم ، شروع به رمزگذاری فایل‌ها می‌کند . تصویر زیر روند جستجو فایل های هدف را نشان می دهد :

```
loc_4014D6:                             ; CODE XREF: WinMain(x,x,x,x)+452↑j
                cmp     esi, 26F9h
                jge     short loc_4014FA
                push    ebx             ; cchBufferLength
                lea     eax, [ebp+szVolumeMountPoint]
                push    eax             ; lpszVolumeMountPoint
                push    offset szRootPathName ; "De yazukesijavo bohisabiyoho xucojanuka"...
                call    ds:FindFirstVolumeMountPointW
                push    ebx             ; cchBufferLength
                push    ebx             ; lpszVolumeMountPoint
                push    ebx             ; hFindVolumeMountPoint
                call    ds:FindNextVolumeMountPointW
```

تابع زیر نوع فایل‌ها را مشخص می‌کند .

```
                                        ; DATA XREF: ...
; DWORD __stdcall GetFileType(HANDLE hFile)
                extrn GetFileType:dword ; CODE XREF: __ioinit+13F↑p
                                        ; __ioinit+1DB↑p
                                        ; DATA XREF: ...
```

تحلیل ترافیک شبکه :

آی پی مرتبط با باج افزار :

IP	کشور
۱۶۷.۱۱٤.۱۹۵.۲۲۵	...

1160…	1596.965599	192.168.111.134	167.114.195.225	UDP	407 61845 →
1160…	1596.965665	192.168.111.134	167.114.196.226	UDP	407 61845 →
1160…	1596.965725	192.168.111.134	167.114.196.227	UDP	407 61845 →
1160…	1596.965739	192.168.111.134	167.114.196.228	UDP	407 61845 →
1160…	1596.965811	192.168.111.134	167.114.196.229	UDP	407 61845 →
1160…	1596.965838	192.168.111.134	167.114.196.230	UDP	407 61845 →
1160…	1596.965907	192.168.111.134	167.114.196.231	UDP	407 61845 →
1160…	1596.965936	192.168.111.134	167.114.196.232	UDP	407 61845 →
1160…	1596.966007	192.168.111.134	167.114.196.233	UDP	407 61845 →
1160…	1596.966024	192.168.111.134	167.114.196.234	UDP	407 61845 →
1160…	1596.966351	192.168.111.134	167.114.196.235	UDP	407 61845 →
1160…	1596.966394	192.168.111.134	167.114.196.236	UDP	407 61845 →
1160…	1596.966472	192.168.111.134	167.114.196.237	UDP	407 61845 →
1160…	1596.966488	192.168.111.134	167.114.196.238	UDP	407 61845 →

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۸ مورد از ۶۹ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.GenericKD.31170134	AhnLab-V3	Win-Trojan/Gandcrab04.Exp
ALYac	Trojan.Ransom.Princess	Antiy-AVL	Trojan/Win32.Fuerboos
Arcabit	Trojan.Generic.D1DB9E56	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Trojan.GenericKD.31170134	CAT-QuickHeal	Trojan.Chapak.ZZ5
Comodo	TrojWare.Win32.PSW.Coins.FS	CrowdStrike Falcon	malicious_confidence_100% (W)
Cybereason	malicious.13d313	Cylance	Unsafe
Cyren	W32/Trojan.DTLE-4889	DrWeb	Trojan.PWS.Panda.13495
Emsisoft	Trojan.GenericKD.31170134 (B)	Endgame	malicious (high confidence)
eScan	Trojan.GenericKD.31170134	ESET-NOD32	a variant of Win32/Kryptik.GJLH
F-Secure	Trojan.GenericKD.31170134	Fortinet	W32/Kryptik.GJNK!tr
GData	Trojan.GenericKD.31170134	Ikarus	Trojan.Win32.Crypt
Jiangmin	TrojanDownloader.Bandit.u	K7AntiVirus	Trojan (0053305e1)
K7GW	Trojan (0053305e1)	Kaspersky	Trojan-Ransom.Win32.Encoder.e
Malwarebytes	Ransom.MalPack	MAX	malware (ai score=100)
McAfee	Packed-FJN!ACAEAF1E1FF0	McAfee-GW-Edition	BehavesLike.Win32.Generic.dc
Microsoft	Trojan:Win32/Skeeyah.A!rfn	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.881
Rising	Trojan.Fuerboos!8.EFC8 (TFE:5:QQ8lUNAfxXJ)	Sophos AV	Troj/PrincEv-B
Sophos ML	heuristic	SUPERAntiSpyware	Ransom.Cerber/Variant
Symantec	Packed.Generic.525	Tencent	Win32.Trojan.Encoder.Lpvi
TrendMicro	Ransom_PRINCESSLOCKER.B	TrendMicro-HouseCall	Ransom_PRINCESSLOCKER.B
VBA32	BScope.Trojan.Chapak	Webroot	W32.Adware.Gen
Zillya	Trojan.GenericKD.Win32.155445	ZoneAlarm	Trojan-Ransom.Win32.Encoder.e

خروجی سامانه ویروس کاو مرکز ماهر :

در حال حاضر تعداد ۷ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس‌کاو مرکز ماهر قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن
پادویش	2.3.190.2675	Clean
sophos	9.15.0	Clean
f_secure	11.00	Dangerous: Trojan.GenericKD.31170134
kaspersky	5.5	Dangerous: Trojan-Ransom.Win32.Encoder.E
eset	4.5.3.38739	Dangerous: Win32/Kryptik.GJLH
drweb	11.0.1.1607061217	Dangerous: Trojan.PWS.Panda.13495
clam_av	0.99.2	Clean
comodo	1.1.268025.1	Dangerous: Malware
bitdefender	11.0.1.18	Dangerous: Trojan.GenericKD.31170134
avast	2.1.2	Clean
symantec	7.9.0.30	Dangerous: Packed.Generic.525