باسمه تعالى

تحليل فنى باجافزار

# Nemty





# فهرست مطالب

۱. مقارمه :
۲. مشخصات فایل اجرایی :۲
۳. شجرهنامه٤
٤. ميزان تهديد فايل باجافزار:٤
٥. تحليل پويا
۵–۱ آناتومی حمله:
٥-٢ روش انتشار:٩
٥-٣ روش جلوگیری:٩
٦- تحليل ايستا
10-1 تحليل كد:
٦-٦ تحليل ترافيک شبکه:
۲-۳ رمز گشایی:





#### ۱. مقدمه :

در تاریخ ۲۱ اوت سال ۲۰۱۹ میلادی، برای نخستین بار خبرهایی از انتشار باجافزار Nemty منتشر گردید. بر اساس مشاهدات صورت گرفته، این باجافزار از طریق سرویس دسترسی از راه دور مبتنی بر پروتکل RDP منتشر می گردد. گزارشهایی نیز مبنی بر سوءاستفاده این باجافزار از اکسپلویت کیت RIG، برای نفوذ به سیستم قربانیان منتشر گردیده است. باجافزار Nemty از الگوریتم AES برای رمزگذاری فایلهای موردنظر خود در سیستم قربانیان استفاده می کند. گزارش پیش رو مربوط به نسخه منتشر شده در تاریخ ۳۱ آگوست ۲۰۱۹ می باشد.

# ۲. مشخصات فایل اجرایی :

Nemty.exe	نام فايل
37aaba6b18c9c1b8150dae4f1d31e97d	MD5
02637179c597eaa821ff190ef89ba9eb013a6ea2	SHA-1
505c0ca5ad0552cce9e047c27120c681ddce127d13afa8a8ad96761b2487191b	SHA-256
Win32 EXE	نوع فايل
۸۷کیلوبایت	اندازه فايل

### فایل اجرایی این باجافزار دارای ۲ بخش است :

اندازه خام	اندازه مجازی	آدرس مجازی	آنتروپی	نام بخش
۸۱۹۲۰	A1AYA	٤٠٩٦	7.79	.text
7122	०९०٦	۸٦٠١٦	٤.٥٤	.reloc





#### ۳. شجرهنامه



٤. ميزان تهديد فايل باجافزار

درحال حاضر تعداد ٤٦ مورد از ٦٥ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باجافزار میباشند.

46	() 46 engines detected this file
Community Score	505c0ca5ad0552cce9e047c27120c681ddce127d13afa8a8ad96761b2487191b Nemty.exe peexe

۲۰۰ تحلیل پویا
 ۲۰۰ آناتومی حمله:
 ۲۰۰ آناتومی حمله:
 ۲۰۰ اینترنت، اجرا نمی شود. درصورت برقرار باجافزار از زمان اجرا تا پایان فرآیند رمزگذاری، بسته به منابع سیستم قربانی با اینترنت، اجرا نمی شود. درصورت برقرار بودن ارتباط، شروع فعالیت این باجافزار از زمان اجرا تا پایان فرآیند رمزگذاری، بسته به منابع سیستم قربانی، بین ۱۰ تا ۲۰ دقیقه به طول می انجامد. به محض شروع فعالیت، فایل های موردنظر باجافزار یکی پس از دیگری رمزگذاری می شوند. فایل های رمزگذاری شده به شکل زیر تغییر پیدا می کنند.



						- •	X
Victim	S		•	Search Vic	tims		م
Organize 👻 Include	in library 🔹 Share with 🔹 New folder				-		0
🚖 Favorites	Name	<ul> <li>Date modified</li> </ul>	Туре	Size			
📃 Desktop	7z1900.exe	3/2/2019 10:30 PM	Application	1,159 KB			
🐌 Downloads	applied.pdf.nemty	9/18/2019 6:46 PM	NEMTY File	1,395 KB			
laces 😓 Recent Places	contacted_hosts.csv.nemty	9/18/2019 6:46 PM	NEMTY File	166 KB			
	DualBoot.txt.nemty	9/18/2019 6:46 PM	NEMTY File	1 KB			
📜 Libraries	FINAL.jpg.nemty	9/18/2019 6:46 PM	NEMTY File	104 KB			
less Documents	intro.mp4.nemty	9/18/2019 6:46 PM	NEMTY File	6,731 KB			
🕹 Music	NEMTY-DECRYPT.txt	9/18/2019 6:46 PM	Text Document	2 KB			
lictures	powerpoint.pptx.nemty	9/18/2019 6:46 PM	NEMTY File	691 KB			
JUDE Videos	sources.docx.nemty	9/18/2019 6:46 PM	NEMTY File	19 KB			
	suspicious.py.nemty	9/18/2019 6:46 PM	NEMTY File	5 KB			
💐 Computer	teapot.webm.nemty	9/18/2019 6:46 PM	NEMTY File	543 KB			

مركزمناهر

همانطور که در تصویر بالا قابل مشاهده است، تمامی انواع فایل ها رمزگذاری شده و پسوند nemty. به انتهای آنها اضافه شده است. پیغام باج خواهی باج افزار نیز با عنوان NEMTY-DECRYPT.txt، درکنار فایل های رمزگذاری شده قرار گرفته است. همزمان با اتمام فعالیت باج افزار در سیستم قربانی و توقف فایل اجرایی آن، پیغام باج خواهی بر روی صفحه نمایش ظاهر می شود.

NEMTY-DECKYPT.txt - Notepad	
File Edit Format View Help	
= NEMTY PROJECT ===	*
[+] whats Happen? [+]	
Your files are encrypted, and currently unavailable. You can check it: all files on you computer has extension .nemty By the way, everything is possible to restore, but you need to follow our instructions. Otherwise, you cant return your data (NEVER).	
[+] What guarantees? [+]	
It's just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. It's not in our interests. If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the pu In practise - time is much more valuable than money.	rivate key.
[+] How to get access on website? [+]	
1) Download and install TOR browser from this site: https://torproject.org/ 2) Open our website: zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad.onion/pay	
when you open our website, follow the instructions and you will get your files back.	
Configuration file path: C:\Users\	
	~
	h. ∢

همانطور که در پیغام باجخواهی این باجافزار قابل مشاهده است، لینکی جهت ارتباط قربانی با مهاجمین درون پیغام قرار داده شده است که فقط از طریق مرورگر Tor قابل مشاهده است. لینک دانلود این مرورگر نیز، برای قربانی درون پیغام قرار داده شده است. قربانی، باید با مراجعه به لینک یادشده و دنبال کردن دستورات مربوطه اقدام به برقراری ارتباط با مهاجمین، جهت برگرداندن فایلهای خود نماید. باجافزار Nemty، فایلی را به عنوان فایل پیکربندی درون سیستم قربانی ایجاد میکند که مسیر آن در انتهای پیغام باجخواهی ذکر شده است.



					7		×
Computer	► Local Disk (C:) ► Users ►			<b>▼</b>   4	Search UBCERT		Q
Organize 👻 📄 Open	Share with   New folder				8	•	0
🚖 Favorites 🔶	Name	Date modified	Туре	Size			
📃 Desktop	🐌 .cisco	9/18/2019 6:46 PM	File folder				
🔈 Downloads	🐚 Contacts	9/18/2019 6:46 PM	File folder				
laces Recent Places	📜 Desktop	9/18/2019 6:46 PM	File folder				
	📕 Downloads	9/18/2019 6:46 PM	File folder				
🞇 Libraries	📙 Favorites	9/18/2019 6:46 PM	File folder				
Documents	🍺 Links	9/18/2019 6:46 PM	File folder				
🕹 Music 😑	📗 My Documents	9/18/2019 6:46 PM	File folder				
lictures	🐌 My Music	9/18/2019 6:46 PM	File folder				
Judeos	属 My Pictures	9/18/2019 6:46 PM	File folder				
	📕 My Videos	9/18/2019 6:46 PM	File folder				
le Computer	🍺 Saved Games	9/18/2019 6:46 PM	File folder				
bcal Disk (C:)	🐌 Searches	9/18/2019 6:46 PM	File folder				
🛫 VM-Share (\\VBo)	👢 TorDir	9/18/2019 6:46 PM	File folder				
		9/18/2019 6:34 PM	NEMTY File	5 KB			
🔍 Network	NEMTY-DECRYPT.txt	9/18/2019 6:46 PM	Text Document	2 KB			
NEMTY_iv4yN NEMTY File	I3rnemty Date modified: 9/18/2019 6:34 PM Size: 4.00 KB	M Date created: 9/1	8/2019 6:34 PM				

مركزماهر

# تصویر بالا محل قرارگیری فایل پیکربندی این باجافزار با عنوان NEMTY\_ZWIOQsU\_.nemty\_ را نشان میدهد. تصویر زیر، محتوای این فایل در تصویر زیر قابل مشاهده است.

به نظر میرسد محتوای تصویر بالا، کلید عمومی استفاده شده در فرآیند رمزگذاری میباشد. برای بررسیهای بیشتر، آدرس ذکر شده در پیغام باجخواهی را دنبال کردیم. تصویر زیر، صفحه اول پورتال طراحی شده جهت ارتباط با قربانیان را نشان میدهد. قربانی برای ورود به قسمت بعد باید فایل پیکربندی





باجافزار که آدرس آن در انتهای پیغام ذکر شده است را در محل مشخص شده با عنوان File، بارگذاری نماید. سپس، با کلیک بر روی گزینه SUBMIT به مرحله بعد هدایت می شود.

Ransom	×	+
$\rightarrow$ G	🛈 🍝 zjoxyw5mkacojk5	5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad.onion/pay
		Upload file to decrypt
		Allowed extensions: jpg, png, bmp. Max file size is 1 Mb
		I File
		SUBMIT

در این قسمت، جهت اطمینان از صحت ادعای مهاجمین، قربانی می تواند فایلی با پسوندهای png. jpg. و bmp. با حجم حداکثر یک مگابایت را در قسمت File بارگذاری کند تا به صورت رایگان رمزگشایی شود. پس از انجام این فرآیند و کلیک مجدد بر روی گزینه SUBMIT، قربانی به قسمت بعدی هدایت می شود.



در این قسمت، همانطور که در سمت چپ تصویر قابل مشاهده میباشد، مبلغ باج که برابر ۱۰۳۹. بیتکوین است، مشخص شده است. همچنین آدرس کیف پول مهاجمین و مهلت تعیین شده جهت پرداخت مبلغ باج نیز در این بخش تصویر، مشخص شده است. در صورت عدم پرداخت باج توسط





قربانی، مبلغ آن به دو برابر افزایش پیدا خواهد کرد. در ضمن قربانی با کلیک بر روی کادر سبز رنگ مشخص شده می تواند فایل رمزگشایی شده خود را دریافت کند. در سمت راست تصویر نیز، بخشی برای ارتباط با مهاجمین درنظر گرفته شده است که قربانی می تواند، پیام خود را در قسمت مشخص شده نوشته و ارسال نماید. این صفحه به دو زبان روسی و انگلیسی قابل ترجمه می باشد.



تغییرات رجیستری ایجاد شده توسط باجافزار در طول فعالیت در سیستم قربانی نیز، به صورت زیر میباشد:

کلیدهای اضافه شده:
HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS
مقادیر اضافه شده:
HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\MaxFileSize: 0x00100000
HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\FileDirectory: "%windir%\tracing"
HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\EnableFileTracing: 0x0000000
HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\MaxFileSize: 0x00100000
HKLM\SOFTWARE\Microsoft\Tracing\RASMANCS\FileDirectory: "%windir%\tracing"
HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\23\52C64B7E\@C:\Windows\system32\notepad.exe,-469: "Text Document"





HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\HO-PREG\Qrfxgbc\505p0pn5nq0552ppr9r047p27120p681qqpr127q13nsn8n8nq96761o2487191o.ova\5 05p0pn5nq0552ppr9r047p27120p681qqpr127q13nsn8n8nq96761o2487191o.rkr: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 80 BF FF FF FF FF A0 B9 0C 4E 55 65 D5 01 00 00 00 00 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\23\52C64B7E\@C:\Windows\system32\notepad.exe,-469: "Text Document" کلیدهایی که مقادیر آنها تغییر پیدا کرده است: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\CurrentLanguage\Counter HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Enter) HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Leave) HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Enter) HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Leave) HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR PGYFRFFVBA HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{7P5N40RS-N0SO-40SP-874N-P0S2R009SN8R}\Ertfubg 1.8.3\i5\_ertfubg\_1.8.3\_orgn1\_jva32\_k64\_fep\_ova\_i5\ertfubg.rkr

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings

# ۵–۲ روش انتشار:

همانطور که در ابتدا اشاره شد باجافزار Nemty عمدتاً از طریق استفاده از پروتکل RDP بدون رعایت ملاحظات امنیتی منتشر میگردد. همچنین گزارشهایی در رابطه با نفوذ این باجافزار با بهرهگیری از اکسپلویتکیت RIG نیز منتشر شده است.





### ٥-٣ روش جلوگيري:

با توجه به اینکه این باجافزار عموماً از طریق پروتکل RDP به سیستم قربانیان نفوذ میکند، اکیداً توصیه می شود که در صورت استفاده از این پروتکل جهت ارتباطات خود، اقدامات مربوط به امن سازی آن از جمله تنظیم رمزعبور پیچیده و فعالسازی احراز هویت دوعاملی و ... را انجام دهید. همچنین توصیه می شود سیستم عامل مورد استفاده خود را به طور دایم به روزرسانی کنید تا آسیب پذیری های آن رفع گردند.

- ٦. تحليل ايستا
  - ٦-١ تحليل كد:

پس از تحلیل کد باجافزار، نتایج زیر حاصل گردید. کد فایل اجرایی از تابع Main شروع می شود که درون این تابع، فایل پیغام باج خواهی باجافزار ایجاد می شود.

mov	edi, eax
add	esp, 24h
mov	eax, esi
call	sub_40A678
push	0Fh
mov	[ebp+var_2C], ebx
mov	[ebp+var_3C], bl
рор	esi
mov	ebx, eax
lea	eax, [ebp+var_3C]
mov	[ebp+var_28], esi
call	sub_4073BE
mov	<pre>ebx, offset aNemtyDecrypt_0 ; "\\NEMTY-DECRYPT.txt\""</pre>
push	ebx ; char *
call	_strlen
pop	ecx

سپس با استفاده از تابع ShellexecuteA دستورات زیر در محیط CMD اجرا می شوند.





	-		
📕 🛃 🖻	<b>3</b>		
100_40	ASED:		
mov	ebx, ShellExe	cuteA	
xor	eax, eax		
push	eax	; nShowCmd	
push	eax	; lpDirectory	
push	ecx	; 1pParameters	
push	offset File	; "cmd.exe"	
push	eax	; 1pOperation	
push	eax	; hwnd	
call	ebx ; ShellEx	ecuteA	
push	1		
xor	edi, edi		
lea	esi, [ebp+1pP	arameters]	
call	sub_405C90		
push	1		
lea	esi, [ebp+var	_3C]	
call	sub_405C90		
push	1		
lea	esi, [ebp+var	_90]	
call	sub_405C90		
push	1		
lea	esi, [ebp+var	_58]	
call	sub_407574		
aCVssa	dmin_exeD db ' ,	/c vssadmin.exe delete shadows /all /quiet & bcdedit /set ; DATA XREF: _main+13Fto	{defau'
	db 11	t} bootstatuspolicy ignoreallfailures & bcdedit /set {def	Fault} r'
	db e db p	coveryenabled no & wbadmin delete catalog -quiet & wmic s y delete',0	shadowco'

/c vssadmin.exe delete shadows /all /quiet wmic shadowcopy delete	حذف فضای VSS
bcdedit /set {default} bootstatuspolicy ignoreallfailures bcdedit /set{default}recoveryenabled no	غیرفعالسازی پنجره نمایش خطا در هنگام بوت شدن ویندوز
wbadmin delete catalog -quiet	حذف تاریخچه فایلهای پشتیبان از سرور/سیستم

همانطور که در بخش قبل اشاره شد، این باجافزار برای فعالیت در سیستم قربانی نیاز به اتصال اینترنت دارد. برای این منظور پس از طی مراحل فوق، ارتباط سیستم قربانی با شبکه اینترنت بررسی میشود.





مركزماهر

پس از بررسی اتصال سیستم قربانی به اینترنت و برقراری ارتباط با سرور فرمان و کنترل (C&C)، باجافزار موقعیت جغرافیایی و زبان سیستم قربانی را مورد بررسی قرار میدهد. در صورتی که سیستم قربانی در محدوده یکی از کشورهای زیر باشد، از رمزگذاری در امان میماند.





proc near ; CODE XREF: sub 4089D2:loc 408AD81p push esi esi, offset dword\_401F10 offset aRussia ; "Russia" mou push eax, esi sub\_407FDB MOV call pop ecx test al, al jnz short loc\_4089B8 push offset aBelarus ; "Belarus" mov eax, esi call sub\_407FDB DOD ecx test al, al short loc 408988 jnz offset aKazakhstan ; "Kazakhstan" push mov eax, esi call sub 407FDB рор ecx test al, al short loc 408988 inz offset aTajikistan ; "Tajikistan" push eax, esi sub\_407FDB mov call рор ecx test al, al short loc\_4089B8 jnz offset aUkraine ; "Ukraine" push eax, esi sub\_407FDB mov call ecx DOD esi, offset aFalse ; "false" mov test al, al short loc\_4089BD iz

در صورتی که سیستم قربانی در محدوده کشورهای مشخص شده نباشد، ابتدا نسخه سیستمعامل استفاده شده در سیستم قربانی مورد بررسی قرار می گیرد.

```
∠יינ
mov
                                   31101 C 100
                                               40070
                                   esi, offset aWindows7 ; "Windows 7"
                                   short loc 40893A
                           jmp
        loc_40890F:
                                                      ; CODE XREF: sub_4088AA+5C<sup>†</sup>j
                           стр
                                   eax, 2
                                   short loc_40891B
                          jnż
                           mov
                                   esi, offset aWindows8 ; "Windows 8"
                                   short loc_40893A
                           jmp
        1oc_40891B:
                                                      ; CODE XREF: sub_4088AA+681j
                          стр
                                   eax, 3
                                   short loc_408935
                           jnz
                           mov
                                   esi, offset aWindows8_1 ; "Windows 8.1"
                           jmp
                                   short loc_40893A
        loc_408927:
                                                      ; CODE XREF: sub_4088AA+57<sup>†</sup>j
                                   ecx, OAh
                          CMP
                                   short loc 408935
                           jnz
                                   esi, offset aWindows10 ; "Windows 10"
                           mov
                                   eax, eax
short loc_40893A
                          test
                          iz
                                                      ; CODE XREF: sub_4088AA+74<sup>†</sup>j
        loc 408935:
                                                        sub 40<u>88AA+80†i</u>
                          mov
                                   esi, offset aWindowsXp ; "Windows XP"
سپس فرآیند رمزگذاری فایلها آغاز میشود. فایلهای زیر در لیست سفید باجافزار قرار داشته و از
```

رمزگذاری در امان میمانند.





aNemty	db 'nemty',0
	align 4
aLog	db 'log',0
aLog_0	db 'LOG',0
aCab	db 'CAB',0
aCab Ø	db 'cab',0
aCmd	db 'CMD',0
aCmd 0	db 'cmd',0
aCom	db 'COM',0
aCom Ø	db 'com',0
aCp1	db 'cpl',0
aCpl 0	db 'CPL',0
aExe	db 'exe',0
aExe Ø	db 'EXE',0
aIni	db 'ini',0
aIni 0	db 'INI',0
aD11	db 'dll',0
aD11 0	db 'DLL',0
aLnk	db 'lnk',0
aLnk Ø	db 'LNK',0
aUrl	db 'url',0
aUrl 0	db 'URL',0
aTtf	db 'ttf',0
aTtf 0	db 'TTF',0
aDecrypt txt	db 'DECRÝPT.txt',0

ضمناً پوشهها و فایلهای زیر نیز در حین فرآیند رمزگذاری توسط باجافزار بررسی نمیشوند.

unicode 0, align 4 aRsa	<\$RECYCLE.BIN>,0	unicode 0, aConfig_sys	<desktop.ini>,0</desktop.ini>	
unicode 0, aNtdetect_com	<pre></pre>	unicode 0, align 10h	<config.sys>,0</config.sys>	D
align 4 aNtldr	; D	unicode 0,	<recycler>,0</recycler>	D
aMsdos_sys	<ntidr>,0 ; D;</ntidr>	aBootsect_bal	:	D
alo_sys	(11.525.0); D	unicode 0, align 10h aBootmor	<bootsect.bak>,</bootsect.bak>	0
align 4 aBoot_ini	; D	unicode 0,	; <bootmgr>,0</bootmgr>	D
unicode 0, align 4 aAutoexec_bat	<boot.ini>,0</boot.ini>	unicode O,	<programdata>,0</programdata>	D
unicode 0, align 4	; D <autoexec.bat>,0</autoexec.bat>	aAppdata	;	D
aNtuser_dat	; D <ntuser.dat>,0</ntuser.dat>	aWindows	(appuara),0	D
aDesktop_ini	; Di {desktop ini} 0	unicode 0, oft[] db 'Microso	<windows>,0</windows>	ก่
unicout o,	Construction and the state of t	GD 11101030	, , , , , , , , , , , , , , , , , , ,	

باجافزار Nemty، نوع درایوهای سیستم قربانی را نیز در حین فرآیند رمزگذاری بررسی میکند.







این باجافزار از الگوریتم متقارن AES جهت رمزگذاری فایلها استفاده می کند. کلید تولید شده توسط این الگوریتم، به وسیله یک جفت کلید عمومی/خصوصی الگوریتم نامتقارن ۲۰٤۸ RSA بیتی، رمزگذاری می شود. کلید عمومی برای رمزگذاری کلید استفاده شده در فرآیند رمزگذاری فایل ها و کلید خصوصی برای رمزگشایی آن استفاده می شود. کلید خصوصی تولید شده، به سرور فرمان و کنترل باجافزار ارسال می شود.







الگوی رمز گذاری فایل ها بدین صورت است که ابتدا اندازه هرفایل با مقدار 7 مگابایت مقایسه می شود.



در صورتی که حجم فایل موردنظر کمتر یا برابر با این مقدار باشد. تمام محتوای فایل رمزگذاری خواهد شد. صحت این موضوع با مقایسه نسخه سالم و رمزشده چند نمونه فایل کمتر از 7 مگابایت مورد آزمایش قرار گرفت.









10 AM | 1.4 MB (1427665)





call esi ; SetFilePointer ; lpOverlapped [ebp+NumberOfBytesRead] push ebx lea eax, 1pNumberOfBytesRead nNumberOfBytesToRead push eax ş 30D400h 3MB push Lebp+1pBu++erJ ; 1pBu++er ; <mark>hFile</mark> push push edi ReadFile call eax, [ebp+var\_78]
edx, [ebp+1pBuffer] mov mov ecx, 30D400h mov sub\_405BCC call push ebx ş dwMoveMethod ; lpDistanceToMoveHigh push ebx push ebx push 2 dword ptr [ebp+FileSize+4] dword ptr [ebp+FileSize] . push push call alldiv eax, 186A00h sub push eax ; 1DistanceToMove push edi ; hFile call esi ; SetFilePointer 1p0ver1apped push ebx . lea eax, [ebp+NumberOfBytesWritten] push ; 1pNumberOfBytesWritten eax [ebp+NumberOfBytesRead] ; nNumberOfBytesToWrite
[ebp+lpBuffer] ; lpBuffer
edi ; hFile . push . push . push call WriteFile

سیس، مجدداً و دو مرتبه دیگر ۱۰۰ کیلوبایت از فایل رمز گذاری می شود.

call	esi ; SetFilePoint	er
push	ebx ;	1pOverlapped
lea	eax, [ebp+NumberOf	BytesRead]
push	eax ;	1pNumberOfBytesRead
push	19000h 100KB ;	nNumberOfBytesToRead
push	<pre>[ebp+1pBuffer] ;</pre>	1pBuffer
push	edi ;	hFile
call	ReadFile	
mov	eax, [ebp+var_78]	_
mov	edx, [ebp+1pBuffer	·]
mov	ecx, 19000h	
call	sub_405BCC	
push	ebx ;	dwMoveMethod
push	ebx ;	1pDistanceToMoveHigh
push	ebx ;	1DistanceToMove
push	edi ;	hFile
call	esi ; SetFilePoint	er
push	ebx ;	1pOverlapped
lea	eax, [ebp+NumberOf	BytesWritten]
push	eax ;	1pNumberOfBytesWritten
push	[ebp+NumberOfBytes	Read] ; nNumberOfBytesToWrite
push	<pre>[ebp+1pBuffer] ;</pre>	1pBuffer
push	edi ;	hFile
call	WriteFile	





add	eax, OFFFE7000h
push	eax ; 1DistanceToMove
push	edi ; <mark>hFile</mark>
call	esi ; SetFilePointer
push	ebx ; lpOverlapped
lea _	eax, [ebp+NumberOfButesRead]
push	eax ; 1pNumberOfBytesRead
push	19000h 100KB ; nNumberOfBytesToRead
push	[ebp+1pBuffer] ; 1pBuffer
push	edi ; <mark>hFile</mark>
call	ReadFile
mov	eax, [ebp+var_78]
mov	edx, [ebp+1pBuffer]
mov	ecx, 19000h
call	sub_405BCC
mov	eax, dword ptr [ebp+FileSize]
push	ebx ; dwMoveMethod
push	ebx ; lpDistanceToMoveHigh
add	eax, OFFFE7000h
push	eax ; 1DistanceToMove
push	edi ; <mark>hFile</mark>
call	esi ; SetFilePointer
push	ebx ; lpOverlapped
lea	eax, [ebp+NumberOfBytesWritten]
push	eax ; 1pNumberOfBytesWritten
push	[ebp+NumberOfBytesRead] ; nNumberOfBytesToWrite
push	[ebp+1pBuffer] ; 1pBuffer
push	edi ; <mark>hFile</mark>
call	WriteFile

<b>– 1</b>	100 KB C:\Users\Cesktop\test\test (1).apk.bin			C:\Users\\Desktop\test\test (1).apk.nemty.bin
	00911C00	AE 42 04 03 B1 61 0E 14 00 00	0E 14 00 00 1 A 009	11C00 45 DC 12 6A C9 9A 54 56 12 F5 07 60 73 72 🔺
	00911c10	00 00 00 00 00 00 00 00 00 00	00 00 CC B5 { 009	011C10 D1 C5 OB 09 14 1A 44 E3 E6 A4 A2 2E DB D5
	00911c20	72 65 73 2F 64 72 61 77 61 62	6C 65 2D 6D ( 009	11C20 F3 D4 E6 BF 59 17 6F 89 C6 0D E8 14 A1 BF
	00911C30	69 2F 69 63 5F 6C 61 75 6E 63	68 65 72 2E 1 009	11C30 BC 8E 08 C9 0E DD 89 6E 0A 12 75 6D 23 B5
	00911C40	67 50 4B 01 02 0A 00 0A 00 00	08 00 00 51 1 009	11C40 07 65 7A 4E 22 5A B8 4F C6 F7 F8 EC 6B 01
	00911C50	42 E3 AE 94 32 EB 01 00 00 EB	01 00 00 27 ( 009	11C50 4D 7E B0 7C BC 1D 23 0A 0F 98 92 34 7D 2C
	00911C60	00 00 00 00 00 00 00 00 00 00	00 19 CA 8D ( 009	11C60 F5 01 69 16 15 25 AB 99 C5 39 A9 3B A8 F0
	00911c70	65 73 2F 64 72 61 77 61 62 6C	65 2D 78 68 € 009	11C70 A9 72 E0 73 66 32 BC 1A B0 70 67 62 5E F7
	00911C80	69 2F 69 63 5F 61 63 74 69 6F	6E 5F 73 65 € 009	11C80 81 40 88 71 6A B3 BF 81 95 99 6C 2C BB 25
	00911C90	63 68 2E 70 6E 67 50 4B 01 02	0A 00 0A 00 ( 009	11C90 1F BD 93 96 88 C5 45 CD F8 5D F6 27 F7 AC
	00911CA0	00 00 51 7D AE 42 5A 36 86 DF	A9 43 00 00 1 009	911CA0 9E 5B 46 0F EC F7 E8 A3 DC 41 69 0C 95 FD
	00911CB0	00 00 22 00 00 00 00 00 00 00	00 00 00 00 ( 009	011CB0 38 E2 2E 9C 1C D5 CF 03 D1 A4 88 FC EA 7E
	00911cc0	49 CC 8D 00 72 65 73 2F 64 72	61 77 61 62 ( 009	011CC0 BB 0E A2 A5 57 B1 40 EE C7 74 D3 B5 21 29
	00911CD0	2D 78 68 64 70 69 2F 69 63 5F	6C 61 75 6E ( 009	011CD0 35 49 B6 E4 7D ED A7 8B 63 C7 02 29 27 89
	00911CE0	65 72 2E 70 6E 67 50 4B 01 02	14 00 14 00 ( 009	11CE0 07 B3 55 C1 B2 48 29 95 4A ED CC D4 74 E4
3	00911CF0	08 00 E0 4A 2E 43 1B 72 24 D1	69 A6 02 00 4 009	11CF0 A6 41 BA 0B 1F CD 7A B9 8D 9F F7 0C 6A 2A
	00911000	06 00 0B 00 00 00 00 00 00 00	00 00 00 00 ( 009	11D00 E2 6F CB C1 FD 0F D3 E4 C6 66 96 F8 49 2F
	00911D10	32 10 8E 00 63 6C 61 73 73 65	73 2E 64 65 1 009	11D10 BB 24 9E E0 07 97 17 5F A5 87 BD 55 C6 C5
	00911020	48 01 02 14 00 14 00 08 08 08	00 E2 4A 2E 4 009	11D20 70 11 91 7E F3 7A B7 A5 A6 E3 29 29 B1 B3
	00911D30	7B 57 48 A9 15 00 00 A2 3B 00		A11D30 AB 8F 4C 08 EA F2 EC 28 59 EC 89 80 9C BD
	00911040	00 00 00 00 00 00 00 00 00 D4	B6 90 00 4D 4 009	MID40 D8 /A 39 6E /I CD 9A 4F 85 B3 5D C6 22 E3
	00911050	41 2D 49 4E 46 2E 4D 41 4E 49	46 45 53 54 2 009	MIDSU DU 66 /C 4D 86 /4 F8 20 8E B9 DD D2 33 38
пп	00911060	46 50 4B 01 02 14 00 14 00 08 42 55 99 54 75 D7 15 00 00 D7	08 08 00 E2 4 009	MID60 4A 98 2B A2 34 2A 2C B3 BA D8 72 BB ED E3
	00911070	43 33 88 E4 A3 DA 13 00 00 D7	3B 00 00 10 ( 009	11D70 62 A3 12 13 62 62 30 31 23 73 D3 23 6D 10
	00911080	45 54 41 2D 40 4E 46 2E 42 45	52 54 2E 52 4 009	11D80 EF 67 F9 CC 0F F5 10 CF 66 A0 06 C2 0D 36
	00911090	45 01 02 14 00 14 00 08 08 08	00 F2 47 2F 4 009	011090 DF F4 64 D6 40 33 E9 F2 D6 33 63 F0 EA DF
	00911080	41 9D F7 1D 04 00 00 B3 04 00	00 11 00 00 ( 009	11DR0 73 76 DF 5F 40 51 DD 11 18 2F BF 7F DB 85
	00911000		E2 90 00 4D 4 009	11DC0 36 5D FC F7 5F C8 6F 3C FB 1B 91 27 6B C5
	00911000	41 2D 49 4F 46 2F 43 45 52 54	28 52 53 41 4 009	11DD0 85 F7 03 AA F2 07 5F F8 58 88 3D 21 AB 71
	00911050	05 06 00 00 00 00 CD 00 CD 00	AB 36 00 00 10 009	11DE0 04 B7 C2 DB A0 73 81 5B 82 99 96 B5 31 F2
	009110F0		- 009	11DE0 58 49 C4 E4 49 72 39 65 66 58 59 58 35 65 -
			F 11	





# ۲-۲ تحلیل ترافیک شبکه:

پس از بررسی ترافیک شبکه ایجاد شده حین اجرای باجافزار، نتایج زیر مشاهده شد.

ار تباطات:

آدرس آیپی	دامنه	شماره پورت	پروتکل	کشور میزبان
۲۳.۲۳.۸۳.۱۵۳	Api.ipify.org	80,433	ТСР,НТТР	آمريكا
۱۰٤.۲٥.۳.۳۳	Api.db-ip.com	80,433	TCP,HTTP	آمريكا

192.168.29.128	23.23.73.124		тср	66 50412 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
23.23.73.124	192.168.29.128		тср	60 80 → 50412 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.29.128	23.23.73.124		тср	54 50412 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.29.128	23.23.73.124		HTTP	131 GET / HTTP/1.1
23.23.73.124	192.168.29.128		тср	60 80 → 50412 [ACK] Seq=1 Ack=78 Win=64240 Len=0
23.23.73.124	192.168.29.128		HTTP	240 HTTP/1.1 200 OK (text/plain)
192.168.29.128	192.168.29.2		DNS	73 Standard query 0xf469 A api.db-ip.com
192.168.29.2	192.168.29.128		DNS	105 Standard query response 0xf469 A api.db-ip.com A 104.25.3.33 A 104.25.2.33
192.168.29.128	104.25.3.33		TCP	66 50413 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
104.25.3.33	192.168.29.128		тср	60 80 → 50413 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.29.128	104.25.3.33		TCP	54 50413 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.29.128	104.25.3.33		нттр	165 GET /v2/free/37.129.101.175/countryName HTTP/1.1
104.25.3.33	192.168.29.128		TCP	60 80 → 50413 [ACK] Seq=1 Ack=112 Win=64240 Len=0
23.23.73.124	192.168.29.128		тср	240 [TCP Retransmission] 80 → 50412 [PSH, ACK] Seq=1 Ack=78 Win=64240 Len=186
192.168.29.128	23.23.73.124		TCP	54 50412 → 80 [ACK] Seq=78 Ack=187 Win=64054 Len=0
104.25.3.33	192.168.29.128		нттр	588 HTTP/1.1 200 OK (text/plain)
104.25.3.33	192.168.29.128		тср	588 [TCP Retransmission] 80 → 50413 [PSH, ACK] Seq=1 Ack=112 Win=64240 Len=534
192.168.29.128	104.25.3.33		TCP	54 50413 → 80 [ACK] Seq=112 Ack=535 Win=63706 Len=0
192.168.29.128	192.168.29.255		BROWSER	258 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
23.23.73.124	192.168.29.128		TCP	60 80 → 50412 [FIN, PSH, ACK] Seq=187 Ack=78 Win=64240 Len=0
192.168.29.128	23.23.73.124		TCP	54 50412 → 80 [ACK] Seq=78 Ack=188 Win=64054 Len=0
104.25.3.33	192.168.29.128		TCP	60 80 → 50413 [FIN, PSH, ACK] Seq=535 Ack=112 Win=64240 Len=0
192.168.29.128	104.25.3.33		TCP	54 50413 → 80 [ACK] Seq=112 Ack=536 Win=63706 Len=0
192.168.29.128	205.185.216.42	TCP	66 50	416 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
205.185.216.42	192.168.29.128	TCP	60 80	→ 50416 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.29.128	205.185.216.42	TCP	54 50	416 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.29.128	205.185.216.42	HTTP	356 GE	T /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1
205.185.216.42	192.168.29.128	TCP	60 80	→ 50416 [ACK] Seq=1 Ack=303 Win=64240 Len=0
205.185.216.42	192.168.29.128	TCP	1454 80	→ 50416 [PSH, ACK] Seq=1 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	тср	1454 80	→ 50416 [PSH, ACK] Seq=1401 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
192.168.29.128	205.185.216.42	тср	54 50	416 → 80 [ACK] Seq=303 Ack=2801 Win=64240 Len=0
205.185.216.42	192.168.29.128	тср	1454 80	→ 50416 [PSH, ACK] Seq=2801 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	TCP	1454 80	$\rightarrow$ 50416 [PSH, ACK] Seq=4201 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	TCP	1454 80	$\rightarrow$ 50416 [PSH, ACK] Seq=5601 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	TCP	1454 80	$\rightarrow$ 50416 [PSH, ACK] Seq=7001 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
192.168.29.128	205.185.216.42	TCP	54 50	416 → 80 [ACK] Seq=303 Ack=8401 Win=64240 Len=0
205.185.216.42	192.168.29.128	ТСР	1454 80	→ 50416 [PSH, ACK] Seq=8401 Ack=303 Win=64240 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	тср	410 80	→ 50416 [PSH, ACK] Seq=9801 Ack=303 Win=64240 Len=356 [TCP segment of a reassembled PDU]
192.168.29.128	205.185.216.42	ТСР	54 50	416 → 80 [ACK] Seq=303 Ack=10157 Win=64240 Len=0

همانطور که در تصویر زیر قابل مشاهده است، آدرس میزبان و نوع مرورگر استفاده شده توسط قربانی مشخص میباشد. در ادامه موقعیت جغرافیایی قربانی برای مهاجم ارسال میگردد.





GET /v2/free/37.129.101.175/countryName HTTP/1.1 User-Agent: Chrome Host: api.db-ip.com Pragma: no-cache HTTP/1.1 200 OK Date: Sat, 07 Sep 2019 07:55:41 GMT Content-Type: text/plain;charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: \_\_cfduid=dela8d68cb14a11f2dc6c76d690aacd6e1567842941; expires=Sun, 06-Sep-20 07:55:41 GMT; path=/; domain=.dbip.com; HttpOnly Vary: Accept-Encoding Access-Control.Allow-Origin: \* Cache-control: public, max-age=1800 X-IPLB-Instance: 30785 CF-Cache-Status: EXPIRED Expires: Sat, 07 Sep 2019 08:25:41 GMT Server: cloudflare CF-RAY: 51271f307c24dffb-FRA



**٦-۳ رمزگشایی:** تاکنون، هیچگونه ابزاری جهت رمزگشایی این باجافزار ارایه نشده است.