باسمه تعالی

گزارش تحلیل باج افزار Satan Cryptor v۲۲

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی به نام Satan Cryptor v۲۲ خبر می‌دهد. بررسی‌های اولیه نشان می‌دهد فعالیت این باج‌افزار در ۸ آوریل سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد همانند نسخه قبلی تمرکز آن بیشتر بر روی کاربران انگلیسی، کره‌ای و چینی می‌باشد. اولین نسخه این باج‌افزار در اواسط ماه دسامبر ۲۰۱۷ میلادی منتشر شد که از قربانیان تقاضای پرداخت ۰.۵ بیت‌کوین به عنوان مبلغ باج‌خواهی می‌کرد، اما در نسخه‌ی جدید این مبلغ به ۰.۳ بیت‌کوین کاهش یافته است. با توجه به اینکه در هر دو نسخه‌ی باج‌افزار از یک ایمیل مشابه جهت برقراری ارتباط با مهاجمین استفاده شده است، این احتمال را می‌دهیم که توسعه‌دهندگان هر دو نسخه باج‌افزار یک فرد یا یک گروه باشند.

مشخصات فایل اجرایی :

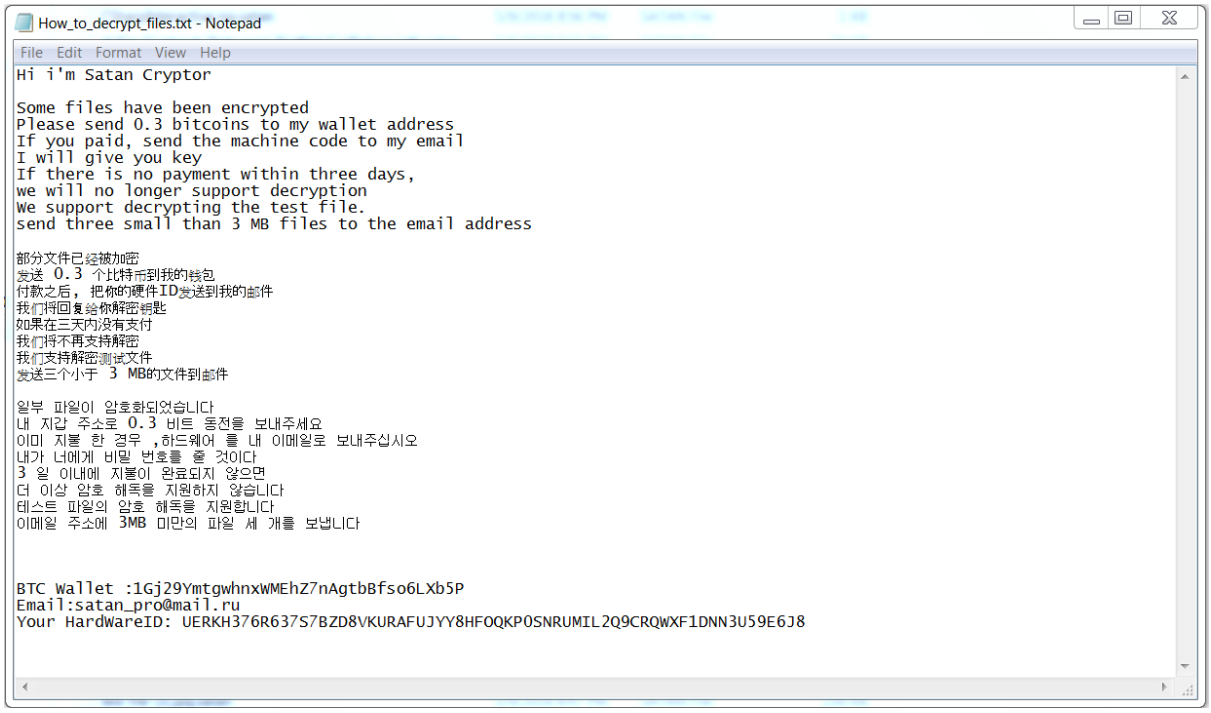
نام فایل	satan v۲.۲ ransomware
MD۵	fcea۲a۲۹fdbd٦c٦۹۸ea۳a۳۷de٤۱۳a۸۱۲
SHA-۱	۹۰۱fcadcd٦٦cb٤۸۸۳۹e۰٦bbc۲۳۸c٤۳c۹ca٥d۸۲ce
SHA-۲٥٦	۷٤۹٤٥c۳de۱da٦٥٥٥cddbac۸b٤۹d۹٥۹۳۲٤۸۰۳ea۱٤۲۰de۸۷d۷fed۹۰c۸۲۰ad۱۲۲a۲
اندازه فایل	۱٦۱ KB
کامپایلر/ پکر	UPX v۱.۲٥ (Delphi) Stub

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
UPX۰	۰	٤۰۹٦	۳۸۹۱۲۰	۰
UPX۱	۷.۹۳	۳۹۳۲۱٦	۱٦۳۸٤۰	۱٦۲۸۱٦
.rsrc	٤.۳۹	٥٥۷۰٥٦	٤۰۹٦	۱۰۲٤

تحلیل پویا :

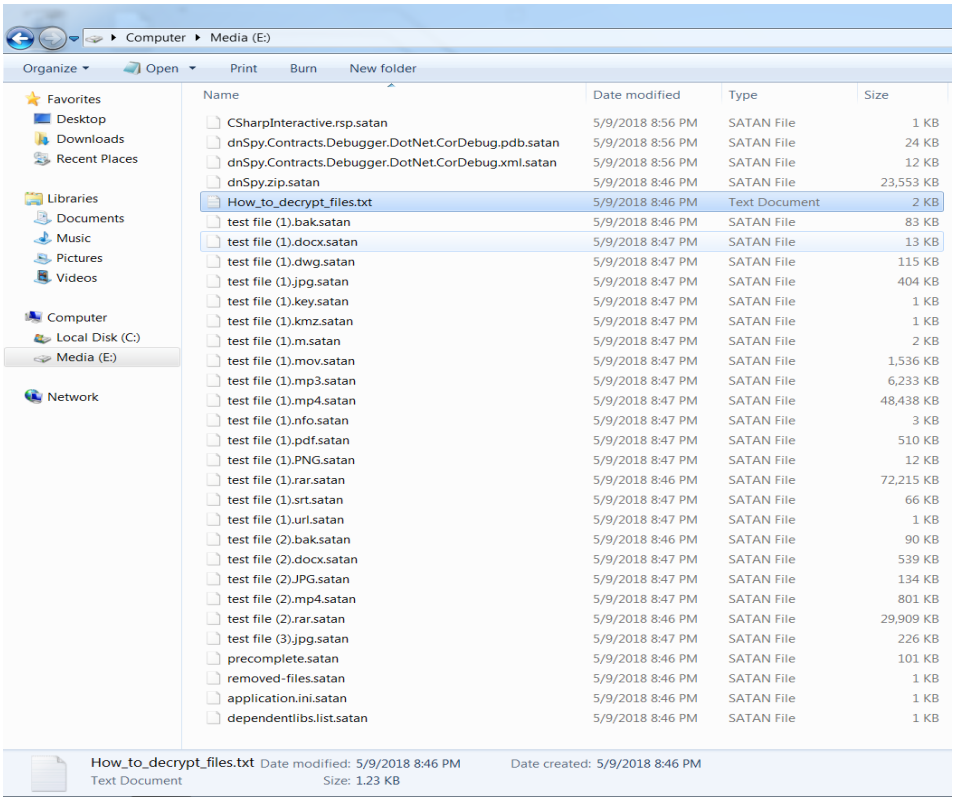
برای بررسی عمیق‌تر باج‌افزار Satan Cryptor v۲۲، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره، فایل‌ها را با استفاده از الگوریتم رمزنگاری DES رمزگذاری کرده و پسوند فایل‌ها را پس از رمزگذاری به satan. تغییر می دهد. سپس فرایند مربوط به اجرای باج‌افزار خاتمه پیدا می‌کند و پیغام باج‌خواهی که یک فایل متنی با فرمت TXT تحت عنوان How_to_decrypt_files می‌باشد، بر روی Desktop به نمایش در می‌آید. همچنین یک نسخه از این فایل در کنار فایل‌های رمزگذاری شده قرار می‌گیرد. تصویر زیر پیغام باج‌خواهی باج افزار Satan Cryptor v۲۲ را نشان می‌دهد.



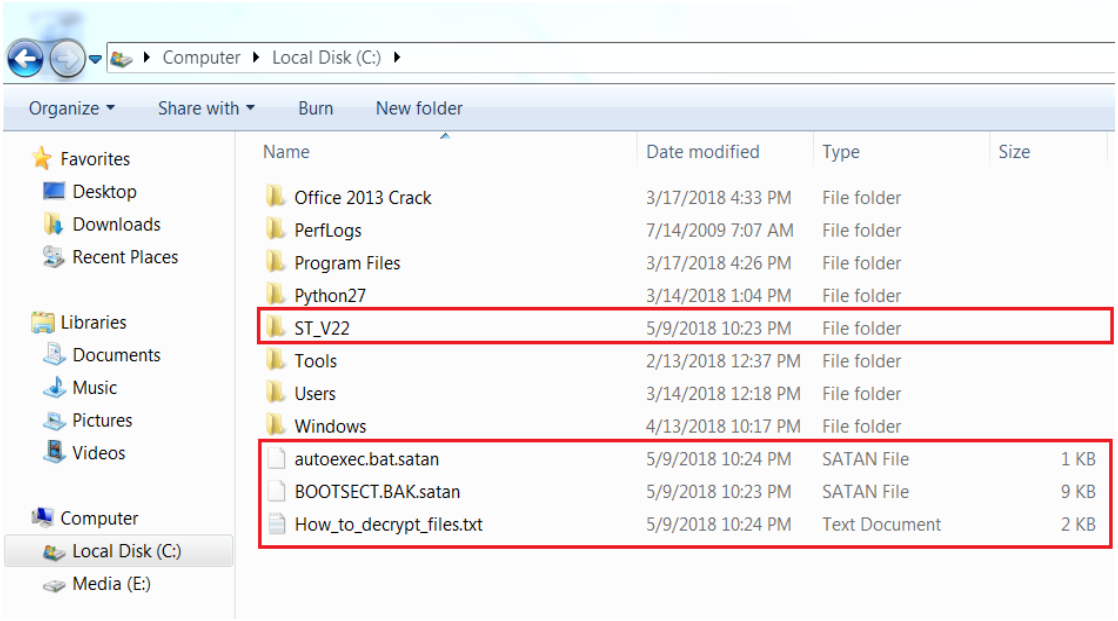
بر اساس پیغام باج‌خواهی که به ۳ زبان انگلیسی، کره‌ای و چینی می‌باشد، مهاجمین برای رمزگشایی فایل‌ها، تقاضای پرداخت مبلغ ۰.۳ بیت‌کوین به آدرس ۱Gj۲۹YmtgwhnxWMEhz۷nAgtbBfso۶LXb۵P نموده‌اند. پس از پرداخت مبلغ باج، قربانیان باید کد شناسایی خود را که این کد برای هر قربانی منحصربفرد می‌باشد، از طریق آدرس ایمیل satan_pro@mail.ru برای مهاجمین ارسال نمایند تا بعد از تایید پرداخت توسط مهاجمین کلید رمزگشایی فایل‌ها در اختیار قربانیان قرار گیرد. مهاجمین برای پرداخت مبلغ باج ۳ روز به قربانیان مهلت داده‌اند. از تفاوت‌هایی که پیغام باج‌خواهی نسخه جدید باج‌افزار با نسخه‌ی قدیمی آن دارد

می‌توان به تغییر شکل ظاهری، تغییر آدرس کیف پول بیت‌کوین، حذف شمارنده مهلت پرداخت در نسخه‌ی جدید و کاهش مبلغ باج‌خواهی به ۰.۳ بیت‌کوین اشاره نمود.

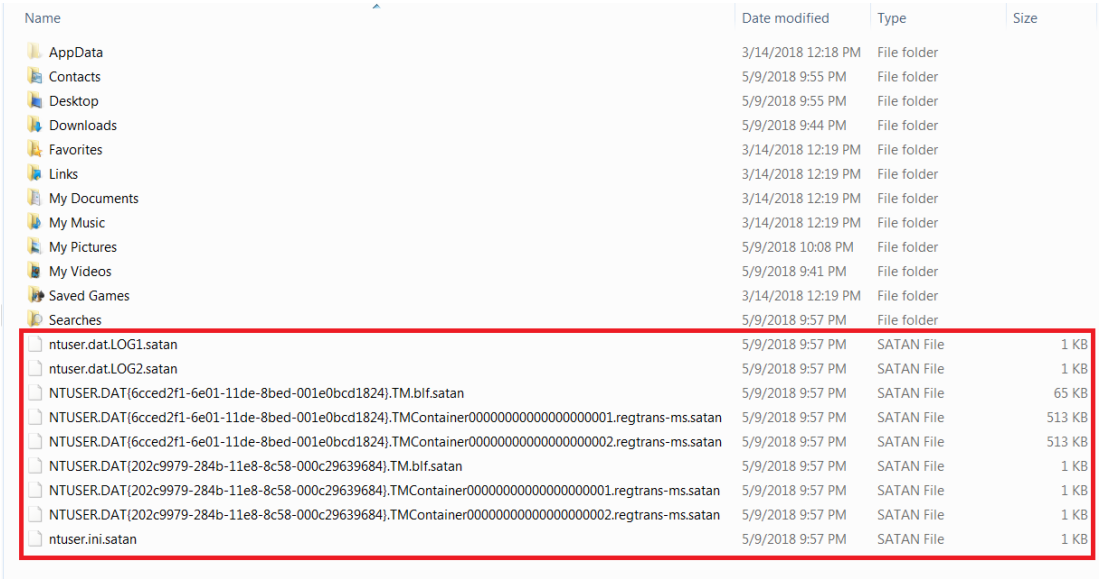
همانطور که پیشتر اشاره کردیم، این باج‌افزار پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به satan. تغییر می‌دهد تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج افزار می‌باشد :



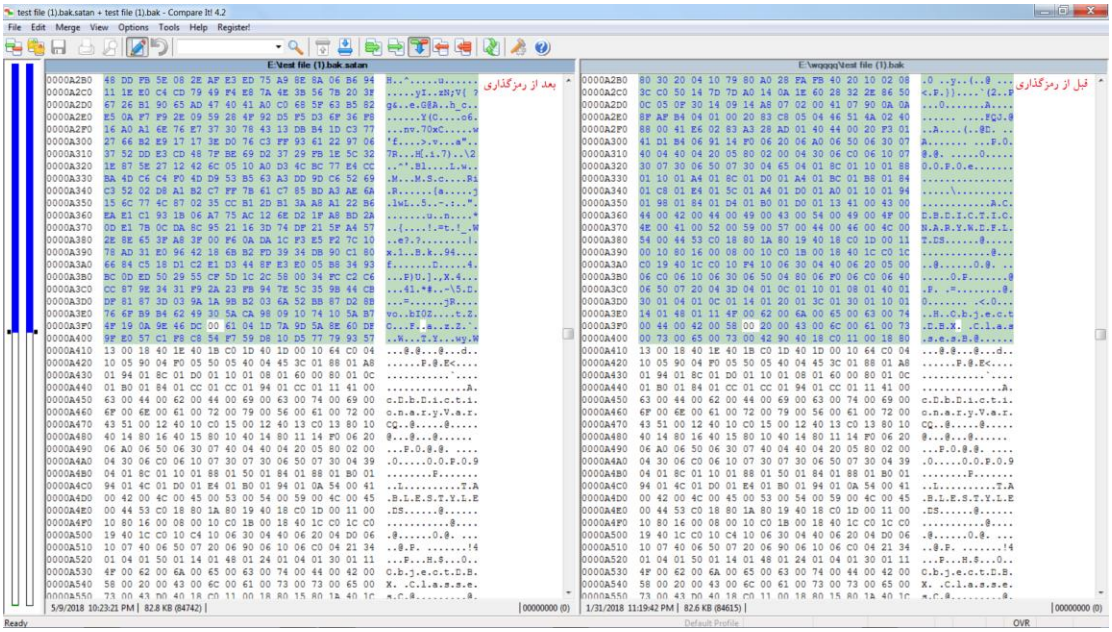
باج‌افزار Satan Cryptor v۲۲ یک پوشه به نام ST_v۲۲ در مسیر C:\ ایجاد می‌کند که درون پوشه یک فایل به نام KSession وجود دارد که محتوای آن کد شناسایی مربوط به قربانی می‌باشد. همچنین این باج‌افزار تعدادی فایل دیگر نیز ایجاد می‌کند که در تصاویر زیر قابل مشاهده می‌باشند.



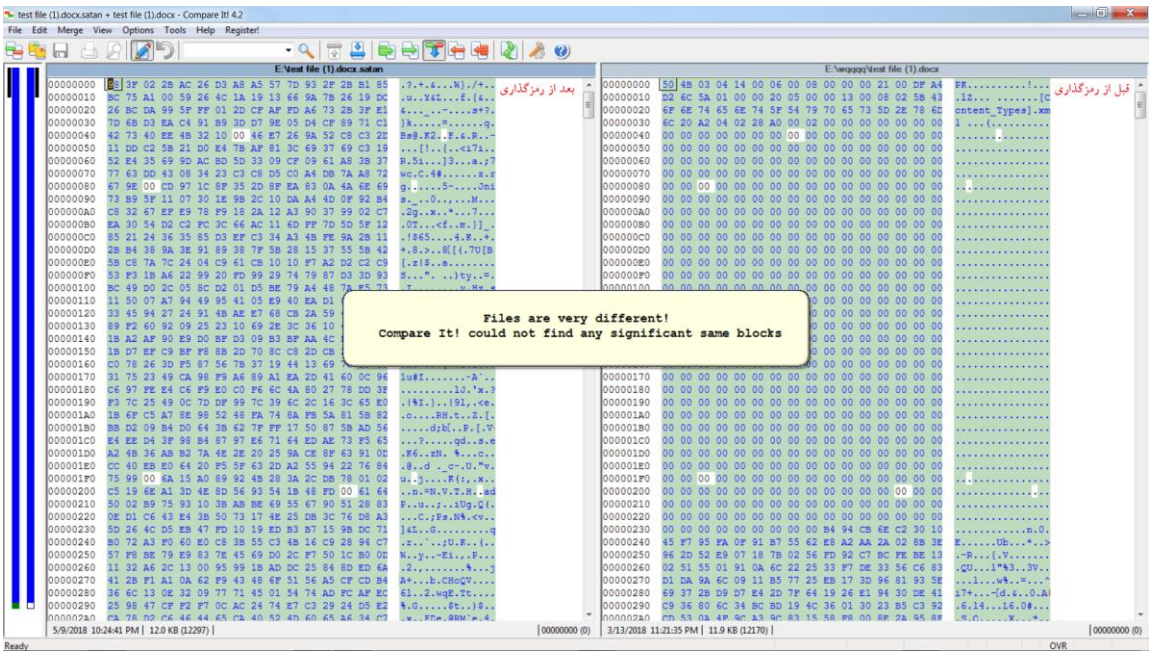
ضمناً مشاهده گردید که در مسیر C:\Users\admin فایل‌های مشخص شده در تصویر زیر نیز توسط باج‌افزار ایجاد می گردند.



طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری توسط باج‌افزار انجام دادیم شاهد این بودیم که باج‌افزار Satan Cryptor v۲۲ ساختار تمام فایل‌ها را به یک شکل رمزگذاری نمی‌کند و در مواجهه با فایل های مختلف رفتار متفاوتی از خود نشان می دهد. بدین صورت که ساختار بعضی از فایل‌ها را پس از رمزگذاری کاملا تغییر می‌دهد اما در مورد برخی از فایل‌ها فقط قسمتی از ساختار آن‌ها را تغییر می‌دهد، نتایج این بررسی‌ها در تصاویر زیر قابل مشاهده است.

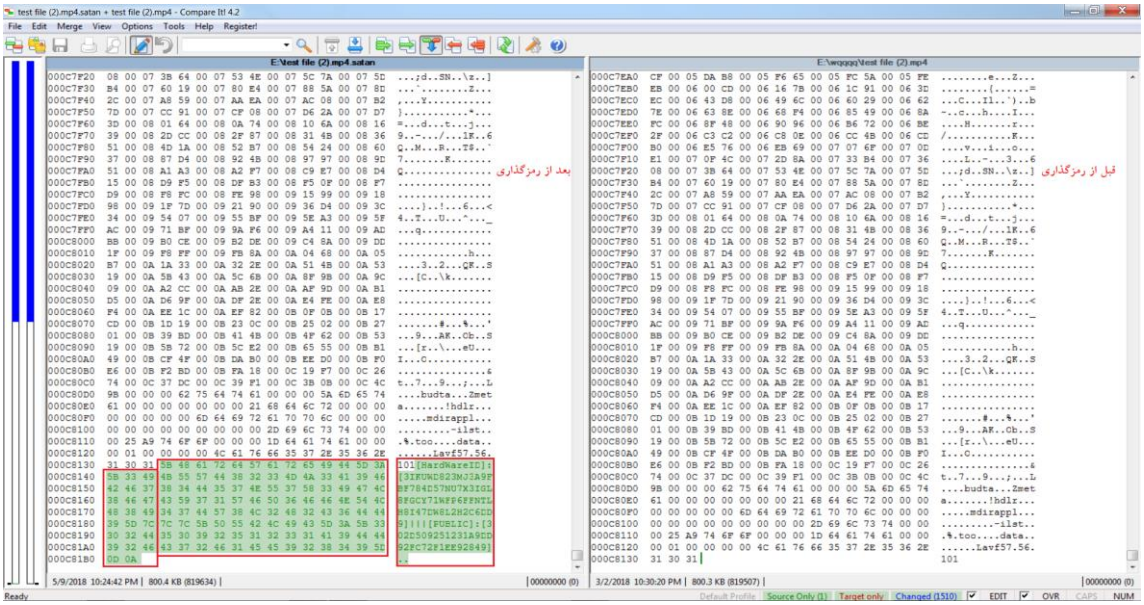


تصویر ۱ فقط بخشی از ساختار فایل تغییر کرده است.



تصویر ۲ تمام ساختار فایل تغییر کرده است.

همچنین پس از بررسی ساختار فایل‌ها پس از رمزگذاری، باج‌افزار کد شناسایی منحصر بفرد مربوط به قربانی را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند، این تغییر به خوبی در تصویر زیر قابل مشاهده است.

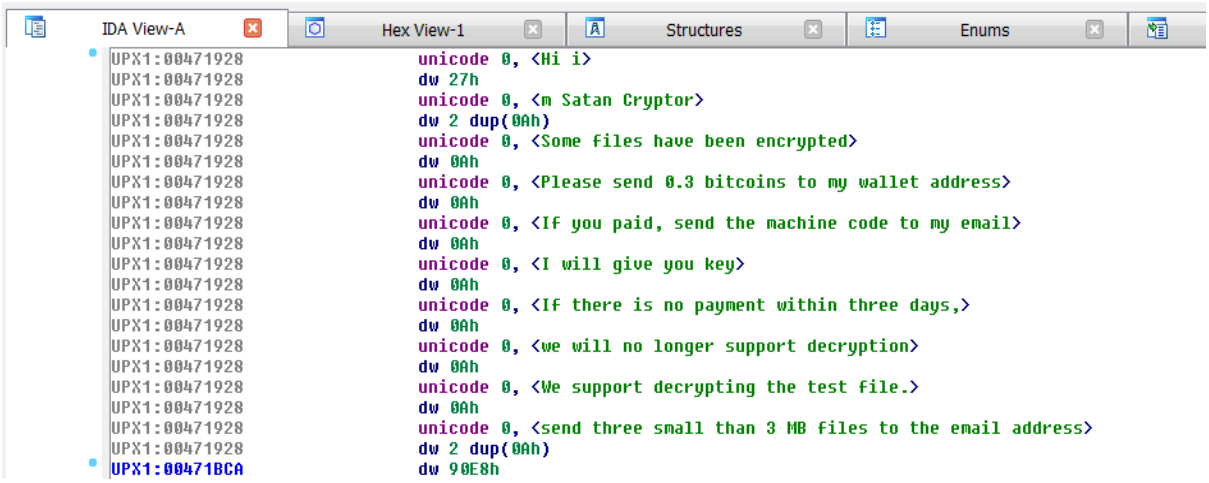


طبق بررسی‌ها اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول نیز مانند هرزنامه‌ها نیز وجود دارد.

تحلیل ایستا:

طبق بررسی کدمنبع باج‌افزار Satan Cryptor v۲۲ به نتایج زیر دست پیدا کردیم.

قطعه کد زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد.



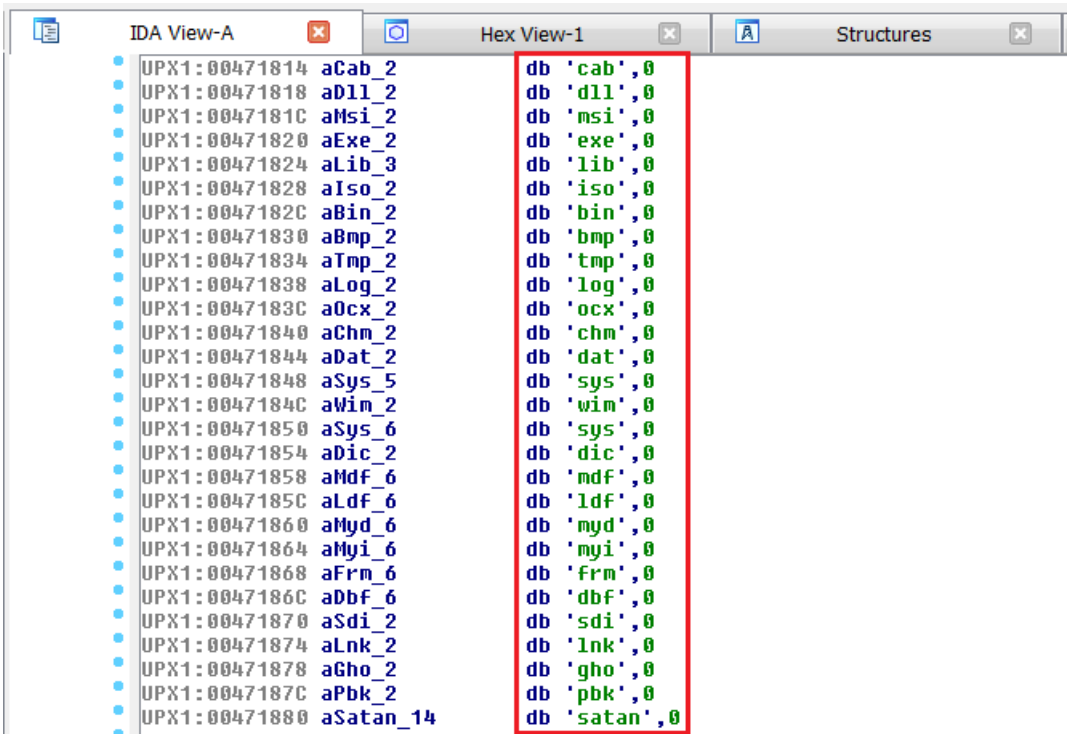
تصویر زیر نشان دهنده ایمیل مهاجم، فرایند notepad.exe برای نمایش پیغام باج‌خواهی و قطعه کد ایجاد کننده پوشه ST_v۲۲ حاوی کد شناسایی سیستم قربانی می‌باشد.

```
IDA View-A | Hex View-1 | Structures | Enums

UPX1:00471E40 ; const WCHAR off_471E40
UPX1:00471E40 off_471E40      dd offset asc_46FFFC+35h ; DATA XREF: sub_40F8B0+E0↑o
UPX1:00471E44 aJ29ymtgwhnxwme:
UPX1:00471E44                 unicode 0, <j29YmtgwhnxWMEhZ7nAgtbBfso6LXb5P>,0
UPX1:00471E86                 align 4
UPX1:00471E88 aEmail          db 0Ah                  ; DATA XREF: sub_40F8B0+F4↑o
UPX1:00471E88                 db 'Email:',0
UPX1:00471E90 ; const WCHAR aSatan_pro_mail
UPX1:00471E90 aSatan_pro@mail:                        ; DATA XREF: sub_40F8B0+113↑o
UPX1:00471E90                 unicode 0, <satan_pro@mail.ru>,0
UPX1:00471EB4 asc_471EB4:                             ; DATA XREF: sub_40F8B0+195↑o
UPX1:00471EB4                 dw 0Ah, 0
UPX1:00471EB8 aYourHardwareid db 0Ah                  ; DATA XREF: sub_40F8B0+163↑o
UPX1:00471EB8                 db 'Your HardWareID: ',0
UPX1:00471ECB                 align 4
UPX1:00471ECC aCSt_v22        db 'C:\ST_V22\',0       ; DATA XREF: sub_40F560+43↑o
UPX1:00471ED7                 align 4
UPX1:00471ED8 aCHow_to_decryp db 'C:\How to decrypt files.txt',0 ; DATA XREF: sub_40FD80+12↑o
UPX1:00471EF4 aSt             db 'ST',0               ; DATA XREF: sub_40FD80+1C↑o
UPX1:00471EF7                 align 4
UPX1:00471EF8 aBk             db 'BK',0               ; DATA XREF: sub_40FD80:loc_40FDDD↑o
UPX1:00471EFB                 align 4
UPX1:00471EFC aDb             db 'DB',0               ; DATA XREF: sub_40FD80:loc_40FE14↑o
UPX1:00471EFF                 align 10h
UPX1:00471F00 aAll            db 'ALL',0              ; DATA XREF: sub_40FD80:loc_40FE4D↑o
UPX1:00471F04 ; CHAR Parameters[]
UPX1:00471F04 Parameters      db 'C:\How_to_decrypt_files.txt',0 ; DATA XREF: sub_40FD80+DB↑o
UPX1:00471F20 ; CHAR File[]
UPX1:00471F20 File            db 'notepad.exe',0      ; DATA XREF: sub_40FD80+E0↑o
UPX1:00471F2C aBadCast        db 'bad cast',0         ; DATA XREF: sub_408560+E8↑o
UPX1:00471F2C                                         ; sub_408F40+E8↑o
UPX1:00471F35                 align 4
UPX1:00471F38 aBadLocaleName  db 'bad locale name',0  ; DATA XREF: sub_4028A0+8F↑o
UPX1:00471F48 aCProgramFile_1 db 'C:\Program Files (x86)\Microsoft Visual Studio 14.0\VC\include\xl'
UPX1:00471F48                                         ; DATA XREF: sub_402AE0+F↑o
UPX1:00471F48                                         ; sub_402C30+3C↑o ...
UPX1:00471F48                 db 'ocale',0
UPX1:00471F8F byte_471F8F     db 0                    ; DATA XREF: sub_402C30+6C↑o
UPX1:00471F8F                                         ; sub_4090D0+6C↑o ...
UPX1:00471F90 aCProgramFile_2:                        ; DATA XREF: sub_402D20+1F↑o
UPX1:00471F90                                         ; sub_402D20+3A↑o ...
```

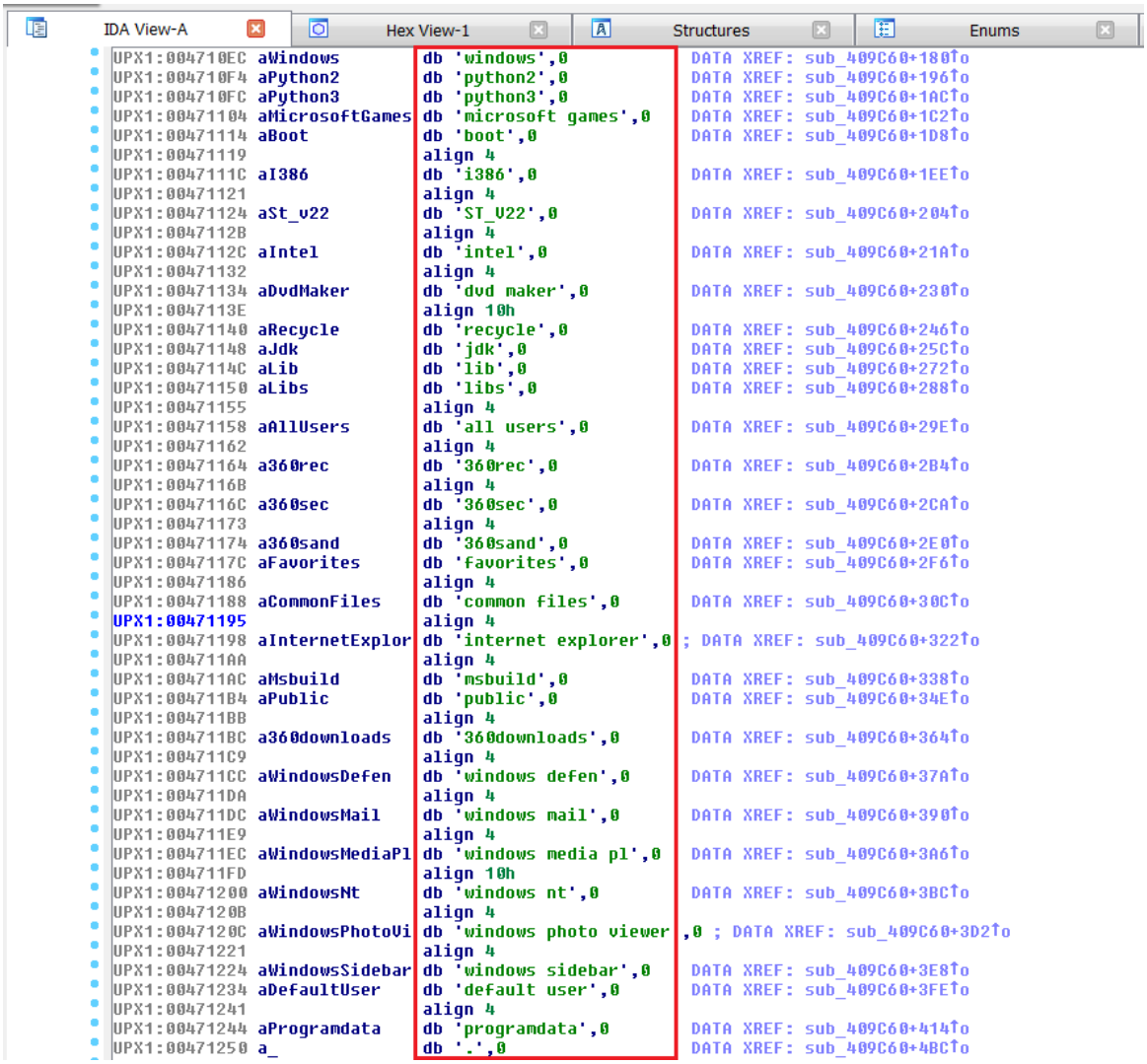
باج‌افزار پس از حمله به سیستم قربانی، با سرور کنترل و فرماندهی (C&C) خود ارتباط برقرار کرده و از این طریق کد شناسایی مربوط به قربانی دریافت می‌شود. تصویر نشان‌دهنده‌ی این فرایند می‌باشد.

```
IDA View-A | Hex View-1 | Structures | Enums

UPX1:00471888 aCabCount_php?s db '/cab/count.php?stauts=',0 ; DATA XREF: sub_40EED0+30↑o
UPX1:0047189F                 align 10h
UPX1:004718A0 aCode           db '&code=',0           ; DATA XREF: sub_40EED0+3D↑o
UPX1:004718A7                 align 4
UPX1:004718A8 ; const WCHAR pszAgentW
UPX1:004718A8 pszAgentW:                              ; DATA XREF: sub_40EED0+131↑o
UPX1:004718A8                 unicode 0, <Winnet Client>,0
UPX1:004718C4 ; const WCHAR pswzServerName
UPX1:004718C4 pswzServerName:                         ; DATA XREF: sub_40EED0+146↑o
UPX1:004718C4                 unicode 0, <58.222.181.122>,0
UPX1:004718E2                 align 4
UPX1:004718E4 ; const WCHAR pwszVersion
UPX1:004718E4 pwszVersion:                            ; DATA XREF: sub_40EED0+164↑o
UPX1:004718E4                 unicode 0, <HTTP/1.1>,0
UPX1:004718F6                 align 4
UPX1:004718F8 ; const WCHAR pwszVerb
UPX1:004718F8 pwszVerb:                               ; DATA XREF: sub_40EED0+180↑o
UPX1:004718F8                 unicode 0, <GET>,0
UPX1:00471900 aCSt_v22Ksess_0 db 'C:\ST_V22\KSession',0 ; DATA XREF: sub_40FE80+C3↑o
UPX1:00471913                 align 4
UPX1:00471914 aCSt_v22Ksessio db 'C:\ST_V22\KSession',0 ; DATA XREF: sub_40F170+18A↑o
UPX1:00471927                 align 4
UPX1:00471928 ; const WCHAR WideCharStr
UPX1:00471928 WideCharStr:                            ; DATA XREF: sub_40F8B0+5E↑o
UPX1:00471928                                         ; sub_40F8B0+A9↑o
```

طبق بررسی‌های انجام شده، فایل‌های موجود در پوشه‌های زیر با پسوندهای اشاره شده، توسط این باج‌افزار رمزگذاری نمی‌شوند.



تصویر ۱: فایل‌ها با پسوندهای مشخص شده در تصویر بالا توسط باج‌افزار رمزگذاری نمی‌شوند.



تصویر ۲: فایل‌های موجود در پوشه‌های مشخص شده در تصویر بالا توسط باج‌افزار رمزگذاری نمی‌شوند.

این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند، لیست کامل این کتابخانه‌ها به همراه توابع مورد استفاده در جدول زیر آمده است:

KERNEL۳۲.dll	shell۳۲.dll	ADVAPI۳۲.dll	WINHTTP.dll
ExitProcess GetProcAddress LoadLibraryA VirtualProtect	ShellExecuteA	OpenServiceA	WinHttpOpen

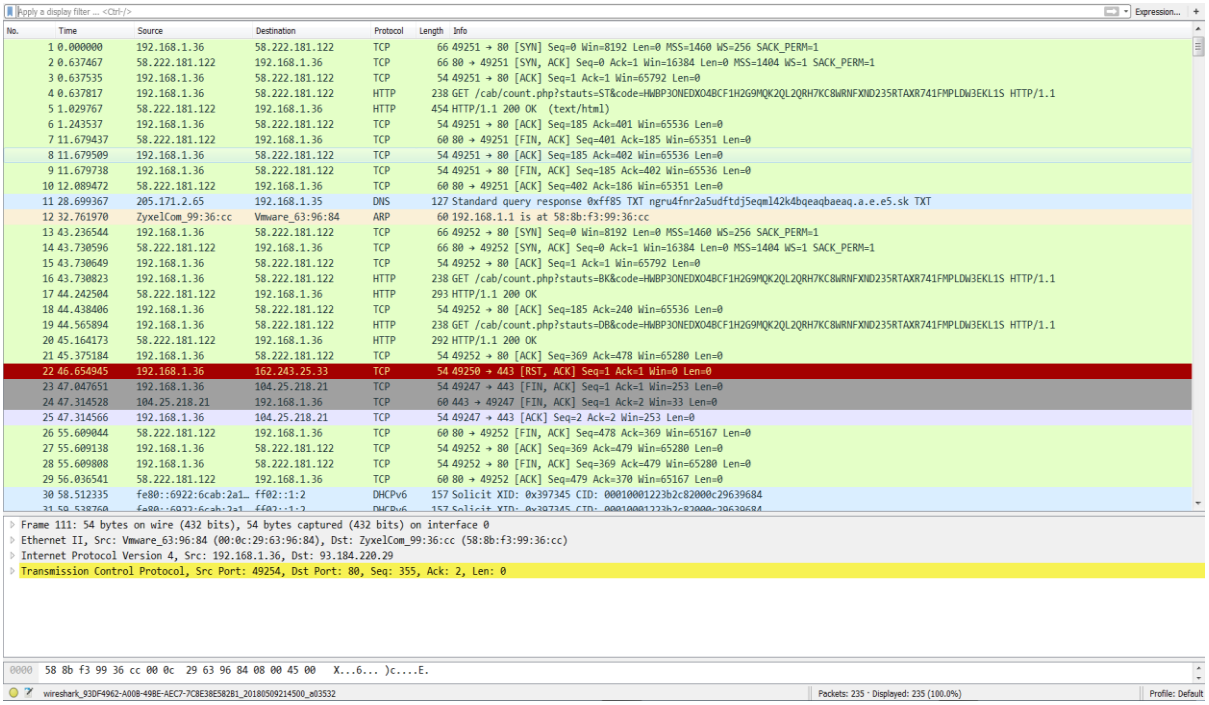
بر اساس بررسی‌های صورت گرفته، باج‌افزار Satan Cryptor v۲۲ پس از اجرا، فقط یک فرایند را ایجاد می‌کند، که آن هم مربوط به فایل اجرایی باج‌افزار می‌باشد و همانطور که قبلا اشاره شد پس از پایان فرایند، رمزگذاری فایل‌ها خاتمه پیدا می یابد.

Satan Cryptor v۲۲.exe

پس از خاتمه فرایند مربوط به باج‌افزار فرایند notepad.exe ایجاد می‌شود و پیغام باج‌خواهی به نمایش در می‌آید.

تحلیل ترافیک شبکه :

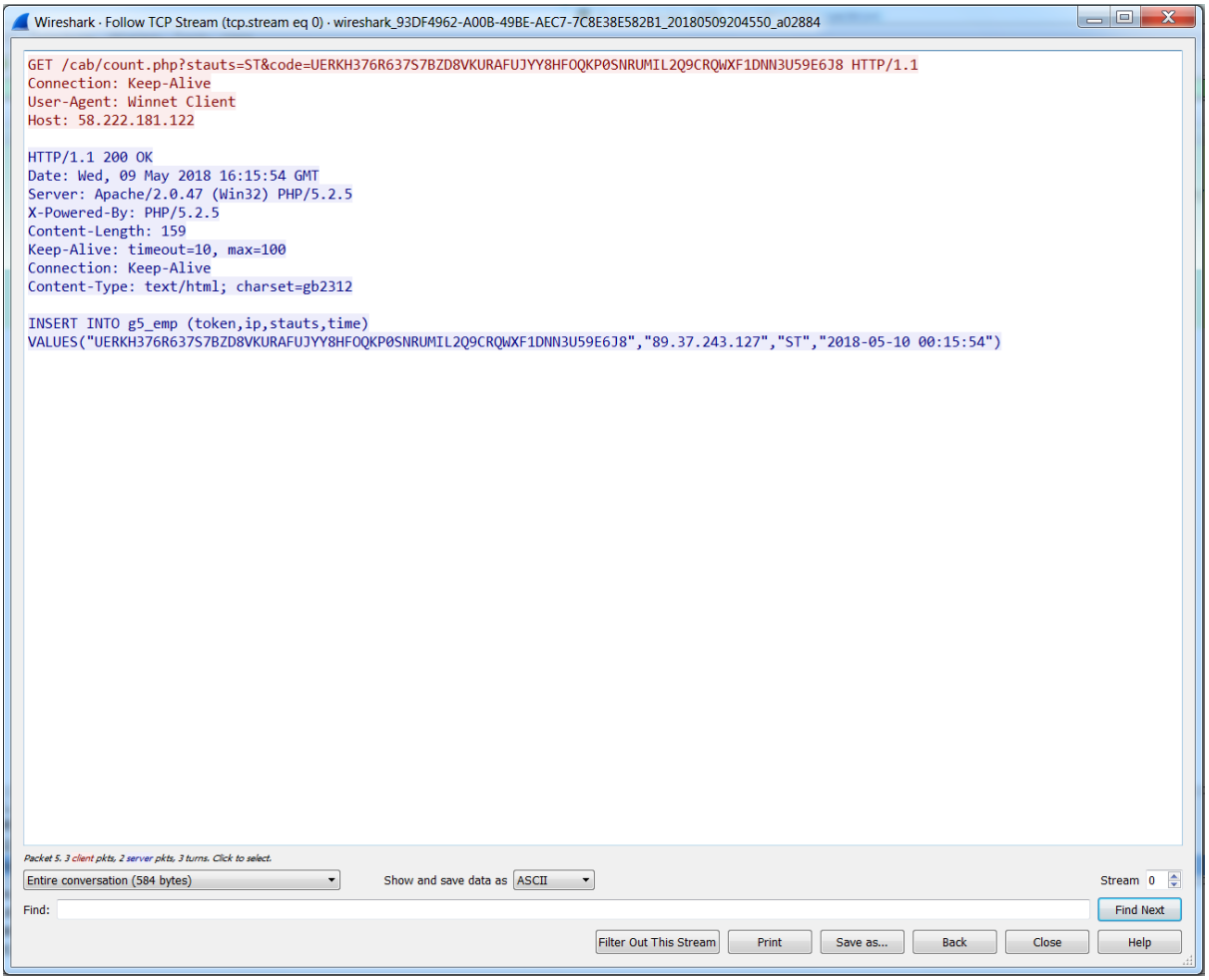
تصویر زیر بخشی از ارتباطات شبکه‌ای باج افزار Satan Cryptor v۲۲ را نشان می‌دهد.



لیست میزبان‌هایی که باج افزار با آن ها ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
چین	۸۰ TCP	۵۸.۲۲۲.۱۸۱.۱۲۲
ایالات متحده امریکا	٤٤٣ TCP	١٦٢.٢٤٣.٢٥.٣٣
اتحادیه اروپا	۸۰ TCP	۹۳.۱۸٤.۲۲۱.۲٤۰
ایالات متحده امریکا	۸۰ TCP	۱۷۲.۲۱۷.۲۲.۱٤۲

از بین موارد فوق، آی پی ۵۸.۲۲۲.۱۸۱.۱۲۲، مربوط به سرور کنترل و فرماندهی باج افزار می‌باشد که جزئیات بیشتر مربوط به آن در تصویر زیر قابل مشاهده است.



شناسایی :

در حال حاضر تعداد ۴۷ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Variant.Razy.289004	AegisLab	Troj.W32.Generic!c
AhnLab-V3	Trojan/Win32.DownLoader.C2452804	ALYac	Trojan.Ransom.Satan
Antiy-AVL	Trojan[Ransom]/Win32.Cryptor	Arcabit	Trojan.Razy.D468EC
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/FileCoder.ygcuy	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Gen:Variant.Razy.289004
CAT-QuickHeal	Trojan.IGENERIC	Comodo	.UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_60% (W)	Cylance	Unsafe
Cyren	W32/Trojan.UHSX-9228	Emsisoft	Gen:Variant.Razy.289004 (B)
eScan	Gen:Variant.Razy.289004	ESET-NOD32	Win32/Filecoder.NQC
F-Secure	Gen:Variant.Razy.289004	Fortinet	W32/Generic!tr
GData	Gen:Variant.Razy.289004	Ikarus	Trojan-Ransom.SatanCryptor
K7AntiVirus	Riskware (0040eff71)	K7GW	Riskware (0040eff71)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Ransom.SatanCryptor
MAX	malware (ai score=99)	McAfee	RDN/Generic Downloader.x
McAfee-GW-Edition	BehavesLike.Win32.Generic.cc	Microsoft	Trojan:Win32/Occamy.C
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	HEUR/QVM11.1.6129.Malware.Gen	SentinelOne	static engine - malicious
Sophos AV	Mal/Generic-S	Sophos ML	heuristic
Symantec	Downloader	Tencent	Win32.Trojan.Filecoder.Eibq
TrendMicro	Ransom_NATAS.THDABAH	TrendMicro-HouseCall	Ransom_NATAS.THDABAH
VBA32	suspected of Trojan.Downloader.gen.h	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Malware.Gen	Yandex	Trojan.Agent!dbELLmkQzm4
ZoneAlarm	HEUR:Trojan.Win32.Generic	Avast Mobile Security	Clean