بسمه تعالی

راهنمای امداد برای رایانه‌های آلوده شده به باج‌افزار wannacry

در سازمان‌ها و شبکه‌های سازمانی

۱- ارتباط رایانه آلوده با شبکه را به طور کامل و فیزیکی قطع نمایید.(تمامی ارتباطات اعم از شبکه‌های کابلی- بی سیم- بلوتوث- 4G-3G و ...)

۲- فرآیندهای مرتبط با بررسی انتشار آلودگی در سایر کامپیوترهای شبکه را مطابق پیوست شماره یک انجام دهید. برای شروع سراغ کامپیوترهایی بروید که در زیرشبکه 24/ کامپیوتر آلوده قرار دارند. به بیان ساده‌تر، کامپیوترهایی که تنها آخرین عدد در آدرس آی پی آنها با کامپیوتر قربانی متفاوت است.

۳- فرآیندهای مربوط به از بین بردن احتمال آلودگی در سایر کامپیوترهای شبکه را مطابق پیوست شماره دو انجام دهید.

٤- به طور همزمان با فرآیندهای ۲و۳ و بدون اتلاف وقت، بدون RESET کردن سیستم، بدون اجرای هرگونه برنامه اضافی اعم از آنتی ویروس یا File Recovery و مخصوصا بدون بستن برنامه مهاجم نسبت به اجرا کردن بازیابی براساس دستورالعمل های پیوست شماره سوم اقدام شود. نکته کلیدی آن است که در حال حاضر ابزارهایی که برای بازیابی اطلاعات در دست است فقط در صورتی می‌توانند به موفقیت برسند که بتوانند به حافظه مورد استفاده فرآیند رمزگذاری باج افزار دسترسی پیدا کنند و با جستجوی اعداد اول در این فضا، کلید بازیابی را بسازند. اجرای هر نوع برنامه اضافی، بستن فرآیند مهاجم، گذشت زمان یا Reset کردن سیستم، این فرآیند را ناممکن خواهد کرد. همچنین در آزمایش‌های انجام گرفته مشخص شده است که تنها درصری از سیستم‌های قربانی واجد این شرایط، نجات می‌یابند.

۵- در صورت موفقیت یا عدم موفقیت در بازیابی اطلاعات، لازم است تا نسبت به تهیه نسخه پشتیبان از تمامی فایل‌های بازیابی شده و نشده بر روی حافظه جانبی قابل حمل (هارد اکسترنال ، فلش و ...). اقدام شود. همچنین ضروری است که پس از کپی کردن اطلاعات، با اتصال حافظه جانبی به

یک یارانه که در آن آنتی ویروس وسیستم عامل به روزرسانی شده باشد به بررسی وجود فایل‌های حاوی نسخه اجرایی بدافزار، حذف آنها در صورت وجود پرداخت.

٦- در صورت عدم موفقیت در بازیابی اطلاعات، لازم است تا از فایل‌ها و اطلاعات رمز گذاری شده کپی تهیه شود و همچنین از حافظه اصلی کامپیوتر رونوشت تهیه شود تا در صورتی که در آینده روش های بازیابی به بلوغ کافی برای رمزگشایی اطلاعات برسند، بتوان نسبت به بازیابی اطلاعات اقدام نمود. به این منظور لازم است تا نسبت بهDump کردن حافظه به شرح منتشر شده در وب‌سایت مایکروسافت (متناسب با نسخه ویندوز)

https://support.microsoft.com/en-us/help/254649/overview-of-memory-dump-file-options-for-windows

https://support.microsoft.com/en-us/help/969028/how-to-generate-a-kernel-or-a-complete-memory-dump-file-in-windows-server-2008-and-windows-server-2008-r2

https://social.technet.microsoft.com/wiki/contents/articles/17222.complete-memory-dump-windows-server-2012.aspx

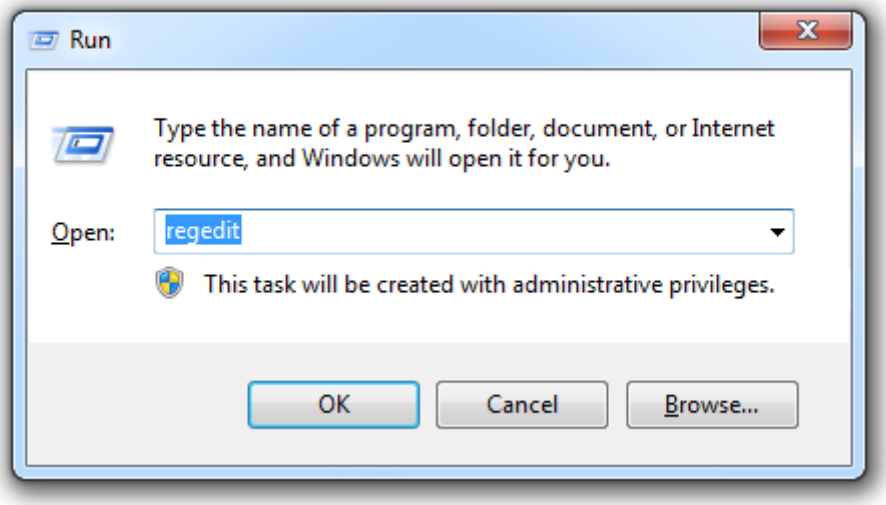
اقدام نمود و پس از آن با تکیه بر همین راهنمایی ها، فایل به دست آمده را نیز به همراه فایل‌های رمزگذاری شده برای اقدامات آتی نگهداری نمود.

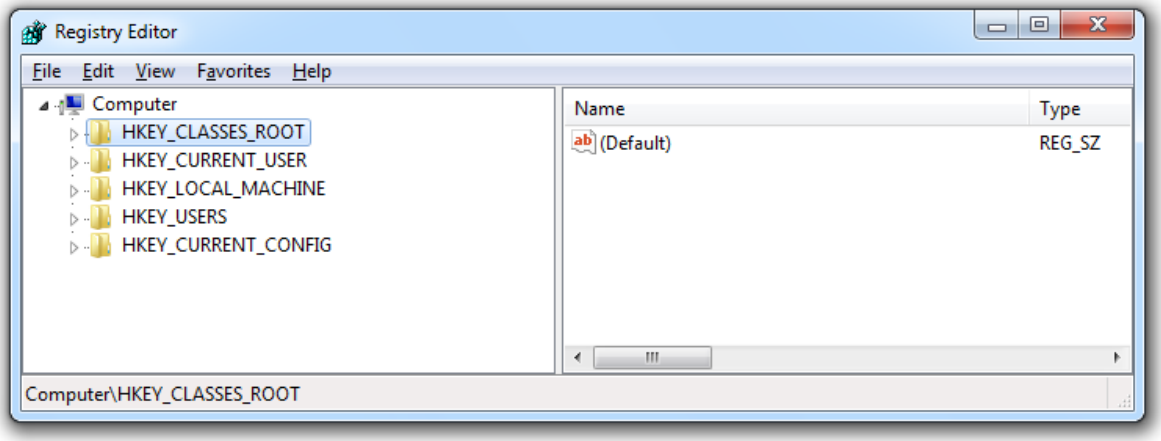
پیوست شماره ۱

وجود کلیدهای زیر را در رجیستری ویندوز بررسی نمایید.

توضیح اینکه برای ورود به رجیستری در محیط Run کافی است که بنویسید Regedit.

علاوه بر انتخاب از نوار منو استارت، محیط Run را می‌توان از با فشردن کلید ویندوز به همراه R نیز اجرا کرد.





برای جستجو کردن به دنبال هر یک از کلیدها، مسیر معرفی شده را در داخل برنامه طی کنید. یا از منو Edit گزینه Find اقدام نمایید.

فهرست کلیدهای رجیستری که باج افزار در سیستم‌های قربانی ایجاد می‌نماید از این قرار است:

HKLM\SOFTWARE\WanaCrypt0r
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<random>: “”< پوشه محتوی فایل اجرایی باج افزار>\tasksche.exe””
HKLM\SOFTWARE\WanaCrypt0r\wd: “<پوشه محتوی فایل اجرایی باج افزار>”
HKU\S-1-5-21-677641349-3533616285-3951951702-1000\Control Panel\Desktop\Wallpaper: “%APPDATA%\Microsoft\Windows\Themes\TranscodedWallpaper.jpg”
HKU\S-1-5-21-677641349-3533616285-3951951702-1000\Control Panel\Desktop\Wallpaper: “< پوشه محتوی فایل اجرایی باج افزار>\@WanaDecryptor@.bmp”

در صورت آلوده شدن به این باج افزار، فایلهایی به شرح زیر در سیستم ایجاد می‌شود. جستجو برای این فایل‌ها نیز به منظور ایجاد اطمینان از سلامت سیستم‌ها، ضروری است.

@Please_Read_Me@.txt – در تمام پوشه هایی که فایل های آنها رمز گذاری شده قرار می گیرد

@WanaDecryptor@.exe.lnk – در تمام پوشه هایی که فایل های آنها رمز گذاری شده قرار می گیرد

%DESKTOP%\@WanaDecryptor@.bmp
%DESKTOP%\@WanaDecryptor@.exe
%APPDATA%\tor\cached-certs
%APPDATA%\tor\cached-microdesc-consensus
%APPDATA%\tor\cached-microdescs.new
%APPDATA%\tor\lock
%APPDATA%\tor\state
<پوشه محتوی فایل اجرایی باج افزار>\00000000.eky
<پوشه محتوی فایل اجرایی باج افزار>\00000000.pky
<پوشه محتوی فایل اجرایی باج افزار>\00000000.res
<پوشه محتوی فایل اجرایی باج افزار>\@WanaDecryptor@.bmp
<پوشه محتوی فایل اجرایی باج افزار>\@WanaDecryptor@.exe
<پوشه محتوی فایل اجرایی باج افزار>\b.wnry
<پوشه محتوی فایل اجرایی باج افزار>\c.wnry
<پوشه محتوی فایل اجرایی باج افزار>\f.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_bulgarian.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_chinese (simplified).wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_chinese (traditional).wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_croatian.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_czech.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_danish.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_dutch.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_english.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_filipino.wnry

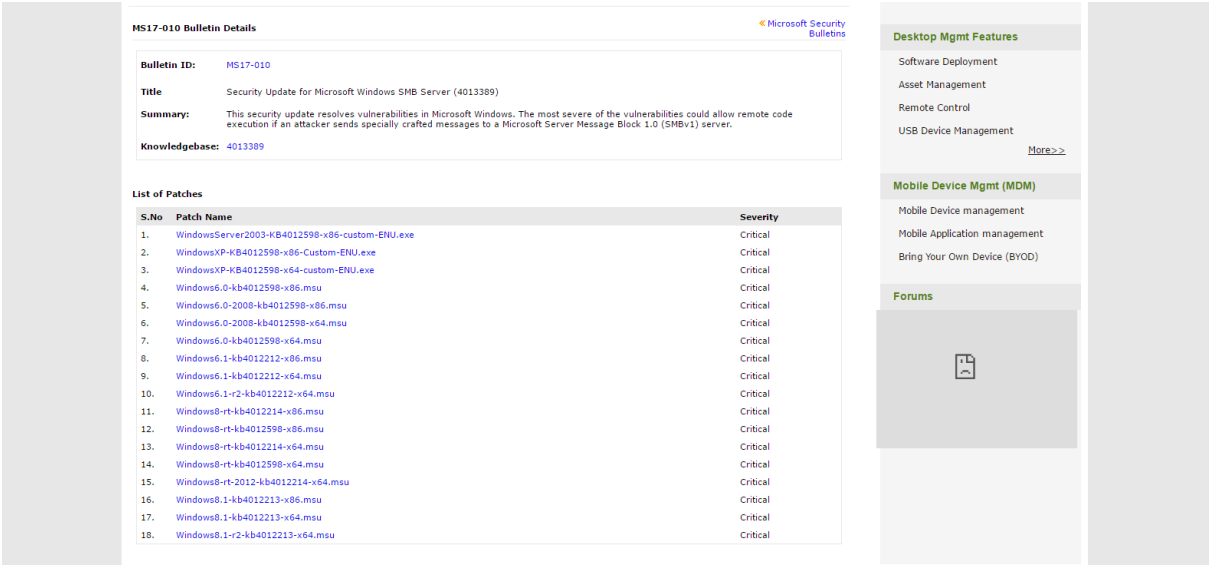
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_finnish.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_french.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_german.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_greek.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_indonesian.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_italian.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_japanese.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_korean.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_latvian.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_norwegian.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_polish.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_portuguese.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_romanian.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_russian.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_slovak.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_spanish.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_swedish.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_turkish.wnry
<پوشه محتوی فایل اجرایی باج افزار>\msg\m_vietnamese.wnry
<پوشه محتوی فایل اجرایی باج افزار>\r.wnry
<پوشه محتوی فایل اجرایی باج افزار>\s.wnry
<پوشه محتوی فایل اجرایی باج افزار>\t.wnry
<پوشه محتوی فایل اجرایی باج افزار>\TaskData\Tor\libeay32.dll
<پوشه محتوی فایل اجرایی باج افزار>\TaskData\Tor\libevent-2-0-5.dll
<پوشه محتوی فایل اجرایی باج افزار>\TaskData\Tor\libevent_core-2-0-5.dll
<پوشه محتوی فایل اجرایی باج افزار>\TaskData\Tor\libevent_extra-2-0-5.dll
<پوشه محتوی فایل اجرایی باج افزار>\TaskData\Tor\libgcc_s_sjlj-1.dll
<پوشه محتوی فایل اجرایی باج افزار>\TaskData\Tor\libssp-0.dll
<پوشه محتوی فایل اجرایی باج افزار>\TaskData\Tor\ssleay32.dll
<پوشه محتوی فایل اجرایی باج افزار>\TaskData\Tor\taskhsvc.exe
<پوشه محتوی فایل اجرایی باج افزار>\TaskData\Tor\tor.exe
<پوشه محتوی فایل اجرایی باج افزار>\TaskData\Tor\zlib1.dll
<پوشه محتوی فایل اجرایی باج افزار>\taskdl.exe
<پوشه محتوی فایل اجرایی باج افزار>\taskse.exe
<پوشه محتوی فایل اجرایی باج افزار>\u.wnry
C:\@WanaDecryptor@.exe

در انتها پیشنهاد می‌شود که پس از به روزرسانی آنتی ویروس در سیستم‌هایی که در معرض آلوودگی بوده اند و سایر سیستم ها، اقدام به یک اسکن کامل از سیستم نمود. در صورتی که آنتی ویروس معتبر بر روی سیستم موجود نباشد می توان با دانلود کردن انواع مجانی آنتی ویروس، مثلا AVAST سیستم‌ها را اسکن نمود.

پیوست شماره ۲

با توجه به اینکه شرکت مایکروسافت برای نسخه‌های ویندوز، به‌روز رسانی‌ها و وصله‌های امنیتی ارایه کرده است. این به‌روزرسانی‌ها در آدرس زیر موجود و در دسترس هستند.

https://www.manageengine.com/products/desktop-central/patch-management/MS17-010.html



MS17-010 Bulletin Details

« Microsoft Security Bulletins

Bulletin ID:	MS17-010
Title	Security Update for Microsoft Windows SMB Server (4013389)
Summary:	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.
Knowledgebase:	4013389

List of Patches

S.No	Patch Name	Severity
1.	WindowsServer2003-KB4012598-x86-custom-ENU.exe	Critical
2.	WindowsXP-KB4012598-x86-Custom-ENU.exe	Critical
3.	WindowsXP-KB4012598-x64-custom-ENU.exe	Critical
4.	Windows6.0-kb4012598-x86.msu	Critical
5.	Windows6.0-2008-kb4012598-x86.msu	Critical
6.	Windows6.0-2008-kb4012598-x64.msu	Critical
7.	Windows6.0-kb4012598-x64.msu	Critical
8.	Windows6.1-kb4012212-x86.msu	Critical
9.	Windows6.1-kb4012212-x64.msu	Critical
10.	Windows6.1-r2-kb4012212-x64.msu	Critical
11.	Windows8-rt-kb4012214-x86.msu	Critical
12.	Windows8-rt-kb4012598-x86.msu	Critical
13.	Windows8-rt-kb4012214-x64.msu	Critical
14.	Windows8-rt-kb4012598-x64.msu	Critical
15.	Windows8-rt-2012-kb4012214-x64.msu	Critical
16.	Windows8.1-kb4012213-x86.msu	Critical
17.	Windows8.1-kb4012213-x64.msu	Critical
18.	Windows8.1-r2-kb4012213-x64.msu	Critical

Desktop Mgmt Features
Software Deployment
Asset Management
Remote Control
USB Device Management
More>>
Mobile Device Mgmt (MDM)
Mobile Device management
Mobile Application management
Bring Your Own Device (BYOD)
Forums

در سریع‌ترین زمان ممکن آنتی‌ویروس موجود بر سیستم و تمام مرورگرهای وب نصب شده بر روی سیستم نیز به‌روز رسانی گردد.

نسبت به مسدودسازی پورت‌های 445 و 139 در پروتکل TCP و پورت‌های 137 و 138 در پروتکل UDP بر روی سیستم‌های کامپیوتری و فایروال نیز اقدام گردد.

موضوع بعدی که باید در اولین فرصت حتما صورت بگیرد، غیرفعال سازی پروتکل آسیب‌پذیر SMB است.

غیرفعال‌سازی SMB بر روی سرور SMB

ویندوز 8 و ویندوز سرور 2012

برای غیرفعال‌سازی SMBv1 بر روی سرور SMB دستور زیر اجرا گردد:

Set-SmbServerConfiguration -EnableSMB1Protocol $false

برای غیرفعال‌سازی SMBv2 و SMBv3 بر روی سرور SMB، دستور زیر اجرا گردد:

Set-SmbServerConfiguration –EnableSMB2Protocol $false

ویندوز 7، ویندوز سرور 2008 R2، ویندوز ویستا و ویندوز سرور 2008

از طریق cmdlet

غیرفعال‌سازی SMBv1 بر روی سرور SMB با دستور زیر:

Set-ItemProperty-Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Para
meters" SMB1 -Type DWORD -Value 0 –Force

غیرفعال‌سازی SMBv2 و SMBv3 بر روی سرور SMB

Set-ItemProperty-Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -
Type DWORD -Value 0 -Force

نکته: برای اعمال تغییرات، باید رایانه دوباره راه‌اندازی شود.

از طریق رجیستری

پیش از هر اعمال تغییرات در رجیستری ابتدا باید یک پشتیبان از رجیستری ایجاد شود و بدین منظور راهنمایی در این باره در انتهای پیوست ارایه شده است.

پس از پشتیبان‌گیری از رجیستری، برای غیرفعال‌سازی SMBv1 بر روی سرور SMB به آدرس زیر در رجیستری مراجعه شود:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\P
arameters

سپس یک رکورد به نام SMB1 ایجاد کرده و مقدار REG_DWORD برابر 0 قرار داده شود.

برای غیرفعال‌سازی SMBv2 نیز به آدرس زیر در رجیستری مراجعه شود:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\P
arameters

و پس از ساخت یک رکورد به نام SMB2، مقدار REG_DWORD برابر 0 قرار داده شود.

غیرفعال‌سازی SMB بر روی کلاینت SMB

ویندوز ویستا، ویندوز سرور 2008، ویندوز 7، ویندوز سرور 2008 R2، ویندوز 8 و ویندوز سرور 2012

برای غیرفعال‌سازی SMBv1 بر روی کلاینت SMB دستورات زیر اجرا گردد:

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi
sc.exe config mrxsmb10 start= disabled
```

برای غیرفعال‌سازی SMBv2 و SMBv3 بر روی کلاینت SMB دستورات زیر اجرا گردد:

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb10/nsi
sc.exe config mrxsmb20 start= disabled
```

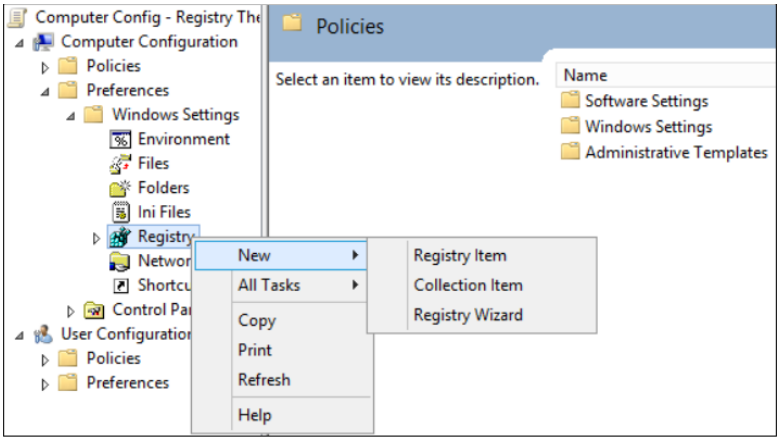
نکته: برای اعمال تغییرات، رایانه باید دوباره راه‌اندازی گردد.

غیرفعال‌سازی سرور SMBv1 با Group Policy

Group Policy Management Console را گشوده و بر روی Group Policy object(GPO) که باید قسمت تنظیمات جدید داشته باشد، کلیک راست کرده و گزینه Edit انتخاب شود.

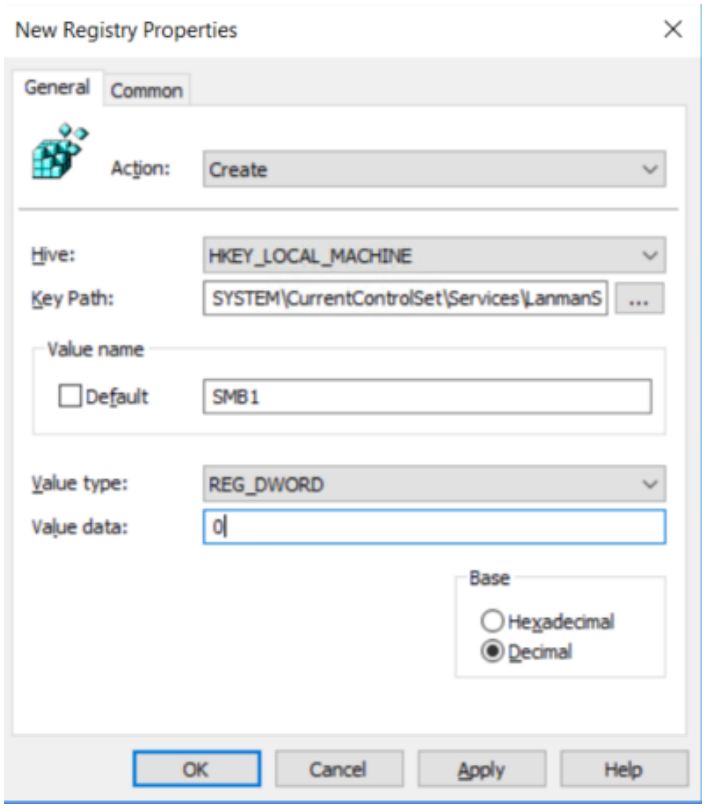
در درخت کنسول زیر Computer Configuration پوشه Preferences و سپس پوشه Windows Settings گسترش داده شود.

همانند تصویر زیر بر روی Registry کلیک نموده و پس از گزینه New بر روی Registry Item کلیک شود.



و در پنجره New Registry Properties نیز تغییرات زیر مانند تصویر اعمال گردد.

Action: Create
Hive: HKEY_LOCAL_MACHINE
Key Path: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Value name: SMB1
Value type: REG_DWORD
Value data: 0



غیرفعال‌سازی کلاینت SMBv1 با Group Policy

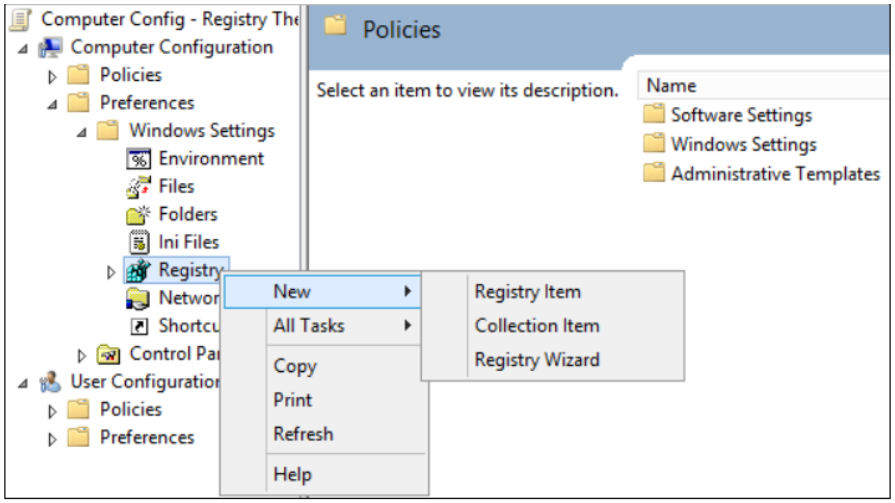
برای غیرفعال‌سازی کلاینت SMBv1، کلید رجیستری سرویس‌ها باید برای غیرفعال‌سازی شروع MRxSMB10 به‌روز باشد و سپس وابستگی موجود بر روی MRxSMB10 باید از ورودی LanmanWorkstation حذف شود که بدین خاطر کلید رجیستری سرویس‌ها بتواند به صورت عادی کار خود را آغاز کند بدون نیاز به اینکه MRxSMB10 ابتدا شروع به کار کند.

برای غیرفعال‌سازی کلاینت SMBv1

Group Policy Management Console را گشوده و بر روی Group Policy object(GPO) که باید قسمت تنظیمات جدید داشته باشد، کلیک راست کرده و گزینه Edit انتخاب شود.

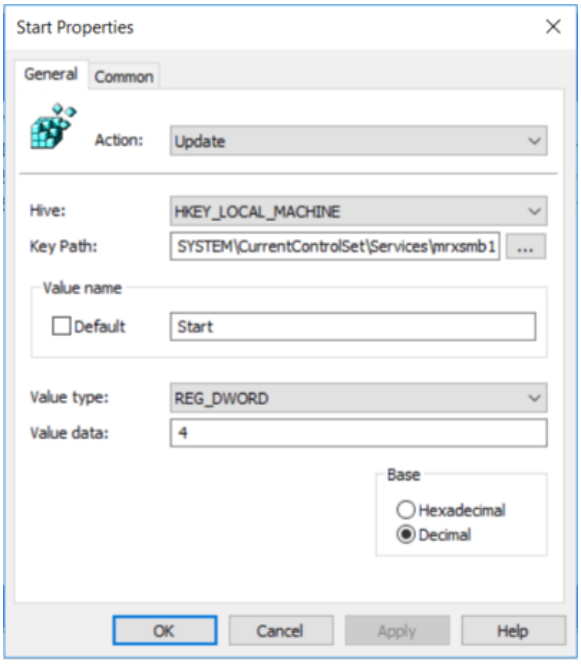
در درخت کنسول زیر Computer Configuration پوشه Preferences و سپس پوشه Windows Settings گسترش داده شود.

همانند تصویر زیر بر روی Registry کلیک نموده و پس از گزینه New بر روی Registry Item کلیک شود.



و در پنجره New Registry Properties نیز تغییرات زیر مانند تصویر اعمال گردد.

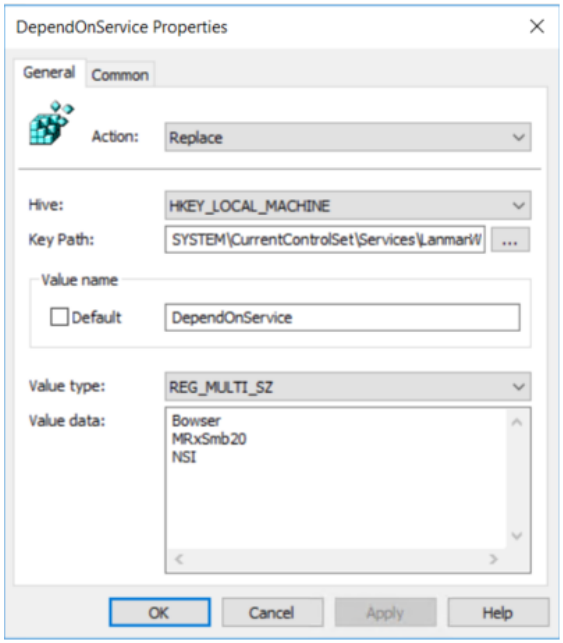
Action: Update
Hive: HKEY_LOCAL_MACHINE
Key Path: SYSTEM\CurrentControlSet\services\mrxsmb10
Value name: Start
Value type: REG_DWORD
Value data: 4



برای حذف وابستگی بر روی MRxSMB10 که غیرفعال گردید، در پنجره New Registry Properties موارد زیر باید اعمال گردد.

Action: Replace
Hive: HKEY_LOCAL_MACHINE
Key Path: SYSTEM\CurrentControlSet\Services\LanmanWorkstation
Value name: DependOnService
Value type REG_MULTI_SZ

Value data:
Bowser
MRxSmb20
NSI

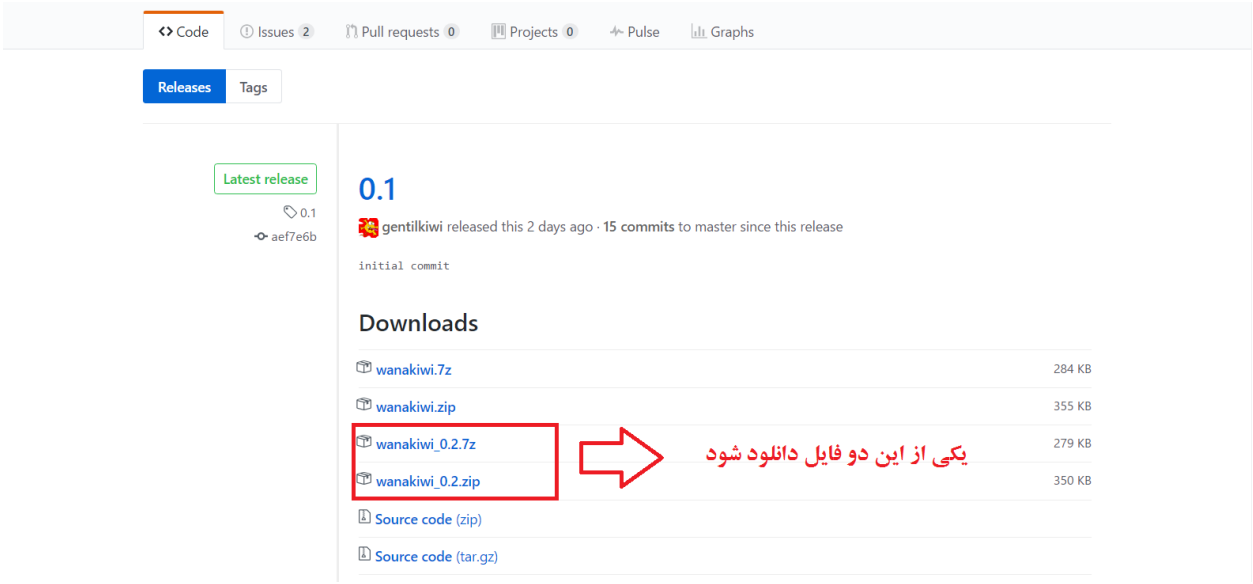


پیوست ۳

احتمال آنکه با وجود رعایت کردن تمام شرطهای کارکرد این ابزار، در بازیابی فایلها توفیق حاصل نشود وجود دارد چرا که تاخیر در اجرای ابزار و برخی رخدادهای دیگر، ممکن است که آن نقطه ضعف در فرآیند رمزگذاری باج‌افزار که برای رمزگشایی مورد بهره‌برداری قرار می‌گیرد را از بین ببرد. به هر حال شرط لازم برای آنکه این فرآیند و بسیاری دیگر از انواع ابزارهای معرفی شده در روزهای اخیر موفق به بازیابی اطلاعات شوند، آن است که سیستم به هیچ عنوان ریستارت نشده باشد، به هیچ عنوان فرآیند رمزگذاری در ویندوز متوقف نشده باشد و زمان زیادی از آلودگی نگذشته باشد. لازم به ذکر است که آزمایش‌های انجام گرفته حاکی از آن است که گروه مهاجم، با تشخیص دادن این نقطه ضعف، نسخه جدیدی از باج‌افزار را با همان شکل و رفتار قبلی منتشر کرده است که انجام این فرآیند برای آن ناممکن است.

برای نصب برنامه بازیابی فایل‌های سیستم، به آدرس زیر مراجعه و مطابق تصویر فایل wanakiwi_0.2.zip و wanakiwi_0.2.7z دانلود شود. (ابزارهای دیگری نیز در این روزها منتشر شده اند که توصیه می‌شود با احتیاط از آنها استفاده شود چرا که ممکن است به همراه هریک بدافزاری نیز منتقل شود)

https://github.com/gentilkiwi/wanakiwi/releases



سپس با نرم‌افزارهای فشرده‌کننده مانند WinRar فایل دانلود شده از حالت فشرده خارج شود.

اکنون برای بدست آوردن PID فرآیند مخرب دو روش موجود است:

روش اول) استفاده از دستور tasklist در خط فرمان (قابل استفاده در تمام سیستم‌عامل ها)

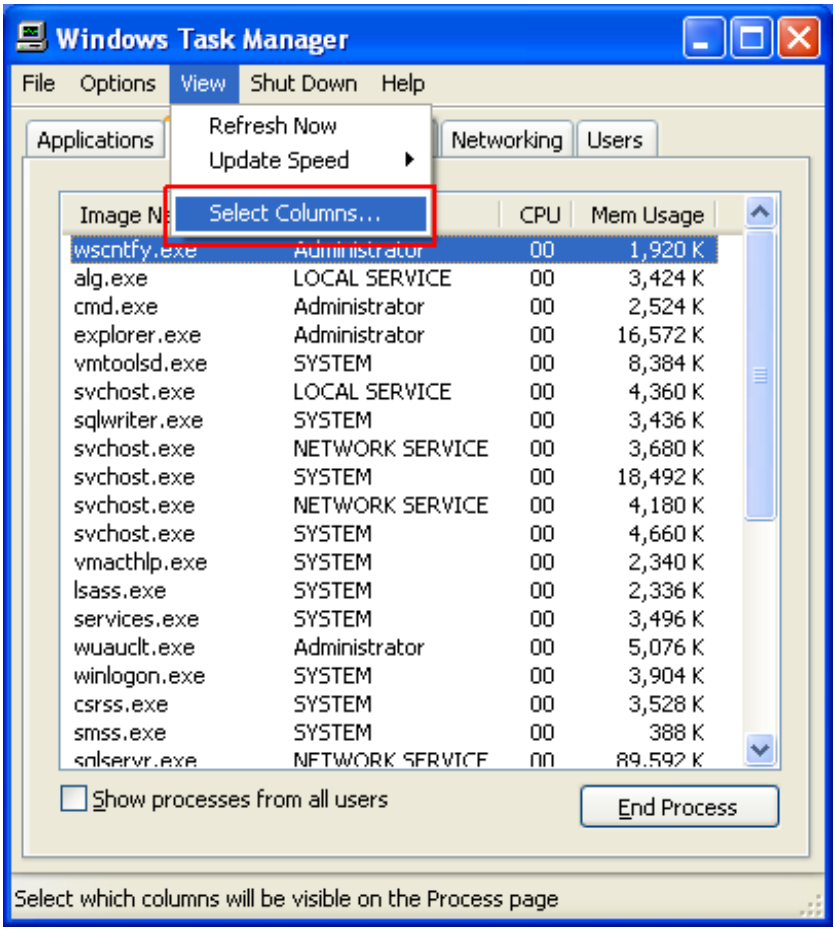
خط فرمان یا CMD را گشوده و با تایپ دستور tasklist و فشردن دکمه Enter دستور ارسال گردد و در لیست فرآیندهای ظاهر شده مقدار PID برای WannaCry.exe (یا فایل اجرایی بدافزار مهاجم با نام مشابه) یادداشت شود.

روش دوم) استفاده از TaskManager

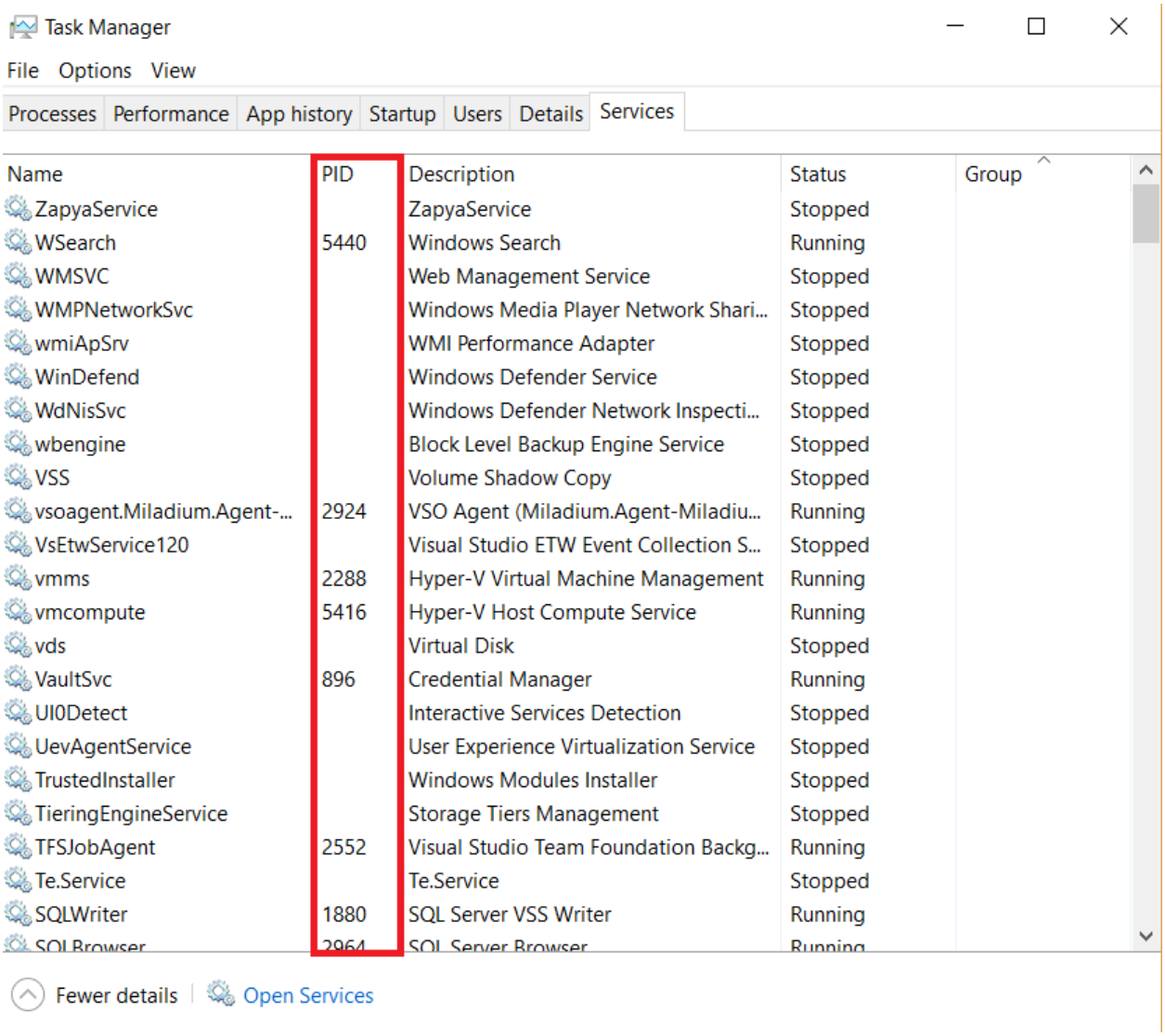
اکنون با فشردن کلیدهای Ctrl+Alt+Del بر روی صفحه کلید، وارد Task Manager شده و با توجه به سیستم‌عامل آلوده مورد نظر برای بدست آوردن PID به روش‌های گفته شده زیر اقدام گردد.

ویندوز XP: پس از کلیک بر روی زبانه Processes مطابق تصاویر زیر در ردیف WanaCry.exe مقدار PID یادداشت گردد.

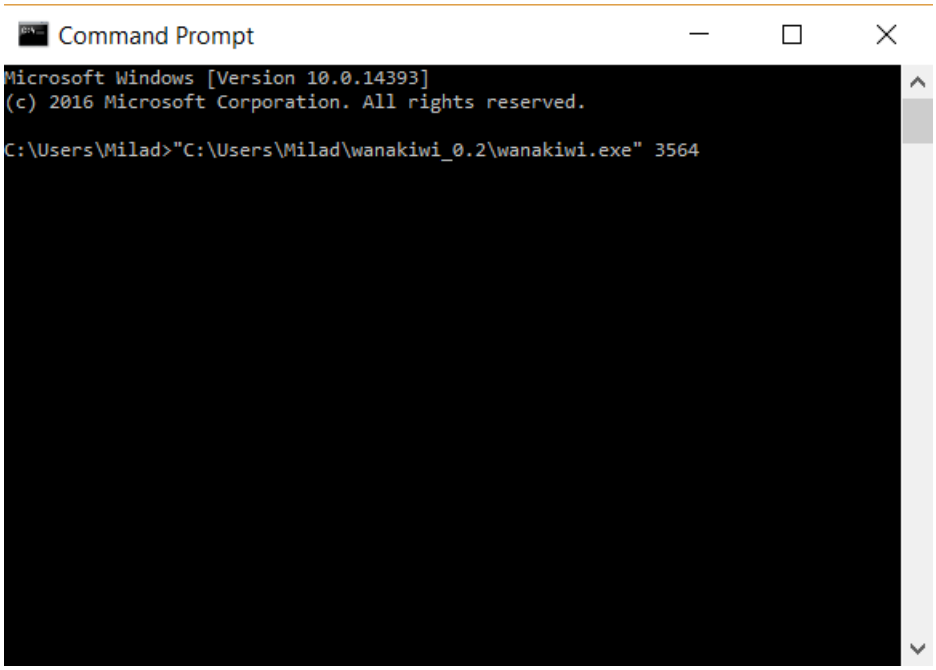
نکته مهم: در صورتی که ستون PID در این زبانه موجود نبود، پس از کلیک بر روی View در منوی بالا مانند تصویر بر روی Select Columns کلیک نموده و با زدن تیک PID، ستون PID نیز در کنار ستون‌های دیگر اضافه می‌شود.



در مورد ویندوز ۷ و سیستم‌عامل‌های پس از آن: با مراجعه به زبانه Services، مقدار PID برای فرآیند مخرب (مثلا WannaCry.exe ، Wcry.exe، Cybered.....exe و امثال آن) یادداشت گردد.



اینک نوبت گام اجرا است. خط فرمان یا CMD را گشوده و فایل را به داخل محیط خط فرمان کشیده (Drag) یا آدرس فایل در خط فرمان و بین دو کوتیشن تایپ شود و PID که در مراحل گذشته یادداشت گردید نیز با یک فاصله تایپ گردیده و با فشردن دکمه Enter اجرا شود.



پس از ارجاع دستور، فایل بازیابی، یافتن فایل 00000000.pky که دارای کلید عمومی است را آغاز می‌کند و پس از یافتن این فایل، با استفاده از PID فضای حافظه‌ای فرآیند رمز گذاری را برای یافتن اعداد اول مورد استفاده در تولید رمز، جستجو کرده و در صورت موفقیت به وسیله این اعداد اول، فایل 00000000.pky را رمزگشایی می‌کند و پس از اینکه کلید مورد نظر رمزگشایی گردید، فایل‌های رمزگذاری شده توسط باج‌افزار را رمزگشایی می‌کند.

```
File c:\Users\Public\Music\Sample Music\AlbumArt_{5FA05D35-A682-4AF6-96F7-0773E4
2D4D16}_Large.jpg.WNCRY -- OK
File c:\Users\Public\Music\Sample Music\AlbumArt_{5FA05D35-A682-4AF6-96F7-0773E4
2D4D16}_Small.jpg.WNCRY -- OK
File c:\Users\Public\Music\Sample Music\Kalimba.mp3.WNCRY -- OK
File c:\Users\Public\Music\Sample Music\Maid with the Flaxen Hair.mp3.WNCRY -- O
K
File c:\Users\Public\Music\Sample Music\Sleep Away.mp3.WNCRY -- OK
File c:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg.WNCRY -- OK
File c:\Users\Public\Pictures\Sample Pictures\Desert.jpg.WNCRY -- OK
File c:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg.WNCRY -- OK
File c:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg.WNCRY -- OK
File c:\Users\Public\Pictures\Sample Pictures\Koala.jpg.WNCRY -- OK
File c:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg.WNCRY -- OK
File c:\Users\Public\Pictures\Sample Pictures\Penguins.jpg.WNCRY -- OK
File c:\Users\Public\Pictures\Sample Pictures\Tulips.jpg.WNCRY -- OK
File c:\Users\Public\Videos\Sample Videos\Wildlife.wmv.WNCRY -- OK
```