باسمه تعالی

تحلیل فنی باج‌افزار RetwyWare

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نسخه جدید باج‌افزار متن باز RetwyWare خبر می‌دهد. فعالیت این باج‌افزار در ماه آگوست سال ۲۰۱۸ میلادی آغاز گردیده است و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می باشد. طبق بررسی‌های صورت گرفته، باج‌افزار RetwyWare از الگوریتم رمزنگاری AES-۲۵۶ برای رمزگذاری فایل‌ها استفاده می‌کند و برای رمزگشایی آن ها از قربانی طلب ۳۴۵ دلار باج می‌کند.

مشخصات فایل اجرایی :

نام فایل	KillRabbit.exe killrabbitV۲-release.exe killrabbitV۲-release.bin
اندازه	۹۸۶ KB
Sha-۱	cdbdf۳۷۹۲۰٤d۹ee۳۳۲٦۵۹eb۲ba٤۵٦fbc۹٦a۰af٦۵
Sha-۲۵٦	۹۲c۵۰cd۲۵۳de٤۲۸۲۳a۲e۱a۵۹f۲۵۵۱aa۳۱۵ceb۱۲b۸f۷٤۱۸۲۰bdbc۱٤b۵ebe۱dfb۹
MD۵	f٦۹cb۰۷۳٦۲۳d۱cd۰۵٤c۱٤۰fc۲۳۱fbeea
کامپایلر	Microsoft Visual C++ ۸

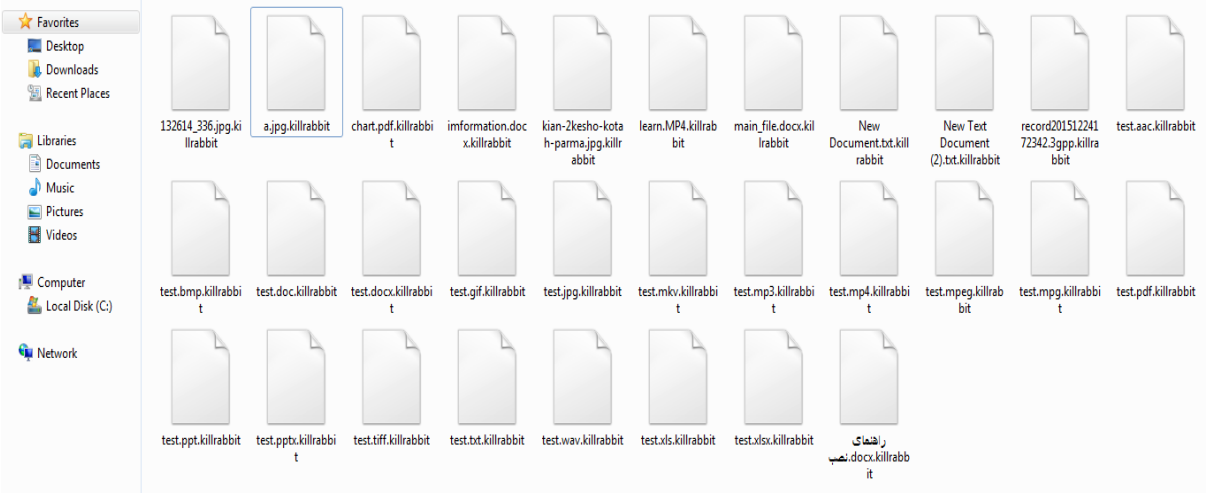
فایل اجرایی این باج‌افزار دارای پنج بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٦۸	٤۰۹٦	۵۸۰۹۱۰	۵۸۱۱۲۰
.rdata	۵.۷٦	۵۸۵۷۲۸	۱۸۸٦۸٦	۱۸۸۹۲۸
.data	۱.۲	۷۷۸۲٤۰	۳٦۷۲٤	۲۰۹۹۲
.rsrc	۷.۷۳	۸۱۵۱۰٤	۱۸۸۱۰۰	۱۸۸٤۱٦
.reloc	٦.۷۸	۱۰۰۳۵۲۰	۲۸۹۷٦	۲۹۱۸٤

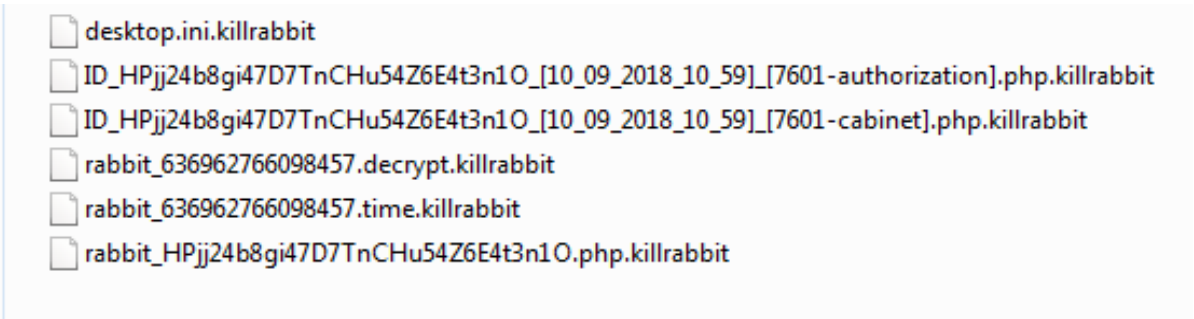
تحلیل پویا

برای بررسی عمیق‌تر باج‌افزار RetwyWare ، 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 باید در حالت مدیر سیستم (Administrator) اجرا شود تا حمله خود را کامل کند در غیر اینصورت قادر به توقف ادامه‌ی فعالیت فرایندها نمی‌باشد. باج‌افزار RetwyWare پس از رمزگذاری فایل ها، پسوند killrabbit. را به نام فایل های رمزگذاری شده اضافه می‌کند.

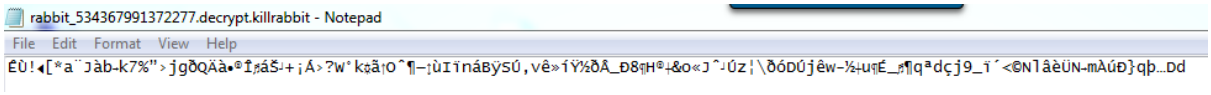
تصویر زیر نشان دهنده ی فایل های رمزگذاری شده توسط باج‌افزار RetwyWare می باشد :

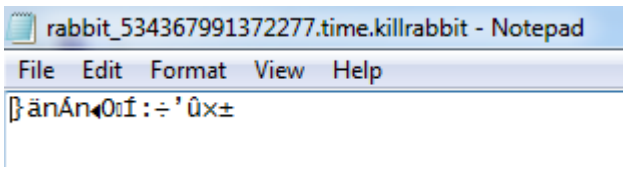


این باج‌افزار پس از اجرا، شش فایل بر روی دسکتاپ قرار می‌دهد. طبق بررسی‌های انجام شده، این فایل ها پس از هر بار اجرای باج‌افزار ، نام های متفاوتی دارند و فقط قسمت اول و آخر نام آنها ثابت است اما قسمت میانی هر بار تغییر می کند :



به نظر می‌رسد محتوای این فایل‌ها به نحوی مبهم سازی (Hardcode) شده و ناخوانا می‌باشند.





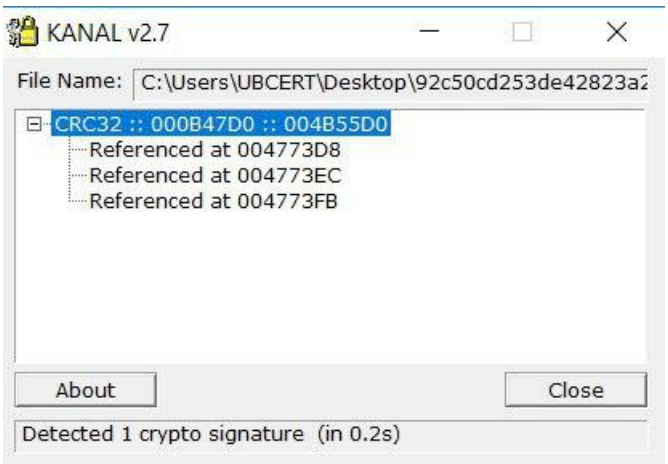
همانطور که گفته شد ، پس از تلاش های متوالی به محتوای این فایل ها دسترسی پیدا نکردیم و به طبع پیغام باج خواهی مشاهده نشد.

طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها وجود دارد.

تحلیل ایستا

با بررسی بیشتر کد های باج‌افزار به نتایج زیر دست یافتیم :

تصویر زیر بیانگر این است که این باج‌افزار از تکنیک رمزگذاری CRC۳۲ استفاده می کند:



در قطعه کد زیر مشخص می‌شود که باج‌افزار RetwyWare با زبان اسکریپت نویسی AutoIt v۳ نوشته شده است ، سپس برای ناخوانا شدن آن، پک شده است.

```
push    eax             ; phkResult
push    1               ; samDesired
push    esi             ; ulOptions
push    offset SubKey   ; "Software\\AutoIt v3\\AutoIt"
push    80000001h       ; hKey
call    ds:RegOpenKeyExW
test    eax, eax
jz      loc_43EC0A
```

قطعه کد زیر بیانگر این است که این باج‌افزار قبل از اجرا محیطی که قرار است در آن اجرا شود را بررسی می کند.

```
                        ; CODE XREF: sub_40C707+61↑j
                        ; DATA XREF: .text:off_40C88F↑o
push    104h            ; jumptable 0040C768 case 87
lea     eax, [ebp+Buffer]
push    eax             ; lpBuffer
push    offset aUserdnsdomain ; "USERDNSDOMAIN"

                        ; CODE XREF: sub_40C707+35A18↑j
                        ; sub_40C707+35AA2↓j ...
call    ds:GetEnvironmentVariableW
jmp     loc_441AD4
```

و همچنین نام کاربری ویندوز را هم بررسی می کند :

```
                        ; CODE XREF: sub_40C707+61↑j
                        ; DATA XREF: .text:off_40C88F↑o
lea     eax, [ebp+nSize] ; jumptable 0040C768 case 79
mov     [ebp+nSize], 104h
push    eax             ; pcbBuffer
lea     eax, [ebp+Buffer]
push    eax             ; lpBuffer
call    ds:GetUserNameW
jmp     loc_441AD4
```

با توجه به قطعه کد زیر ، این باج‌افزار فضای خالی دیسک و پارتیشن ها را نیز بررسی می کند :

```
lea     eax, [ebp+TotalNumberOfFreeBytes]
push    eax             ; lpTotalNumberOfFreeBytes
lea     eax, [ebp+TotalNumberOfBytes]
push    eax             ; lpTotalNumberOfBytes
lea     eax, [ebp+FreeBytesAvailableToCaller]
push    eax             ; lpFreeBytesAvailableToCaller
push    [ebp+lpDirectoryName] ; lpDirectoryName
call    ds:GetDiskFreeSpaceExW
test    eax, eax
jz      short loc_46B45A
fild    qword ptr [ebp+FreeBytesAvailableToCaller]
```

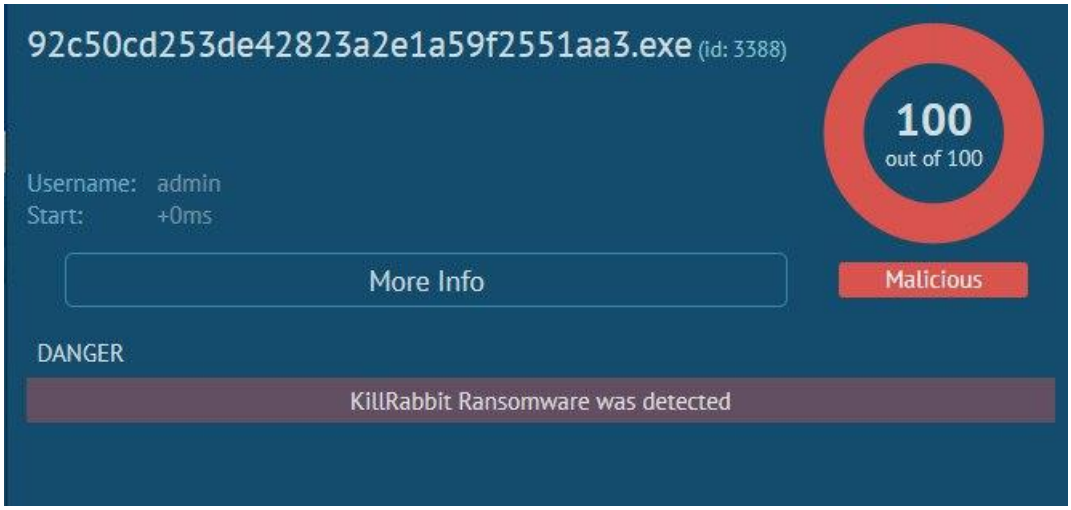
قطعه کد زیر ip مشکوکی را نشان می دهد که در حافظه یافت شده است که آدرس broadcast می باشد :

```
jnz     short loc_477EF7
mov     ecx, [ebp+cbMultiByte]
mov     edx, offset a255_255_255_25 ; "255.255.255.255"
call    sub_45A14D
test    al, al
jz      short loc_477EF7
```

طبق بررسی‌های صورت گرفته، باج‌افزار RetwyWare تشابهاتی با باج‌افزار CTB-Locker دارد :

details TrID distribution is very similar to the "CTB-Locker" family (e.g. SHA256: cbba56bd16222191f1468a1d93b63945394371cfb9ffe38f34a9575c5655e57a)
source TrID Evaluation

سندباکس ها نیز این باج‌افزار را با نام KillRabbit می شناسند :



بر اساس بررسی‌های صورت گرفته، باج‌افزار RetwyWare پس از اجرا، فرایند زیر را ایجاد می‌کند:

killrabbitV2-release.exe (PID: 2748)

کتابخانه های به کار برده شده در این باج‌افزار به شرح زیر هستند :

wsock32.dll
winmm.dll
mpr.dll
wininet.dll
psapi.dll
iphlpapi.dll
userenv.dll
version.dll
comctl32.dll
uxtheme.dll
kernel32.dll
user32.dll
gdi32.dll
comdlg32.dll
advapi32.dll
shell32.dll
ole32.dll
oleaut32.dll

تغییرات رجیستری

تغییرات رجیستری حاصل از بررسی باج‌افزار مطابق زیر می باشد.

مقادیراضافه شده:

HKU\S-۱-۵-۲۱-۲۸۵۳۸۶۲۵۳۲-۱۸۲۳۴۷۸۴۶۵-۲۸۸۳۷۲۳۸۳۱۱۰۰۰\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF۵CD-ACE۲-۴F۴F-۹۱۷۸-۹۹۲۶F۴۱۷۴۹EA}\Count\P:\Hfref\HOPREG\Qrfxgbc\۹۲p۵۰pq۲۵۳qr۴۲۸۲۳n۲r۱n۵۹s۲۵۵۱nn۳۱۵pro۱۲o۸s۷۴۱۸۲۰oqop۱۴o۵ror۱qso۹.rkr: ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۱ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ ۸۰ BF ۰۰ ۰۰ ۸۰ BF ۰۰ ۰۰ ۸۰ BF ۰۰ ۰۰ ۸۰ BF ۰۰ ۰۰ ۸۰ BF ۰۰ ۰۰ ۸۰ BF ۰۰ ۰۰ ۸۰ BF ۰۰ ۰۰ ۸۰ BF ۰۰ ۰۰ ۸۰ BF ۰۰ ۰۰ ۸۰ BF ۰۰ ۰۰ ۸۰ BF FF FF FF FF F۰ ۸C ۱۹ AD CF ۴۸ D۴ ۰۱ ۰۰ ۰۰ ۰۰ ۰۰

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبـان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار RetwyWare نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ٤٥ مورد از ٦٧ 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.31155041	AhnLab-V3	Malware/Win32.Generic.C2656723
ALYac	Trojan.Ransom.KillRabbit	Antiy-AVL	Trojan/Generic.ASVCS3S.1E5
Arcabit	Trojan.Generic.D1DB6361	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	TR/FileCoder.mponi
AVware	Trojan.Win32.Generic!BT	BitDefender	Trojan.GenericKD.31155041
CAT-QuickHeal	Trojan.Genasom	ClamAV	Win.Trojan.Agent-6638162-0
Comodo	.UnclassifiedMalware	CrowdStrike Falcon	malicious_confidence_100% (W)
Cylance	Unsafe	Cyren	W32/Trojan.FKXR-0205
DrWeb	Trojan.Encoder.25778	Emsisoft	Trojan.GenericKD.31155041 (B)
eScan	Trojan.GenericKD.31155041	ESET-NOD32	a variant of Win32/Filecoder.Autoit.T
F-Secure	Trojan.GenericKD.31155041	Fortinet	W32/Filecoder_Autoit.T!tr
GData	Trojan.GenericKD.31155041	Ikarus	Trojan-Ransom.Autoit
K7AntiVirus	Trojan (00539cbb1)	K7GW	Trojan (00539cbb1)
Kaspersky	Trojan-Ransom.Win32.Gen.khy	Malwarebytes	Ransom.FileCryptor.AutoIt
MAX	malware (ai score=100)	McAfee	Artemis!F69CB073623D
McAfee-GW-Edition	BehavesLike.Win32.Downloader.dh	Microsoft	Ransom:Win32/Genasom
Palo Alto Networks	generic.ml	Panda	Trj/CI.A
Qihoo-360	Win32/Trojan.Ransom.5e8	SentinelOne	static engine - malicious
Sophos AV	Mal/Generic-S	Sophos ML	heuristic
Symantec	Backdoor.Tinybaron	Tencent	Win32.Trojan.Gen.Edxk
TrendMicro	Ransom_KILLRABBIT.THHOGAH	TrendMicro-HouseCall	Ransom_KILLRABBIT.THHOGAH
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Trojan.GenKD
ZoneAlarm	Trojan-Ransom.Win32.Gen.khy	AegisLab	Clean
Avast Mobile Security	Clean	Babable	Clean
Baidu	Clean	Bkav	Clean
CMC	Clean	Cybereason	Clean
eGambit	Clean	Endgame	Clean
F-Prot	Clean	Jiangmin	Clean
Kingsoft	Clean	NANO-Antivirus	Clean
Rising	Clean	SUPERAntiSpyware	Clean
TACHYON	Clean	TheHacker	Clean
VBA32	Clean	ViRobot	Clean
Yandex	Clean	Zillya	Clean
Zoner	Clean	Alibaba	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۸ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس کاو قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Clean	✔	2.3.190.2675	پادویش
Clean	✔	9.15.0	sophos
Dangerous: Trojan.GenericKD.31155041	ii	11.00	f_secure
Dangerous: Trojan-Ransom.Win32.Gen.Khy	ii	5.5	kaspersky
Dangerous: Win32/Filecoder.Autoit.T	ii	4.5.3.38669	eset
Dangerous: Trojan.Encoder.25778	ii	11.0.1.1607061217	drweb
Dangerous: Win.Trojan.Agent-6638162-0	ii	0.99.2	clam_av
Dangerous: Malware	ii	1.1.268025.1	comodo
Dangerous: Trojan.GenericKD.31155041	ii	11.0.1.18	bitdefender
Clean	✔	2.1.2	avast
Dangerous: Backdoor.Tinybaron	ii	7.9.0.30	symantec