

??? ????????

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

ي ف تسي ل تامي لعت ذي فن ت ي ل ع ب ة ي ل م ع ، أ (ة راض ام ب ر) ة ي ل م ع ر ب ج ت ام دن ع ي ه تاي ل م ع ل ن ق ح ءاش ن إ وه أعوي ش اهر ث ك أو ، ة ف ل ت خ م ل تاي ن ق ت ل ن م دي د ع ل تاي ل م ع ل ن ق ح ل . ا ه د و ك ن م أع ز ج ل ص أ ل ة ي ح ض ل ل ة ي ل م ع ل ل خ ا د د ب ن ع (thread) ذي فن ت ط ي خ .

ر ث أ ت ت ال ث ي ح ب ، ي ل ص أ ل ا ج م ا ن ر ب ل ا ع م ب ن ج ي ل إ ا ب ن ج ة دي د ج ل ت ا م ي ل ع ت ل ه ذ ه ءاش ن إ م ت ي ام أ ب ل ا غ ط ح ال ي ن أ ن و د ن ق ح ل ا ر م ي ام أ ب ل ا غ ، ب ب س ل ا ا ذ ه ل و . ب ة ي ح ض ل ل ة ي ل م ع ل ل ة ي ع ي ب ط ل تاي ل م ع ل ا

??????? Mitre ??? ??????:

- [Mitre T1055](#) - تاي ج م ر ب ل ف ا ش ت ك ا ب ن ج ت ل م د خ ت س ئ ي . ه ا ل ع أ ح ض و م وه ام ك ، تاي ل م ع ل ن ق ح - [Mitre T1055](#) ا ن ث أ ي ع ي ب ط ل ك ش ب ل م ع ل ا ل ص ا و م ب ة ف د ه ت س م ل ا ة ي ل م ع ل ل ا م س ل ل ا ل خ ن م ة ث ي ب خ ل ا راض ل ا د و ك ل ذي فن ت
- [Mitre T1559](#) - ح ن م ي ن أ (Inter-Process communication) تاي ل م ع ل ن ي ب ل ا ص ت ا ل ل ن ك م ي - [Mitre T1559](#) ن ق ح ل ا ة ي ل م ع ل ا م ت ك ا د ر ج م ب ن ق ح ل ا ه ج ل ب ق ن م ة ف د ه ت س م ل ا ة ي ل م ع ل ا ي ف م ك ح ت ل ا
- [Mitre T1569](#) - راض ل ا د و ك ل ا ي ف خ ئ ي ن أ ة د و ج و م `svchost` ل ث م م ا ط ن ة م د خ ي ف ن ق ح ل ل ن ك م ي - [Mitre T1569](#) ة ق و ث و م و ة ف و ر ع م ة ي ل م ع ن م ل م ع ي ه ن أ ي ل ع ه ن ع غ ا ل ب إ ل م ت ي ل

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

ر ي غ ت ي ب ث ت ر ا ب ج إ ن ك م ي . ة ق و ث و م د ع ت م ل ا ه ن أ ي ن ع ي ة ق و ث و م ة ي ل م ع ي ف ة ق و ث و م ر ي غ تاي ل م ع ن ق ح ت و م د ع ب . ة ث ي ب خ تاي ج م ر ب ت ا ل و م ح ذي فن ت ي ل ع ، SQL م دا خ ل ث م ، ن م و م ج م ا ن ر ب ل ل ص أ ل ا ي ف د س ا ف ل ك ش ب ء ي ش ل ك م ت ث ي ح ، ب ع ا ل ت ل ا ا ذ ه ي ل ع ة ل د أ ي أ ي ف ت خ ت س ، م ا ط ن ل ل ا ل ي غ ش ت ة د ا ع إ و / أ و ة ي ل م ع ل ا ي ك ي م ا ن ي د ذي فن ت ط و ي خ ءاش ن إ ر ب ع ة ر ك ا ذ ل ا ي ف ت ح ب

???? ????? Cyber Crucible?

ا ذ إ ل ط ا ش ن ل ا ف ق و ت الو ، م ا ط ن ل ا ي ل ع ث د ح ت ي ت ل ا تاي ل م ع ل ن ق ح تاي ل م ع Cyber Crucible ب ق ا ر ت م ا ط ن ل ا ي ل ع تاي ل م ع ل ا ض ع ب ن أ ل ك ل ذ و . ة ي د ف ل ا ج م ا ر ب ر ي ف ش ت و أ ت ا ن ا ي ب ل ا ز ا ز ت ب ا ة ط ش ن أ ت أ د ب راض ك و ل س ي أ ب م و ق ت الو ، ة ف ل ت خ م تاي ل م ع ن ق ح تاي ن ق ت ر ب ع ل ص ا و ت ت

يطلع على علم لك إلى أو نم تحدث التي لنق الح التاي لمع Cyber Crucible عبتتتس ،كلذ نمّ الدب اننكمي ،عقيرطال هذوب .لمتحم الم يرذل ببس لل ليلحت في أقحال اهم ادختسال اهلجستو ،ماظن لل تآدب على مع يأضيأ لب ،ةركاذل في لالح اقووثوم ريغ عني عم على نم أن طقف سيل فرعن أن راضل طاشن لل ةلسلس

???

31784977.png?width=510

يفرّج حص (untrusted remote threads) "ةقووثومل ريغ ةديعبل ذيفننل طويخ" لقل نوكل امدنع فرعم ذخأ اننكمي هنأ وه ديجل ربخاو. تايلمع نلق عم لماعتن ان أن ملعن، ةيئاقلت ةباجتسا، ةثداحل تقو لوح تايلمعل نلق تايلمع نمض ثحبلاو، ةباجتسالاب صاخلا (pid) ةيلمعل يناليل عل روثلعلو.

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

???????? ?????:

- تایلم علانقح - یبیردت ویرانیس

Revision #1

Created 2026-07-24 02:20:20 UTC by Dennis Underwood

Updated 2026-07-24 02:20:20 UTC by Dennis Underwood