

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

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

RAT (Quasar) ربع تانايب جارختسا - ةبيردت تانايب

??????????

دادعتل همدختساو ،ةيحصلا زاهج ىلع RAT لىغشتب موقننس ،بييردتلا ويرانيسل اذه يف تافللمل جارختسا فدهب ،صرقلال ىلع ةدوجومل تانايبلا

نمض جردنت RAT اهمدختسي يتلا تايكولسل نأ ال ،ةيدف موجه سيل اذه نأ نم مغرلا ىلع ثداحلل ةباجتسالا ودبتو . Cyber Crucible اهفشتكى يتلا تانايبلا زازتبا تايكولسل لـ ةبسنلاب هنأل ،ةيدف ةلومحل ةباجتسالاب ةصاخلا كلتل آدج ةهباشم ةلصل اذ تانايبلاو !اهسفن ةقيرطلاب لمأغي 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 يدؤيو system32 يف دوجوم هنكل ،ءيشلا ضعب أبيرغ يذيفنتلا فلملا اذه ودبي تاراسملا نع ثحبلا بءبل اننكمي .انه ثدح ام ةفرعمل قيقتحتلا نم ديزملا ءارجإ مزلي .ةرركتم ةباجتسالاراسمب ةطبترملا ةيعرفلا

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 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\SubDir\Client.exe

client-build.exe فلم ال لي غش تب مدخ تس م مق .ةصق ل ا حي ضو ت ل ةلدأ ل ا نم د يز م ل ا ل ع ل لص ح ن ا نه ال svchost. ربع ت ا ز ا ي ت م ا ل ا دي ع ص تب موق ي ه ن ا و د ب ي م ث . RAT طاق س ا ةا د ا وه ، ب ت ك م ا ح ط س ن م ء ي ش در ج م س ي ل و RAT وه ا ذه ن ا فر ع ن ف ي ك . ك ل ذ ع م ، ء ي ح ا ل ا ي ف ةدوق ف م ا ع ط ق ل ا ض ع ب ك ا نه ل ا ز ت svchost؟ ع م ل ع ا ف ت ي

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\dlhhost.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

ا ط ا ش ن ك ا نه ن ا ن ي ق ي ل ا ه ج و ل ع ن ا ل ا فر ع ن ط ق ف ن ح ن ا ل ف ! ر ي ث ك ب ع س و ا ء ي ؤ ر ا ن ل ح ت ف ي ا ذه ء ي ر ا ر م ت س ا ء ي ل ا ء ا ش ن ا م ت ي ه ن ا ا ض ي ا فر ع ن ل ب ، ه ب ء ط ب ت ر م ل ا ت ا ر ا س م ل ا و ، ر ج ي ا ه و ب ش م ا د ي ح ف و ر ع م RAT وه ، Quasar ع م ل م ا ع ت ن ا ن ا ا ض ي ا ر ن ل ب . (persistence).

م ا د خ ت س ا ا ل ض ف م ، ص ا خ ل ا ي ذ ي ف ن ت ل ا ه ف ل م ل خ ا د ن م ه ك و ل س م ط ع م ذ ف ن ي و ، ر و ط ت م RAT وه Quasar ن م د ي د ع ل ل ء ي ض ا ر ت ف ا ل ا Windows ت ا و د ا م ا د خ ت س ا ن م ا ل د ب ه ب ء ص ا خ ل ا ء ي ت ب ا ث ء ع م ج م ل ا ه ت ا ب ت ك م schtasks. ل ث م ت ا و د ا ل ه م ا د خ ت س ا د ن ع ا ن ا ي ح ا ط ب ض ي Quasar ت ح ن ك ل . م ا ه م ل ا

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

- [Mitre T1566](#) - ن ا ك ا م ا ر ج ا ذ ي ف ن ت ل م د خ ت س م ل ا ع ا د خ ل ا ي ل ا ي ح ا ل ا د ي ص ت ل ا م د خ ت س ي د ق - ر و ر م ء م ل ك ء ك ر ا ش م و ا ت ب ر ك س ل ي غ ش ت ل ث م ، ك ل ذ ا ل و ل ه ب موق ي ل
- [Mitre T1091](#) - ء ل ا ز ا ل ل ء ل ب ا ق ط ئ ا س و ل ا ا ه س ف ن خ س ن ب ء ث ي ب خ ل ا ء ي ج م ر ب ل ا موق ت د ق - و ا ي ئ ا ق ل ل ت ل ا ل ي غ ش ت ل ا ر ب ع ا ه ذ ي ف ن ت ا ه ب ل ص ت ي ي ذ ل ا ي ل ا ت ل ا ز ا ه ج ل ل ن ك م ي ث ي ح ب ل . ل ي غ ش ت ل ا ج م ا ر ب ت ا ر غ ث
- [Mitre T1204](#) - د ي ص ت ل ا ر ب ع ه ي ل ع ل و ص ح ل ا م ت ي ا م ا ب ل ا غ ي ذ ل ا ، م د خ ت س م ل ا ذ ي ف ن ت - ء ث ي ب خ ل ا ء ي ج م ر ب ل ا ذ ي ف ن ت ء د ب ل ء ق ي ر ط ط س ب ا وه ، ي ل ا ي ح ا ل ا
- [Mitre T1547](#) - د ن ع ء ر ا ض ج م ا ر ب ذ ي ف ن ت ل Windows م ا ط ن ء ث ي ب خ ل ا ء ي ج م ر ب ل ا ء ج و ت د ق - م د خ ت س م ل ا ل و خ د ل ي ج س ت د ن ع و ا ع ا ل ق ا ل ا

- [Mitre T1037](#) - دنع ةراض تات بركس ذي فنن ل Windows ماظن ةثي بخل ا ةي جمر ب ل ةجوت دق - مدخت سمل لوخد ليجست دنع و ا عالق ا
- [Mitre T1543](#) - ةرفي ش ل اءافخ ا ل ا ةي ماظن ةي لمع ل يدعت و اءاشن ا يدؤي ن ا نكمي - تاي جمر ب ل فاشتك ا نع اديعب ، ةقو و م و ةي داع ةي ماظن ةي لمع اهن ا ل ع ةثي بخل ا ةثي بخل ا

Revision #1

Created 2026-07-24 02:22:32 UTC by Dennis Underwood

Updated 2026-07-24 02:22:32 UTC by Dennis Underwood