باسمه تعالی

گزارش تحلیل باج افزار

RapidV۱

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت باج افزار RapidV۱ خبر می‌دهد. این باج‌افزار برای نخستین بار در ابتدای سال ۲۰۱۸ مشاهده گردید. براساس بررسی های صورت گرفته، مشخص گردید که باج افزار مورد اشاره علاوه بر فایل‌ها، نرم‌افزارهای نصب شده بر روی سیستم قربانی را نیز رمزگزاری می‌کند. اما اصلی ترین نکته درباره این باج افزار، ادامه فعالیت باج‌افزار پس از اتمام فرایند رمزگزاری می‌باشد. به طوری که باج‌افزار فایل‌های جدید اضافه شده به سیستم را نیز رمزگزاری می‌کند.

مشخصات فایل اجرایی :

نام فایل	Sample_٥b٨٥٠٩٥ca٠٣٤٢e٥a٦cf٥c٢٨d.exe
MD٥	٠da٩٥fbc٨٠٩٩٨٦٠٣bade٨ba٢٢e٠a٦٥٦٦
SHA-١	٩٦dbe١b٥d٧٣٤cf٧٢fa٦fe٠٣d٣٦ece٩٨f١٧efb٣f٤
SHA-٢٥٦	ad٦ba٠٤acbc٤٩٠d٣٦cc٦٤٩e٦٩a٩٢a٣٤١٣٠٠٧c١١٧١٣١٣e١٢٤٦٠٢٩٧e٧٥d٤٦٤٨b٧٥
اندازه فایل	٩١١.٥ KB
کامپایلر	Microsoft Visual C++ ٨.٠ Debug

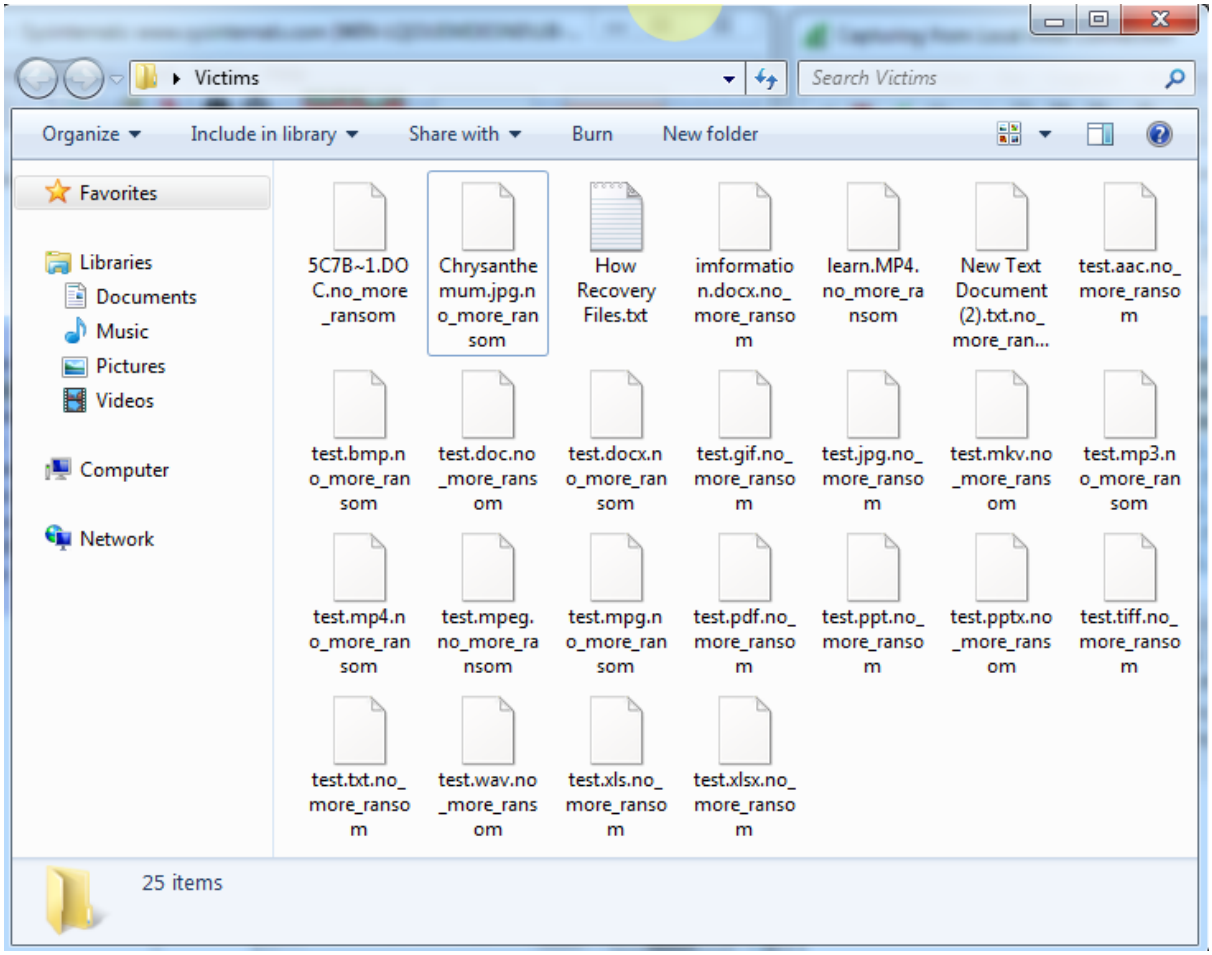
فایل اجرایی این باج افزار دارای سه بخش است :

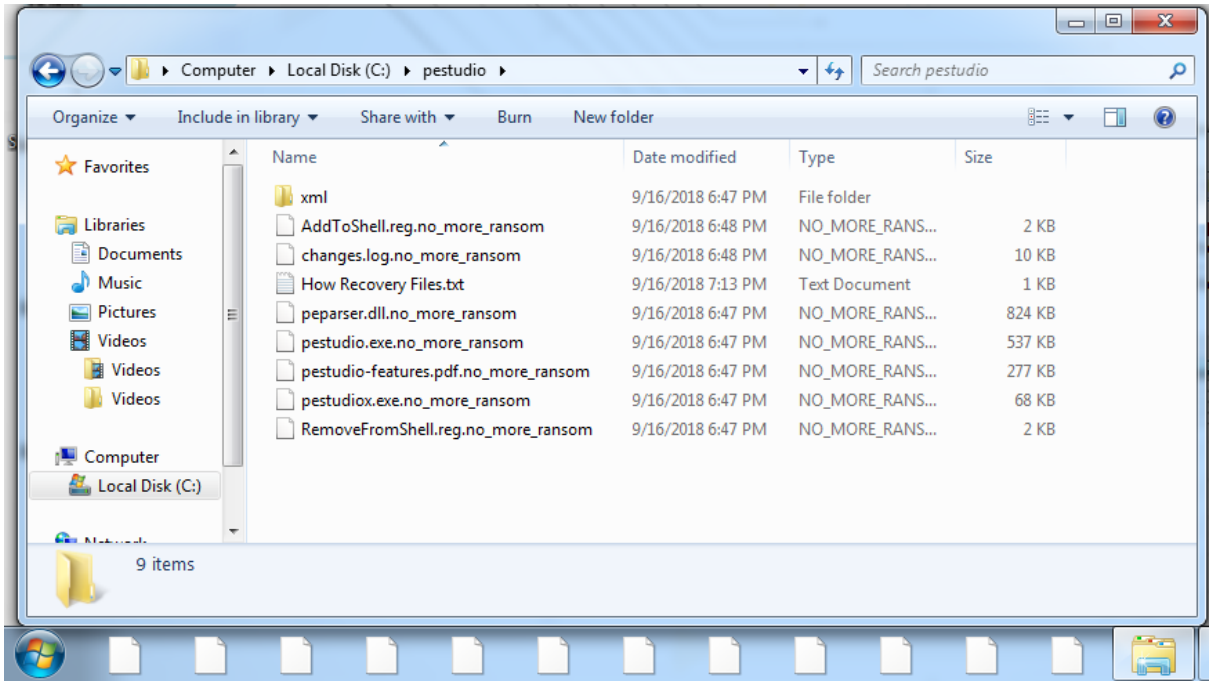
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٥.٤٤	٤٠٩٦	٧٣٢٨٤٥	٧٣٣١٨٤
.rdata	٣.٥٧	٧٣٧٢٨٠	١٦٢٣١٧	١٦٢٨١٦
.data	٢.٢٧	٩٠١١٢٠	٢٧٥٢٠	٤٠٩٦
.idata	٤.٣٩	٩٢٩٧٩٢	٤٦٣٧	٥١٢٠
.٠٠cfg	٠.٠٦	٩٣٧٩٨٤	٢٦٠	٥١٢
.rsrc	٢.١٤	٩٤٢٠٨٠	١٠٨٤	١٥٣٦
.reloc	٦.٢٩	٩٤٦١٧٦	٢٥٠٦٩	٢٥٠٨٨

تحلیل پویا :

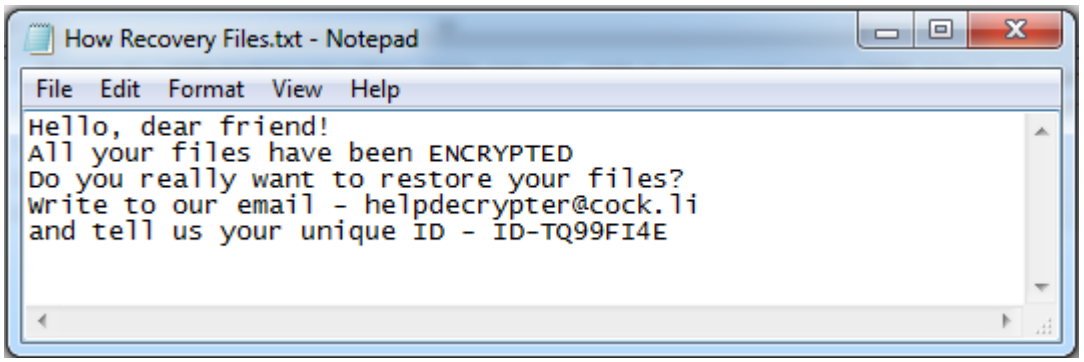
برای بررسی عمیق‌تر باج‌افزار RapidV۱، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. این باج افزار پس از ورود به سیستم اقدام به رمزگذاری فایل‌ها با استفاده از الگوریتم رمزنگاری AES می کند .این باج‌افزار تمامی فایل‌ها و نرم‌افزارهای نصب شده توسط کاربر را نیز مورد هدف قرار داده و پسوند no_more_ransom. به انتهای آن ها اضافه می کند.

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





حال پیغام باج‌خواهی باج‌افزار به صورت پنجره‌ای تحت عنوان HowRecoveryFile.txt برای قربانی نمایش داده می‌شود:



در این پیغام سازنده از قربانی می خواهد کلید منحصر به فردی که در پیغام باج خواهی ذکر شده است را به ایمیل helpdecrypter@cock.li برای تعیین مبلغ باج‌خواهی ارسال کند.

این پیغام ، که با فرمت txt می‌باشد در کنار تمامی فایل‌های رمزگزاری شده و دو بار در دسکتاب قرار داده شده است ، و هر چند ثانیه مجددا نمایش داده می‌شود .

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 سیستم میکند . تصاویر زیر روند جستجو فایل های هدف در هارد دیسک را نشان می دهد :

```
; =============== S U B R O U T I N E =======================================

; Attributes: thunk

; int __cdecl sub_403508(LPCSTR lpFileName)
sub_403508      proc near               ; CODE XREF: sub_4103D0+63↓p
                jmp     sub_410640
sub_403508      endp

; =============== S U B R O U T I N E =======================================
```

PCSTR lpFileName یکی از متد های تابع "GetFullPathName" می باشد که وظیفه بازیابی مسیر و نام فایل به خصوصی را بر عهده دارد .

```
stdcall CryptAcquireContextA(HCRYPTPROV *phProv, LPCSTR szContainer, LPCSTR szProvider, DWORD dwProvType, DWORD dwFlags)
      extrn CryptAcquireContextA:dword ; CODE XREF: sub_40BD40+2F↑p
                                       ; sub_40C2A0+36↑p ...
```

_ تابع فوق عملیات جست و جو جهت یافتن محتوا برای رمزگزاری را انجام می‌دهد .

_ تابع زیر اطلاعات مربوط به سیستم را بازیابی می کند .

```
; void __stdcall GetSystemInfo(LPSYSTEM_INFO lpSystemInfo)
          extrn GetSystemInfo:dword ; CODE XREF: sub_471FF0+56↑p
                                    ; DATA XREF: sub_471FF0+56↑r ...

        mov     dword ptr [ebp+SystemInfo.anonymous_0], eax
        mov     [ebp+SystemInfo.dwPageSize], eax
        mov     [ebp+SystemInfo.lpMinimumApplicationAddress], eax
        mov     [ebp+SystemInfo.lpMaximumApplicationAddress], eax
        mov     [ebp+SystemInfo.dwActiveProcessorMask], eax
        mov     [ebp+SystemInfo.dwNumberOfProcessors], eax
        mov     [ebp+SystemInfo.dwProcessorType], eax
        mov     [ebp+SystemInfo.dwAllocationGranularity], eax
        mov     dword ptr [ebp+SystemInfo.wProcessorLevel], eax
        lea     ecx, [ebp+SystemInfo]
        push    ecx             ; lpSystemInfo
        call    ds:GetSystemInfo
        mov     edx, [ebp+SystemInfo.dwPageSize]
```

_ تابع زیر نوع فایل ها را تشخیص می‌دهد .

```
loc_485FDC:                             ; CODE XREF: sub_485F00+D8↑j
                mov     ecx, [ebp+var_C]
                movzx   edx, byte ptr [ecx]
                and     edx, 8
                jnz     short loc_485FF7
                mov     eax, [ebp+hFile]
                push    eax             ; hFile
                call    ds:GetFileType
                test    eax, eax
                jnz     short loc_485FF7
                jmp     short loc_485F92
```

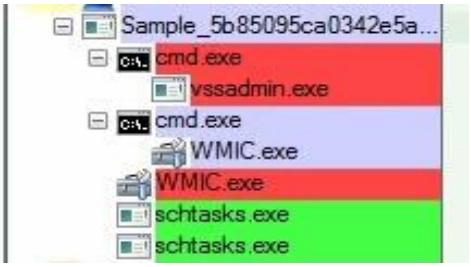
_ توابع زیر فرمت تاریخ و ساعت سیستم را مشخص می‌کنند .

```
int __stdcall GetDateFormatW(LCID Locale, DWORD dwFlags, const SYSTEMTIME *lpDate, LPCWSTR lpFormat, LPWSTR lpDateStr, int cchDate)
            extrn GetDateFormatW:dword ; CODE XREF: .text:00484650↑p
                                       ; DATA XREF: .text:00484650↑r ...
int __stdcall GetTimeFormatW(LCID Locale, DWORD dwFlags, const SYSTEMTIME *lpTime, LPCWSTR lpFormat, LPWSTR lpTimeStr, int cchTime)
            extrn GetTimeFormatW:dword ; CODE XREF: .text:0048485C↑p
                                       ; DATA XREF: .text:0048485C↑r ...
```

_ در تصویر زیر قطعه کد مربوط به پیغام باج‌خواهی نمایش داده شده است .

```
                dd offset aSr           ; "sr"
aHelloDearFrien db 'Hello, dear friend!',0Dh,0Ah ; DATA XREF: sub_407F50+1E↑o
                db 'All your files have been ENCRYPTED',0Dh,0Ah
                db 'Do you really want to restore your files?',0Dh,0Ah
                db 'Write to our email - helpdecrypter@cock.li',0Dh,0Ah
                db 'and tell us your unique ID - ID-',0
```

- این باج‌افزار پس از اجرا فرایندهای زیر را اجرا می‌کند.



تغییرات رجیستری :

Keys added:۱

HKU\S-۱-۵-۲۱-۲۸۵۳۸۶۲۵۳۲-۱۸۲۳۴۷۸۴۶۵-۲۸۸۳۷۲۳۸۳۱-۱۰۰۰\Software\EncryptKeys

---

Values added:۷

HKU\S-۱-۵-۲۱-۲۸۵۳۸۶۲۵۳۲-۱۸۲۳۴۷۸۴۶۵-۲۸۸۳۷۲۳۸۳۱-۱۰۰۰\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

HKU\S-۱-۵-۲۱-۲۸۵۳۸۶۲۵۳۲-۱۸۲۳۴۷۸۴۶۵-۲۸۸۳۷۲۳۸۳۱-۱۰۰۰\Software\Microsoft\Windows\CurrentVersion\Run\Encrypter_۰۷۴: ...

HKU\S-۱-۵-۲۱-۲۸۵۳۸۶۲۵۳۲-۱۸۲۳۴۷۸۴۶۵-۲۸۸۳۷۲۳۸۳۱-۱۰۰۰\Software\Microsoft\Windows\CurrentVersion\Run\userinfo: ...

HKU\S-۱-۵-۲۱-۲۸۵۳۸۶۲۵۳۲-۱۸۲۳۴۷۸۴۶۵-۲۸۸۳۷۲۳۸۳۱-۱۰۰۰\Software\EncryptKeys\local_enc_private_key_len: ۳۱ ۳۰ ۳۲ ۳۴ ۰۰ CD CD CD CD CD

HKU\S-۱-۵-۲۱-۲۸۵۳۸۶۲۵۳۲-۱۸۲۳۴۷۸۴۶۵-۲۸۸۳۷۲۳۸۳۱-۱۰۰۰\Software\EncryptKeys\local_enc_private_key: ۶۹ ۱۷ ۹F ۹B ED ۵۰ ۸۷ ۱C B۳ D۷ ۸۳ CF EB ۳A ۱A ۳B EB ۶E ۲۳ ۳۰ FD ۲۲ FE ۷A ۶B ۷D E۲ ۰۸ C۰ ۸۵ ۰B ۹۲ EF ۷۴ FF BE C۰ ۰۴ ...

HKU\S-۱-۵-۲۱-۲۸۵۳۸۶۲۵۳۲-۱۸۲۳۴۷۸۴۶۵-۲۸۸۳۷۲۳۸۳۱-۱۰۰۰\Software\EncryptKeys\local_public_key_len: ۳۱ ۳۴ ۳۸ ۰۰ CD CD CD CD CD CD

HKU\S-۱-۵-۲۱-۲۸۵۳۸۶۲۵۳۲-۱۸۲۳۴۷۸۴۶۵-۲۸۸۳۷۲۳۸۳۱-۱۰۰۰\Software\EncryptKeys\local_public_key: ۰۶ ۰۲ ۰۰ ۰۰ ۰۰ A۴ ۰۰ ۰۰ ۵۲ ۵۳ ۴۱ ۳۱ ۰۰ ۰۴ ۰۰ ۰۰ ۰۱ ۰۰ ۰۱ ...

_این‌طور به‌نظر می‌رسد که این باج‌فزار کلید خصوصی رمزنگـاری وهمچنـین کلیـد عمـومی رمزنگـاری را همراه با طول کلیدها به سیستم اضافه می‌نماید .

HKLM\SYSTEM\ControlSet۰۰۱\services\Tcpip\Parameters\Interfaces\{۸۱۶۷A۸F۱-۲۴۶C-۴A۴۴-۸F۵۶-D۷۱BA۹D۲C۱D۳}\T۱: ۰x۵B۹E۷۹۶۸

HKLM\SYSTEM\ControlSet۰۰۱\services\Tcpip\Parameters\Interfaces\{۸۱۶۷A۸F۱-۲۴۶C-۴A۴۴-۸F۵۶-D۷۱BA۹D۲C۱D۳}\T۲: ۰x۵B۹E۷۸۸۶

HKLM\SYSTEM\ControlSet۰۰۱\services\VSS\Diag\VolSnap\Volume{۴۷۰۴۷۸۹۸-۱e۶d-۱۱e۸-۸۷۸b-۸۰۶e۶f۶e۶۹۶۳}ComputeIgnorableProduct (Enter): ۴۸ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ C۰ ۶E B۴ ۱B ۵E ۰۸ D۴ ۰۱ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰C ۰۰ ۰۰ ۰۰ ۰۱ ۰۰

HKLM\SYSTEM\ControlSet۰۰۱\services\VSS\Diag\VolSnap\Volume{۴۷۰۴۷۸۹۸-۱e۶d-۱۱e۸-۸۷۸b-۸۰۶e۶f۶e۶۹۶۳}ComputeIgnorableProduct (Enter): ۴۸ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۹۳ ۶۸ ۹۷ ۹۷ D۱ ۴D D۴ ۰۱ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰C ۰۰ ۰۰ ۰۰ ۰۱ ۰۰

HKLM\SYSTEM\ControlSet۰۰۱\services\VSS\Diag\VolSnap\Volume{۴۷۰۴۷۸۹۸-۱e۶d-۱۱e۸-۸۷۸b-۸۰۶e۶f۶e۶۹۶۳}ComputeIgnorableProduct (Leave): ۴۸ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ EF ۹۴ DA ۱B ۵E ۰۸ D۴ ۰۱ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰D ۰۰

این باج‌افزار (VSS) Volume Shadow copy را از سیستم میزبان حذف می‌کند .

تحلیل ترافیک شبکه :

آی پی مرتبط با باج افزار :

IP	دامنه	کشور
۵٤.۱۹۲.۳۷.۵۲	amazon.com https://www.digicert.com	ایالات متحده آمریکا

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۵۰ 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.Ransom.Rapid.2	AhnLab-V3	Trojan/Win32.Generic.C2526331
ALYac	Trojan.Ransom.Rapid	Antiy-AVL	Trojan/Win32.AGeneric
Arcabit	Trojan.Ransom.Rapid.2	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira	HEUR/AGEN.1004117
AVware	Trojan.Win32.Generic!BT	BitDefender	Gen:Variant.Ransom.Rapid.2
CAT-QuickHeal	Ransom.Rapid.S2998282	ClamAV	Win.Ransomware.Generic-6545091-0
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.c80998
Cylance	Unsafe	Cyren	W32/Trojan.NZJQ-3474
DrWeb	Trojan.Encoder.25874	Emsisoft	Gen:Variant.Ransom.Rapid.2 (B)
Endgame	malicious (high confidence)	eScan	Gen:Variant.Ransom.Rapid.2
ESET-NOD32	a variant of Win32/Filecoder.Rapid.A	F-Secure	Gen:Variant.Ransom.Rapid.2
Fortinet	W32/Filecoder.NOZ!tr.ransom	GData	Win32.Trojan-Ransom.Filecoder.CF@gen
Jiangmin	Trojan.Generic.cnvub	K7AntiVirus	Trojan (00533c551)
K7GW	Trojan (00533c551)	Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Ransom.Rapid	MAX	malware (ai score=94)
McAfee	Artemis!0DA95FBC8099	McAfee-GW-Edition	BehavesLike.Win32.Generic.dm
Microsoft	Trojan:Win32/Malex.gen!F	NANO-Antivirus	Trojan.Win32.Filecoder.fgrnfk
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.b06	Rising	Trojan.Filecoder!8.68 (TFE:5:TBk6Tb8bToP)
SentinelOne	static engine - malicious	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Ransom.BTCware
Tencent	Win32.Trojan.Filecoder.Isv	TheHacker	Trojan/Filecoder.Rapid.a
TrendMicro	Ransom_RAPID.THHBCAH	TrendMicro-HouseCall	Ransom_RAPID.THHBCAH
VBA32	BScope.Trojan.Encoder	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Trojan.Gen	ZoneAlarm	HEUR:Trojan.Win32.Generic

خروجی سامانه ویروس کاو مرکز ماهر :

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	✔	Clean
sophos	9.15.0	✔	Clean
f_secure	11.00	!!	Dangerous: Gen:Variant.Ransom.Rapid.2
kaspersky	5.5	!	Suspicious: HEUR:Trojan.Win32.Generic
eset	4.5.3.38739	!!	Dangerous: Win32/Filecoder.Rapid.A
drweb	11.0.1.1607061217	!!	Dangerous: Trojan.Encoder.25874
clam_av	0.99.2	!!	Dangerous: Win.Ransomware.Generic-6545091-0
comodo	1.1.268025.1	!!	Dangerous: TrojWare.Win32.Ransom.Filecoder.NOZ
bitdefender	11.0.1.18	!!	Dangerous: Gen:Variant.Ransom.Rapid.2
avast	2.1.2	✔	Clean
symantec	7.9.0.30	!!	Dangerous: Ransom.BTCware