

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

??? ?????

(Redline) ةيوله قرس - بي ردتل تانايب

????????

(stealer) "قراسل" عون نم ةثيخ ةيجمرب ذي فنن تب موقننس ،بي ردتل ويرانيسل اذه في
ال ، **RAT** ويرانيس سكع لىل . دامتعال تانايب قرسي هو ، موجهل نم لولأل ةلحرمال ذي فنن تل
عزج اذه ، كلذ نم ال دب . ةيدفلل جم انرب اهم دختسي يتل تايكولسل سفن ويرانيسل اذه مدختسي
Cyber Crucible. دل ةيمانتمال ةيوله ةيامح تاردق نم

ربع كرتللا يه مجاهملا اهب موقى يتل لولأل تاوطخلل نوكت ، سفن زازتبالا ثودح لب قوآبلا غ
نم آجيزم اذه نوكتي ، تالاحل ضعبي في . دامتعال تانايب نم نكمم ردق ربكأ لىل لوصحلل او ةكبشلل
اهي لىل لوصحلل متي API حيتافم نوكت رخأ تالاح في و ، AD - ب صاخلا رورملا ةملك/مدختسملا مسا
ح ف ص ت م ل ل ت اس ل ج نم

????? ???? ?

لوؤسملل يعيبطلال ريغ لوصولل روهظ ةيفيك في قمعتن انعد ، يلاحللقولا في

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
C:\Users\User\Desktop\redline.exe	False	False	True

الف ،ام جم ان رب ىل ع نولو وؤس مل اذ ف ،أم 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
Statistic	1	AF4F45833C13F1A0971CA6DEE50FB21A	169.254.71.86	victim86753	10/19/2022 7:15...	US	☒	☐		4j0j0j0		

Guest Links

Loader Tasks

Logs Sorter

Wallet Checker

Builder

Misc

Telegram

Notifications

Black Lists

Settings

Contacts

Total logs: 1

Total pages: 1

Search filter:

<<

>>

Go to Page

Current page: 1

Enter a comment:

Search

Save all logs

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 ،ةيديلقالت انايبل رازتبا ثادحأب ةصاخل تاباجتسالاك تسيل تاباجتسالال هذه (process injections)، تايلمعل نقحب هبشأ يهف ،كلذ نمً ادب .ةيئاقلت فاقيل ةاءارجإ تسيل لوصولو ودبي فيك انملعت ،انتاليلحت ومن عمو .اهقيرط يف آقئاع Cyber Crucible فقت مل ثيح 2023، ماع لولحب .تاقيبطتال نم ةفلتخم عاونأل ةبسنللاب ةيوهل نزاخم يلإ "يعيبطلال" يلإ ،ةاونللا ةوتسم يلل ،لوصولو دّيقست يتلاو ،انب ةصاخل ةيامحل ةزيم لّعفنس اهيلل لوصولاب اهب ةطبترملا تايجمربلل الإ حمست نلو ةيوهل تانايب دعاوق لاكشأ فلتخم .

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

• (Process Injection) تايلمعل نقح

- [Mitre T1559](#) - ريفوت (Inter-Process communication) تايلمعل نيبل لاصتال نكمي -
نقحل ةيلمعل لامتكأ درجمب نقحل ةهجل بقل نم ةفدهتسمل ةيلمعل مكلحتال .
- [Mitre T1106](#) - برقأ (Native APIs) ةيلصلأل تاقيبطتال ةجمربت تاهجاو نوكت امآبلا -
تايلمعل ليغشتو تافلمل يلإ لوصولل ليغشتال ماطن فئاظو يلإ لوصولل ةليسو ديزملاو .
- [Mitre T1569](#) - ءافخإ يلإ ةدوجوملا `svchost` لثم ماطن ةمدخ يف نقحل يذؤي نأ نكمي -
ةقوثومو ةفورعم ةيلمعل نم لمعت اهنأك اهنع غالبالا متي ثيح ةثبخلل ةرفيشال .
- [Mitre T1055](#) - ةيلمعل يف ةثبخلل ةرفيش ليغشتل ةداع مدمتسُي ،تايلمعل نقح -
رارمتسالاب ةيلصلأل ةيلمعلل حامسلال عم ةفدهتسم .
- [Mitre T1543](#) - ةثبخلل ةرفيشال ءافخإ يلإ ماطن ةيلمعل ليدعت وأ ءاشنإ يذؤي نأ نكمي -
ةثبخلل تايجمربلل فشك ةمظنأ نع ةقوثومو ةيداع ماطن ةيلمعل .
- [Mitre T1555](#) - وأ رورملا تاملك يريدم نم ةنزملا دامتعالا تانايب مادختسا نكمي -
تازايمالا تاذ تانايبالا يلإ لوصولل ةرفشملا ريغ تاحفصتال .
- [Mitre T1212](#) - موقت ال ةفيعض تايجمربلل لالغتسا لالخل نم دامتعالا تانايب ةقرس نكمي -
مدختسملال اهلخدي تال دامتعالا تانايب ريفشتب .