

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

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

(Hive) تاي لمعل ن قح - بي ردتل تانايب

??????????

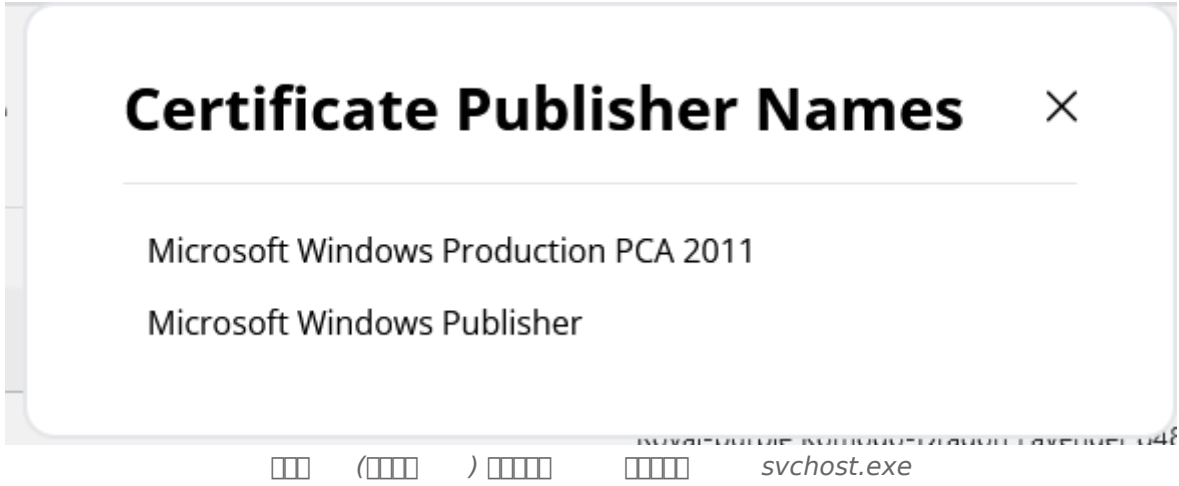
في تاي لمعل ن قح ربع ية دفل تاي جمر بة لومح ذي فن تب موقن س، بي ردتل ويراني سل اذه في
ماظن لي غشت ية لمعل ية نعمل Svchost ية لمعل. لعل لاب لي غشتل دي ق Svchost.exe ية لمعل
LocalSystem. مدختسم باسح تحت لمعل تو، عقوقومو، وليوط قرتف ذنم لمعلت، ية دغا

Svchost خسن نم ديدعل نأ نولوؤسم ملعل. اهل هاجت متي ام آبل اغف، "ية قيققح" Svchost نأل آرطن
اهرم أكرتوي و "دوسأ قودنص" اهنأ لعل لماغت، عحيص ودبت جمان ربل تا طيسو نأ ام لاطو، لمعلت
(zero day) رقص موي لومح عم بولسأل اذه جمدن. نصارقل اهل غتسي ام آبل اغو، حضاو قرغت هذ دغت
ية دفل تاي جمر بة تامجه افخ إ 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 هذبه طيحملا عضولا Microsoft لبق نم عُقوم يذيفنتلا فلملاو ،Svchost-ل ةبسنلاب ةحلص 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 يعبطللا لصاوتلل

وه اذهف ،قوٲوم ريغ هنأ ىلع مِّلغُي و ،ةيعيبط ريغ ةقيرطب ةيلمع لخاد ديعب طيخ أشُنُي 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 امَّ ةداع .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

st.exe

Injector Pid

Injector Path

Injectee Pid ▾

Injectee Path ↑

9168

C:\svchost_injector.exe

6224

C:\Windows\System32\svchost.exe

في سيل ديكتالاب نكلو،ةقيرطال هذه Svchost في نقحي نأ دحل يغبني ال هنا لعفلاب ملعن
ةفرعمو "malware.exe" تناك ول امك ةلمعلال هذه عم لماعتال اننكمي ادعاصف انه نم !ةلمعلال هذه
كلذ لعف دق مهذحأ نأ دب ال ذا،اهليغشتب 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

قِيضَت ان نكَمِي، اَمَامَت نَات فَلَ تَخَم ام هُو، 9168 (pid) ة لِمَع ل ا فَرَع مَب ءاش ن ا ي ت ي لِمَع د و ج و ل ا ر ط ن
ة ط س ا و ب ت ئ ش ن ا ه ن ا ى ر ن و ، ة ي ع ر ف ل ا ة لِمَع ل ا ر ا س م و ا / و ي ن م ز ل ا ع با ط ل ا ى ل ع ا ن ب ث ح ب ل ا ق ا ط ن
ر م ا ل ا ن و ك ي ن ا ن ك م ي ا ل و ، ن ق ا ح ل ا ة لِمَع ل ا ي غ ش ت ب ا ي و د ي م ا ق ا م ا ص خ ش ن ا ي ن ع ي ا ذ ه .
explorer.exe. ا ذ ه .
ئ ط ا خ ل ك ش ب ا ه ف ي ن ص ت م ت S v c h o s t ك و ل س ي ف ة ف د ا ص م د ر ج م .

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

- **تاي لِمَع ل ا ن ق ح (Process Injection)**
- [Mitre T1559](#) - (Inter-Process communication) تاي لِمَع ل ا ن ي ب ل ص ا و ت ل ا ر ف و ي ن ا ن ك م ي -
ن ق ح ل ا ة لِمَع ل ا م ت ك ا د ر ج م ب ن ق ا ح ل ا ل ب ق ن م ة ف د ه ت س م ل ا ة لِمَع ل ا ى ل ع ة ر ط ي س .
- [Mitre T1106](#) - ب ر ق ا (Native APIs) ة ل ص ا ل ا ت ا ق ي ب ط ت ل ا ة ج م ر ب ت ا ه ج ا و ن و ك ت ا م ا ب ل ا غ -
، تاي لِمَع ل ا ل ي غ ش ت و ، ت ا ف ل م ل ا ى ل ا ل و ص و ل ل ل ي غ ش ت ل ا م ا ط ن ف ا ط و ى ل ا ل و ص و ل ل ة ل ي س و .
د ي ز م ل ا و .
- [Mitre T1569](#) - ه ي و م ت ى ل ا ة د و ج و م s v c h o s t ة لِمَع ل م ل ث م م ا ط ن ة م د خ ي ف ن ق ح ل ا ي د و ي ن ا ن ك م ي -
ة ق و ث و م و ة ف و ر ع م ة لِمَع ل ن م ل م ع ت ا ه ن ا ك ا ه ن ع ا ل ا ل م ت ي ث ي ح ب ة ث ي ب خ ل ا ة ر ف ي ش ل ا .
- [Mitre T1055](#) - ة ث ي ب خ ة ر ف ي ش ل ي غ ش ت ل ة د ا ع م د خ ت س ئ ي ، (Process injection) تاي لِمَع ل ا ن ق ح -
ر ا ر م ت س ا ل ا ب ا ة ل ص ا ل ا ة لِمَع ل ل ح ا م س ل ا ع م ة ف د ه ت س م ة لِمَع ل خ ا د .