

باسمه تعالیٰ

تحلیل فنی باج افزار

Jemd

مقدمه :

رصد فضای سایبری در حوزه باج افزار، از ظهور باج افزار Jemid خبر می دهد. فعالیت این باج افزار نخستین بار در تاریخ ۱۶ دسامبر ۲۰۱۸ میلادی گزارش شده است. این باج افزار، از الگوریتم AES برای رمزگذاری فایل های سیستم قربانی استفاده می کند. نکته جالب در مورد باج افزار Jemid این است که هیچ تغییری در نام فایل ها ایجاد نکرده و پسوندی به آنها اضافه نمی کند. همچنین تا زمانی که فایل باج افزار در سیستم قربانی فعال باشد، نمی توان هیچ عملی (تغییر نام، کپی و...) بر روی فایل های رمزگذاری شده انجام داد.

مشخصات فایل اجرایی :

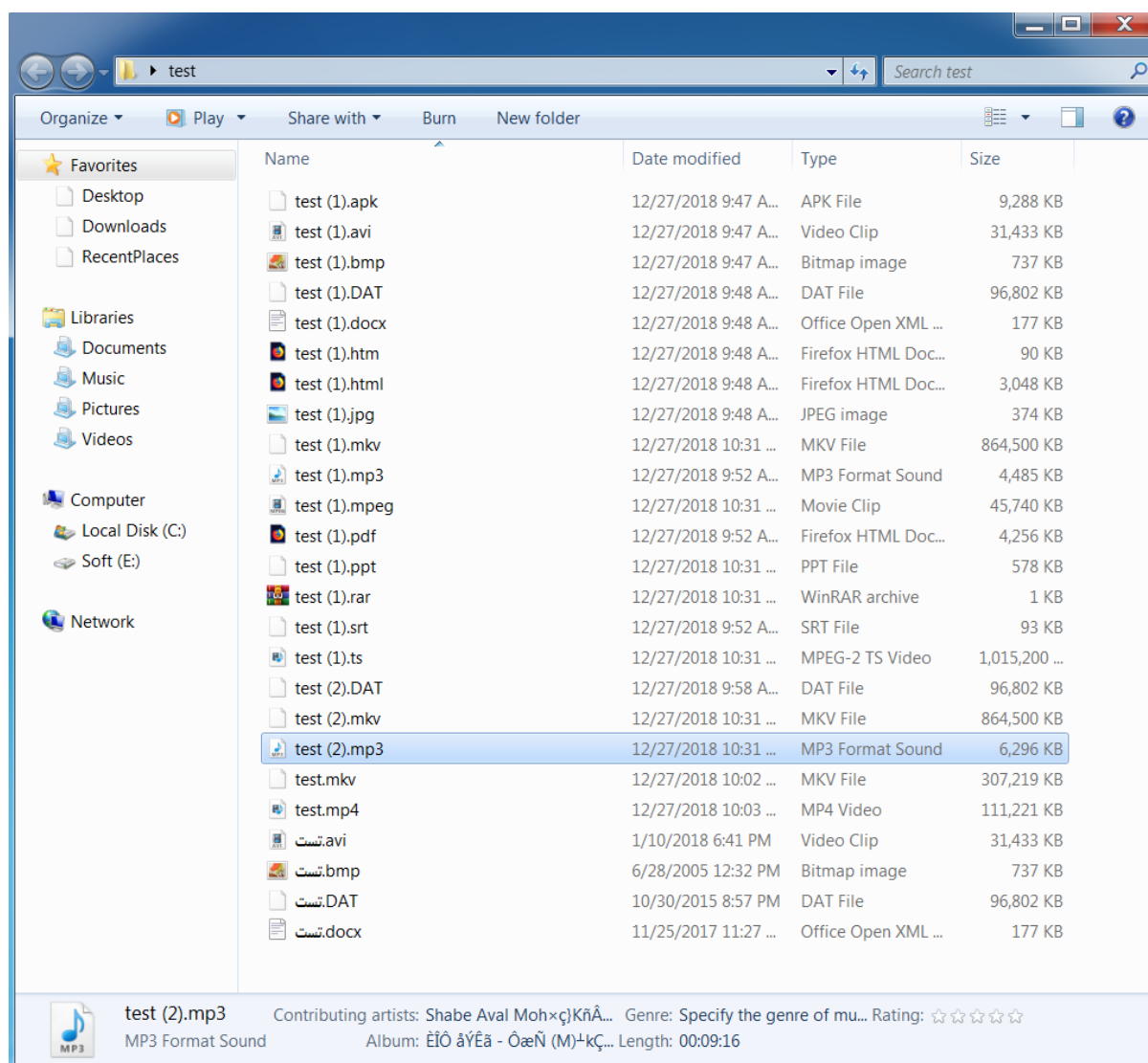
نام فایل	Project.exe
MD۵	۱f۸۵ac۹۲e۶ea۷۹a۴d۱cave۲۰ef۲۹۴d۷۶
SHA-۱	ee۸۱۸۴fff۲f۸۳۳d۱a۱c۶۵۹۱۷۹۶de۶۳۵d۸۴۴۶۵۲bd
SHA-۲۵۶	f۳۳۷۸۵b۱۲a۵۶a۰eb۷۰b۸f۴fab۱۰۸۷۷۷۷a۵۵۸e۷۵af۶b۱۱ae۶۲۹۴۹bb۵۶۸f۳c۸b۳۲۳
اندازه فایل	۱۰۲.۵ کیلوبایت

فایل اجرایی این باج افزار دارای ۸ بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
CODE	۶.۴۶	۴۰۹۶	۸۳۴۵۶	۸۳۴۵۶
DATA	۵.۴۱	۹۰۱۱۲	۳۵۷۲	۳۵۸۴
BSS	۰	۹۴۲۰۸	۲۳۰۱	۰
.idata	4.39	۹۸۳۰۴	۳۰۸۶	۳۵۸۴
.tls	0	۱۰۲۴۰۰	۱۲	۰
.rdata	0.2	۱۰۶۴۹۶	۲۴	۵۱۲
.reloc	6.62	۱۱۰۵۹۲	۶۵۴۰	۶۶۵۶
.rsrc	3.69	۱۱۸۷۸۴	۶۱۴۴	۶۱۴۴

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Jemd، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. فعالیت این باج‌افزار در سیستم بسیار زمان می‌برد و در طول این مدت، هیچ اثری از وجود باج‌افزار در سیستم مشاهده نمی‌شود. به گونه‌ای که برخلاف اکثر باج‌افزارها هیچ تغییری در نام و آیکن فایل‌های رمزگذاری شده نیز، ایجاد نمی‌کند. تصویر زیر مربوط به فایل‌ها پس از رمزگذاری می‌باشد:



همانطور که مشاهده می‌کنید، هیچ تغییری در ظاهر فایل‌ها ایجاد نشده است. با بررسی‌هایی که انجام دادیم، متوجه شدیم که این باج‌افزار، فایل‌های با اسامی فارسی را رمزگذاری نمی‌کند. همچنین تمامی آیکن‌ها در قسمت Taskbar سیستم، غیرفعال می‌شوند. باج‌افزار Jemd پس از پایان فعالیت خود، متوقف شده و در محلی از سیستم عامل که از آنجا اجرا شده است، باقی می‌ماند. همزمان با توقف فعالیت باج‌افزار در

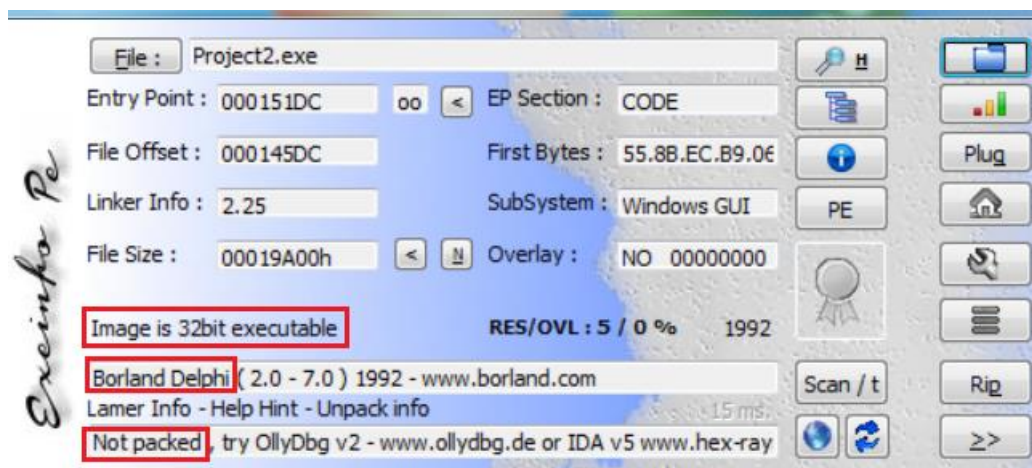
سیستم، فایل پیغام باج خواهی آن بر روی صفحه نمایش قرار می‌گیرد. تصویر مربوط به این فایل را در ادامه مشاهده می‌کنید:

همانطور که در تصویر بالا مشاهده می‌کنید، این باج‌افزار Jemd معرفی شده است. در ادامه عنوان شده است که تمامی فایل‌های قربانی توسط Jemd رمزگذاری شده است و از الگوریتم AES برای این کار استفاده شده است. قربانی برای رمزگشایی فایل‌های خود باید شناسه خود را که در انتهای پیغام آمده است، به آدرس rezko@prottykon.mit.edu ارسال کند.

تحلیل ایستا:

پس از بررسی فایل اجرایی باج‌افزار، نتایج زیر حاصل گردید:

این باج‌افزار با زبان Delphi توسعه یافته و با ابزاری پک نشده است. اطلاعات مذکور در تصویر زیر قابل مشاهده می‌باشند:



همچنین ساختار فایل ۳۲ بیتی می باشد.

تصویر زیر مربوط به اطلاعات هدر این فایل می باشد:

property	value
signature	0x00004550
machine	Intel
sections	8
compiler-stamp	0x2A425E19 (Fri Jun 19 15:22:17 1992)
pointer-symbol-table	0x00000000
number-of-symbols	0
size-of-optional-header	224 (bytes)
processor-32bit	true
relocation-stripped	false
large-address-aware	false
uniprocessor-only	false
system-image	false
dynamic-link-library	false
executable	true
debug information stripped	false
if on a removable media, copy and run from the swap	false
if on a Network, copy and run from the swap	false

همانطور که مشاهده می کنید، تعداد بخش های فایل، ساختار و نوع آن در تصویر بالا مشخص شده است.

تعدادی از توابع استفاده شده توسط این باج افزار به همراه کتابخانه آن ها در تصویر زیر قابل مشاهده می باشند:

name (47)	group (11)	anonymous (0)	type (1)	blacklist (9)	anti-debug (0)	undocumented (0)	deprecated (7)	library (5)
UnhandledExceptionFilter	18	-	implicit	-	-	-	-	kernel32.dll
RaiseException	18	-	implicit	x	-	-	-	kernel32.dll
DeleteCriticalSection	7	-	implicit	-	-	-	-	kernel32.dll
LeaveCriticalSection	7	-	implicit	-	-	-	-	kernel32.dll
EnterCriticalSection	7	-	implicit	-	-	-	-	kernel32.dll
InitializeCriticalSection	7	-	implicit	-	-	-	-	kernel32.dll
InterlockedDecrement	7	-	implicit	-	-	-	-	kernel32.dll
InterlockedIncrement	7	-	implicit	-	-	-	-	kernel32.dll
FindFirstFileA	6	-	implicit	x	-	-	-	kernel32.dll
FindClose	6	-	implicit	x	-	-	-	kernel32.dll
WriteFile	6	-	implicit	-	-	-	-	kernel32.dll
VirtualFree	5	-	implicit	-	-	-	-	kernel32.dll
VirtualAlloc	5	-	implicit	-	-	-	-	kernel32.dll
LocalFree	5	-	implicit	-	-	-	x	kernel32.dll
LocalAlloc	5	-	implicit	-	-	-	x	kernel32.dll
VirtualQuery	5	-	implicit	-	-	-	-	kernel32.dll
GetCurrentThreadld	2	-	implicit	x	-	-	-	kernel32.dll
GetStartupInfoA	2	-	implicit	-	-	-	-	kernel32.dll
GetCommandLineA	2	-	implicit	-	-	-	-	kernel32.dll
ExitProcess	2	-	implicit	-	-	-	-	kernel32.dll
RegQueryValueExA	1	-	implicit	-	-	-	-	advapi32.dll
RegOpenKeyExA	1	-	implicit	-	-	-	-	advapi32.dll
RegCloseKey	1	-	implicit	-	-	-	-	advapi32.dll
GetVersion	-	-	implicit	-	-	-	x	kernel32.dll
WideCharToMultiByte	-	-	implicit	-	-	-	-	kernel32.dll
MultiByteToWideChar	-	-	implicit	-	-	-	-	kernel32.dll
IstrlenA	-	-	implicit	-	-	-	x	kernel32.dll
IstrcpynA	-	-	implicit	-	-	-	x	kernel32.dll
GetThreadLocale	-	-	implicit	x	-	-	-	kernel32.dll
GetLocaleInfoA	-	-	implicit	-	-	-	x	kernel32.dll
RtlUnwind	-	-	implicit	-	-	-	-	kernel32.dll
LoadStringA	-	-	implicit	-	-	-	-	user32.dll
MessageBoxA	-	-	implicit	-	-	-	-	user32.dll

متن پیغام باج‌خواهی این باج‌افزار در بین رشته‌های استخراج شده قابل مشاهده است:

n/a	<><><><><><>jemd<><><><><><>
n/a	All your files were encrypted by jemd.
n/a	Used a AES encryption.
n/a	AES a best alorgytm. If you - gruja, decryption inpossible
n/a	Contact us: rezko@prottykon.mit.edu
n/a	Personal id:
n/a	Error
n/a	Runtime error at 00000000

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

از قطعه کد زیر، برای دریافت نام سیستم‌عامل قربانی استفاده شده است:

```
CODE:00405B4C LookupPrivilegeValueA proc near ; CODE XREF: sub_414360+22↓p
CODE:00405B4C
CODE:00405B4C lpSystemName = dword ptr 4
CODE:00405B4C lpName = dword ptr 8
CODE:00405B4C lpLuid = dword ptr 0Ch
CODE:00405B4C
CODE:00405B4C jmp ds:__imp_LookupPrivilegeValueA
CODE:00405B4C LookupPrivilegeValueA endp
```

متن پیغام باج‌خواهی باج‌افزار، در تصویر زیر قابل مشاهده است:

```
CODE:00415212 mov edx, offset aJemd ; "<><><><><><>jemd<><><><><><>"
CODE:00415217 mov eax, esi
CODE:00415219 mov ecx, [eax]
CODE:0041521B call dword ptr [ecx+38h]
CODE:0041521E mov edx, offset aAllYourFilesWe ; "All your files were encrypted by jemd."
CODE:00415223 mov eax, esi
CODE:00415225 mov ecx, [eax]
CODE:00415227 call dword ptr [ecx+38h]
CODE:0041522A mov edx, offset aUsedAAesEncryp ; "Used a AES encryption."
CODE:0041522F mov eax, esi
CODE:00415231 mov ecx, [eax]
CODE:00415233 call dword ptr [ecx+38h]
CODE:00415236 mov edx, offset aResABestAlorgy ; "AES a best alorgytm. If you - gruja, de"...
CODE:0041523B mov eax, esi
CODE:0041523D mov ecx, [eax]
CODE:0041523F call dword ptr [ecx+38h]
CODE:00415242 mov edx, offset aContactUsRezko ; "Contact us: rezko@prottykon.mit.edu"
CODE:00415247 mov eax, esi
CODE:00415249 mov ecx, [eax]
CODE:0041524B call dword ptr [ecx+38h]
CODE:0041524E mov edx, offset aJemd ; "<><><><><><>jemd<><><><><><>"
```

این باج‌افزار از قطعه کد زیر برای دریافت مسیر و فایل‌ها درون سیستم‌عامل استفاده می‌کند:

```
CODE:004011A8 ; HANDLE __stdcall FindFirstFileA(LPCSTR lpFileName, LPWIN32_FIND_DATA lpFindFileData)
CODE:004011A8 FindFirstFileA proc near ; CODE XREF: sub_404D2C+121↓p
CODE:004011A8
CODE:004011A8 lpFileName = dword ptr 4
CODE:004011A8 lpFindFileData = dword ptr 8
CODE:004011A8
CODE:004011A8 jmp ds:__imp_FindFirstFileA
CODE:004011A8 FindFirstFileA endp
```

در قطعه کدهای زیر مقادیری که از هر فایل خوانده و در آن نوشته می‌شود را مشاهده می‌کنید:

```

ReadFile      proc near          ; CODE XREF: sub_407268+14↓p
              hFile             = dword ptr  4
              lpBuffer          = dword ptr  8
              nNumberOfBytesToRead= dword ptr  0Ch
              lpNumberOfBytesRead= dword ptr  10h 16 byte
              lpOverlapped      = dword ptr  14h

              jmp     ds:__imp_ReadFile
ReadFile      endp

CODE:00401180 WriteFile      proc near          ; CODE XREF: sub_403B7C+3F↓p
CODE:00401180                                     ; sub_403B7C+5A↓p
CODE:00401180 hFile             = dword ptr  4
CODE:00401180 lpBuffer          = dword ptr  8
CODE:00401180 nNumberOfButesToWrite= dword ptr  0Ch
CODE:00401180 lpNumberOfBytesWritten= dword ptr  10h 16 Byte
CODE:00401180 lpOverlapped      = dword ptr  14h

CODE:00401180 jmp     ds:__imp_WriteFile
CODE:00401180 WriteFile      endp

CODE:00403BA5 loc_403BA5:          ; CODE XREF: sub_403B7C+13↑j
CODE:00403BA5                                     ; sub_403B7C+1C↑j
CODE:00403BA5 push     0             ; lpOverlapped
CODE:00403BA7 lea     eax, [esp+8+NumberOfBytesWritten]
CODE:00403BAA push     eax           ; lpNumberOfBytesWritten
CODE:00403BAC push     1Eh          ; nNumberOfBytesToWrite
CODE:00403BAE push     offset Text   ; "Runtime error at 00000000"
CODE:00403BB3 push     0FFFFFFF5h   ; nStdHandle
CODE:00403BB5 call    GetStdHandle
CODE:00403BBA push     eax           ; hFile
CODE:00403BBB call    WriteFile
CODE:00403BC0 push     0             ; lpOverlapped
CODE:00403BC2 lea     eax, [esp+8+NumberOfBytesWritten]
CODE:00403BC6 push     eax           ; lpNumberOfBytesWritten
CODE:00403BC7 push     2             ; nNumberOfBytesToWrite
CODE:00403BC9 push     offset dword_403C04 ; lpBuffer
CODE:00403BCE push     0FFFFFFF5h   ; nStdHandle
CODE:00403BD0 call    GetStdHandle
CODE:00403BD5 push     eax           ; hFile
CODE:00403BD6 call    WriteFile
CODE:00403BDB pop     edx
CODE:00403BDC retn

```

با بررسی‌هایی که بر روی چند نمونه فایل رمز شده با نمونه سالم آن‌ها انجام دادیم، متوجه شدیم این باج‌افزار دقیقا همان مقدار مشخص شده را در هر فایل تغییر می‌دهد. تصویر زیر که مربوط به مقایسه یک نمونه فایل رمز شده با نمونه سالم آن می‌باشد، الگوی تغییر در فایل را به طور کامل نشان می‌دهد:

The screenshot displays the Hex Editor Neo interface with two windows open, both showing the hex dump of a file named 'test(1).mp3.bin'. Below the hex dump, a 'File Comparison' window is visible, showing a table of differences between the two files.

Type	Offset (Source)	Offset (Dest)	Size
Matched	0	0	16
Modified	16	16	16
Matched	32	32	16
Modified	48	48	16
Matched	64	64	16
Modified	80	80	16
Matched	96	96	16
Modified	112	112	16
Matched	128	128	16
Modified	144	144	16
Matched	160	160	16
Modified	176	176	16
Matched	192	192	16
Modified	208	208	16
Matched	224	224	16
Modified	240	240	16
Matched	256	256	16
Modified	272	272	16

تحلیل ترافیک شبکه :

پس از اجرای باج افزار در محیط آزمایشگاهی و سندباکس های آنلاین و بررسی ترافیک شبکه ایجاد شده، هیچگونه ترافیک مشکوکی مربوط به باج افزار مشاهده نکردیم. این باج افزار در حالت آفلاین بدون هیچ مشکلی اجرا می شود.

خروجی سامانه VirusTotal :

در حال حاضر تنها تعداد مورد ۳۹ از ۶۹ 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.Generic.23263784	AegisLab	⚠ Trojan.Win32.Generic.4!c
Arcabit	⚠ Trojan.Generic.D162FA28	Avast	⚠ FileRepMalware
AVG	⚠ FileRepMalware	Avira	⚠ TR/ATRAPS.Gen
BitDefender	⚠ Trojan.Generic.23263784	Comodo	⚠ Malware@#3lga3sw6lcrt
CrowdStrike Falcon	⚠ malicious_confidence_90% (W)	Cylance	⚠ Unsafe
Cyren	⚠ W32/Trojan.AWZQ-7006	DrWeb	⚠ Trojan.Encoder.26910
Emsisoft	⚠ Trojan.Generic.23263784 (B)	eScan	⚠ Trojan.Generic.23263784
F-Secure	⚠ Trojan.Generic.23263784	Fortinet	⚠ W32/Generic!tr
GData	⚠ Trojan.Generic.23263784	Ikarus	⚠ Virus.Win32.DelfInject
Kaspersky	⚠ HEUR:Trojan.Win32.Generic	MAX	⚠ malware (ai score=99)
McAfee	⚠ Artemis!1F85AC92E6EA	McAfee-GW-Edition	⚠ BehavesLike.Win32.Dropper.ch
Microsoft	⚠ Trojan.Win32/Occamy.C	NANO-Antivirus	⚠ Trojan.Win32.Encoder.flffpv
Palo Alto Networks	⚠ generic.ml	Rising	⚠ Trojan.Generic!8.C3 (CLOUD)
Symantec	⚠ Trojan.Gen.2	Trapmine	⚠ malicious.moderate.ml.score
TrendMicro	⚠ Ransom.Win32.JEMD.THABAGAH	TrendMicro-HouseCall	⚠ Ransom.Win32.JEMD.THABAGAH
ZoneAlarm	⚠ HEUR:Trojan.Win32.Generic	AhnLab-V3	✔ Clean

خروجی سامانه ویروس کاو مرکز ماهر :

در حال حاضر تعداد ۷ مورد از ۱۶ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس کاو قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

نتیجه اسکن	آنتی ویروس
Dangerous	comodo
Clean	یادویش
Dangerous	bitdefender
Clean	avast
Dangerous Trojan.Generic.23263784	gdata
Clean	fprot
Clean	mcafee
Dangerous Trojan.Generic.23263784(DB)	escan
Clean	clamav
Clean	kaspersky
Clean	fsecure
Clean	eset
Dangerous TR/ATRAPS.Gen	avira
Clean	sophos
Dangerous Trojan.Encoder.26910	drweb
Dangerous Trojan.Gen.2	symantec