باسمه تعالی

تحلیل فنی باج‌افزار Horsuke

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام Horsuke خبر می‌دهد. این باج‌افزار که از خانواده باج‌افزار Scarab می باشد به نام Scarab-Horsia نیز شناخته می شود و پس از رمزگذاری فایل‌ها پسوند horsuke@nuke.africa. را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در ماه می سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES استفاده می‌کند و از طریق هرزنامه و سرویس دسترسی از راه دور(RDP) وارد سیستم قربانی می‌شود.

مشخصات فایل اجرایی :

نام فایل	inside.exe Horsuke.exe
MD۵	de۸d۹۷۹۸۸٤eec۲cef۵ded٦۲۸eef٤۲۹۰c
SHA-۱	۰٦eedbb٤۹۸۹٦۲aa۱۷a۵۳a۷۱۲e۵۹e۱۹ffefd۷cd۸d
SHA-۲۵٦	e۷c۵۵۸۳۵cee۱e۳۹۰bde۹b٤a۲۱c۸٦٤c۷٤f۱٦٤۱٤f۳۹۱a۱۲۲۱c۳f۰۳۸f٦ce۷b۳d۷ee
اندازه فایل	٤۰۲.۵ KB
کامپایلر / پکر	BobSoft Mini Delphi -> BoB / BobSoft

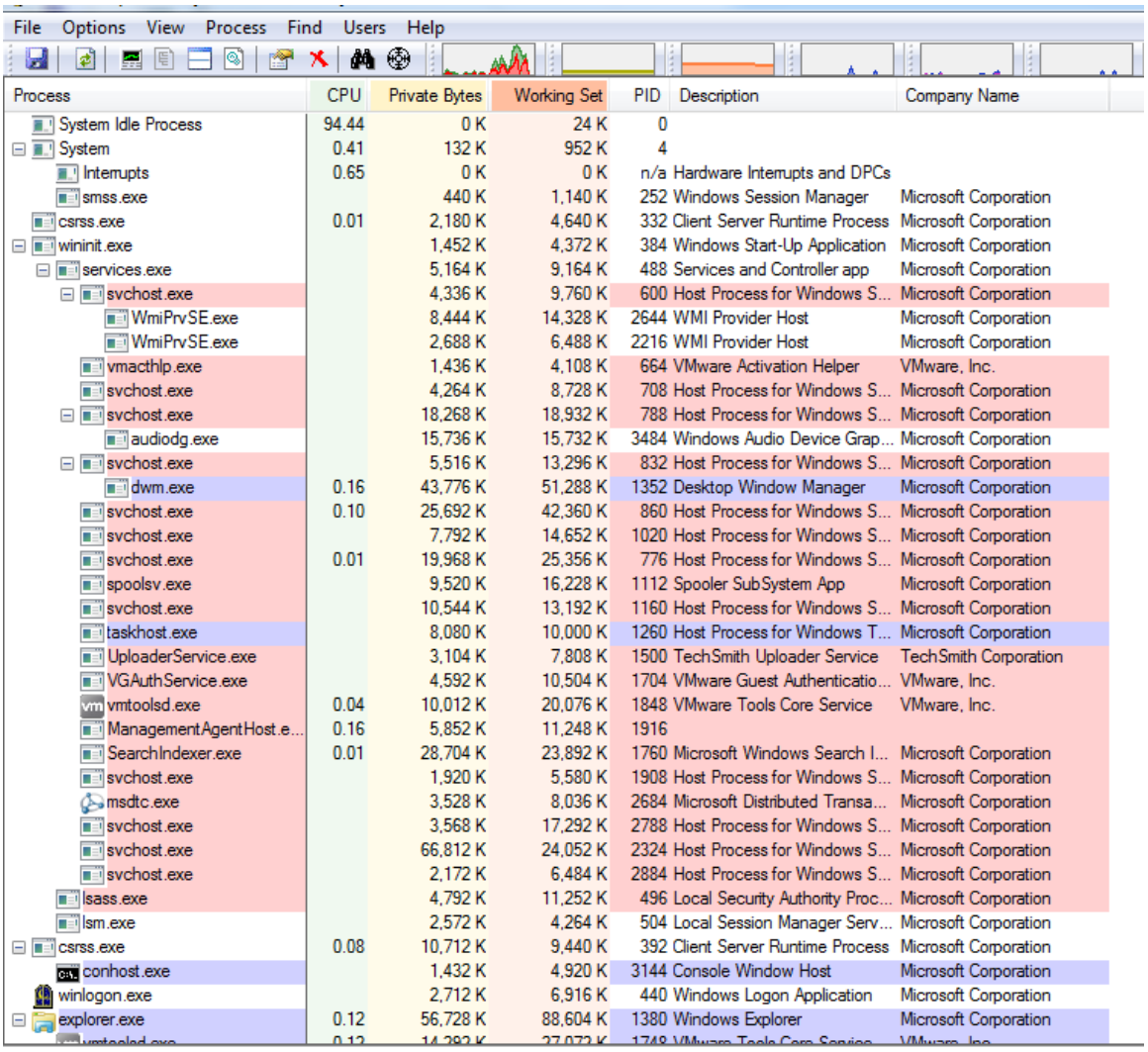
فایل اجرایی این باج‌افزار دارای هشت بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.txt	۷.۱۸	٤۰۹٦	۲۳٦۸۰٤	۲۳۷۰۵٦
.itext	٤.۷۱	۲٤۱٦٦٤	٦۹۲	۱۰۲٤
.data	٤.۷٦	۲٤۵۷٦۰	۱۱٤٦٤	۱۱۷۷٦
.bss	۰	۲۵۸۰٤۸	۲۵۳۰٤	۰
.idata	٤.٦٤	۲۸٦۷۲۰	٤۳۳۲	٤٦۰۸
.tls	۰	۲۹٤۹۱۲	۸	۰
.rdata	۰.۲۱	۲۹۹۰۰۸	۲٤	۵۱۲
.rsrc	۸	۳۰۳۱۰٤	۱۵۵۷۰۸	۱۵٦۱٦۰

تحلیل پویا :

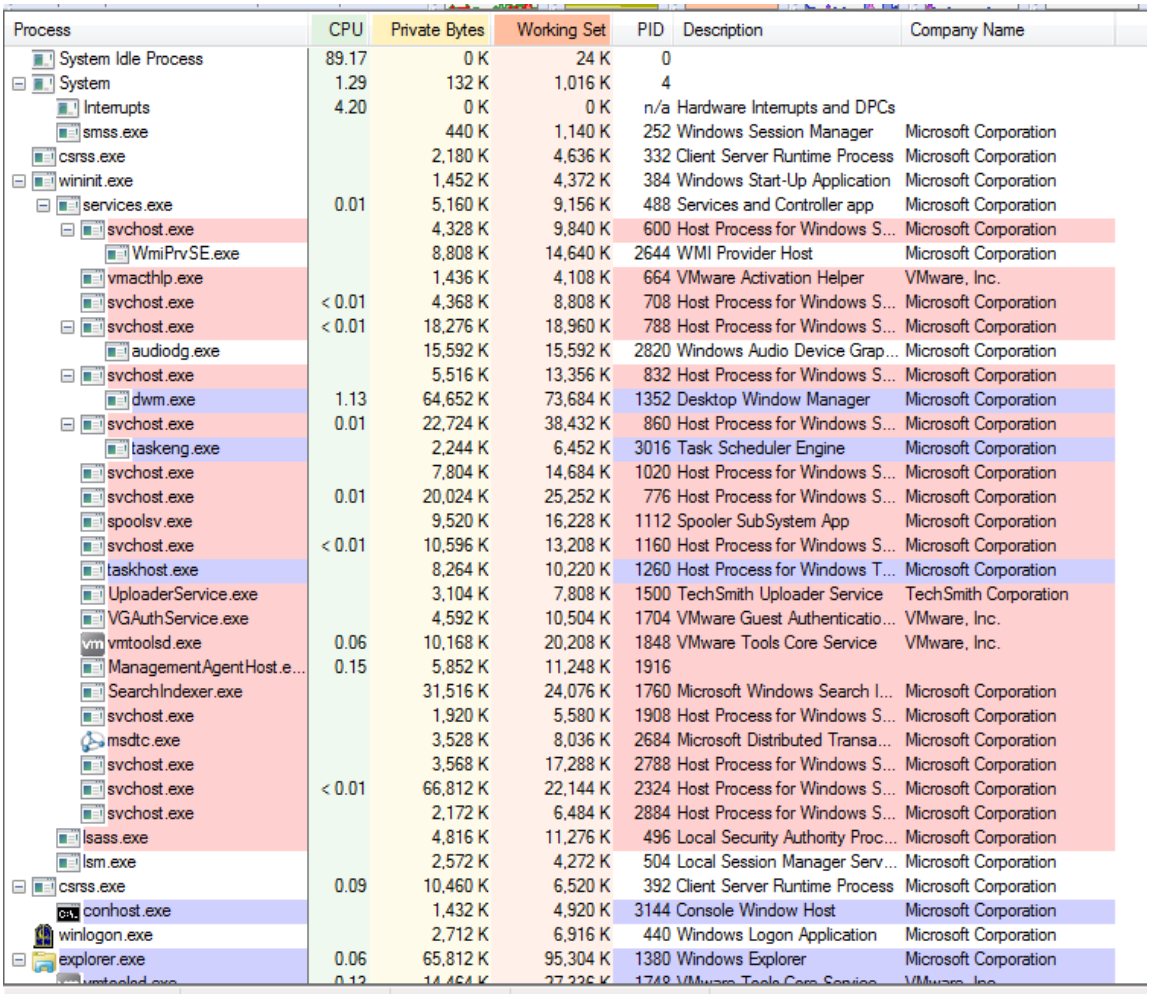
برای بررسی عمیق‌تر باج‌افزار Horsuke فایل اجرایی آن را در محیط آزمایشگاهی اجرا کـردیم تـا عملکـرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم.

در دو تصویر زیر وضعیت فرآیندها قبل و بعد از آلودگی را مشاهده میکنید:



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	94.44	0 K	24 K	0		
System	0.41	132 K	952 K	4		
Interrupts	0.65	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		440 K	1,140 K	252	Windows Session Manager	Microsoft Corporation
csrss.exe	0.01	2,180 K	4,640 K	332	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,452 K	4,372 K	384	Windows Start-Up Application	Microsoft Corporation
services.exe		5,164 K	9,164 K	488	Services and Controller app	Microsoft Corporation
svchost.exe		4,336 K	9,760 K	600	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		8,444 K	14,328 K	2644	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		2,688 K	6,488 K	2216	WMI Provider Host	Microsoft Corporation
vmacthlp.exe		1,436 K	4,108 K	664	VMware Activation Helper	VMware, Inc.
svchost.exe		4,264 K	8,728 K	708	Host Process for Windows S...	Microsoft Corporation
svchost.exe		18,268 K	18,932 K	788	Host Process for Windows S...	Microsoft Corporation
audiodg.exe		15,736 K	15,732 K	3484	Windows Audio Device Grap...	Microsoft Corporation
svchost.exe		5,516 K	13,296 K	832	Host Process for Windows S...	Microsoft Corporation
dwm.exe	0.16	43,776 K	51,288 K	1352	Desktop Window Manager	Microsoft Corporation
svchost.exe	0.10	25,692 K	42,360 K	860	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,792 K	14,652 K	1020	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	19,968 K	25,356 K	776	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		9,520 K	16,228 K	1112	Spooler SubSystem App	Microsoft Corporation
svchost.exe		10,544 K	13,192 K	1160	Host Process for Windows S...	Microsoft Corporation
taskhost.exe		8,080 K	10,000 K	1260	Host Process for Windows T...	Microsoft Corporation
UploaderService.exe		3,104 K	7,808 K	1500	TechSmith Uploader Service	TechSmith Corporation
VGAuthService.exe		4,592 K	10,504 K	1704	VMware Guest Authenticatio...	VMware, Inc.
vmtoolsd.exe	0.04	10,012 K	20,076 K	1848	VMware Tools Core Service	VMware, Inc.
ManagementAgentHost.e...	0.16	5,852 K	11,248 K	1916		
SearchIndexer.exe	0.01	28,704 K	23,892 K	1760	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe		1,920 K	5,580 K	1908	Host Process for Windows S...	Microsoft Corporation
msdtc.exe		3,528 K	8,036 K	2684	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe		3,568 K	17,292 K	2788	Host Process for Windows S...	Microsoft Corporation
svchost.exe		66,812 K	24,052 K	2324	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,172 K	6,484 K	2884	Host Process for Windows S...	Microsoft Corporation
lsass.exe		4,792 K	11,252 K	496	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		2,572 K	4,264 K	504	Local Session Manager Serv...	Microsoft Corporation
csrss.exe	0.08	10,712 K	9,440 K	392	Client Server Runtime Process	Microsoft Corporation
conhost.exe		1,432 K	4,920 K	3144	Console Window Host	Microsoft Corporation
winlogon.exe		2,712 K	6,916 K	440	Windows Logon Application	Microsoft Corporation
explorer.exe	0.12	56,728 K	88,604 K	1380	Windows Explorer	Microsoft Corporation

تصویر ۱: فرایندهای در حال اجرای سیستم عامل قبل از اجرای باج‌افزار

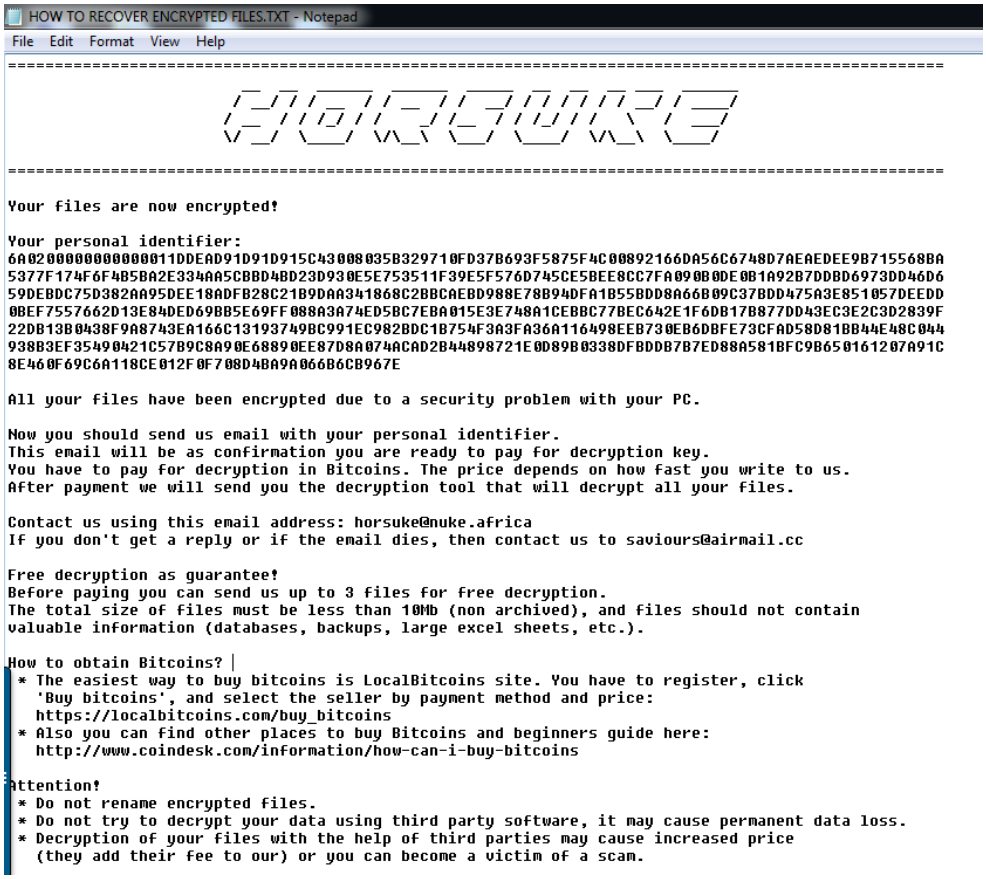


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	89.17	0 K	24 K	0		
System	1.29	132 K	1,016 K	4		
Interrupts	4.20	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		440 K	1,140 K	252	Windows Session Manager	Microsoft Corporation
csrss.exe		2,180 K	4,636 K	332	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,452 K	4,372 K	384	Windows Start-Up Application	Microsoft Corporation
services.exe	0.01	5,160 K	9,156 K	488	Services and Controller app	Microsoft Corporation
svchost.exe		4,328 K	9,840 K	600	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		8,808 K	14,640 K	2644	WMI Provider Host	Microsoft Corporation
vmacthlp.exe		1,436 K	4,108 K	664	VMware Activation Helper	VMware, Inc.
svchost.exe	< 0.01	4,368 K	8,808 K	708	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	18,276 K	18,960 K	788	Host Process for Windows S...	Microsoft Corporation
audiodg.exe		15,592 K	15,592 K	2820	Windows Audio Device Grap...	Microsoft Corporation
svchost.exe		5,516 K	13,356 K	832	Host Process for Windows S...	Microsoft Corporation
dwm.exe	1.13	64,652 K	73,684 K	1352	Desktop Window Manager	Microsoft Corporation
svchost.exe	0.01	22,724 K	38,432 K	860	Host Process for Windows S...	Microsoft Corporation
taskeng.exe		2,244 K	6,452 K	3016	Task Scheduler Engine	Microsoft Corporation
svchost.exe		7,804 K	14,684 K	1020	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	20,024 K	25,252 K	776	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		9,520 K	16,228 K	1112	Spooler SubSystem App	Microsoft Corporation
svchost.exe	< 0.01	10,596 K	13,208 K	1160	Host Process for Windows S...	Microsoft Corporation
taskhost.exe		8,264 K	10,220 K	1260	Host Process for Windows T...	Microsoft Corporation
UploaderService.exe		3,104 K	7,808 K	1500	TechSmith Uploader Service	TechSmith Corporation
VGAuthService.exe		4,592 K	10,504 K	1704	VMware Guest Authenticatio...	VMware, Inc.
vmtoolsd.exe	0.06	10,168 K	20,208 K	1848	VMware Tools Core Service	VMware, Inc.
ManagementAgentHost.e...	0.15	5,852 K	11,248 K	1916		
SearchIndexer.exe		31,516 K	24,076 K	1760	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe		1,920 K	5,580 K	1908	Host Process for Windows S...	Microsoft Corporation
msdtc.exe		3,528 K	8,036 K	2684	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe		3,568 K	17,288 K	2788	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	66,812 K	22,144 K	2324	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,172 K	6,484 K	2884	Host Process for Windows S...	Microsoft Corporation
lsass.exe		4,816 K	11,276 K	496	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		2,572 K	4,272 K	504	Local Session Manager Serv...	Microsoft Corporation
csrss.exe	0.09	10,460 K	6,520 K	392	Client Server Runtime Process	Microsoft Corporation
conhost.exe		1,432 K	4,920 K	3144	Console Window Host	Microsoft Corporation
winlogon.exe		2,712 K	6,916 K	440	Windows Logon Application	Microsoft Corporation
explorer.exe	0.06	65,812 K	95,304 K	1380	Windows Explorer	Microsoft Corporation

تصویر ۲: باج‌افزار در حال اجرا می‌باشد و از شروع فعالیت فرایندها و نرم‌افزارها جلوگیری می‌کند.

طبق بررسی‌های صورت گرفته، باج‌افزار Horsuke پس از اجرا از شروع فعالیت برخی فرآیندها و نرم‌افزارها جلوگیری می کند. پس از اجرای باج‌افزار پیغام باج‌خواهی گشوده می‌شود که این پیغام در تمامی فولدرهای رمزگذاری شده نیز وجود دارد.

تصویر زیر پیغام باج‌خواهی باج‌افزار Horsuke را با نام HOW TO RECOVER ENCRYPTED FILES.TXT نشان می دهد که بر روی پس زمینه سیستم قربانی مستقر شده است :



بر اساس پیغام باج‌خواهی، که در ابتدای آن شناسه ای با طول ٦٤٤ کاراکتر مختص هر قربانی قرار داده شده، مهاجم اعلام می‌کند که فایل های قربانی را رمزگذاری کرده و سپس قربانی را ملزم به فرستادن ایمیل با شناسه یاد شده برای دریافت کلید رمزگشا می‌کند. مهاجم مبلغ باج را به صورت بیت کوین تعیین کرده و اعلام می‌کند که مبلغ باج به سرعت فرستادن ایمیل بستگی دارد. ضمناً برای برقراری ارتباط، ایمیلی به آدرس horsuke@nuke.africa در نظر گرفته شده که در صورت عدم دریافت پاسخ از ایمیل مذکور، ایمیل جایگزین به آدرس saviours@airmail.cc نیز تعبیه شده است.

در ادامه برای حصول اطمینان قربانی، تعدادی از فایل های وی را تحت شرایط زیر به صورت رایگان رمزگشایی می‌کند :

۱- حداکثر سه فایل که آرشیو نشده باشند.

۲- مجموع حجم فایل ها حداکثر ۱۰ مگابایت باشد

۳- فایل ها شامل اطلاعات ارزشمند نباشند. (پایگاه های داده، فایل‌های پشتیبان، صفحات اکسل و...).

سپس در ادامه نحوه تهیه بیت‌کوین را آموزش داده و هشدارهایی را نیز برای تهدید قربانی می‌دهد.

ضمناً در پیغام باج‌خواهی مهلتی برای پرداخت باج نیز تعیین نشده است.

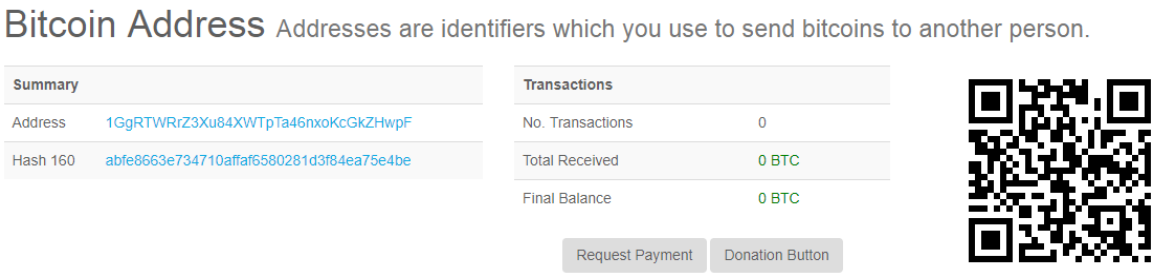
پس از برقراری ارتباط به صورت ناشناس با مهاجم، پاسخ اولیه مبنی بر گذشت زمان و عدم توانایی رمزگشایی بود :

```
Hello. It was not easy to get your decryption key cuz it's so much time
passed... Here is your files uploaded down bellow:
https://privatlab.com/s/v/XyZ7DG9R5dsoaOLm5XkZ
```

در پاسخ بعدی ایمیلی دریافت نمودیم که در آن مهاجم مبلغ ۰.۷ بیت کوین را جهت ارسال به آدرس کیف پول ۱GgRTWRrZ۳Xu۸٤XWTpTa٤٦nxoKcGkZHwpF تعیین نمود.

```
To restore all files that belong to your id transfer 0.7 btc to wallet
address 1GgRTWRrZ3Xu84XWTpTa46nxoKcGkZHwpF
After confiration of your transaction we will send you a decryptor
software and instruction how to use it.
Please, contact us just in case of you're agree to pay. Respect your and
our time.
```

طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تراکنشی نداشته است.

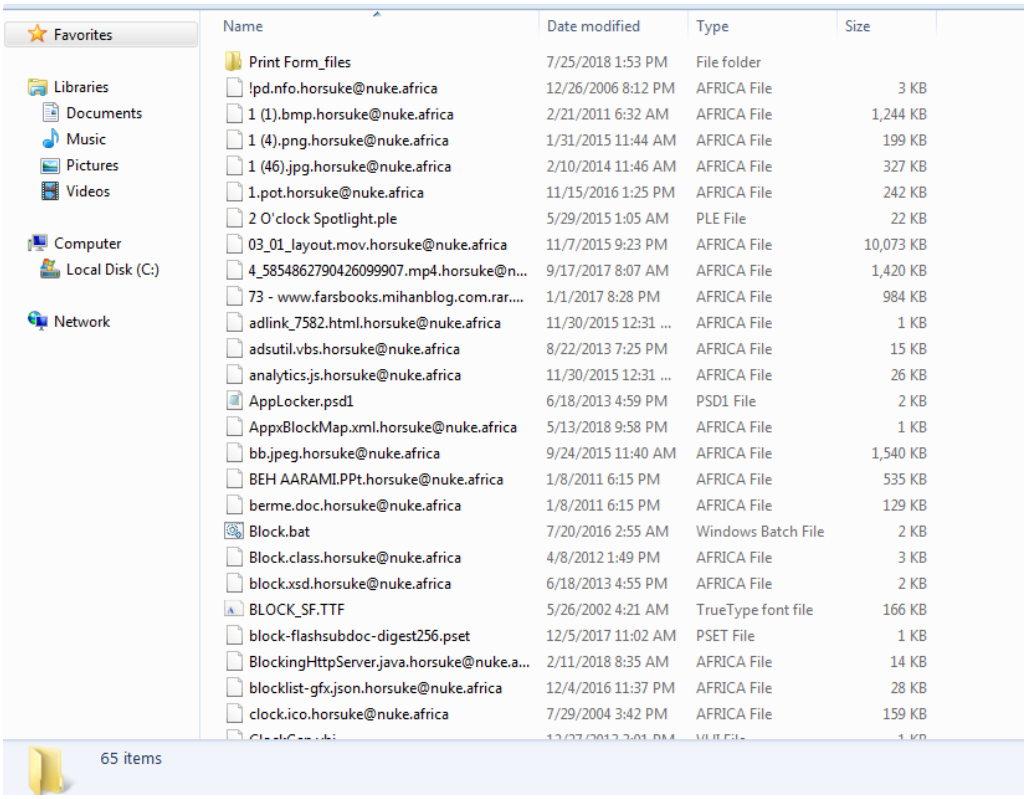

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1GgRTWRrZ3Xu84XWTpTa46nxoKcGkZHwpF
Hash 160	abfe8663e734710affaf6580281d3f84ea75e4be

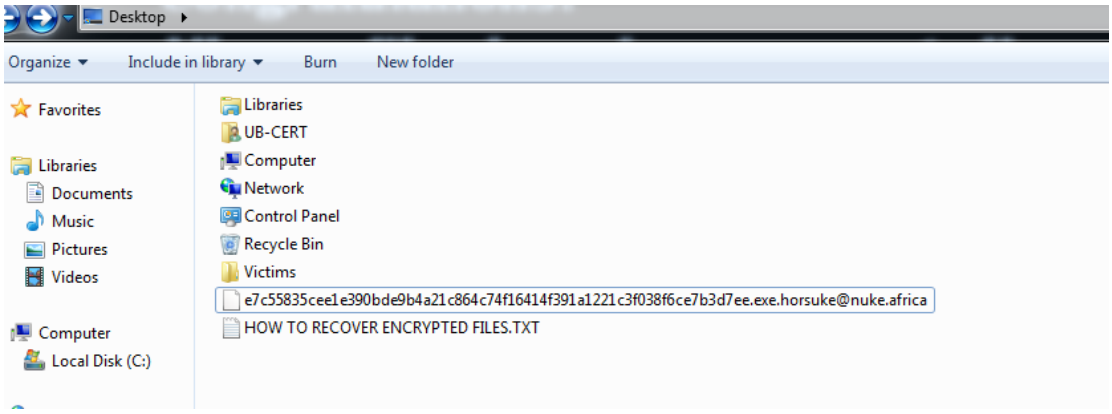
Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment Donation Button

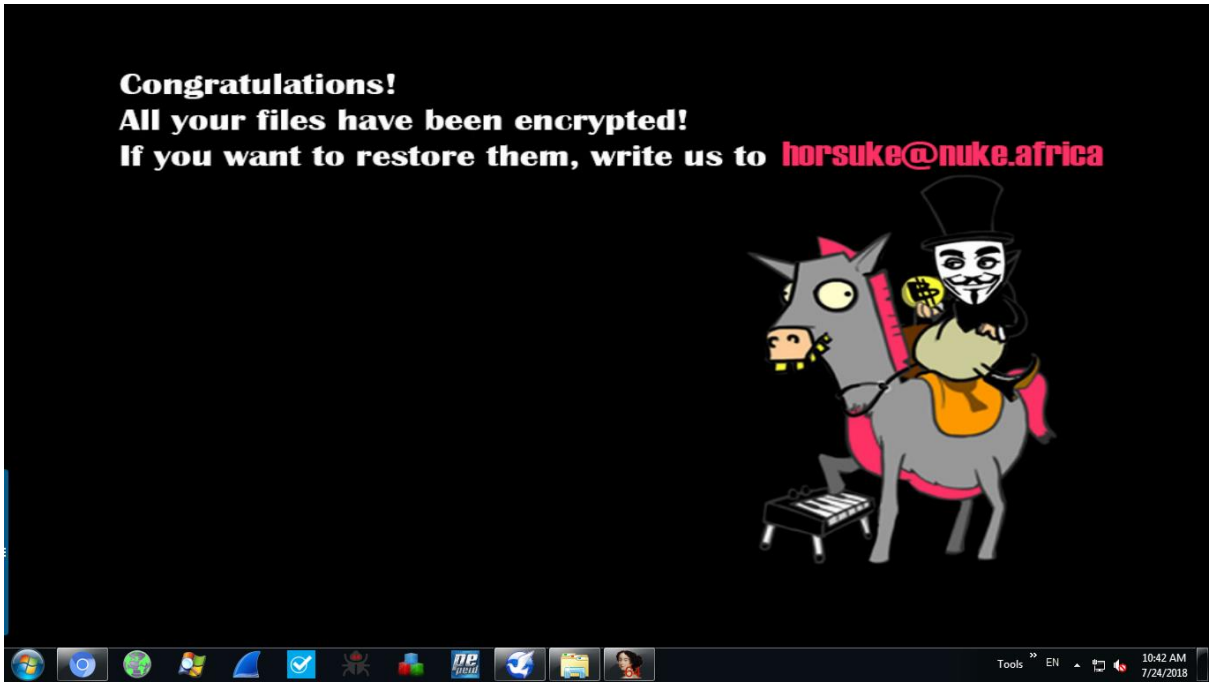
همانطور که اشاره شد، باج‌افزار Horsuke پس از رمزگذاری پسوند .horsuke@nuke.africa را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند. تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد:



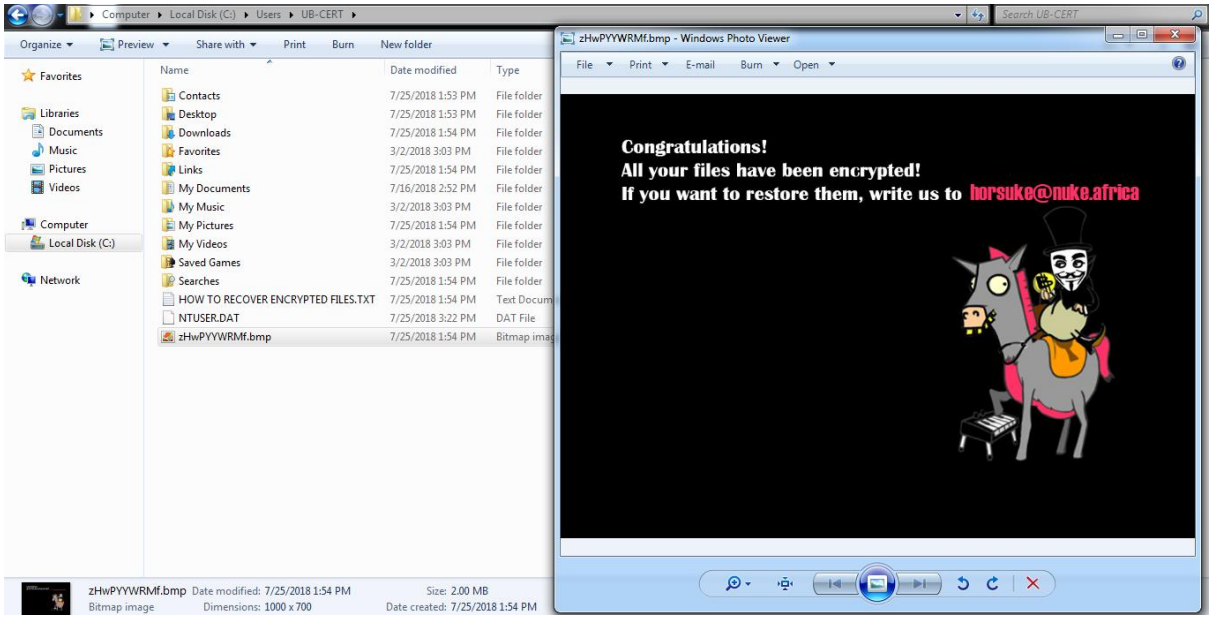
طبق مشاهدات صورت گرفته، باج‌افزار فایل اجرایی خود را نیز رمزگذاری می‌کند :



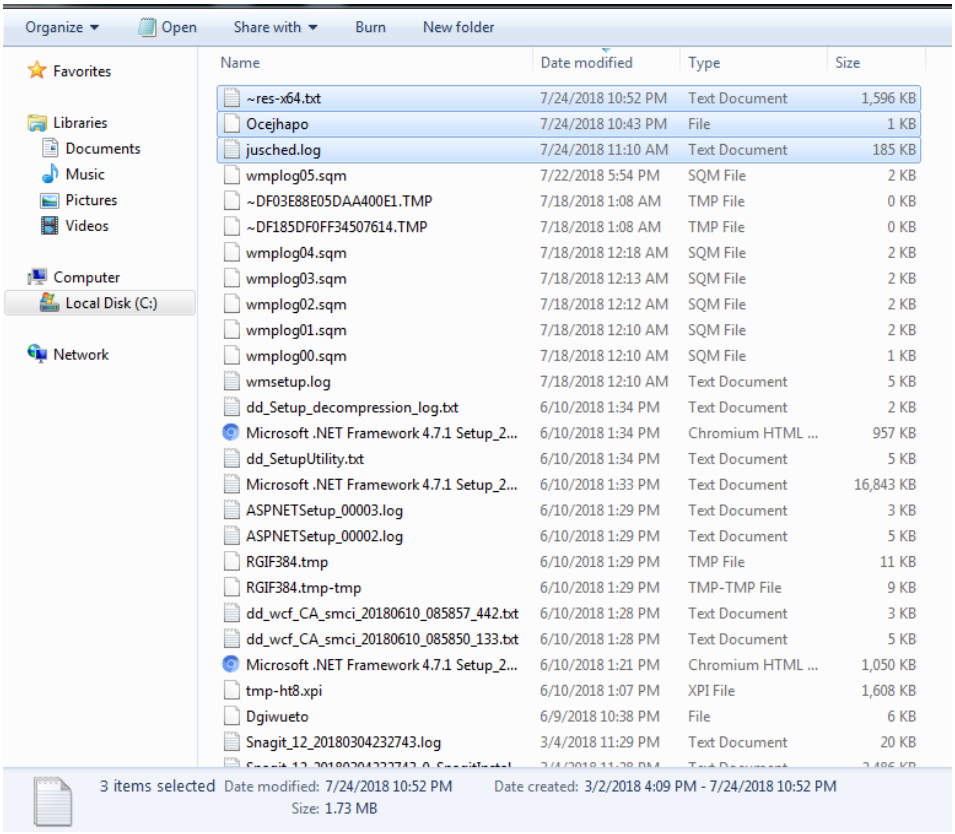
در ادامه، تصویر پس زمینه توسط باج‌افزار تغییر پیدا می کند.

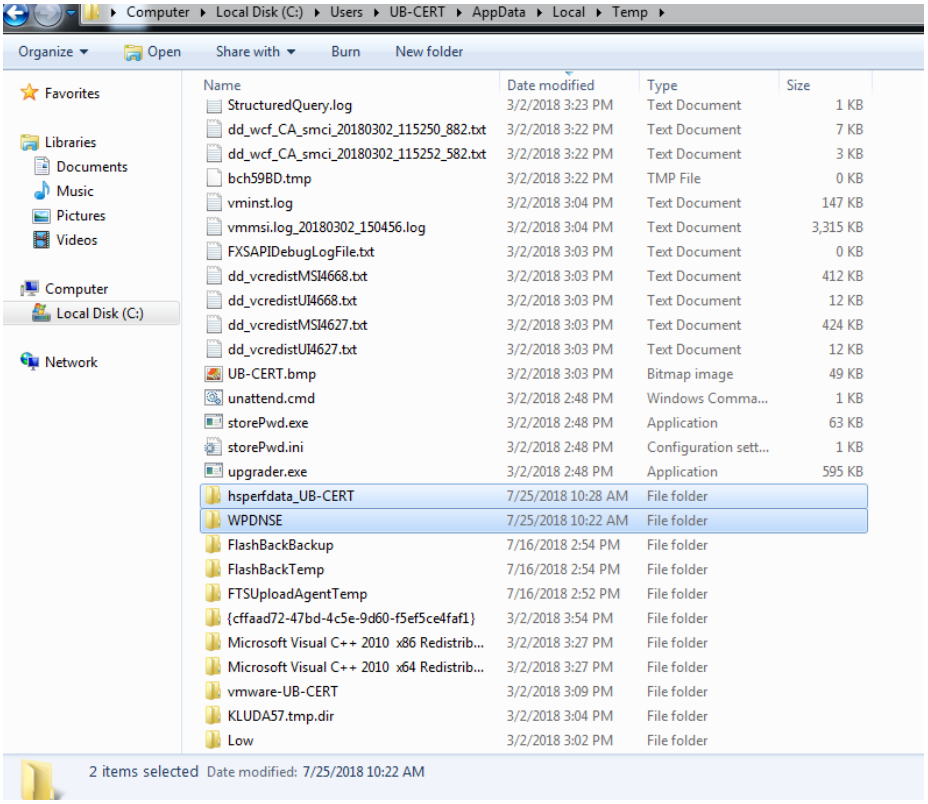


باج‌افزار در این تصویر ضمن تبریک و اعلام رمزگذاری فایل های قربانی، ایمیلی به آدرس horsuke@nuke.africa را به قربانی معرفی می‌کند. فایل این تصویر به نام zHwPYYWRMf.bmp در فولدر users در درایو اصلی سیستم قربانی قرار گرفته است.

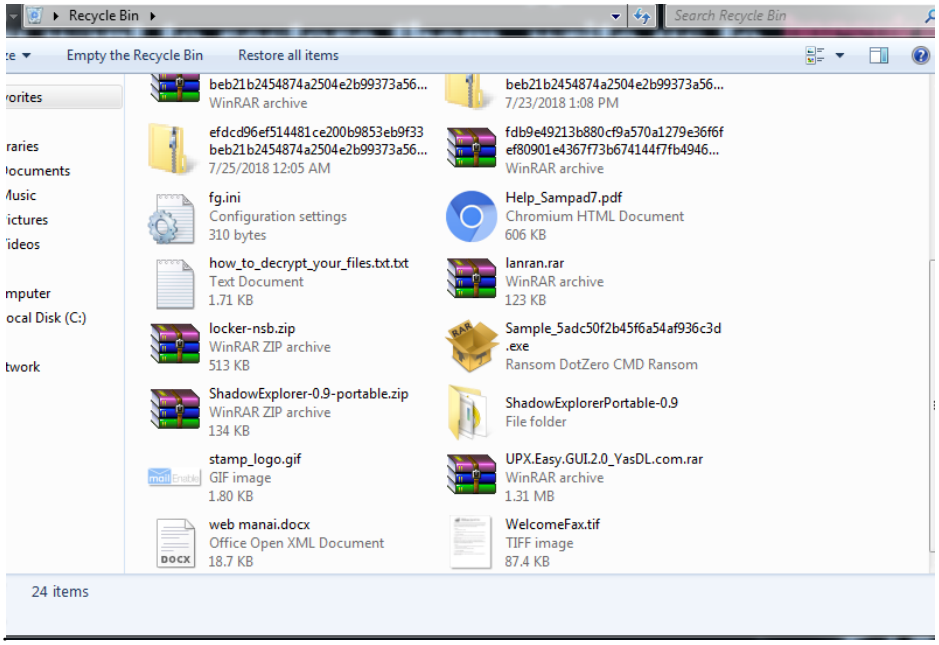


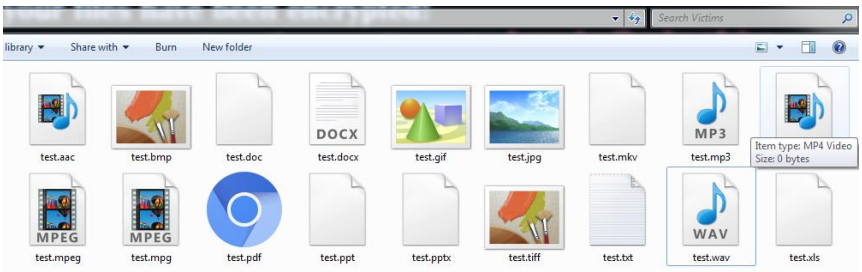
در تصاویر زیر فایل های اضافه شده و تغییر یافته در مسیر درایو سیستم عامل و پوشه Windows را مشاهده می کنید :





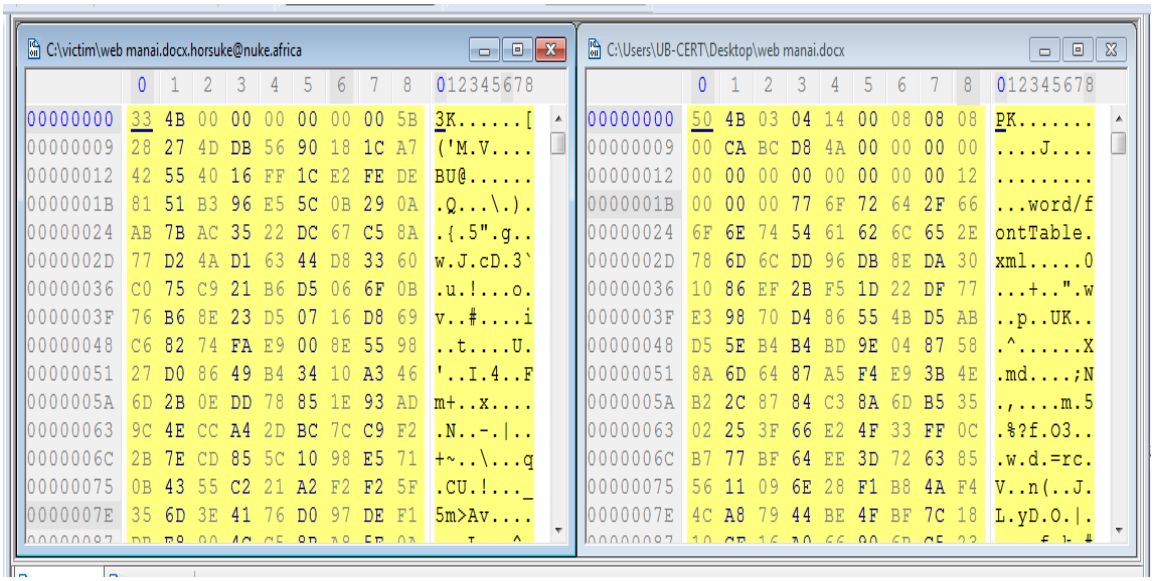
طبق بررسی‌های صورت گرفته، محتویات Recycle bin و فایل های فاق محتوا (با حجـم ۰ بایـت) توسـط باج‌افزار رمزگذاری نمی شوند.





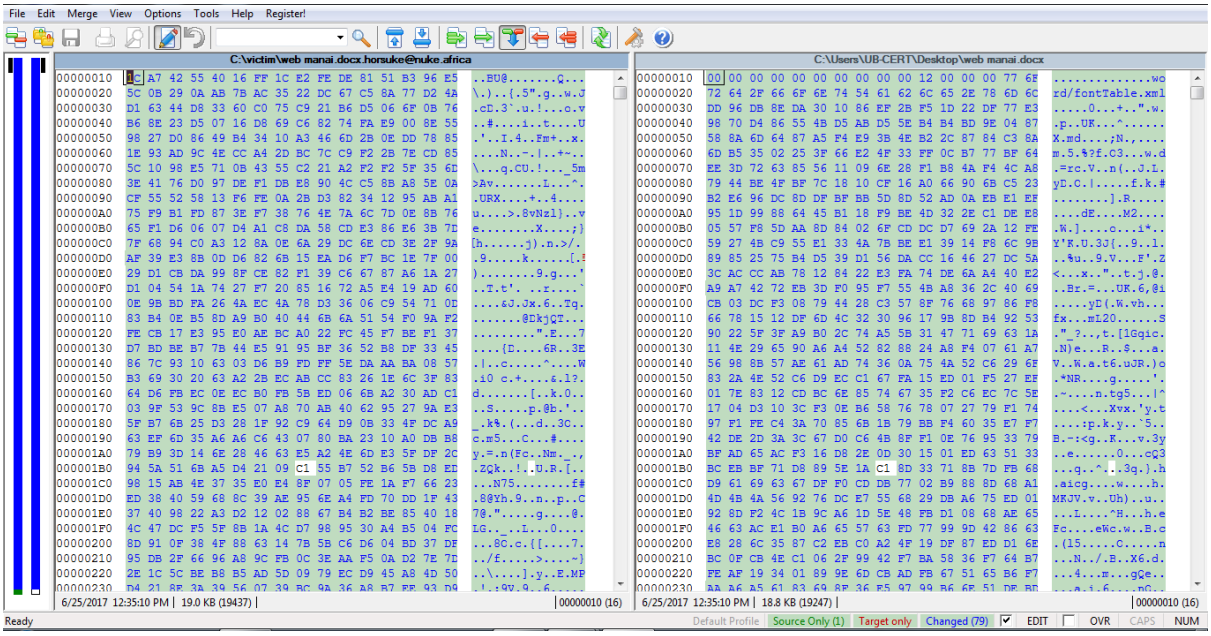
تحلیل ایستا:

پس از تحلیل کد باج‌افزار Horsuke به نتایج زیر دست پیدا کردیم.

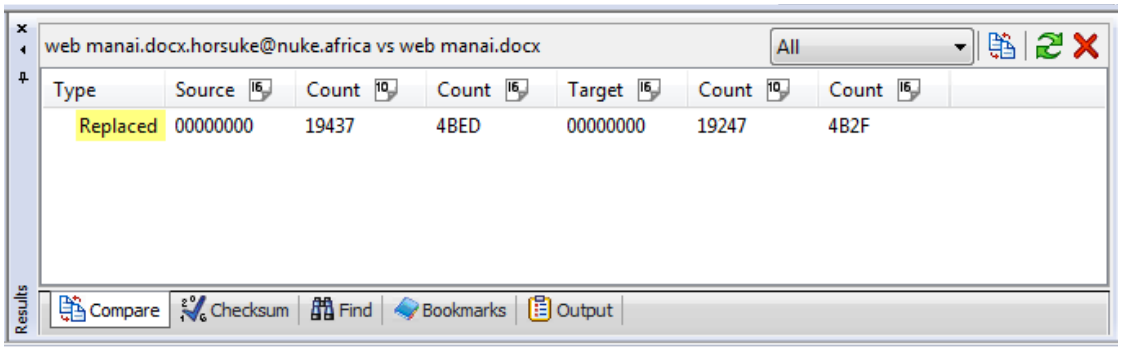


نمونه فایل قبل و بعد از رمزگذاری

بیش از دوبرابر محتوای اولیه حجم افزوده شده است.



تعداد بایت های جایگزین شده نمونه فایل بعد از رمزگذاری:



قطعه کد دریافت زمان محلی سیستم قربانی :

```
:004061E4 ; =============== S U B R O U T I N E =======================================
:004061E4
:004061E4 ; Attributes: thunk
:004061E4
:004061E4 ; void __stdcall GetLocalTime(LPSYSTEMTIME lpSystemTime)
:004061E4 GetLocalTime    proc near               ; CODE XREF: sub_40CEAC+8↓p
:004061E4                                         ; sub_40CED8+4↓p
:004061E4
:004061E4 lpSystemTime    = dword ptr  4
:004061E4
:004061E4                 jmp     ds:__imp_GetLocalTime
:004061E4 GetLocalTime    endp
:004061E4
:004061E4 ; ---------------------------------------------------------------------------
:004061EA                 align 4
:004061EC ; [00000006 BYTES: COLLAPSED FUNCTION GetLocaleInfoA_0. PRESS CTRL-NUMPAD+ TO EXPAND]
:004061F2                 align 4
:004061F4 ; [00000006 BYTES: COLLAPSED FUNCTION GetModuleFileNameA_0. PRESS CTRL-NUMPAD+ TO EXPAND]
:004061FA                 align 4
:004061FC ; [00000006 BYTES: COLLAPSED FUNCTION GetModuleFileNameW. PRESS CTRL-NUMPAD+ TO EXPAND]
000055E4 00000000004061E4: GetLocalTime (Synchronized with Hex View-1)
```

کلید رجیستری اضافه شده:

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\zHwPYYWRMf

مقادیر اضافه شده:

HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\system32\MCTRes.dll,-200005: "Websites for United States" *HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\System32\ieframe.dll,-12385: "Favorites Bar"* *HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Program Files\Common Files\system\wab32res.dll,-10100: "Contacts"* *HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\iPointSize:* *HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfCharSet:* *HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfWeight:* *HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfItalic:* *HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfUnderline:* *HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfOrientation:* *HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfStrikeOut:* *HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfFaceName: "Fixedsys"* *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\r7p55835prr1r390oqr9o4n21p864p74s16414s391n1221p3s038s6pr7o3q7rr.rkr:* *HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Run\zHwPYYWRMf: "notepad.exe "C:\Users\UB-CERT\HOW TO RECOVER ENCRYPTED FILES.TXT""* *HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\zHwPYYWRMf\idle: "1"* *HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\system32\MCTRes.dll,-200005: "Websites for United States"* *HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Windows\System32\ieframe.dll,-12385: "Favorites Bar"* *HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Program Files\Common Files\system\wab32res.dll,-10100: "Contacts"*

کلیدهای رجیستری تغییر یافته:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{D4546416-77DE-4750-923A-1ED584EB8218}\DateLastConnected *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter* *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\CurrentLanguage\Counter* *HKLM\SOFTWARE\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{47047898-1E6D-11E8-878B-806E6F6E6963}: "70564856"* *HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter*

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Perflib\CurrentLanguage\Counter
HKLM\SYSTEM\ControlSet001\services\SharedAccess\Epoch\Epoch:
HKLM\SYSTEM\ControlSet001\services\SharedAccess\Epoch2\Epoch:
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\LeaseObtainedTime:
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\T1:
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\T2:
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\LeaseTerminatesTime:
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Leave):
HKLM\SYSTEM\RNG\Seed
HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Epoch\Epoch:
HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Epoch2\Epoch:
HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Epoch2\Epoch:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\LeaseObtainedTime: 0x5B5DBD3A
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\LeaseObtainedTime: 0x5B5DC803
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\T1:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\T1:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\T2:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\T2:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\LeaseTerminatesTime:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\LeaseTerminatesTime:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-D71BA9D2C1D3}\DhcpInterfaceOptions:
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\Control Panel\Desktop\WallpaperStyle: "10"
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Control Panel\Desktop\WallpaperStyle: "2"
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Control Panel\Desktop\Wallpaper: "C:\Users\UB-CERT\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg"
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Control Panel\Desktop\Wallpaper: "C:\Users\UB-CERT\zHwPYYWRMf.bmp"

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\{S38OS404-1Q43-42S2-9305-67QR0O28SP23}\rkcybere.rkr:
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\ertfubg_1.8.3_orgn1_jva32_k64\ertfubg_k64.rkr
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1162x591x96(1).x:
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1162x591x96(1).y
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1162x591x96(1).x: 0xFFFF8300
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1162x591x96(1).y: 0xFFFFFFFF:

این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند که در جدول زیر قابل مشاهده است :

advapi۳۲.dll	kernel۳۲.dll	kernel۳۲.dll	kernel۳۲.dll	oleaut۳۲.dll
RegDeleteKeyA RegCloseKey RegQueryValueExA RegSetValueExA RegEnumValueA RegCreateKeyExA RegOpenKeyExA RegDeleteValueA RegEnumKeyExA	GetLastError GetEnvironmentVariableA GetStdHandle FileTimeToDosDateTime lstrlenA GetModuleFileNameW GlobalFree WaitForSingleObject FreeLibrary QueryPerformanceCounter EnterCriticalSection	GetTickCount GetThreadLocale GetVersionExA GlobalUnlock GetModuleFileNameA GlobalHandle RtlUnwind LoadLibraryA WinExec CreateProcessW DeleteCriticalSection GetStartupInfoA GetDateFormatA LoadLibraryExA SizeofResource	FindNextFileW GetLocaleInfoA LocalAlloc OpenProcess LockResource SetFileTime GetCommandLineW CreateThread UnhandledExceptionFilter MultiByteToWideChar GetLocalTime GetCPInfo GetCommandLineA GetProcAddress	VariantChangeType SafeArrayGetLBound SafeArrayPtrOfIndex SysAllocStringLen VariantClear SafeArrayCreate SysReAllocStringLen SafeArrayGetUBound VariantCopy SysFreeString VariantInit

shell۳۲.dll	user۳۲.dll	wininet.dll	kernel۳۲.dll	kernel۳۲.dll
SHGetMalloc ShellExecuteW	CharLowerBuffW GetSystemMetrics	InternetReadFile InternetOpenUrlA	EnumCalendarInfoA ReadFile	FormatMessageA OpenMutexA

SHGetPathFromIDListW SHGetSpecialFolderLocation	GetLastInputInfo LoadStringA DispatchMessageA CharLowerBuffA SystemParametersInfoW CharToOemA CharNextA CharUpperBuffA MessageBoxA PeekMessageA TranslateMessage CharNextW GetKeyboardType DestroyWindow	InternetCloseHandle InternetOpenA	lstrcpynA FindFirstFileW GetACP GetDiskFreeSpaceA GlobalLock FreeResource GlobalAlloc TerminateProcess CreateProcessA FileTimeToLocalFileTime InitializeCriticalSection LoadResource CreateFileW VirtualQuery VirtualFree FindClose TlsGetValue Sleep MoveFileW SetFileAttributesW TlsSetValue CloseHandle ExitProcess GetCurrentThreadId FindResourceA VirtualAlloc DeleteFileW LeaveCriticalSection	CreateMutexA SetFilePointer RaiseException CompareStringA WideCharToMultiByte GetFileAttributesA GetModuleHandleA CreatePipe FindFirstFileA SetEndOfFile GlobalReAlloc WriteFile

```
004452D8 _bss           ends
004452D8
a:004463B4 ;
a:004463B4 ; Imports from oleaut32.dll
a:004463B4 ;
a:004463B4 ; Section 5. (virtual address 00046000)
a:004463B4 ; Virtual size                  : 000010EC (   4332.)
a:004463B4 ; Section size in file          : 00001200 (   4608.)
a:004463B4 ; Offset to raw data for section: 0003D400
a:004463B4 ; Flags C0000040: Data Readable Writable
a:004463B4 ; Alignment     : default
a:004463B4 ; ===========================================================================
a:004463B4
a:004463B4 ; Segment type: Externs
a:004463B4 ; _idata
a:004463B4 ; void __stdcall SysFreeString(BSTR bstrString)
a:004463B4                 extrn __imp_SysFreeString:dword
a:004463B4                                         ; DATA XREF: SysFreeString↑r
a:004463B8 ; INT __stdcall SysReAllocStringLen(BSTR *pbstr, const OLECHAR *psz, unsigned int len)
a:004463B8                 extrn __imp_SysReAllocStringLen:dword
a:004463B8                                         ; DATA XREF: SysReAllocStringLen↑r
a:004463BC ; BSTR __stdcall SysAllocStringLen(const OLECHAR *strIn, UINT ui)
a:004463BC                 extrn __imp_SysAllocStringLen:dword
0003D400 00000000004463B4: .idata:__imp_SysFreeString (Synchronized with Hex View-1)
```

بر اساس بررسی‌های صورت گرفته، باج‌افزار Horsuke پس از اجرا، فرایندهای زیر را ایجاد می‌کند :

- HonestSample_٥afd٤a٩٥٩٩٣١٣٦٥٦٤٤caeb٨٨.exe (PID: ٣٦٨٨)
  - cmd.exe /c copy /y "C:\HonestSample_٥afd٤a٩٥٩٩٣١٣٦٥٦٤٤caeb٨٨.exe" "%APPDATA%\winlogon.exe" (PID: ٣٩٦٨)
  - HonestSample_٥afd٤a٩٥٩٩٣١٣٦٥٦٤٤caeb٨٨.exe runas (PID: ٣٢٩٢)

- cmd.exe /c copy /y "C:\HonestSample_٥afd٤a٩٥٩٩٣١٣٦٥٦٤٤caeb٨٨.exe" "%APPDATA%\winlogon.exe" (PID: ٢٣٢٤)
- winlogon.exe (PID: ١٢٧٢)
  - mshta.exe "javascript:o=new ActiveXObject('WScript.Shell');x=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{i=x.GetFile('winlogon.exe').Path;o.RegWrite('HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\zHwPYYWRMf',i);}catch(e){}},١٠);" (PID: ٣٦٩٦)
  - mshta.exe "javascript:eval(new ActiveXObject('WScript.Shell').RegRead('HKCU\\Software\\MCDVV\\TOFLK'));close();" (PID: ١٩٢٨)
    - cmd.exe /c wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:٠ (PID: ٢٧٧٢)
      - wbadmin.exe wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:٠ (PID: ٣٣٧٦)
    - cmd.exe /c wmic SHADOWCOPY DELETE (PID: ٤٦٤)
      - WMIC.exe wmic SHADOWCOPY DELETE (PID: ٣٧٢٤)
    - cmd.exe /c vssadmin Delete Shadows /All /Quiet (PID: ٢٤٩٢)
      - vssadmin.exe vssadmin Delete Shadows /All /Quiet (PID: ٢٩٣٦)
    - cmd.exe /c bcdedit /set {default} recoveryenabled No (PID: ٤٣٢)
      - bcdedit.exe bcdedit /set {default} recoveryenabled No (PID: ٣٦٤٤)
    - cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures (PID: ٣٠٢٤)
      - bcdedit.exe bcdedit /set {default} bootstatuspolicy ignoreallfailures (PID: ٢٢٤٠)
  - ~wtmp٠٠١.exe (PID: ٢٣٩٢)
    - walm.exe (PID: ١٠٤٨)
  - cmd.exe /c start /max notepad.exe "%USERPROFILE%\HOW TO RECOVER ENCRYPTED FILES.TXT" (PID: ٣٢٢٠)
    - notepad.exe "%USERPROFILE%\HOW TO RECOVER ENCRYPTED FILES.TXT" (PID: ٢٥٥٦)
  - mshta.exe "javascript:o=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{o.DeleteFile('winlogon.exe');close()}catch(e){}},١٠);" (PID: ٣٢١٢)

تحلیل ترافیک شبکه :

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

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۵۳ مورد از ٦٧ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Kaspersky	HEUR:Trojan-Ransom.Win32.Generic	Malwarebytes	Ransom.Horsuke
MAX	malware (ai score=99)	McAfee	GenericRXDM-JB!DE8D979884EE
McAfee-GW-Edition	BehavesLike.Win32.Generic.gc	Microsoft	Ransom:Win32/Higuniel.A
NANO-Antivirus	Trojan.Win32.Filecoder.fbyqbw	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.793
SentinelOne	static engine - malicious	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Trojan.Gen.2
Tencent	Win32.Trojan.Generic.Wurd	TrendMicro	Ransom_HORSUKE.THEAGAH
TrendMicro-HouseCall	Ransom_HORSUKE.THEAGAH	VBA32	BScope.Trojan.Encoder
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Ransom.412160
Yandex	Trojan.Filecoder!4ozwfU+5bfY	Zillya	Trojan.Filecoder.Win32.7754
ZoneAlarm	HEUR:Trojan-Ransom.Win32.Generic	Antiy-AVL	Clean
Ad-Aware	DeepScan:Generic.Ransom.Amnesia.4...	AegisLab	Troj.Ransom.W32!c
AhnLab-V3	Trojan/Win32.Ransom.C2527025	ALYac	Trojan.Ransom.Scarab
Arcabit	DeepScan:Generic.Ransom.Amnesia.4...	Avast	FileRepMalware
AVG	FileRepMalware	Avira	TR/Dropper.Gen
AVware	Trojan.Win32.Generic!BT	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	DeepScan:Generic.Ransom.Amnesia.4...	CAT-QuickHeal	Trojan.Higuniel
ClamAV	Win.Ransomware.Scarab-6336012-1	Comodo	TrojWare.Win32.TrojanDownloader.De...
CrowdStrike Falcon	malicious_confidence_100% (W)	Cybereason	malicious.884eec
Cylance	Unsafe	Cyren	W32/Trojan.MNYA-8045
DrWeb	Trojan.Encoder.11464	Emsisoft	DeepScan:Generic.Ransom.Amnesia.4... (B)
Endgame	malicious (high confidence)	eScan	DeepScan:Generic.Ransom.Amnesia.4...
ESET-NOD32	a variant of Win32/Filecoder.FS	F-Secure	DeepScan:Generic.Ransom.Amnesia.4...
Fortinet	W32/Msht.GJ!tr	GData	DeepScan:Generic.Ransom.Amnesia.4...
Ikarus	Trojan-Ransom.FileCoder	Jiangmin	Trojan.Generic.cefmz
K7AntiVirus	Trojan (004f6e981)	K7GW	Trojan (004f6e981)

خروجی سامانه ویروس‌کاو مرکز ماهر :

پرینت

نام فایل: e7c55835cee1e390bde9b4a21c864c74f16414f391a1221c3f038f6ce7b3d7ee.exe

حجم فایل: ۴۰۳ کیلوبایت

تاریخ اسکن: ۶ مرداد ۱۳۹۷ - ۱۲:۰۴

MD5: de8d979884eec2cef5ded628eef4290c

SHA1: 06eedbb498962aa17a53a712e59e19ffefd7cd8d

SHA256: e7c55835cee1e390bde9b4a21c864c74f16414f391a1221c3f038f6ce7b3d7ee

وضعیت:

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن	
پادویش	2.3.190.2675	ii	Malware: Malware.SubId.127805343
sophos	9.14.2	✔	Clean
f_secure	11.00	ii	Dangerous: Trojan.Ransom.BYN
kaspersky	5.5	i	Suspicious: HEUR:Trojan-Ransom.Win32.Generic
eset	4.5.3.38123	ii	Dangerous: Win32/Filecoder.FS
drweb	11.0.1.1607061217	ii	Dangerous: Trojan.Encoder.11464
clam_av	0.99.2	ii	Dangerous: Win.Ransomware.Scarab-6336012-1
comodo	1.1.268025.1	ii	Dangerous: TrojWare.Win32.TrojanDownloader.Delf.Gen
bitdefender	11.0.1.18	ii	Dangerous: Trojan.Ransom.BYN
avast	2.1.2	✔	Clean
symantec	7.9.0.30	ii	Dangerous: Trojan.Gen.2