باسمه تعالی

# تحلیل فنی باج‌افزار CyberSCCP

## مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی باج‌افزار CyberSCCP خبر می‌دهد . بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در روز نوزدهم ماه ژوئن سال ۲۰۱۸ میلادی شروع شده است و به نظر می‌رسد که شیوع آن بیشتر در خاورمیانه و به‌خصوص در میان جامعه ایرانیان است و کاربران شبکه های اجتماعی هدف اصلی این باج‌افزار می باشند. طبق مشاهدات صورت گرفته، این باج‌افزار از خانواده باج‌افزار متن باز HiddenTear می‌باشد که تحت عنوان Cyber.exe با حجم ۱.۴۲ مگابایت و در پوشش اپلیکیشنی برای جعل مدارک هویتی از جمله کارت ملی و شناسنامه در حال گسترش در بین کاربران تلگرام فارسی زبان است. طبق بررسی های صورت گرفته، این باج‌افزار برای محیط های دارای سیستم عامل ویندوز ٦٤ بیتی توسعه یافته و عملکرد آن مشابه باج‌افزارهای Qnbqw, Donut, DBGer, Leen و dozens می باشد. این باج‌افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل ها از قربانیان تقاضای بیت کوین می‌کند.

## مشخصات فایل اجرایی :

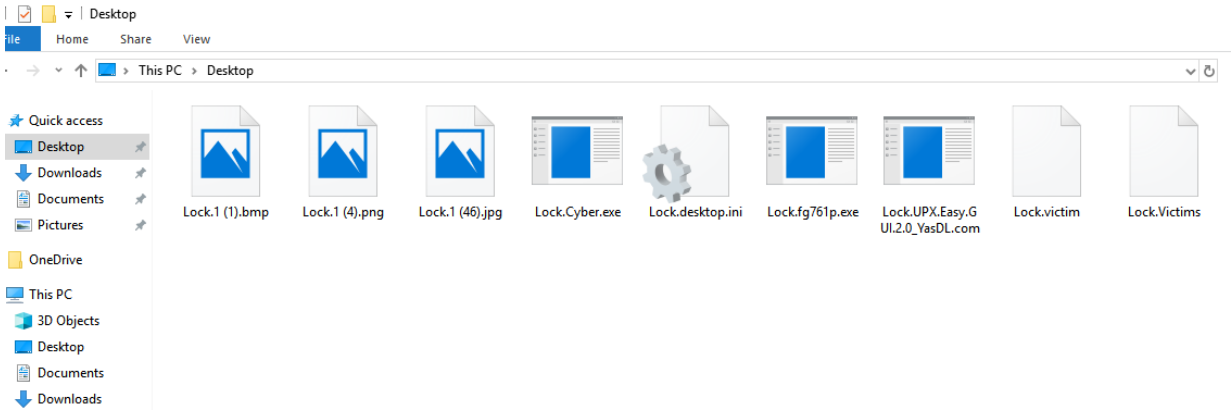
| نام فایل | *setup.exe* |
|---|---|
| اندازه | ۱.۴۲ MB |
| SHA-۱ | d٥٤٩٥٥٩b٥b٠ad٨٣a٢٢e٩١ffbv٩٦٤١b٩٢a٠٣٢e٤cb |
| SHA-٢٥٦ | f٠cf٦eb٤da٣٨vdee٤a٩١fd٦٢٦٠d٣٧c٩٥٨e٢c٦aba١cv٢d٩٢٢aba٢٥fcdv٢٠٥v٤٠c |
| MD٥ | ٣d١٨٨ff٩cd٥٥٥٩٢c٢٢١٤١d٣٧e٩٨٩٢٢٧٠ |
| کامپایلر | UPX |

فایل اجرایی این باج‌افزار دارای سه بخش است :

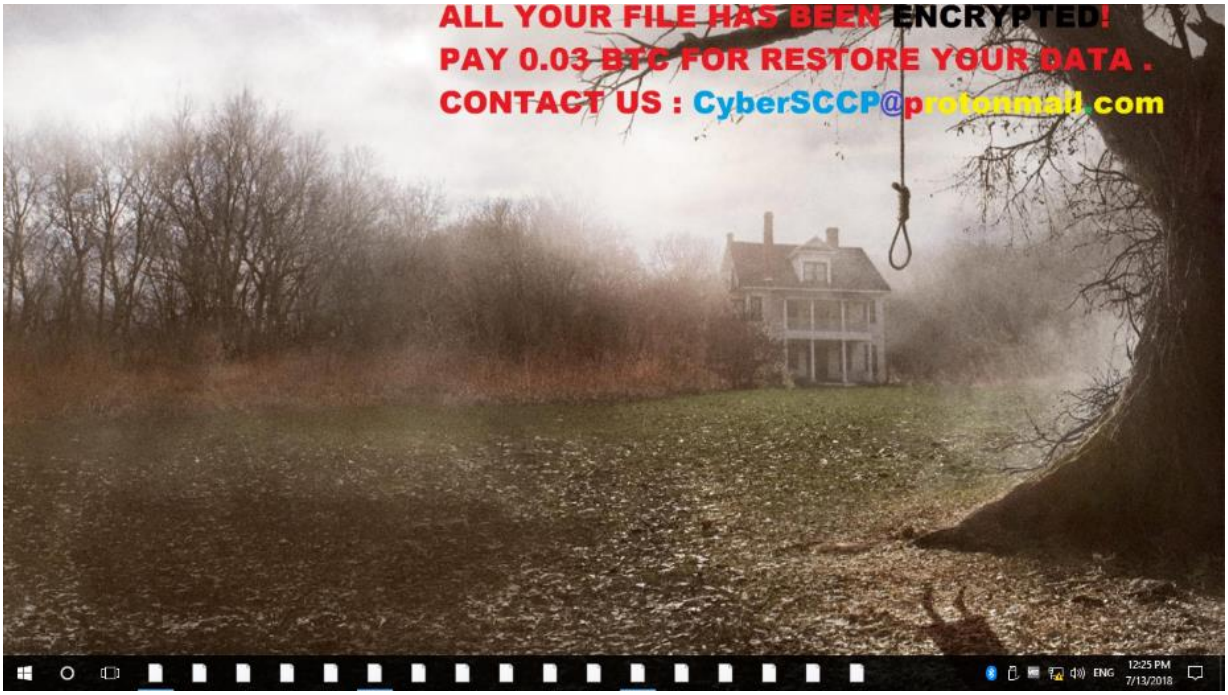
| نام بخش | آنتروپی | آدرس مجازی | اندازه مجازی | اندازه خام |
|---|---|---|---|---|
| **UPX٠** | ٠ | ٤٠٩٦ | ٤٩٩٧١٢ | ٠ |
| **UPX١** | ٧.٩٣ | ٥٠٣٨٠٨ | ٢٧٤٤٣٢ | ٢٧٠٨٤٨ |
| **.rsrc** | ٦.٦٣ | ٧٧٨٢٤٠ | ٤٩١٥٢ | ٤٥٥٦٨ |

## تحلیل پویا :

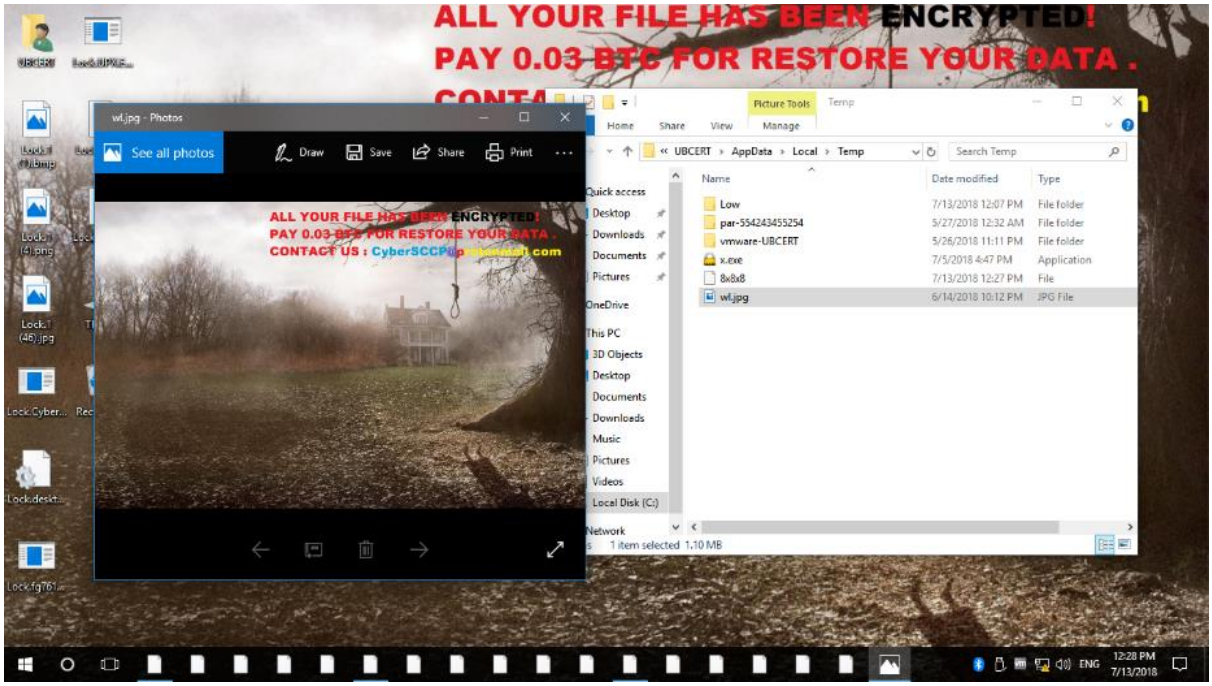
برای بررسی عمیق‌تر باج‌افزار CyberSCCP ، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره، تمام فایل های موجود در سیستم قربانی را رمزگذاری می‌کند و به ابتدای فایلهای رمزگذاری شده، پسوند Lock. اضافه می‌کند. تصویر زیر چند نمونه از فایل های رمزگذاری شده توسط باج‌افزار مذکور را نشان می دهد.




در ادامه، تصویر پس زمینه دسکتاپ توسط باج‌افزار تغییر پیدا می کند. باج‌افزار برای رمزگشایی فایلها، از قربانیان طلب ۰.۰۳ بیت کوین باج می‌کند. ضمناً مهاجم، ایمیلی به آدرس CyberSCCP@protonmail.com را نیز برای ارتباط‌گیری قربانی با وی، در تصویر پس زمینه قرار داده است.

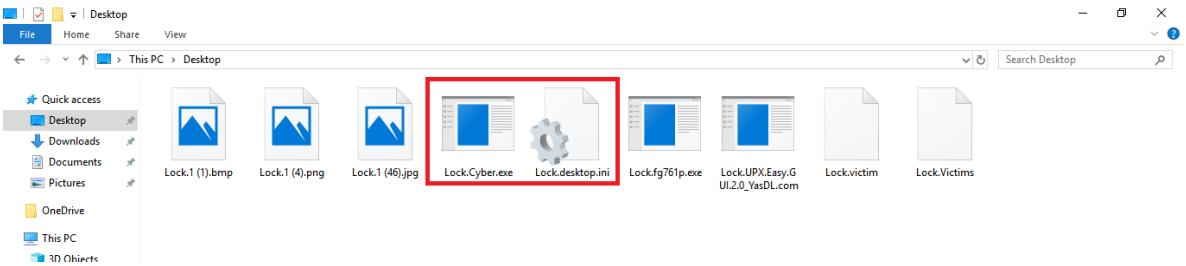



بررسی ها نشان می دهد که فایل اجرایی x.exe به همراه تصویر wl.jpg که توسط باج‌افزار در پوشه Temp ویندوز کپی می‌شوند مسئول ساخت این تصویر پس زمینه می باشند که مانع تغییر پس زمینه توسط کاربر می‌شود. این فایل اجرایی در فایل پوشه Temp ویندوز قرار گرفته است و در حالت عادی قابل حذف شدن نمی باشد.

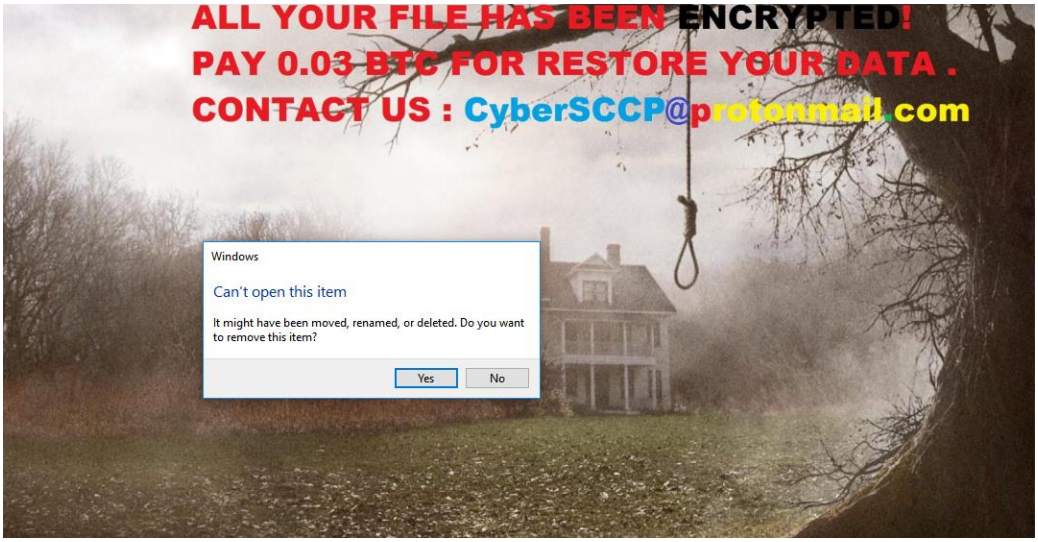


اما می توان فعالیت آن را از پنجره Task Manager پایان داد و اقدام به حذف آن نمود. که پس از اینکار قادر به تغییر تصویر پس زمینه خواهیم بود و پس از راه اندازی های مجدد سیستم دیگر شاهد تصویر باج‌خواهی نخواهیم بود.

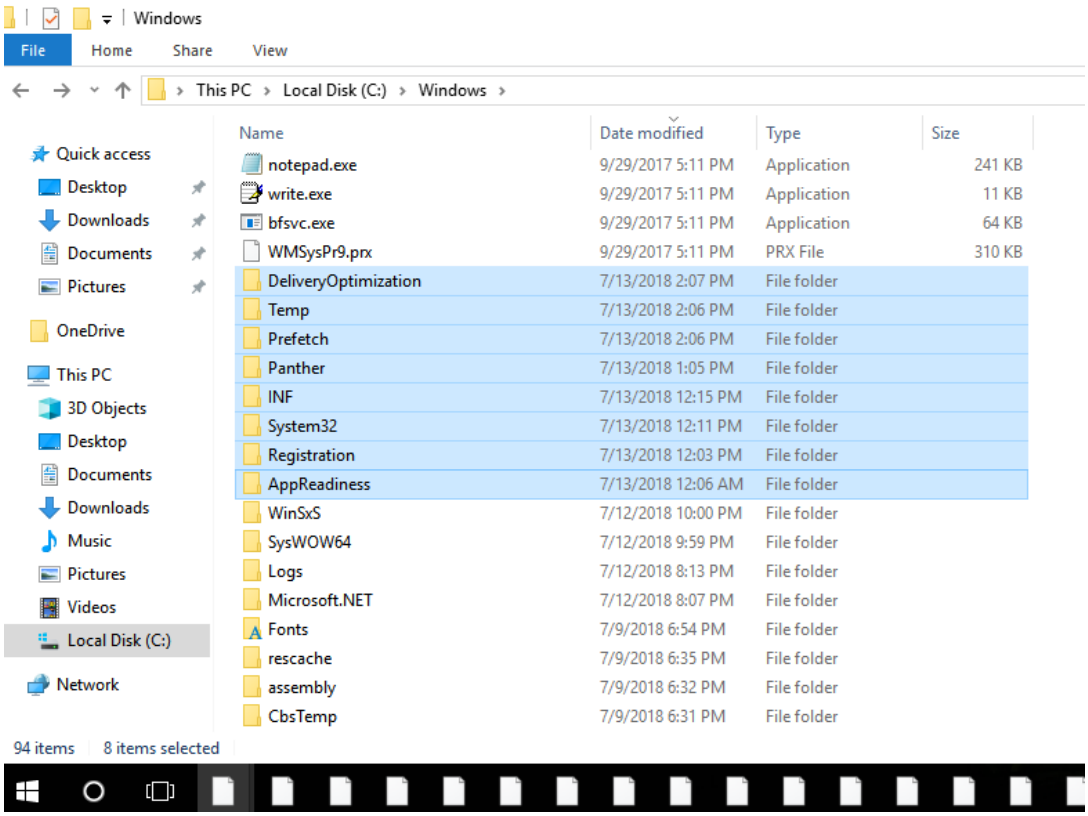
نتایج حاصل از بررسی ها نشان می دهد که فایل های موجود در Recycle Bin در اثر حمله باج‌افزار رمزگذاری نخواهند شد. پس از اتمام فرآیند رمزگذاری، دو فایل به نامهای Lock.Cyber.exe و Lock.desktop.iniروی دسکتاپ سیستم قربانی ایجاد خواهند شد.

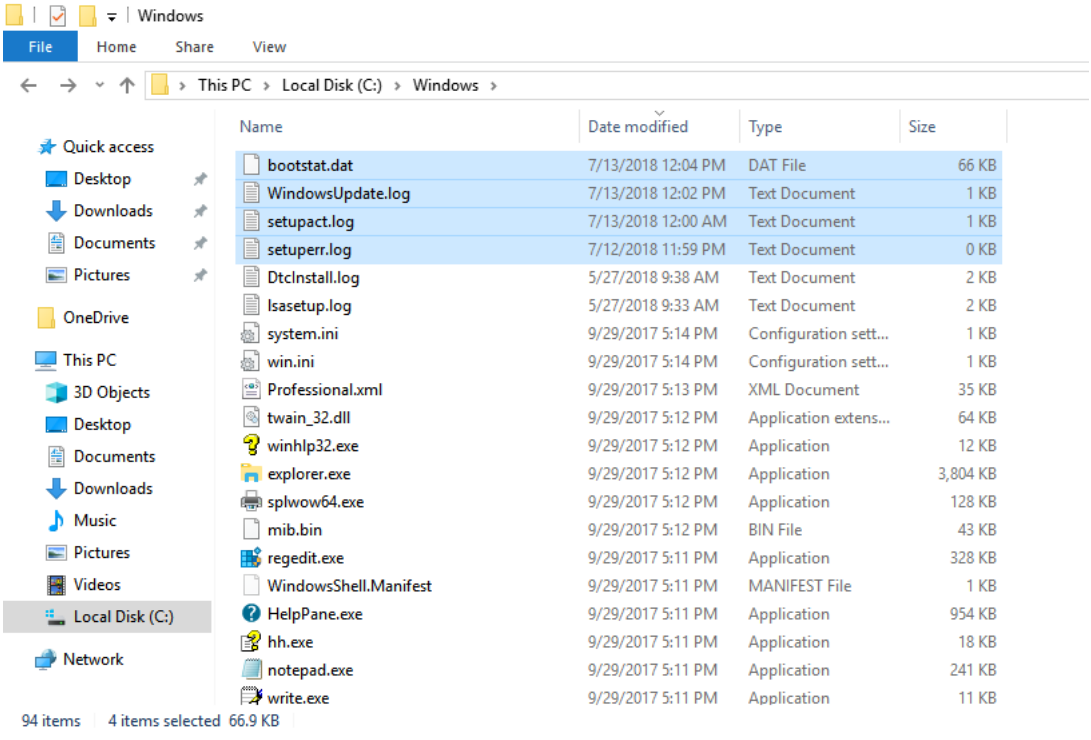


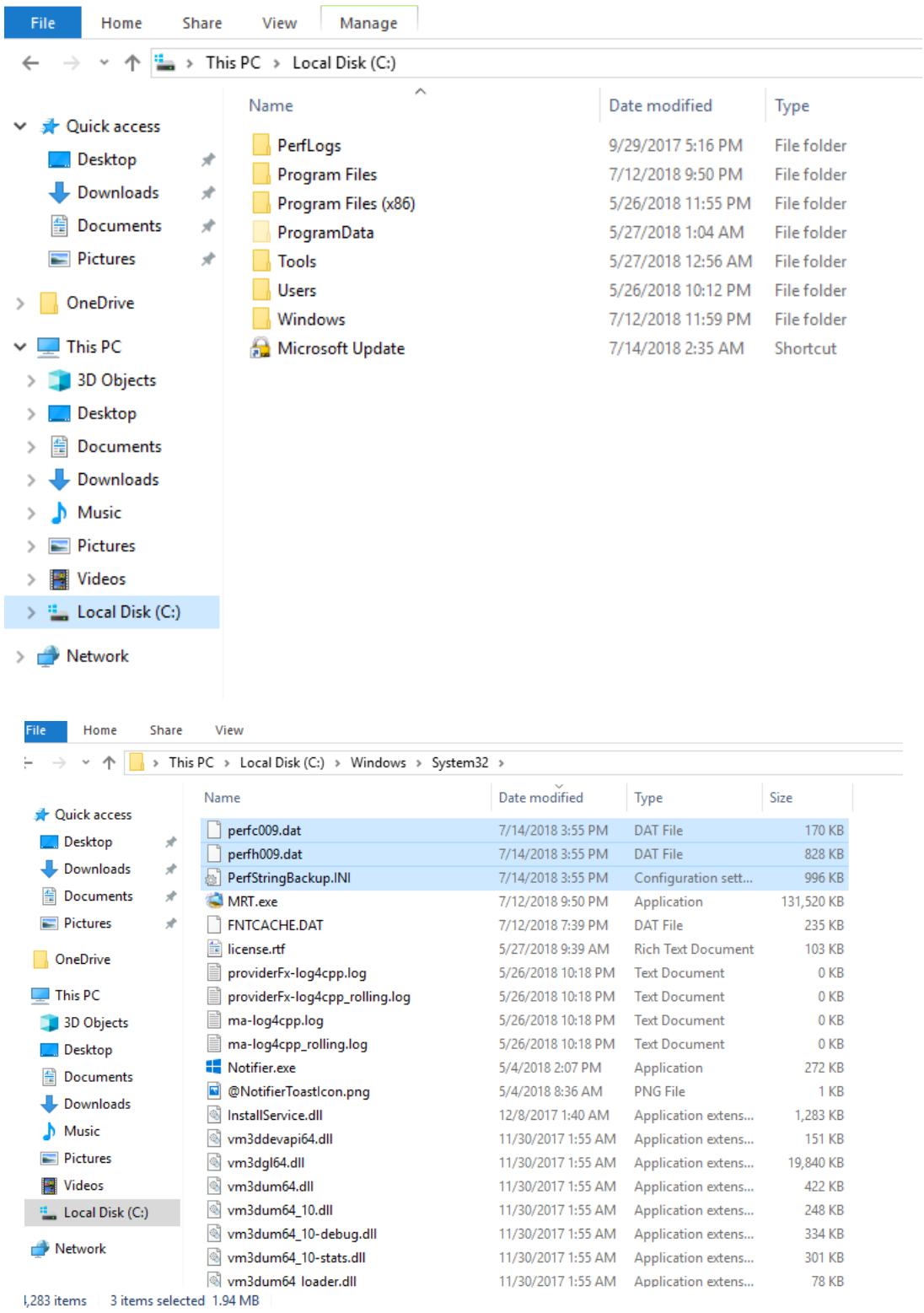

این باج‌افزار تنها فایل های موجود در دایرکتوری Users از درایو ویندوز که شامل Desktop ، Pictures و ... می شود را رمزگذاری می کند. همچنین میانبر نرم افزارهای موجود در نوار وظیفه نیز پس از حمله باج‌افزار قابل اجرا نخواهند بود.




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

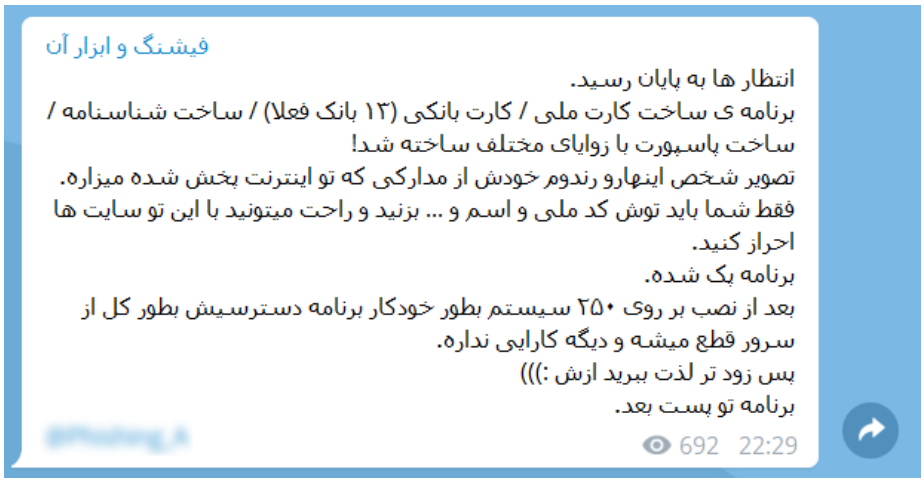

Windows
File Home Share View
This PC › Local Disk (C:) › Windows ›
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Name Date modified Type Size
notepad.exe 9/29/2017 5:11 PM Application 241 KB
write.exe 9/29/2017 5:11 PM Application 11 KB
bfsvc.exe 9/29/2017 5:11 PM Application 64 KB
WMSysPr9.prx 9/29/2017 5:11 PM PRX File 310 KB
DeliveryOptimization 7/13/2018 2:07 PM File folder
Temp 7/13/2018 2:06 PM File folder
Prefetch 7/13/2018 2:06 PM File folder
Panther 7/13/2018 1:05 PM File folder
INF 7/13/2018 12:15 PM File folder
System32 7/13/2018 12:11 PM File folder
Registration 7/13/2018 12:03 PM File folder
AppReadiness 7/13/2018 12:06 AM File folder
WinSxS 7/12/2018 10:00 PM File folder
SysWOW64 7/12/2018 9:59 PM File folder
Logs 7/12/2018 8:13 PM File folder
Microsoft.NET 7/12/2018 8:07 PM File folder
Fonts 7/9/2018 6:54 PM File folder
rescache 7/9/2018 6:35 PM File folder
assembly 7/9/2018 6:32 PM File folder
CbsTemp 7/9/2018 6:31 PM File folder
94 items 8 items selected

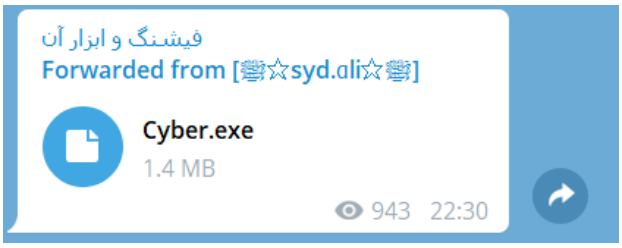

Windows
File Home Share View
This PC › Local Disk (C:) › Windows ›
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Name Date modified Type Size
bootstat.dat 7/13/2018 12:04 PM DAT File 66 KB
WindowsUpdate.log 7/13/2018 12:02 PM Text Document 1 KB
setupact.log 7/13/2018 12:00 AM Text Document 1 KB
setuperr.log 7/12/2018 11:59 PM Text Document 0 KB
DtcInstall.log 5/27/2018 9:38 AM Text Document 2 KB
lsasetup.log 5/27/2018 9:33 AM Text Document 2 KB
system.ini 9/29/2017 5:14 PM Configuration sett... 1 KB
win.ini 9/29/2017 5:14 PM Configuration sett... 1 KB
Professional.xml 9/29/2017 5:13 PM XML Document 35 KB
twain_32.dll 9/29/2017 5:12 PM Application extens... 64 KB
winhlp32.exe 9/29/2017 5:12 PM Application 12 KB
explorer.exe 9/29/2017 5:12 PM Application 3,804 KB
splwow64.exe 9/29/2017 5:12 PM Application 128 KB
mib.bin 9/29/2017 5:12 PM BIN File 43 KB
regedit.exe 9/29/2017 5:11 PM Application 328 KB
WindowsShell.Manifest 9/29/2017 5:11 PM MANIFEST File 1 KB
HelpPane.exe 9/29/2017 5:11 PM Application 954 KB
hh.exe 9/29/2017 5:11 PM Application 18 KB
notepad.exe 9/29/2017 5:11 PM Application 241 KB
write.exe 9/29/2017 5:11 PM Application 11 KB
94 items 4 items selected 66.9 KB




طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها وجود دارد. ضمناً همانطور که اشاره شد این باج‌افزار با نام Cyber.exe در پوشش اپلیکیشنی برای جعل مدارک هویتی از

جمله کارت ملی و شناسنامه در حال گسترش در بین کاربران تلگرام فارسی زبان است. بنابراین به کاربران در فضای مجازی توصیه می گردد که از دریافت و اجرای فایل‌های اجرایی از منابع ناشناخته پرهیز نمایند.




## تحلیل ایستا :

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

فایل اجرایی باج‌افزار حاوی انتروپی غیر معمولی بود که مشخص گردید برای جلوگیری از تحلیل، با استفاده از UPX پک شده است.

```
UPX١ with unusual entropies ٧.٩٢٩٢١١٧٤٠٨٥
"Cyber.exe.bin.exe.bin" has a section named "UPX٠"
"Cyber.exe.bin.exe.bin" has a section named "UPX١"
```

پس از آنپک نمودن فایل اجرایی باج‌افزار، موارد زیر از آن استخراج گردید

قطعه کد زیر مربوط به تنظیم زمان‌سنج می باشد :

```
; ---------------------------------------------------------------------------

loc_4011DB:                             ; CODE XREF: sub_401100+AF↑j
                                        ; DATA XREF: .text:off_40122C↓o
                push    0               ; jumptable 004011AF case 1
                push    2EEh            ; uElapse
                push    1               ; nIDEvent
                push    ebx             ; hWnd
                call    ds:SetTimer
                push    offset String   ; "TaskbarCreated"
                call    ds:RegisterWindowMessageW
                cmp     dword_4A8710, 0
                mov     dword_4A95E8, eax
                jnz     short loc_401193
                call    ds:CreatePopupMenu
                pop     esi
                mov     dword_4A8710, eax
                xor     eax, eax
                pop     ebx
                mov     esp, ebp
                pop     ebp
                retn    0Ch
; ---------------------------------------------------------------------------
```

تابع IsDebuggerPresent که از توابع کتابخانه Kernel۳۲ می‌باشد برای جلوگیری از اجرای باج‌افزار در محیط‌های دیباگر استفاده میشود تا در هنگام تحلیل با تولید خطا در دیباگرها مانع فعالیت گردد.

```
                                        ; CODE XREF: sub_401460+45↑p
                                        ; sub_4033C0+A7↑p ...
; BOOL __stdcall SetCurrentDirectoryW(LPCWSTR lpPathName)
                extrn SetCurrentDirectoryW:dword
                                        ; CODE XREF: sub_4033C0+10C↑p
                                        ; sub_4033C0+395↑p ...
; BOOL __stdcall IsDebuggerPresent()
                extrn IsDebuggerPresent:dword
                                        ; CODE XREF: sub_40D590+26↑p
                                        ; sub_417DAA+EA↑p ...
; DWORD __stdcall GetCurrentDirectoryW(DWORD nBufferLength, LPWSTR lpBuffer)
                extrn GetCurrentDirectoryW:dword
                                        ; CODE XREF: sub_4033C0+91↑p
                                        ; sub_40D590+1A↑p ...
```

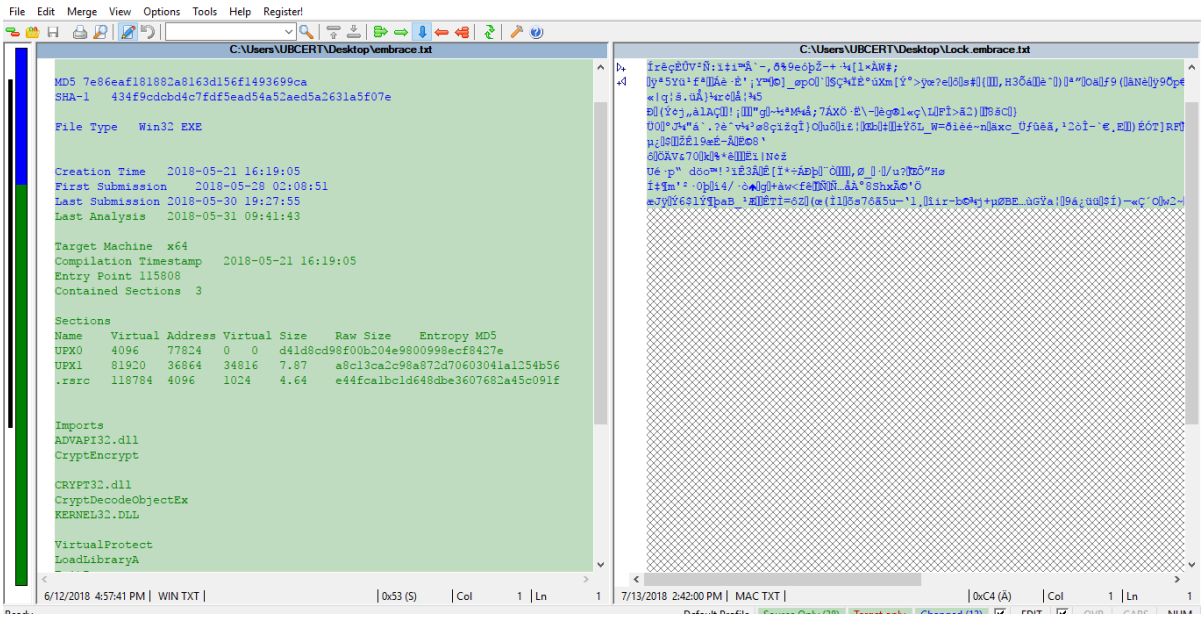
در صورتی‌که فایل، هنگام اجرا تشخیص دهد که از محیط دیباگر استفاده شده است، با تولید خطا و قرار دادن مقدار در تابع SetUnhandledExceptionFilter از ادامه کار جلوگیری می‌کند. از این روش در چندین محل استفاده شده‌است.

ابتدا تابع check_debugger_Present فراخوانی شده و مقدار آن بررسی می‌گردد. سپس با استفاده از تابع IsDebuggerPresent() اقدام به بررسی محیط دیباگر می‌کند. اگر نتیجه بدست‌آمده، مثبت باشد با استفاده از توابع SetUnhandleException باعث ایجاد خطا شده و از ادامه فعالیت جلوگیری می‌کنند.

```
push    ebx
push    esi
push    edi
mov     edi, eax
lea     eax, [ebp+Buffer]
push    eax             ; lpBuffer
push    104h            ; nBufferLength
call    ds:GetCurrentDirectoryW
push    edi
call    sub_401F20
call    ds:IsDebuggerPresent
test    eax, eax
jnz     loc_42E1BB
mov     eax, dword_4A7F54
test    eax, eax
jz      loc_42E1D4
mov     [ebp+var_1], 0
mov     esi, offset dword_4A90E8
cmp     eax, 1
jz      loc_42E1EA
push    offset dword_4A7F54

mov     ecx, [ebp+arg_8]
mov     [ebp+var_31C], ecx
mov     [ebp+var_314], eax
call    ds:IsDebuggerPresent
push    0               ; lpTopLevelExceptionFilter
mov     edi, eax
call    ds:SetUnhandledExceptionFilter
lea     eax, [ebp+ExceptionInfo]
push    eax             ; ExceptionInfo
call    ds:UnhandledExceptionFilter
test    eax, eax
jnz     short loc_417EC5
test    edi, edi
jnz     short loc_417EC5
cmp     ebx, 0FFFFFFFFh
jz      short loc_417EC5
push    ebx
call    sub_41FE19
```

با مقایسه نمونه فایل، قبل و بعد از رمزگذاری مشاهده کردیم که بیش از دوبرابر محتوای اولیه ی فایل حذف شده است.



| ADVAPI۳۲.dll | COMCTL۳۲.dll | COMDLG۳۲.dll | GDI۳۲.dll | KERNEL۳۲.DLL |
|---|---|---|---|---|
| GetAce | ImageList_Remove | GetSaveFileNameW | LineTo | VirtualFree<br>ExitProcess<br>VirtualProtect<br>LoadLibraryA<br>VirtualAlloc<br>GetProcAddress |

کتابخانه‌های مورد استفاده توسط باج‌افزار CyberSCCP

| MPR.dll | OLEAUT۳۲.dll | PSAPI.DLL | SHELL۳۲.dll | USER۳۲.dll |
|---|---|---|---|---|
| WNetGetConnectionW | VariantInit | EnumProcesses | DragFinish | GetDC |

## تغییرات رجیستری:

کلیدهای رجیستری اضافه شده:

*HKLM\SOFTWARE\Microsoft\Phone\ShellUI\WindowSizing\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy!App*
*HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances*
*HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\c2f2cff2-0fdd-49d2-8aaf-f9ceb4d57e1e*
*HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances*
*HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\c2f2cff2-0fdd-49d2-8aaf-f9ceb4d57e1e*
*HKLM\SOFTWARE\WOW6432Node\Microsoft\Phone\ShellUI\WindowSizing\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy!App*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\IdentityCRL\Immersive\production\Token\{C89E2069-AF13-46DB-9E39-216131494B87}*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\UserData\UninstallTimes*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\ApplicationFrame\WindowSizing\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy!App*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000050218*

HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000050240
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000050332
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000602A0
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000070312
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000070326
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000902B6
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000C00E0
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000018024A
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001D024A
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{218E3D0E-350A-42FD-BDF3-CF1F240B341E}
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER\SOFTWARE
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER\SOFTWARE\Microsoft
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Speech_OneCore
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw

HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZ5n1h2txyewy
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\SOFTWARE\Microsoft\Speech_OneCore\Recognizers
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\ShellRefresh
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\7
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER\SOFTWARE
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER\SOFTWARE\Microsoft
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Speech_OneCore
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Speech_OneCore\Recognizers
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\ShellRefresh
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\7
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}

مقادیر اضافه شده:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\41C64E6DA3B570E5

HKLM\SYSTEM\ControlSet001\Services\bam\UserSettings\S-1-5-21-2421227731-3904311691-1636309405-1000\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{EF21BD7A-5DDA-4858-94F7-7506036A9293}
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{E8084A0B-FB6D-403C-949C-B193B0B1DF35}
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{D7E340F5-5553-4AAA-AB91-ABABC7EFBB83}
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{F56A628A-2FDE-486E-94B9-3DBB912DB9BE}
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{637C5DAC-13BA-4D19-AC70-D8F0489D8C6D}
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{79027F3D-093E-4DB2-A64B-F4990CC1E094}
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{DAE228D2-C92A-4D47-943F-8FA26D5D9C80}
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{4715883D-E9A3-4D1D-96BD-4790CD662A27}
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{54975262-9901-4C40-96CE-A7418860E05D}
HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-2421227731-3904311691-1636309405-1000\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{EF21BD7A-5DDA-4858-94F7-7506036A9293}
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{E8084A0B-FB6D-403C-949C-B193B0B1DF35}
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{D7E340F5-5553-4AAA-AB91-ABABC7EFBB83}
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{F56A628A-2FDE-486E-94B9-3DBB912DB9BE}
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{637C5DAC-13BA-4D19-AC70-D8F0489D8C6D}
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{79027F3D-093E-4DB2-A64B-F4990CC1E094}
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{DAE228D2-C92A-4D47-943F-8FA26D5D9C80}
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{4715883D-E9A3-4D1D-96BD-4790CD662A27}
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules\{54975262-9901-4C40-96CE-A7418860E05D}
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\IdentityCRL\Immersive\production\Token\{C89E2069-AF13-46DB-9E39-216131494B87}\DeviceTicket
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\IdentityCRL\Immersive\production\Token\{C89E2069-AF13-46DB-9E39-216131494B87}\DeviceId

HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\IdentityCRL\Immersive\production\Token\{C89E2069-AF13-46DB-9E39-216131494B87}\ApplicationFlags
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol\50
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol\0
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol\11
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol\1
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol\6
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol\9
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol\33
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol\12
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol\14
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\HighWaterMarks\C:_Users_UBCERT_AppData_Local_Comms_UnistoreDB_store.vol\16
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\UserData\UninstallTimes\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\ApplicationFrame\WindowSizing\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy!App\PreferredLaunchViewSize: 84 03 00 00 84 03 00 00
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\ApplicationFrame\WindowSizing\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy!App\PreferredLaunchWindowingMode: 0x00000001
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Nccerc.PukNcc_pj5a1u2gklrjl!Ncc
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\HOPREG\Qrfxgbc\Plore.rkr
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\PlmVolatile\TerminationType\Microsoft.Windows.Apprep.ChxApp_1000.16299.15.0_neutral_neutral_cw5n1h2txyewy+App: 0x00000005
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000050218\VirtualDesktop
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000050240\VirtualDesktop

HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000050332\VirtualDesktop
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000602A0\VirtualDesktop
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000070312\VirtualDesktop
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000070326\VirtualDesktop
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000902B6\VirtualDesktop
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000C00E0\VirtualDesktop
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000018024A\VirtualDesktop
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001D024A\VirtualDesktop
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{218E3D0E-350A-42FD-BDF3-CF1F240B341E}\LastAccessedTime
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{218E3D0E-350A-42FD-BDF3-CF1F240B341E}\AppId: "C:\Users\UBCERT\Desktop\Cyber.exe"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{218E3D0E-350A-42FD-BDF3-CF1F240B341E}\LaunchCount
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{218E3D0E-350A-42FD-BDF3-CF1F240B341E}\AppPath
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\UBCERT\Desktop\Cyber.exe
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\MuiCache\9\52C64B7E\@%SystemRoot%\System32\urlmon.dll,-4200: "Open File - Security Warning"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\MuiCache\9\52C64B7E\@C:\Program Files\Common Files\system\wab32res.dll,-10100: "Contacts"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Speech_OneCore\Recognizers\DefaultTokenId:

*"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Speech_OneCore\Recognizers\Tokens\MS-1033-110-WINMO-DNN"*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\WasEverActivated*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\7*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\7\NodeSlot*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\7\MRUListEx*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\KnownFolderDerivedFolderType*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\SniffedFolderType: "Generic"*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Rev*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\FFlags*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Vid*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Mode*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\LogicalViewMode*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\IconSize*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Sort*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\ColInfo*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupView: 0x00000000*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:FMTID: "{00000000-0000-0000-0000-000000000000}"*

HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:PID: 0x00000000
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByDirection: 0x00000001
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\MuiCache\9\52C64B7E\@%SystemRoot%\System32\urlmon.dll,-4200: "Open File - Security Warning"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\MuiCache\9\52C64B7E\@C:\Program Files\Common Files\system\wab32res.dll,-10100: "Contacts"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\SOFTWARE\Microsoft\Speech_OneCore\Isolated\jWXZvMzcRxToSdOzNgXV_L3ZSrLDNbZuY5NZNWCCUd8\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Speech_OneCore\Recognizers\DefaultTokenId: "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Speech_OneCore\Recognizers\Tokens\MS-1033-110-WINMO-DNN"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\WasEverActivated: 0x00000001
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\7
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\7\NodeSlot
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\7\MRUListEx
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\KnownFolderDerivedFolderType
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\SniffedFolderType: "Generic"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Rev
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\FFlags
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Vid
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Mode
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\LogicalViewMode
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\IconSize

HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Sort
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\ColInfo
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupView
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:FMTID
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByDirection

کلیدهای رجیستری تغییر یافته:

HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\AllUsers\{373D6429-614B-4763-BAD6-1601AFF8CE31}\From
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\AllUsers\{7c35503F-7D09-4FA7-B6E4-7FDF152EFC80}\From
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-2421227731-3904311691-1636309405-1000\{524DE373-9FAB-4171-8D5F-36CD5D03BED0}\From
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-2421227731-3904311691-1636309405-1000\{EFCEC7FF-334D-4A76-898E-84C97C9083EF}\From
HKLM\SOFTWARE\Microsoft\IdentityCRL\ClockData\ClockTimeSeconds
HKLM\SOFTWARE\Microsoft\IdentityCRL\ClockData\TickCount
HKLM\SOFTWARE\Microsoft\SMB1Uninstall\SMB1ClientCounter
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateChange\PackageVersion
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepositoryStatus\DeploymentDatabaseStatisticsLastUpdated
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepositoryStatus\MachineDatabaseStatisticsLastUpdated
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\LastSuccessfulUploadTime
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\SequenceNumber
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418B1D29A3BC0C75
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418B1D29A3BC1475

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{545B5BF9-3D17-4EC0-8F78-A08C9F56FBCF}\DynamicInfo
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{5C020530-D866-421B-B15E-7EB9C7FA4D3B}\DynamicInfo
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F322AEB8-9975-47C8-879F-0E32A5EAF6A5}\DynamicInfo
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F4D8C2F5-8D0F-46C5-B6A9-F766A9E4B26E}\DynamicInfo
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileService\References\S-1-5-21-2421227731-3904311691-1636309405-1000\RefCount
HKLM\SOFTWARE\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{F9FE1B7C-7CDC-4795-BB6F-93E003F9C809}
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{F9FE1B7C-7CDC-4795-BB6F-93E003F9C809}
HKLM\SYSTEM\ControlSet001\Control\GraphicsDrivers\Configuration\NOEDID_15AD_0405_00000000_000F0000_0^20ED182961F2CFDB3A2D28C95A99744F\Timestamp
HKLM\SYSTEM\ControlSet001\Services\bam\UserSettings\S-1-5-21-2421227731-3904311691-1636309405-1000\SequenceNumber
HKLM\SYSTEM\ControlSet001\Services\bam\UserSettings\S-1-5-21-2421227731-3904311691-1636309405-1000\Microsoft.Windows.Cortana_cw5n1h2txyewy
HKLM\SYSTEM\ControlSet001\Services\bam\UserSettings\S-1-5-21-2421227731-3904311691-1636309405-1000\\Device\HarddiskVolume3\Windows\System32\dllhost.exe
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{223f6222-f164-4a3b-a39b-e60d40333b3e}\LeaseObtainedTime
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{223f6222-f164-4a3b-a39b-e60d40333b3e}\T1
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{223f6222-f164-4a3b-a39b-e60d40333b3e}\T2
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{223f6222-f164-4a3b-a39b-e60d40333b3e}\LeaseTerminatesTime
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{223f6222-f164-4a3b-a39b-e60d40333b3e}\DhcpInterfaceOptions
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeEstimated
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeHigh
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeLow
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeConfidence
HKLM\SYSTEM\CurrentControlSet\Control\GraphicsDrivers\Configuration\NOEDID_15AD_0405_00000000_000F0000_0^20ED182961F2CFDB3A2D28C95A99744F\Timestamp
HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-2421227731-3904311691-1636309405-1000\SequenceNumber
HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-2421227731-3904311691-1636309405-1000\Microsoft.Windows.Cortana_cw5n1h2txyewy
HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-2421227731-3904311691-1636309405-1000\\Device\HarddiskVolume3\Windows\System32\dllhost.exe
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch\Epoch

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{223f6222-f164-4a3b-a39b-e60d40333b3e}\LeaseObtainedTime
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{223f6222-f164-4a3b-a39b-e60d40333b3e}\T1
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{223f6222-f164-4a3b-a39b-e60d40333b3e}\T2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{223f6222-f164-4a3b-a39b-e60d40333b3e}\LeaseTerminatesTime
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{223f6222-f164-4a3b-a39b-e60d40333b3e}\DhcpInterfaceOptions
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeEstimated
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeHigh
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeLow
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeConfidence
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Control Panel\Desktop\WallPaper
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Control Panel\Desktop\TranscodedImageCache
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\AuthCookies\Live\Default\DIDC\Data
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\IdentityCRL\Immersive\production\Property\00180002DB052C68
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Poom\AggregateCacheGeneration
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Poom\calendarColorIndex
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Poom\Indexing\TrackedStores
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Poom\Indexing\RunCookie
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\LastStoreGroupingId
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Unified Store\LastStoreId
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\$$windows.data.taskflow.shellactivities\Current\Data
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\$$windows.data.unifiedtile.localstartvolatiletilepropertiesmap\Current\Data
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Rkcybere

HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Pbegnan_pj5a1u2gklrjl!PbegnanHV
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Gbbyf\Ertfubg-1.9.0\Ertfubg-k64-Havpbqr.rkr
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath0: "C:\Windows\web\wallpaper\Windows\img0.jpg"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath0: "C:\Users\UBCERT\AppData\Local\Temp\wl.jpg"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath1: "c:\windows\web\wallpaper\theme1\img1.jpg"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath1: "C:\Windows\web\wallpaper\Windows\img0.jpg"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath2: "c:\windows\web\wallpaper\theme1\img13.jpg"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath2: "c:\windows\web\wallpaper\theme1\img1.jpg"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath3: "c:\windows\web\wallpaper\theme1\img2.jpg"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath3: "c:\windows\web\wallpaper\theme1\img13.jpg"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath4: "c:\windows\web\wallpaper\theme1\img3.jpg"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath4: "c:\windows\web\wallpaper\theme1\img2.jpg"
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\CurrentVersion\Search\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppsConstraintIndex\LatestConstraintIndexFolder
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Microsoft\Windows\Shell\Bags\1\Desktop\IconLayouts
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\Internet Explorer\DOMStorage\bing.com\Total
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\Internet Explorer\DOMStorage\Total\

HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\Internet Explorer\DOMStorage\www.bing.com\
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Families\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Microsoft.AAD.BrokerPlugin_1000.16299.15.0_neutral_neutral_cw5n1h2txyewy\InstallTime
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\PSR\WnfStateName
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\NodeSlots
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\MRUListEx
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WFlags
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\ShowCmd
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1162x591x96(1).top
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1162x591x96(1).bottom
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\Internet Explorer\DOMStorage\bing.com\Total
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\Internet Explorer\DOMStorage\Total
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.cortana_cw5n1h2txyewy\Internet Explorer\DOMStorage\www.bing.com
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Families\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Microsoft.AAD.BrokerPlugin_1000.16299.15.0_neutral_neutral_cw5n1h2txyewy\InstallTime
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\PSR\WnfStateName
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\NodeSlots
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx
HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\MRUListEx

*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WFlags*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\ShowCmd*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1162x591x96(1).top*
*HKU\S-1-5-21-2421227731-3904311691-1636309405-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1162x591x96(1).bottom*

## تحلیل ترافیک شبکه :

پس از اجرای موفقیت آمیز باج‌افزار در محیط آزمایشگاهی، هیچ گونه ترافیک شبکه اعم از درخواست DNS یا HTTP مشاهده نگردید.

## ابزار رمزگشایی :

در حال حاضر وجود ندارد.

## شناسایی :

در حال حاضر تعداد ٤٧ مورد از ٦٨ آنتی‌ویروس معتبر دنیا قادر به تشخیص آلودگی این باج‌افزار در سامانه VirusTotal شده‌اند.

| | | | |
|---|---|---|---|
| Ad-Aware | AIT:Trojan.Nymeria.200 | AegisLab | Ait.Troj.Nymeria!c |
| AhnLab-V3 | Trojan/Win32.Ransom.C1627388 | ALYac | Trojan.Ransom.HiddenTear |
| Arcabit | AIT:Trojan.Nymeria.200 | Avast | Win32:Malware-gen |
| AVG | Win32:Malware-gen | Avira | DR/AutoIt.Gen |
| Baidu | Win32.Trojan.WisdomEyes.16070401.... | BitDefender | AIT:Trojan.Nymeria.200 |
| Bkav | W32.eHeur.Malware14 | CAT-QuickHeal | Trojan.IGENERIC |
| ClamAV | Win.Trojan.Autoit-73 | CrowdStrike Falcon | malicious_confidence_90% (W) |
| Cybereason | malicious.9cd555 | Cyren | W32/Trojan.LHOR-8984 |
| DrWeb | Trojan.MulDrop8.26395 | Emsisoft | AIT:Trojan.Nymeria.200 (B) |
| Endgame | malicious (moderate confidence) | eScan | AIT:Trojan.Nymeria.200 |
| ESET-NOD32 | Win32/Packed.Autoit.H suspicious | Fortinet | Riskware/Application |
| GData | AIT:Trojan.Nymeria.200 (2x) | K7AntiVirus | Trojan ( 004f28dd1 ) |
| K7GW | Trojan ( 004f28dd1 ) | Kaspersky | Trojan.Win32.Fakeoff.dik |
| Malwarebytes | Ransom.Microcop | MAX | malware (ai score=99) |
| McAfee | Artemis!3D188FF9CD55 | McAfee-GW-Edition | BehavesLike.Win32.Injector.tc |
| Microsoft | Ransom:Win32/Genasom | NANO-Antivirus | Trojan.Win32.AutoIt.fefeyc |
| Palo Alto Networks | generic.ml | Qihoo-360 | Win32/Trojan.5b4 |
| Rising | Ransom.Genasom!8.293 (CLOUD) | SentinelOne | static engine - malicious |
| Sophos AV | Mal/Generic-S | Sophos ML | heuristic |
| Symantec | Trojan.Gen.2 | Tencent | Win32.Trojan.Fakeoff.Lkea |
| TrendMicro | TROJ_FRS.VSN0FF18 | TrendMicro-HouseCall | TROJ_FRS.VSN0FF18 |
| VBA32 | Trojan.Autoit.F | ViRobot | Trojan.Win32.Z.Autoit.1493645 |
| Webroot | W32.Rogue.Gen | Zillya | Trojan.Fakeoff.Win32.181 |
| ZoneAlarm | Trojan.Win32.Fakeoff.dik | | |