باسمه تعالی

تحلیل فنی باج‌افزار

Termite

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور باج‌افزار Termite خبر می‌دهد. به نظر می‌رسد که فعالیت این باج‌افزار از اواخر ماه اوت ۲۰۱۸ میلادی شروع شده است. براساس گزارش‌های بدست آمده از مراجع امنیتی دنیا، این باج‌افزار با باج‌افزارهای SmartScreen، Xiaoba و Barak the Obama's EBBV ارتباط دارد. طبق بررسی‌های صورت گرفته، باج‌افزار Termite از الگوریتم AES برای رمزگذاری فایل‌های موردنظر خود در سیستم قربانی، استفاده می‌کند.

مشخصات فایل اجرایی :

نام فایل	
MD۵	٤٨e٤a٨c٤٢a٧e٨٤c٨٢٧٩d١b٤٨٩dc٥١٠٢٣
SHA-١	٦٤٦٢١٧٨١٥٥٠٠٥٨٦٧٦ef٥٦bc٤٤٥f٢٠٨c٨٣١d٣٧٨٧٩
SHA-٢٥٦	٠٢١ca٤٦٩٢d٣a٧٢١af٥١٠f٢٩٤٣٢٦a٣١٧٨٠d٦f٨fcd٩be٢٠٤٦d١c٢a٠٩٠٢a٧d٥٨١٣٣
اندازه فایل	١.٨٧ مگابایت

فایل اجرایی این باج‌افزار دارای ٤ بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٥٧	٤٠٩٦	٥٢٠٧٧٤	٥٢٤٢٨٨
.rdata	٦.١٧	٥٢٨٣٨٤	١٢٥٨٥٤٨	١٢٦١٥٦٨
.data	٤.٩٣	١٧٨٩٩٥٢	٢٢١٢٥٨	٨١٩٢٠
.rsrc	٢.١٩	٢٠١٥٢٣٢	٨٥٦٠٠	٨٦٠١٦

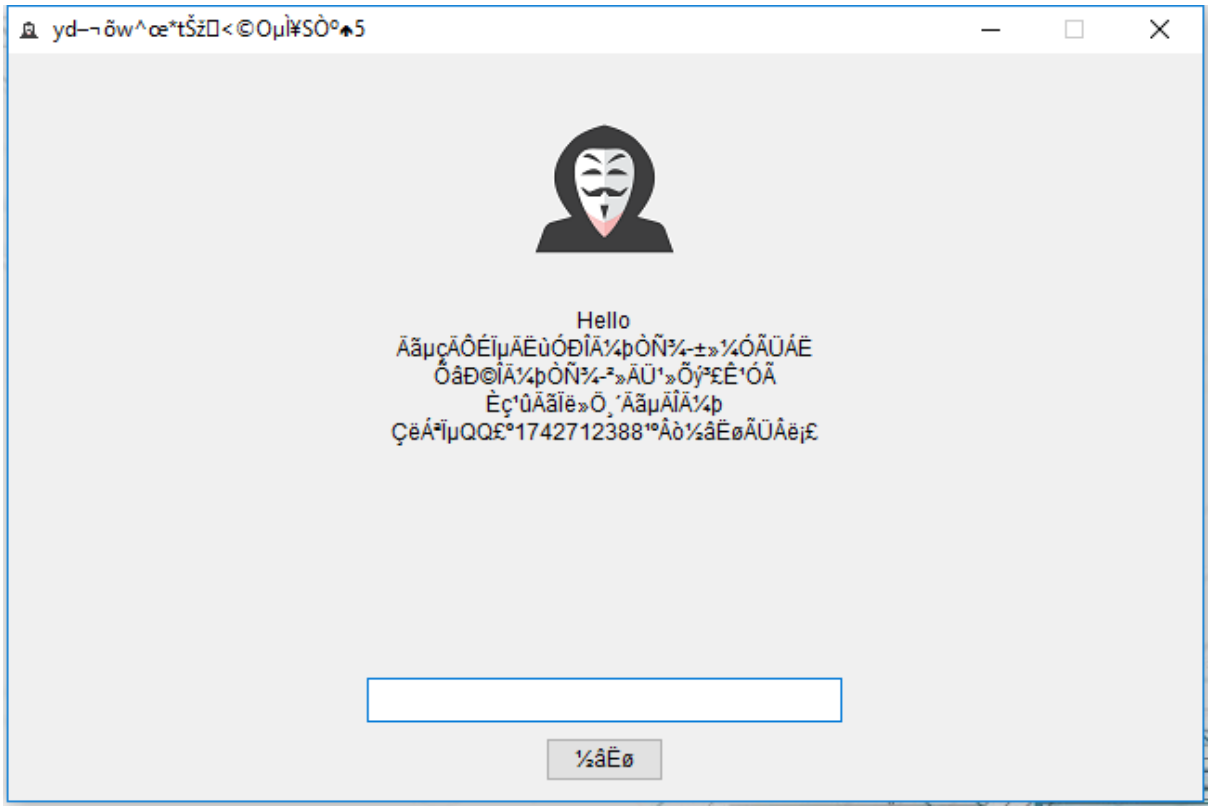
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Termite، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. باج‌افزار Termite به محض ورود به سیستم قربانی، از مسیر زیر اجرا می‌شود:

```
C:\Windows
```

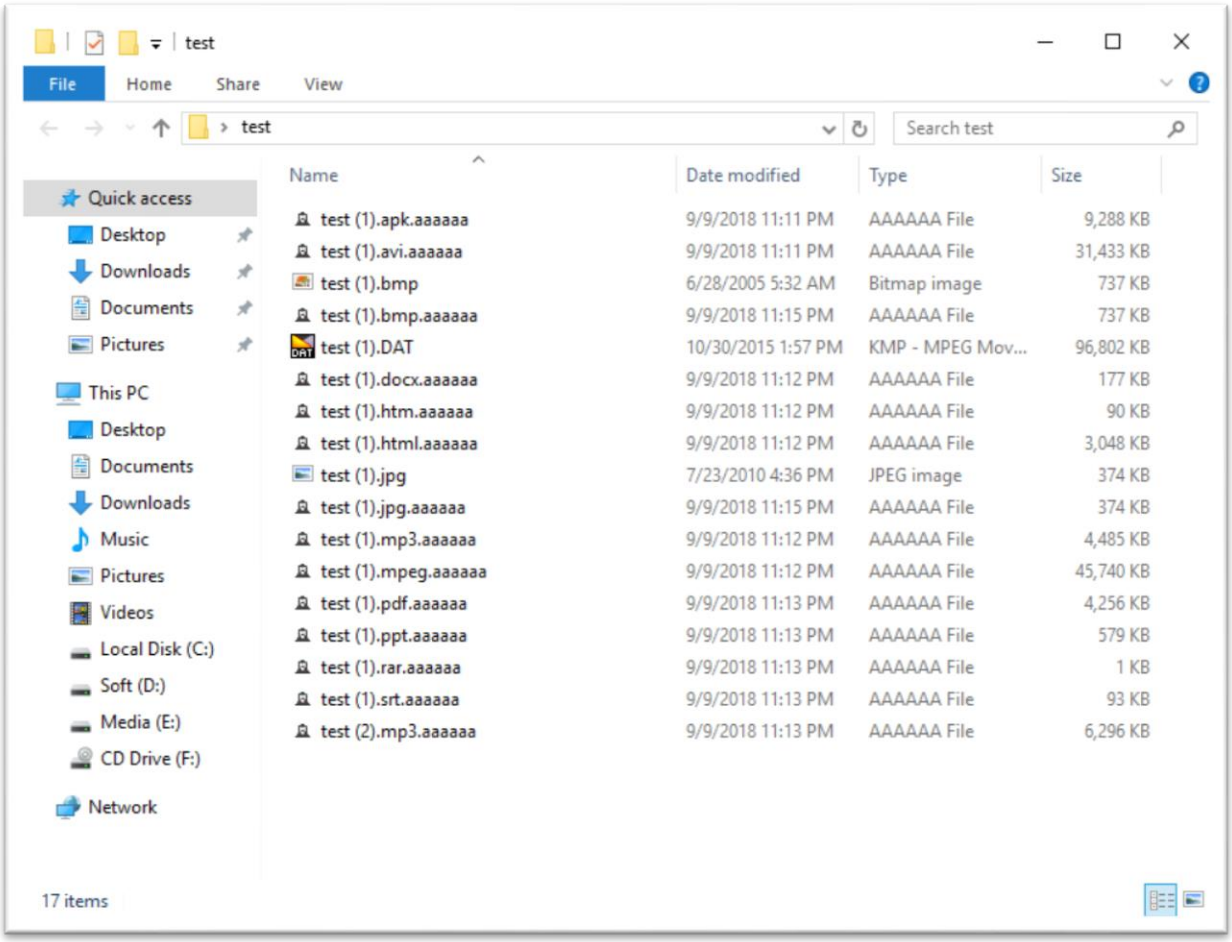
فایلی که در مسیر بالا قرار گرفته و اجرا می‌شود، Termite.exe نام دارد. در واقع باج‌افزار نیز به همین علت Termite نام‌گذاری شده است.

باج‌افزار Termite در مدت کوتاهی پس از شروع فعالیت در سیستم قربانی، فایل پیغام باج خود که یک فایل اجرایی با نام Payment.exe می‌باشد را، اجرا می‌کند و پنجره پیغام باج‌خواهی آن بر روی صفحه نمایش سیستم قربانی نمایش داده می‌شود. این فایل اجرایی بر روی صفحه دسکتاپ سیستم قربانی قرار می‌گیرد. پنجره پیغام باج‌خواهی به صورت زیر است:



همانطور که در تصویر بالا مشاهده می‌کنید، پیغام باج به یک زبان ناآشنا است که نمی‌توان از آن اطلاعات زیادی بدست آورد. پس از بررسی منابع معتبر موجود، آدرس ایمیلی با عنوان t٣١٤.٥٢٠@qq.com مربوط به باج‌افزار مشاهده کردیم. برای بررسی وضعیت فعالیت باج‌افزار و کسب اطلاعات در مورد مبلغ باج، به آدرس مذکور ایمیلی ارسال کردیم اما متأسفانه تا این لحظه پاسخی دریافت نکردیم. در هیچ یک از منابع معتبر نیز اطلاعات بیشتری در رابطه با این باج‌افزار مشاهده نکردیم.

پس از اتمام فرآیند رمزگذاری، فایل‌های سیستم قربانی به شکل زیر تغییر پیدا می‌کنند :



همانطور که در تصویر بالا مشاهده می‌کنید، باج‌افزار تعداد ٦ کاراکتر a را به انتهای فایل‌های رمزشده اضافه کرده است. با بررسی‌های بیشتری که بر روی فایل‌ها و مسیرهای مختلف سیستم‌عامل انجام دادیم، متوجه شدیم که این باج‌افزار فایل‌های dll، exe وDAT را رمزگذاری نمی‌کند و از فایل‌های با پسوند jpg. و bmp. یک کپی ایجاد می‌کند. دیگر انواع فایل‌ها با هر پسوندی، در سیستم قربانی رمزگذاری شده بودند. ضمناً این باج‌افزار هیچ فایلی را در پوشه ویندوز رمزگذاری نمی‌کند. *هر نوع فایل با نام فارسی نیز از هر تغییری توسط این باج‌افزار در امان است.* نکته بسیار جالب در مورد باج‌افزار Termite این است که فایل‌های با حجم کمتر از ۵۰ مگابایت را کاملا رمزگذاری می‌کند و فایل‌های با حجم بیشتر را از این مقدار را از سیستم پاک می‌کند.

این باج‌افزار پس از پایان عملیات رمزگذاری همچنان در سیستم قربانی به صورت فعال باقی می‌ماند و پس از چند دقیقه، تصویر زمینه سیستم قربانی به رنگ سیاه تغییر پیدا می‌کند.

تحلیل ایستا:

پس از تحلیل کد فایل اجرایی باج‌افزار نتایج زیر حاصل گردید:

همانطور که در بخش تحلیل در حال اجرا اشاره شد، این باج‌افزار فایل‌های با حجم بیشتر از ۵۰ مگابایت به غیر از یک نوع ذکر شده را، از سیستم قربانی پاک می‌کند. قطعه کد مربوط به آن را در ادامه مشاهده می‌کنید:

```
.text:00404270 loc_404270:                             ; DATA XREF: sub_4022A2+4FC↑o
.text:00404270                                         ; sub_4022A2+6A6↑o
.text:00404270                 mov     eax, [esp+0Ch]
.text:00404274                 mov     ecx, [eax]
.text:00404276                 push    ecx
.text:00404277                 call    ds:DeleteFileA
.text:0040427D                 mov     edx, [esp+4]
.text:00404281                 mov     [edx], eax
.text:00404283                 retn
```

از قطعه زیر برای تغییر تصویر زمینه سیستم قربانی استفاده شده است:

```
.text:00434A82                 call    ds:SetBkColor
.text:00434A88                 mov     ecx, [esi+58h]
.text:00434A8B                 mov     edx, [esi+54h]
.text:00434A8E                 push    330008h         ; rop
.text:00434A93                 push    0               ; y1
.text:00434A95                 push    0               ; x1
.text:00434A97                 push    edi             ; hdcSrc
.text:00434A98                 push    ecx             ; cy
.text:00434A99                 push    edx             ; cx
.text:00434A9A                 push    0               ; y
.text:00434A9C                 push    0               ; x
.text:00434A9E                 push    ebp             ; hdc
```

از قطعه کد زیر برای دریافت و نمایش پنجره پیغام باج‌خواهی استفاده شده است. این پنجره با فاصله زمانی چند ثانیه‌ای به صورت خودکار بر روی صفحه نمایش سیستم قربانی نمایش داده می‌شود:

```
.text:004734B8 loc_4734B8:                             ; CODE XREF: _AfxHandleSetCursor(CWnd *,uint,uint)
.text:004734B8                                         ; _AfxHandleSetCursor(CWnd *,uint,uint)+1A↑j
.text:004734B8                 mov     ecx, [ebp+arg_0]
.text:004734BB                 call    sub_474CA0
.text:004734C0                 test    eax, eax
.text:004734C2                 jz      short loc_473502
.text:004734C4                 push    dword ptr [eax+1Ch] ; hWnd
.text:004734C7                 call    ds:GetLastActivePopup
.text:004734CD                 push    eax
.text:004734CE                 call    sub_4736D4
.text:004734D3                 mov     esi, eax
.text:004734D5                 test    esi, esi
.text:004734D7                 jz      short loc_473502
.text:004734D9                 call    ds:GetForegroundWindow
.text:004734DF                 push    eax
.text:004734E0                 call    sub_4736D4
.text:004734E5                 cmp     esi, eax
.text:004734E7                 jz      short loc_473502
.text:004734E9                 mov     ecx, esi
.text:004734EB                 call    sub_4760A0
.text:004734F0                 test    eax, eax
.text:004734F2                 jz      short loc_473502
.text:004734F4                 push    dword ptr [esi+1Ch] ; hWnd
.text:004734F7                 call    ds:SetForegroundWindow
.text:004734FD                 push    1
.text:004734FF                 pop     eax
.text:00473500                 jmp     short loc_473504
```

از قطعه کد زیر برای دریافت اطلاعات فایل همچون آخرین زمان ایجاد، دسترسی و تغییر فایل و همینطـور اندازه فایل مورد نظر، استفاده شده است:

```
.text:004762D0                 lea     ecx, [ebp+LastWriteTime]
.text:004762D3                 push    ecx             ; lpLastWriteTime
.text:004762D4                 lea     ecx, [ebp+LastAccessTime]
.text:004762D7                 push    ecx             ; lpLastAccessTime
.text:004762D8                 lea     ecx, [ebp+CreationTime]
.text:004762DB                 push    ecx             ; lpCreationTime
.text:004762DC                 push    eax             ; hFile
.text:004762DD                 call    ds:GetFileTime
.text:004762E3                 test    eax, eax
.text:004762E5                 jz      short loc_4762F9
.text:004762E7                 push    0               ; lpFileSizeHigh
.text:004762E9                 push    dword ptr [edi+4] ; hFile
.text:004762EC                 call    ds:GetFileSize
.text:004762F2                 cmp     eax, ebx
.text:004762F4                 mov     [esi+0Ch], eax
.text:004762F7                 jnz     short loc_4762FD
```

از قطعه کد زیر برای دریافت نام و مسیر کامل فایل استفاده شده است:

```
.text:0047275C                 push    edi             ; lpBuffer
.text:0047275D                 push    esi             ; nBufferLength
.text:0047275E                 push    [ebp+lpFileName] ; lpFileName
.text:00472761                 call    ds:GetFullPathNameA
.text:00472767                 test    eax, eax
.text:00472769                 jnz     short loc_47277D
.text:0047276B                 push    esi             ; iMaxLength
.text:0047276C                 push    [ebp+lpFileName] ; lpString2
.text:0047276F                 push    edi             ; lpString1
```

از قطعه کد زیر برای دریافت نوع فایل استفاده شده است:

```
.text:00466472 loc_466472:                             ; CODE XREF: __ioinit+15F↑j
.text:00466472                 push    eax             ; nStdHandle
.text:00466473                 call    ds:GetStdHandle
.text:00466479                 mov     edi, eax
.text:0046647B                 cmp     edi, 0FFFFFFFFh
.text:0046647E                 jz      short loc_466497
.text:00466480                 push    edi             ; hFile
.text:00466481                 call    ds:GetFileType
.text:00466487                 test    eax, eax
.text:00466489                 jz      short loc_466497
.text:0046648B                 and     eax, 0FFh
.text:00466490                 mov     [esi], edi
.text:00466492                 cmp     eax, 2
.text:00466495                 jnz     short loc_46649D
```

از قطعه کد زیر برای دریافت مسیر دایرکتوری ویندوز استفاده شده است. همانطور که در قسمت تحلیل پویا اشاره شد، باج‌افزار فایل اجرایی خود را در این دایرکتوری قرار می‌دهد و هیچ نوع فایلی را در آن رمزگذاری نمی‌کند:

```
.text:0045D6FB
.text:0045D6FB loc_45D6FB:                             ; CODE XREF: sub_45D660+25↑j
.text:0045D6FB                                         ; sub_45D660+2A↑j
.text:0045D6FB                 cmp     eax, 9
.text:0045D6FE                 jnz     short loc_45D712
.text:0045D700                 lea     edx, [esp+108h+pszPath]
.text:0045D704                 push    104h            ; uSize
.text:0045D709                 push    edx             ; lpBuffer
.text:0045D70A                 call    ds:GetWindowsDirectoryA
.text:0045D710                 jmp     short loc_45D73E
```

درنهایت پس از پایان فرآیند رمزگذاری، باج‌افزار Termite با استفاده از قطعه کد زیر، نام فایل‌های رمزشده را به الگوی مورد نظر خود تغییر می‌دهد:

```
.text:004700B0 loc_4700B0:                             ; CODE XREF: sub_470032+76↑j
.text:004700B0                 cmp     dword ptr [esi+0A8h], 0
.text:004700B7                 lea     eax, [esi+5Ch]
.text:004700BA                 push    eax             ; LPOPENFILENAMEA
.text:004700BB                 jz      short loc_4700C4
.text:004700BD                 call    GetOpenFileNameA
.text:004700C2                 jmp     short loc_4700C9
.text:004700C4 ; ---------------------------------------------------------------------
.text:004700C4
.text:004700C4 loc_4700C4:                             ; CODE XREF: sub_470032+89↑j
.text:004700C4                 call    GetSaveFileNameA
```

اطلاعات کلید رجیستری مربوط به پسوند اضافه شده به فایل‌های رمزگذاری شده، به صورت زیر می‌باشد:

Path: HKLM\SOFTWARE\WOW٦٤٣٢NODE\MICROSOFT\TAIL

Key: TAIL

Value: aaaaaa

تحلیل ترافیک شبکه :

پس از بررسی وضعیت ترافیک شبکه ایجاد شده در سندباکس‌های آنلاین، پس از اجرای باج‌افزار، نتایج زیر حاصل گردید:

کشور	نام پروتکل	شماره پورت	آی پی
محدوده اتحادیه اروپا	TCP	۸۰	۲.۲۲.۴۸.۳۳
آمریکا	TCP	۸۰	۵۲.۱۳۸.۱۴۸.۱۵۲

خروجی سامانه VirusTotal :

در حال حاضر تنها تعداد ۴۷ مورد از ۶۸ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.GenericKD.40432542	AegisLab	Troj.W32.Gen.lwoF
AhnLab-V3	Trojan/Win32.Agent.C2689035	ALYac	Trojan.Ransom.Filecoder
Antiy-AVL	Trojan[Ransom]/Win32.Encoder	Arcabit	Trojan.Generic.D268F39E
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Agent.Y.7555	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Trojan.GenericKD.40432542	CAT-QuickHeal	Program.Unwaders
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.155005
Cylance	Unsafe	Cyren	W32/Trojan.ITZX-1653
DrWeb	Trojan.Encoder.25897	Emsisoft	Trojan.GenericKD.40432542 (B)
Endgame	malicious (high confidence)	eScan	Trojan.GenericKD.40432542
ESET-NOD32	a variant of Win32/Packed.FlyStudio.AA potentially unwanted	Fortinet	W32/Generic!tr
GData	Win32.Trojan.FlyStudio.F	Ikarus	Trojan-Ransom.Termite
K7AntiVirus	Trojan (005246d51)	K7GW	Trojan (005246d51)
Kaspersky	Trojan-Ransom.Win32.Encoder.fr	Malwarebytes	Ransom.Termite
MAX	malware (ai score=100)	McAfee	GenericR-NHJ!48E4A8C42A7E
McAfee-GW-Edition	BehavesLike.Win32.Generic.th	Microsoft	Trojan:Win32/Occamy.C

NANO-Antivirus	Trojan.Win32.FlyStudio.fgxnbo	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.e6d
Rising	Ransom.Encoder!8.FFD4 (CLOUD)	SentinelOne	static engine - malicious
Sophos AV	Generic PUA GE (PUA)	Sophos ML	heuristic
Symantec	Downloader	Tencent	Win32.Trojan.Encoder.Pgdg
TrendMicro	Ransom_TERMITE.THHBIAH	TrendMicro-HouseCall	Ransom_TERMITE.THHBIAH
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Trojan.Gen
ZoneAlarm	Trojan-Ransom.Win32.Encoder.fr		

خروجی سامانه ویروس‌کاو مرکز ماهر :

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

نتیجه اسکن Sample_5b851c51a0342e5a6cf5c2b4.exe

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن
پادویش	2.3.190.2675	Clean
sophos	9.15.0	Clean
f_secure	11.00	Dangerous: Trojan.GenericKD.40432542
kaspersky	5.5	Dangerous: Trojan-Ransom.Win32.Encoder.Fr
eset	4.5.3.38665	Dangerous: Win32/Packed.FlyStudio.AA Potentially Unwanted
drweb	11.0.1.1607061217	Dangerous: Trojan.Encoder.25897
clam_av	0.99.2	Clean
comodo	1.1.268025.1	Dangerous: Worm.Win32.Dropper.RA
bitdefender	11.0.1.18	Dangerous: Trojan.GenericKD.40432542
avast	2.1.2	Clean
symantec	7.9.0.30	Dangerous: Downloader