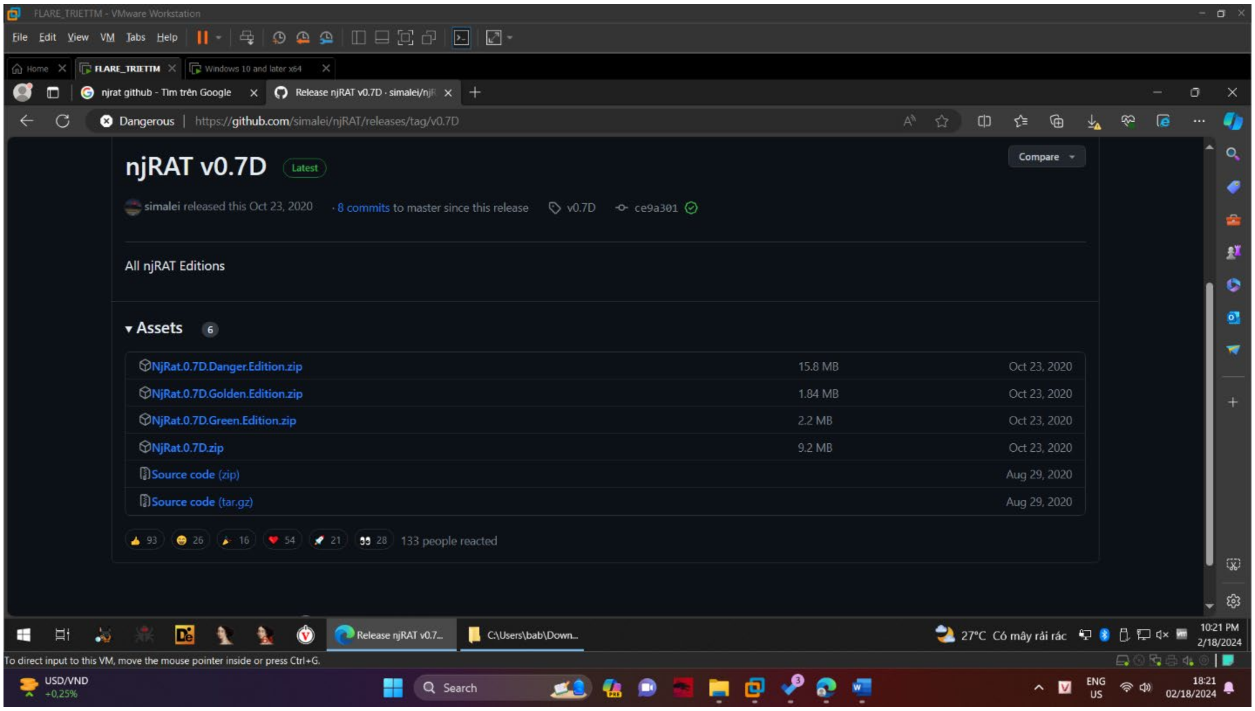
Họ và tên: Trần Minh Triết

MSSV: SE172241

Class: IA1702

Module 7: Malware threat

Gain Control over a Victim Machine using the njRAT RAT Trojan


FLARE_TRIETTM - VMware Workstation
njrat github - Tìm trên Google
Release njRAT v0.7D · simalei/njRAT
Dangerous
https://github.com/simalei/njRAT/releases/tag/v0.7D
Compare

njRAT v0.7D Latest

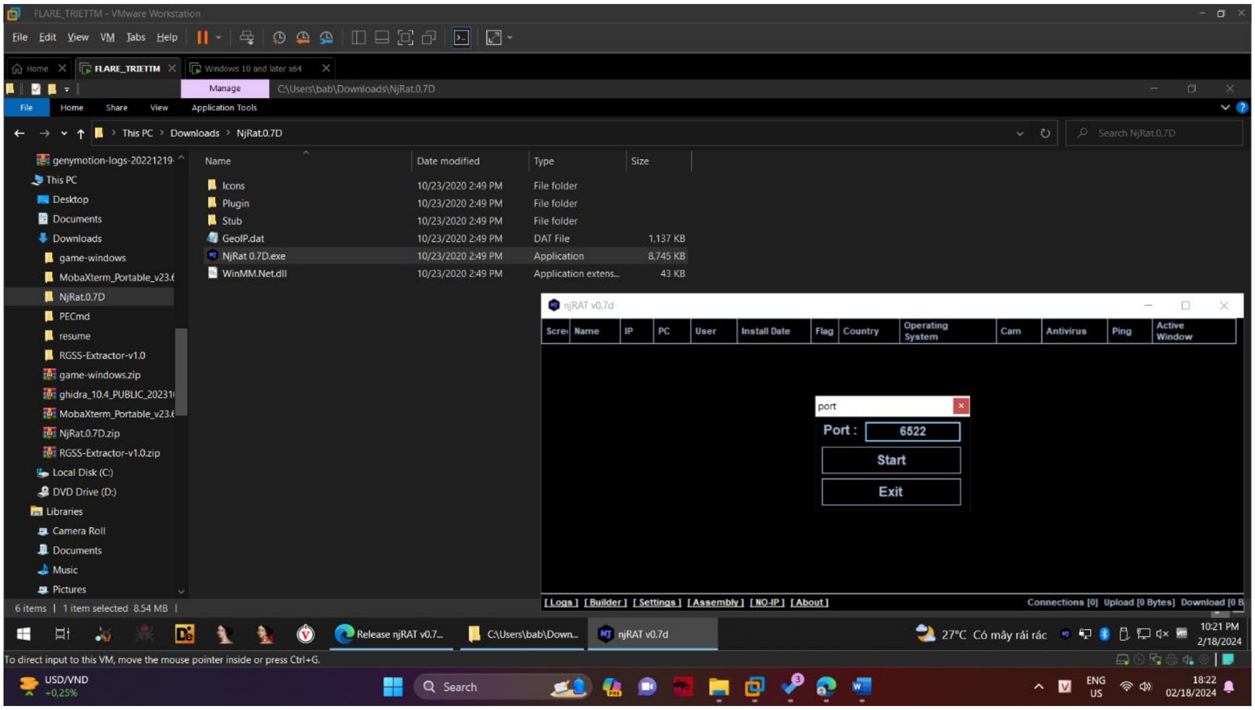
simalei released this Oct 23, 2020 · 8 commits to master since this release v0.7D ce9a301

All njRAT Editions

Assets 6

NjRat.0.7D.Danger.Edition.zip	15.8 MB	Oct 23, 2020
NjRat.0.7D.Golden.Edition.zip	1.84 MB	Oct 23, 2020
NjRat.0.7D.Green.Edition.zip	2.2 MB	Oct 23, 2020
NjRat.0.7D.zip	9.2 MB	Oct 23, 2020
Source code (zip)		Aug 29, 2020
Source code (tar.gz)		Aug 29, 2020

👍 93 😄 26 🎉 16 ❤️ 54 🚀 21 👀 28 133 people reacted

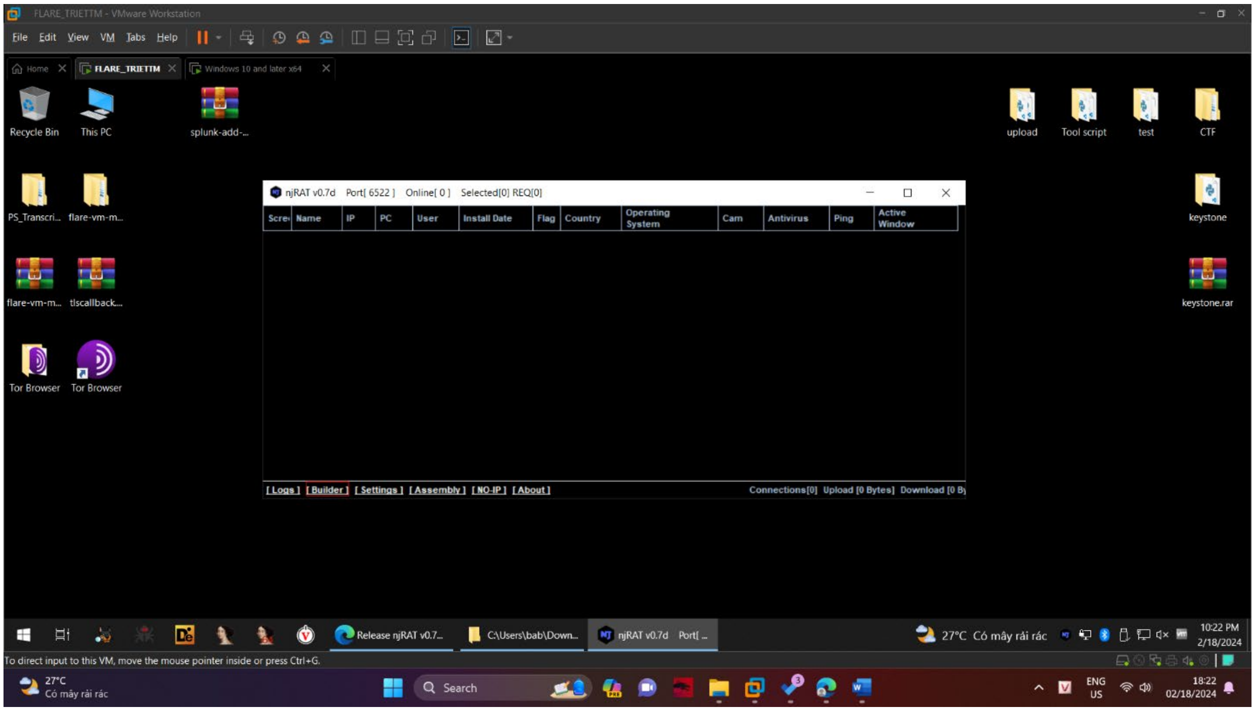


C:\Users\bab\Downloads\NjRat.0.7D

Name	Date modified	Type	Size
Icons	10/23/2020 2:49 PM	File folder	
Plugin	10/23/2020 2:49 PM	File folder	
Stub	10/23/2020 2:49 PM	File folder	
GeoIP.dat	10/23/2020 2:49 PM	DAT File	1,137 KB
NjRat 0.7D.exe	10/23/2020 2:49 PM	Application	8,745 KB
WinMM.Net.dll	10/23/2020 2:49 PM	Application extens...	43 KB

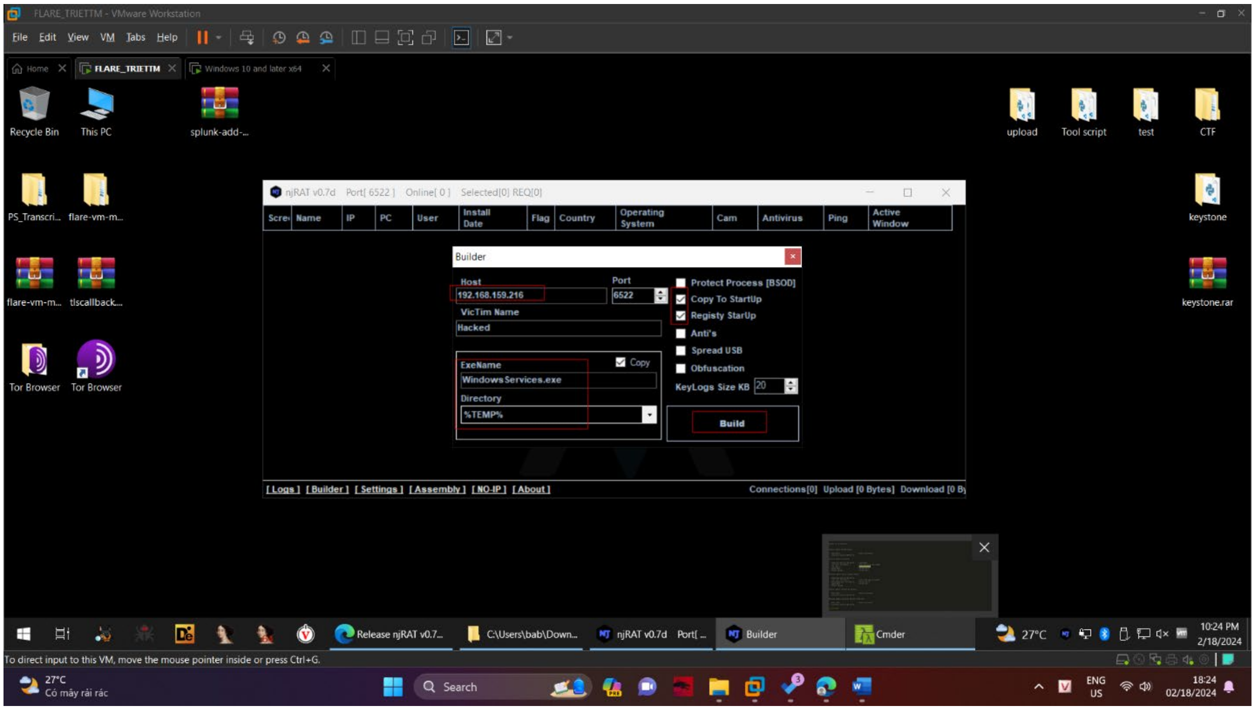
port

Port : 6522



njRAT v0.7d Port[6522] Online[0] Selected[0] REQ[0]

FLARE_TRIETTM - VMware Workstation
File Edit View VM Tabs Help
Home
FLARE_TRIETTM
Windows 10 and later x64
Recycle Bin
This PC
splunk-add-...
upload
Tool script
test
CTF
PS_Transcri...
flare-vm-m...
keystone
flare-vm-m...
tlscallback...
keystone.rar
Tor Browser
Tor Browser
Scre Name IP PC User Install Date Flag Country Operating System Cam Antivirus Ping Active Window
[Logs] [Builder] [Settings] [Assembly] [NO-IP] [About]
Connections[0] Upload [0 Bytes] Download [0 By
Release njRAT v0.7...
C:\Users\bab\Down...
njRAT v0.7d Port[...
27°C Có mây rải rác
10:22 PM
2/18/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C
Có mây rải rác
Search
ENG
US
18:22
02/18/2024



FLARE_TRIETTM - VMware Workstation

njRAT v0.7d Port[6522] Online[0] Selected[0] REQ[0]

Scre	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Antivirus	Ping	Active Window

Builder

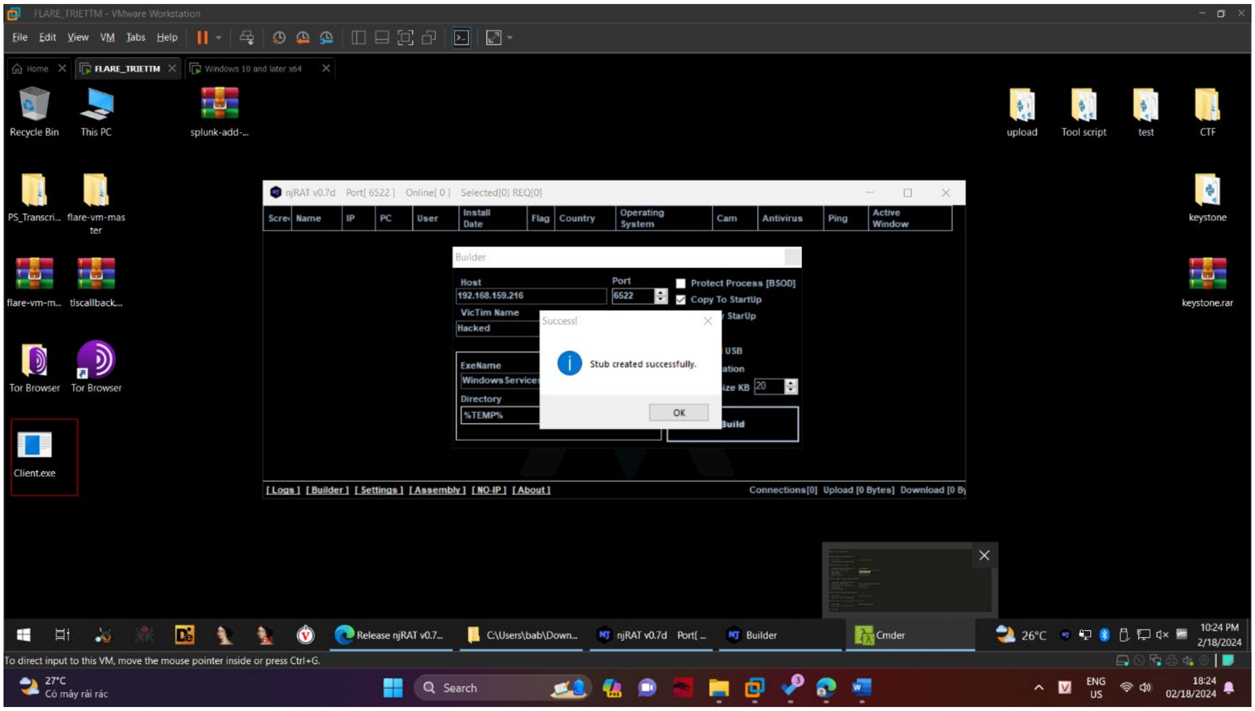
Host: 192.168.159.216
Port: 6522
VicTim Name: Hacked
ExeName: WindowsServices.exe ☑ Copy
Directory: %TEMP%

□ Protect Process [BSOD]
☑ Copy To StartUp
☑ Registy StartUp
□ Anti's
□ Spread USB
□ Obfuscation
KeyLogs Size KB: 20

Build

[Logs] [Builder] [Settings] [Assembly] [NO-IP] [About] Connections[0] Upload [0 Bytes] Download [0 B

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



FLARE_TRIETTM - VMware Workstation

njRAT v0.7d Port[6522] Online[0] Selected[0] REQ[0]

Builder

Host: 192.168.159.216
Port: 6522
VicTim Name: Hacked

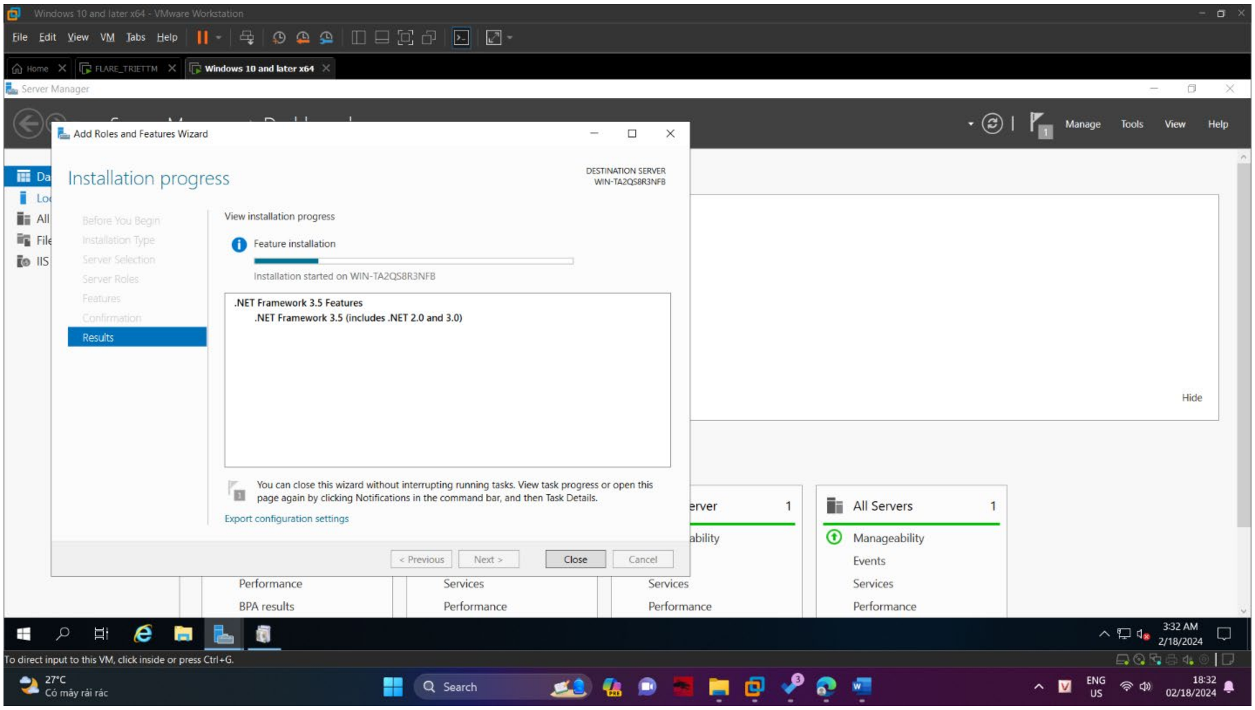
Success!

Stub created successfully.

OK

[Logs] [Builder] [Settings] [Assembly] [NO-IP] [About] Connections[0] Upload [0 Bytes] Download [0 B

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
WIN-TA2QS8R3NFB

View installation progress

Feature installation

Installation started on WIN-TA2QS8R3NFB

.NET Framework 3.5 Features
.NET Framework 3.5 (includes .NET 2.0 and 3.0)

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

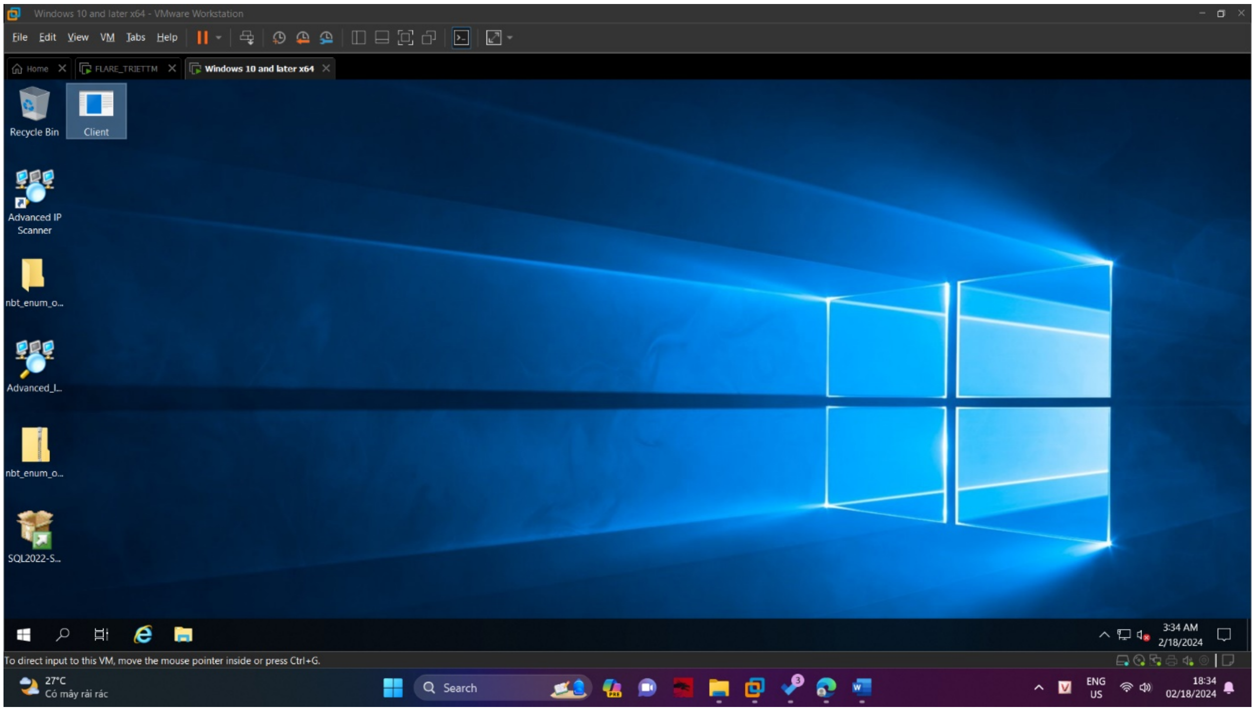
Export configuration settings

< Previous | Next > | Close | Cancel

3:32 AM 2/18/2024

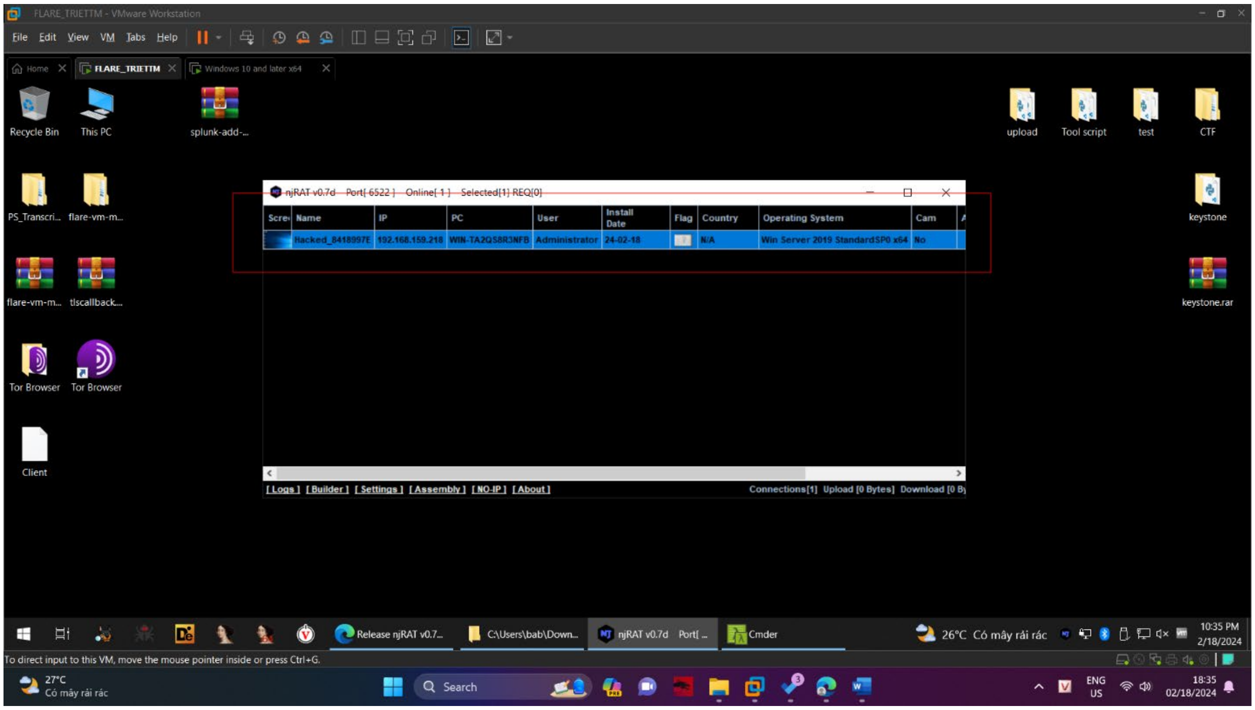
To direct input to this VM, click inside or press Ctrl+G.

27°C Có mây rải rác | Search | ENG US | 18:32 02/18/2024



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

27°C Có mây rải rác | Search | ENG US | 18:34 02/18/2024

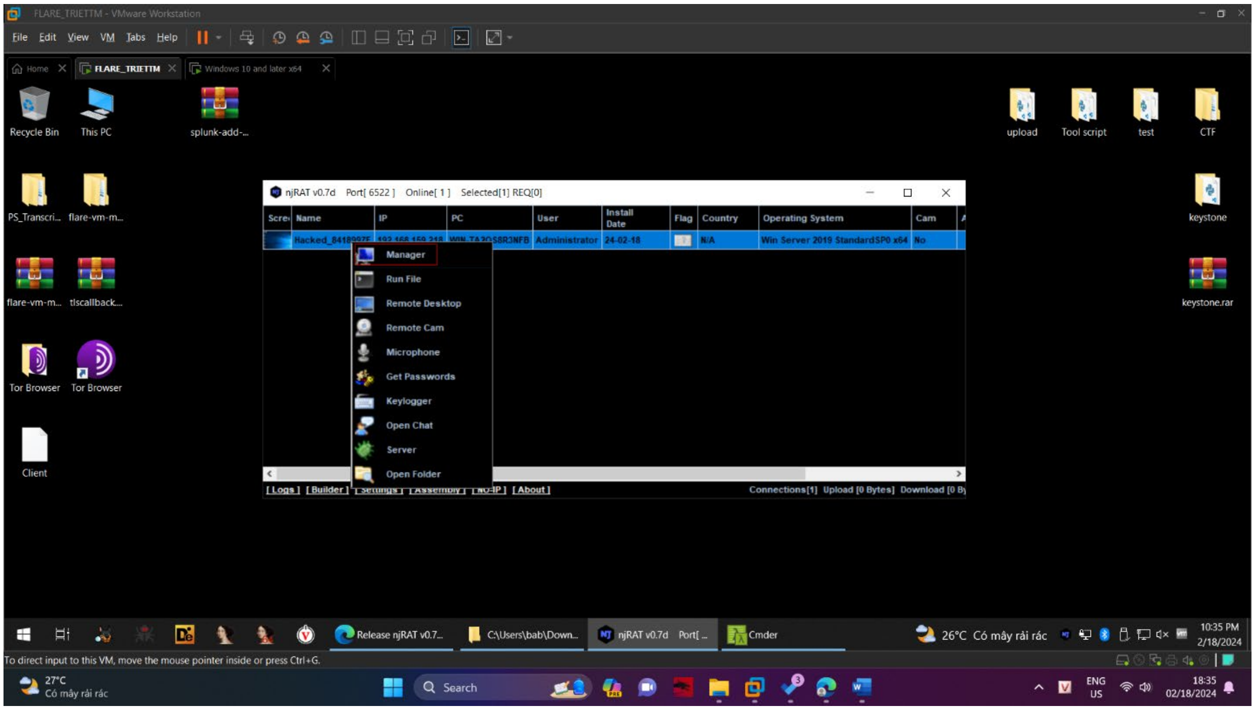


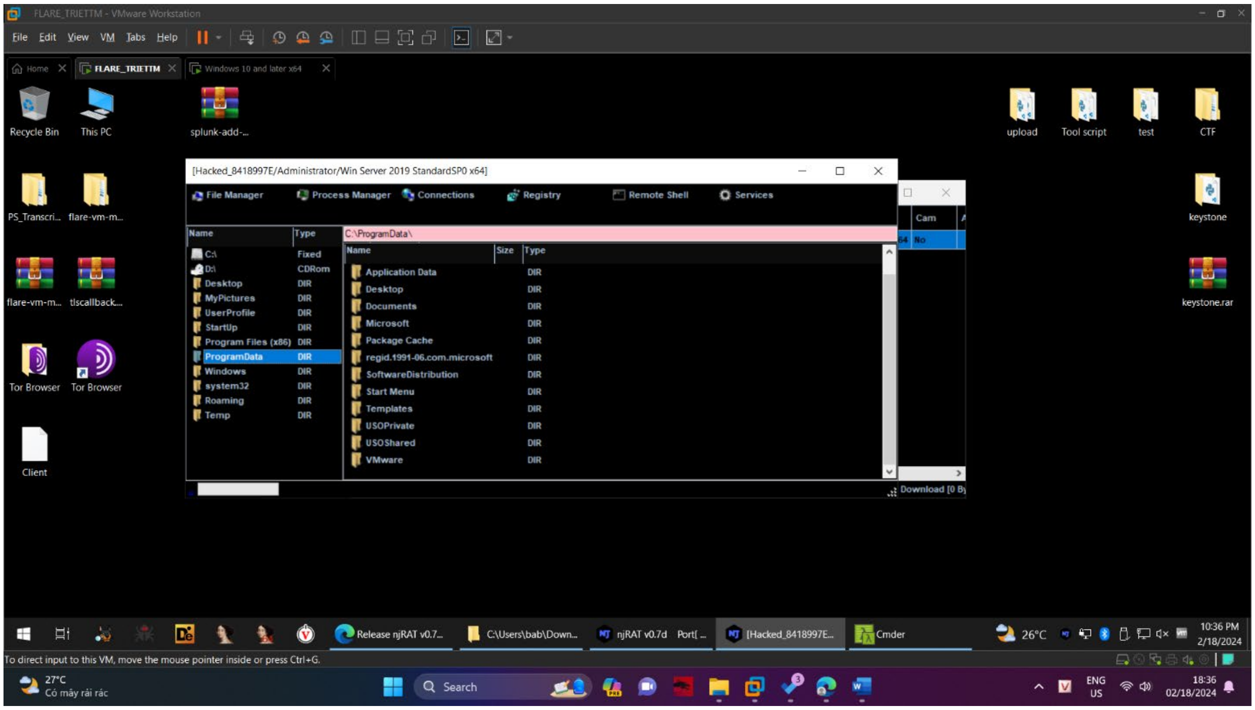
njRAT v0.7d Port[6522] Online[1] Selected[1] REQ[0]

Scre	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	A
	Hacked_8418997E	192.168.159.218	WIN-TA2QS8R3NFB	Administrator	24-02-18		N/A	Win Server 2019 StandardSP0 x64	No	

[Logs] [Builder] [Settings] [Assembly] [NO-IP] [About]

Connections[1] Upload [0 Bytes] Download [0 By


FLARE_TRIETTM - VMware Workstation
njRAT v0.7d Port[6522] Online[1] Selected[1] REQ[0]
Manager
Run File
Remote Desktop
Remote Cam
Microphone
Get Passwords
Keylogger
Open Chat
Server
Open Folder
[Logs] [Builder]
[About]
Connections[1] Upload [0 Bytes] Download [0 By

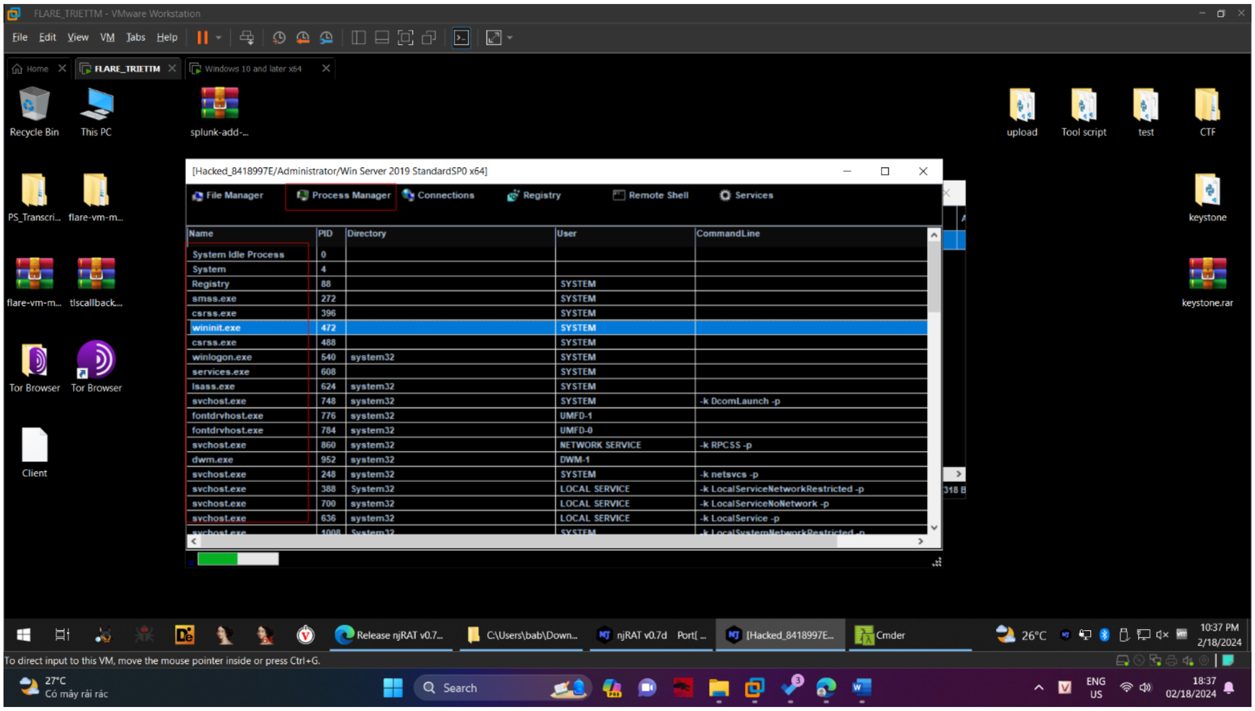


[Hacked_8418997E/Administrator/Win Server 2019 StandardSP0 x64]

Name	Type
C:\	Fixed
D:\	CDRom
Desktop	DIR
MyPictures	DIR
UserProfile	DIR
StartUp	DIR
Program Files (x86)	DIR
ProgramData	DIR
Windows	DIR
system32	DIR
Roaming	DIR
Temp	DIR

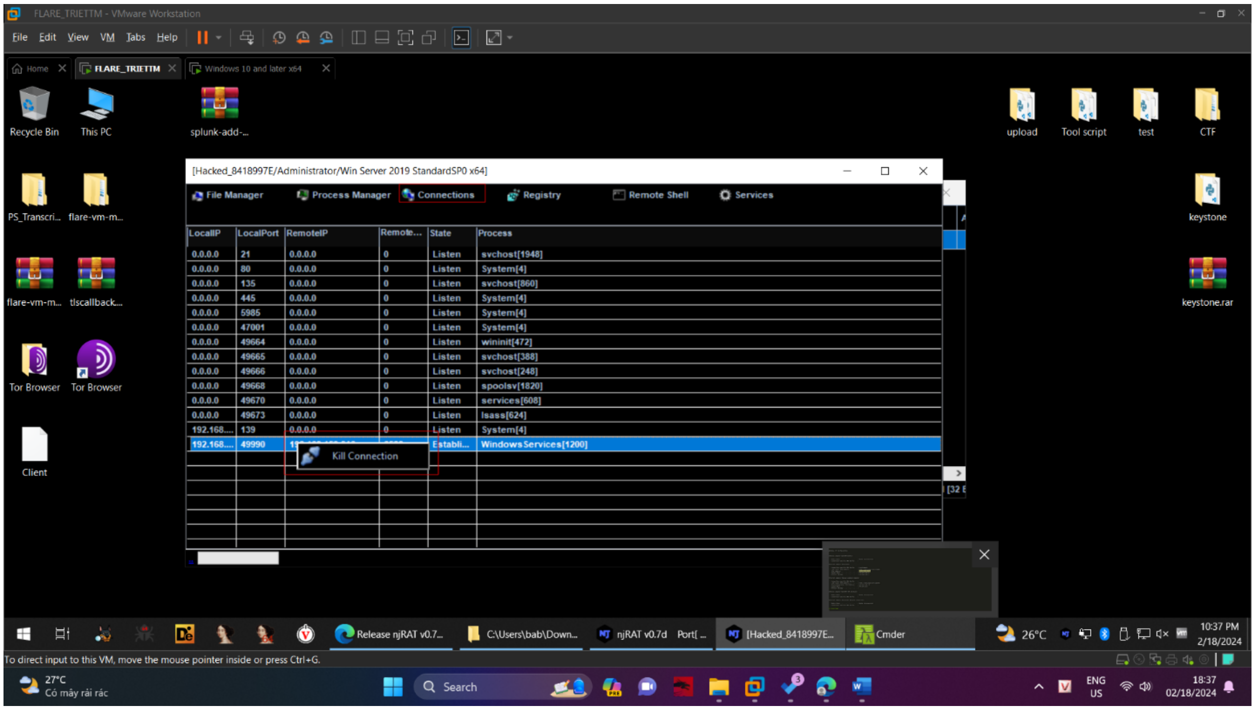
C:\ProgramData\

Name	Size	Type
Application Data		DIR
Desktop		DIR
Documents		DIR
Microsoft		DIR
Package Cache		DIR
regid.1991-06.com.microsoft		DIR
SoftwareDistribution		DIR
Start Menu		DIR
Templates		DIR
USOPrivate		DIR
USOShared		DIR
VMware		DIR



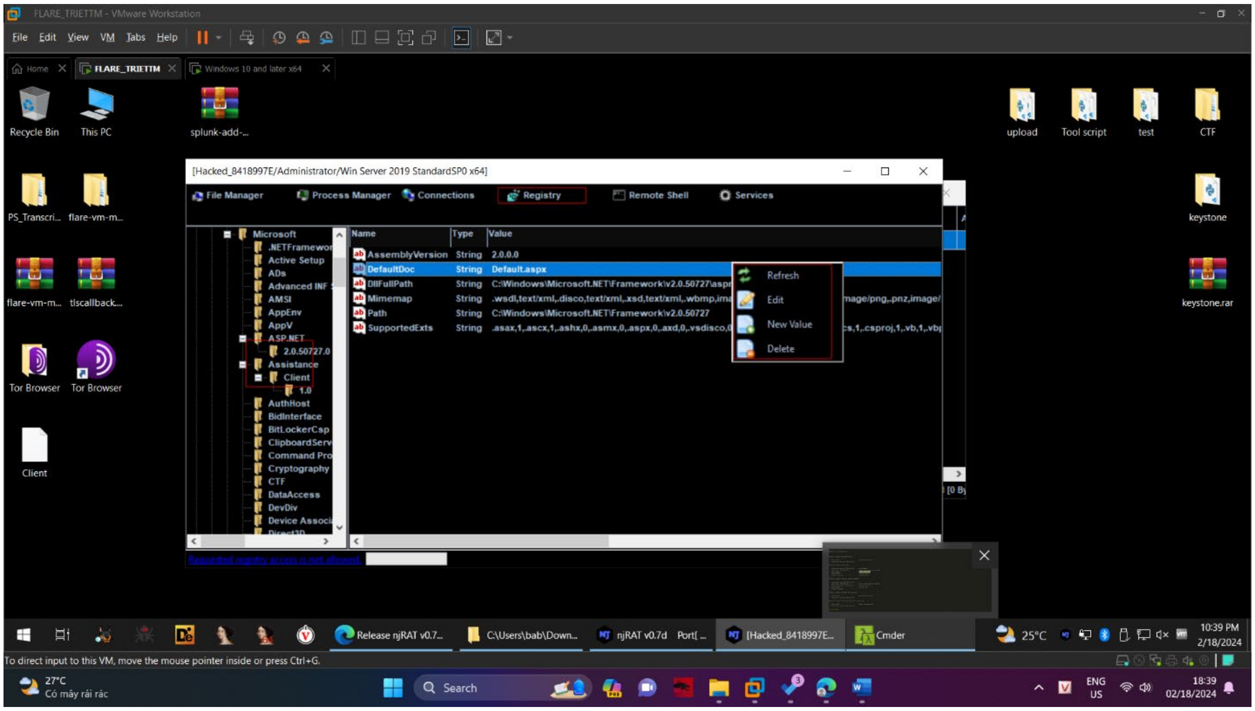
[Hacked_8418997E/Administrator/Win Server 2019 StandardSP0 x64]

Name	PID	Directory	User	CommandLine
System Idle Process	0			
System	4			
Registry	88		SYSTEM	
smss.exe	272		SYSTEM	
csrss.exe	396		SYSTEM	
wininit.exe	472		SYSTEM	
csrss.exe	488		SYSTEM	
winlogon.exe	540	system32	SYSTEM	
services.exe	608		SYSTEM	
lsass.exe	624	system32	SYSTEM	
svchost.exe	748	system32	SYSTEM	-k DcomLaunch -p
fontdrvhost.exe	776	system32	UMFD-1	
fontdrvhost.exe	784	system32	UMFD-0	
svchost.exe	860	system32	NETWORK SERVICE	-k RPCSS -p
dwm.exe	952	system32	DWM-1	
svchost.exe	248	system32	SYSTEM	-k netsvcs -p
svchost.exe	388	System32	LOCAL SERVICE	-k LocalServiceNetworkRestricted -p
svchost.exe	700	system32	LOCAL SERVICE	-k LocalServiceNoNetwork -p
svchost.exe	636	system32	LOCAL SERVICE	-k LocalService -p
svchost.exe	1008	System32	SYSTEM	-k LocalSystemNetworkRestricted -p



[Hacked_8418997E/Administrator/Win Server 2019 StandardSP0 x64]

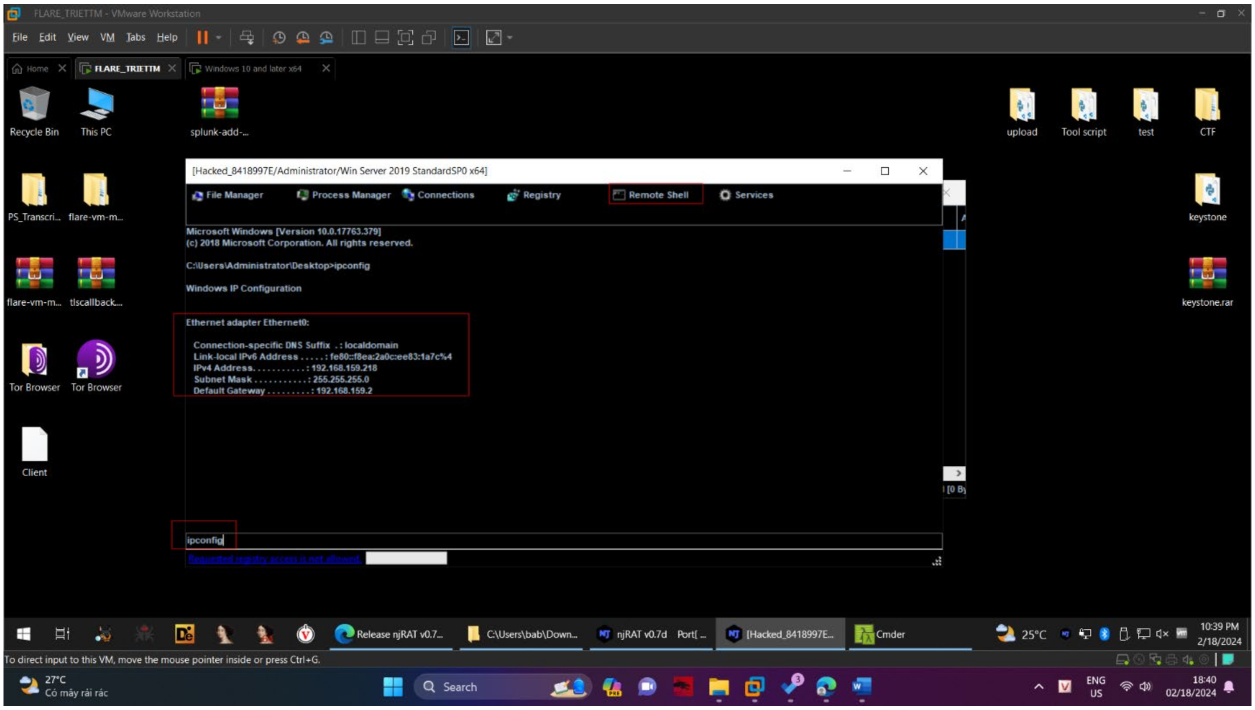
LocalIP	LocalPort	RemoteIP	Remote...	State	Process
0.0.0.0	21	0.0.0.0	0	Listen	svchost[1948]
0.0.0.0	80	0.0.0.0	0	Listen	System[4]
0.0.0.0	135	0.0.0.0	0	Listen	svchost[860]
0.0.0.0	445	0.0.0.0	0	Listen	System[4]
0.0.0.0	5985	0.0.0.0	0	Listen	System[4]
0.0.0.0	47001	0.0.0.0	0	Listen	System[4]
0.0.0.0	49664	0.0.0.0	0	Listen	wininit[472]
0.0.0.0	49665	0.0.0.0	0	Listen	svchost[388]
0.0.0.0	49666	0.0.0.0	0	Listen	svchost[248]
0.0.0.0	49668	0.0.0.0	0	Listen	spoolsv[1820]
0.0.0.0	49670	0.0.0.0	0	Listen	services[608]
0.0.0.0	49673	0.0.0.0	0	Listen	lsass[624]
192.168....	139	0.0.0.0	0	Listen	System[4]
192.168....	49990	19		Establi...	WindowsServices[1200]



[Hacked_8418997E/Administrator/Win Server 2019 StandardSP0 x64]

Name	Type	Value
AssemblyVersion	String	2.0.0.0
DefaultDoc	String	Default.aspx
DllFullPath	String	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspr
Mimemap	String	.wsdl,text/xml,.disco,text/xml,.xsd,text/xml,.wbmp,ima ... mage/png,.pnz,image/
Path	String	C:\Windows\Microsoft.NET\Framework\v2.0.50727
SupportedExts	String	.asax,1,.ascx,1,.ashx,0,.asmx,0,.aspx,0,.axd,0,.vsdisco,0 ... cs,1,.csproj,1,.vb,1,.vbp

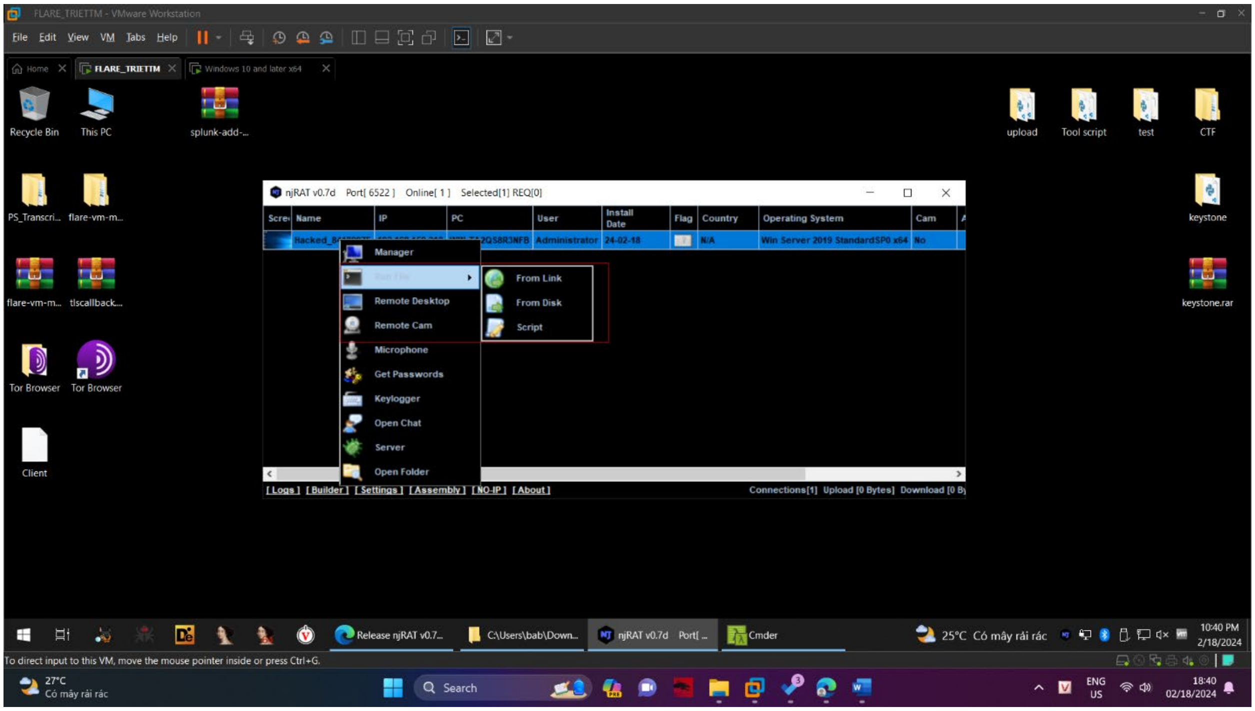
Requested registry access is not allowed.



[Hacked_8418997E/Administrator/Win Server 2019 StandardSP0 x64]

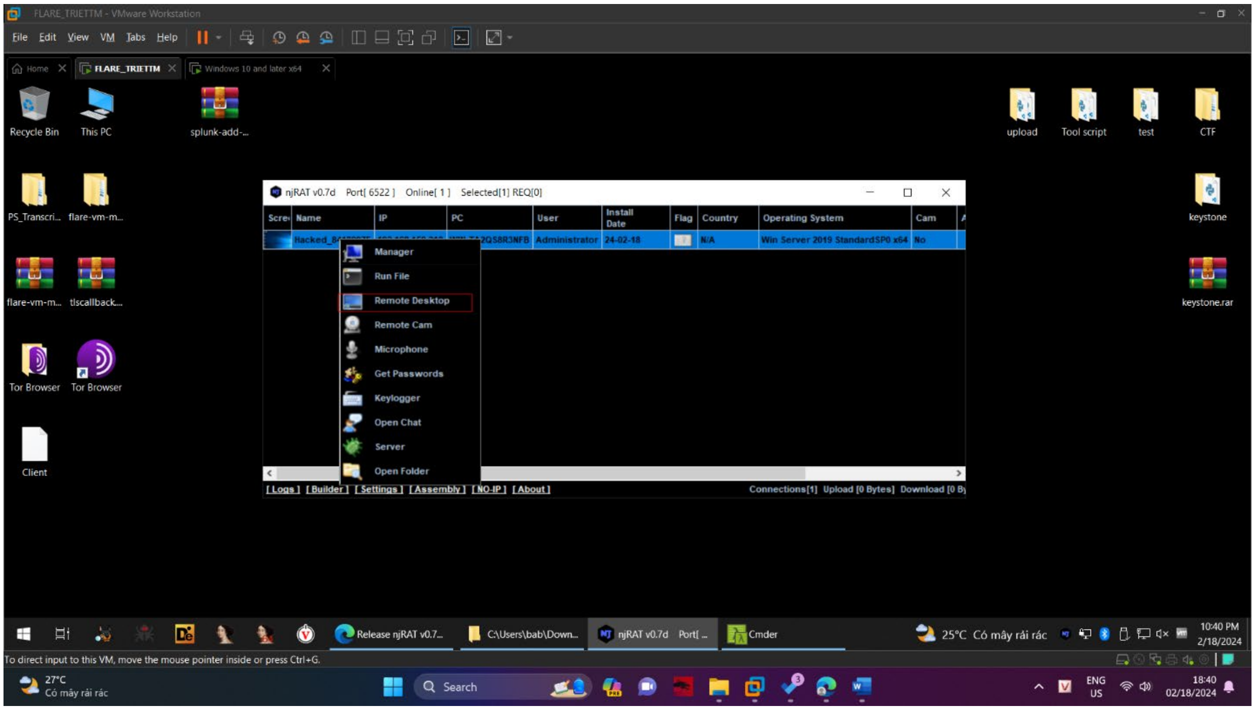
```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::f8ea:2a0c:ee83:1a7c%4
   IPv4 Address. . . . . . . . . . . : 192.168.159.218
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.159.2
```

```
ipconfig
```



njRAT v0.7d Port[6522] Online[1] Selected[1] REQ[0]

Scre	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam
	Hacked_8		2QS8R3NFB	Administrator	24-02-18		N/A	Win Server 2019 StandardSP0 x64	No

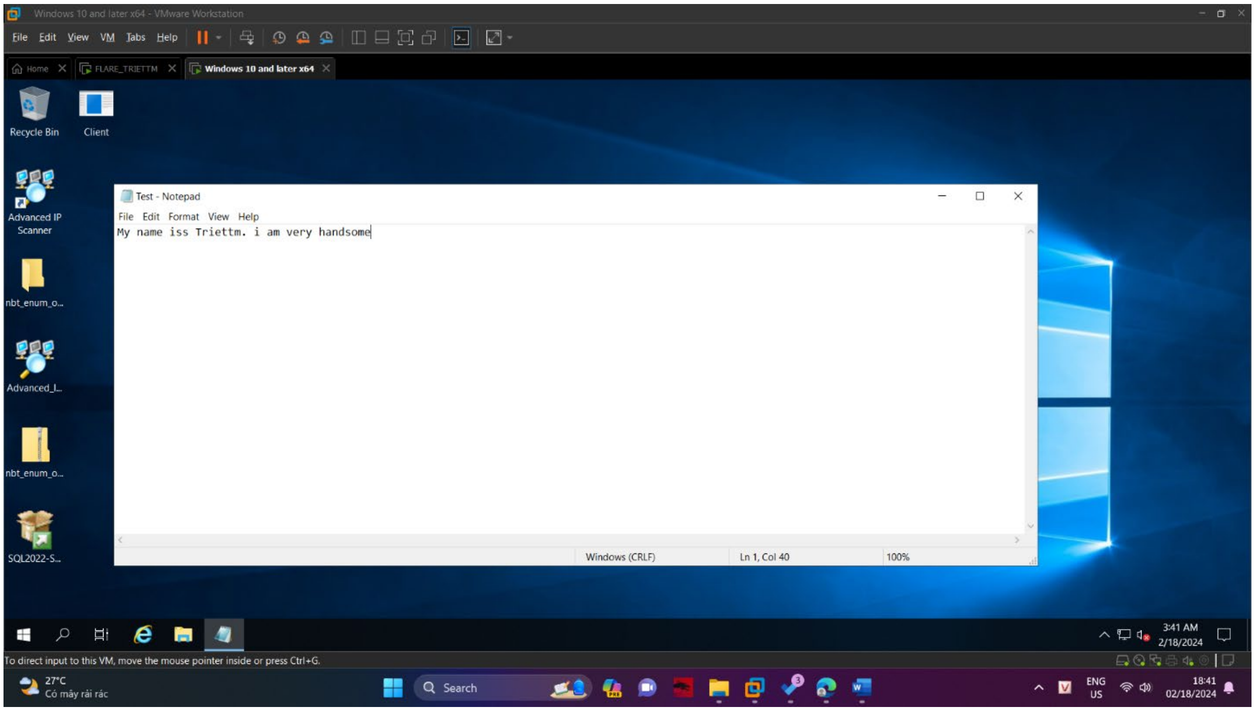


FLARE_TRIETTM - VMware Workstation

njRAT v0.7d Port[6522] Online[1] Selected[1] REQ[0]

Scre	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam
	Hacked_8		TA2QS8R3NFB	Administrator	24-02-18		N/A	Win Server 2019 StandardSP0 x64	No

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



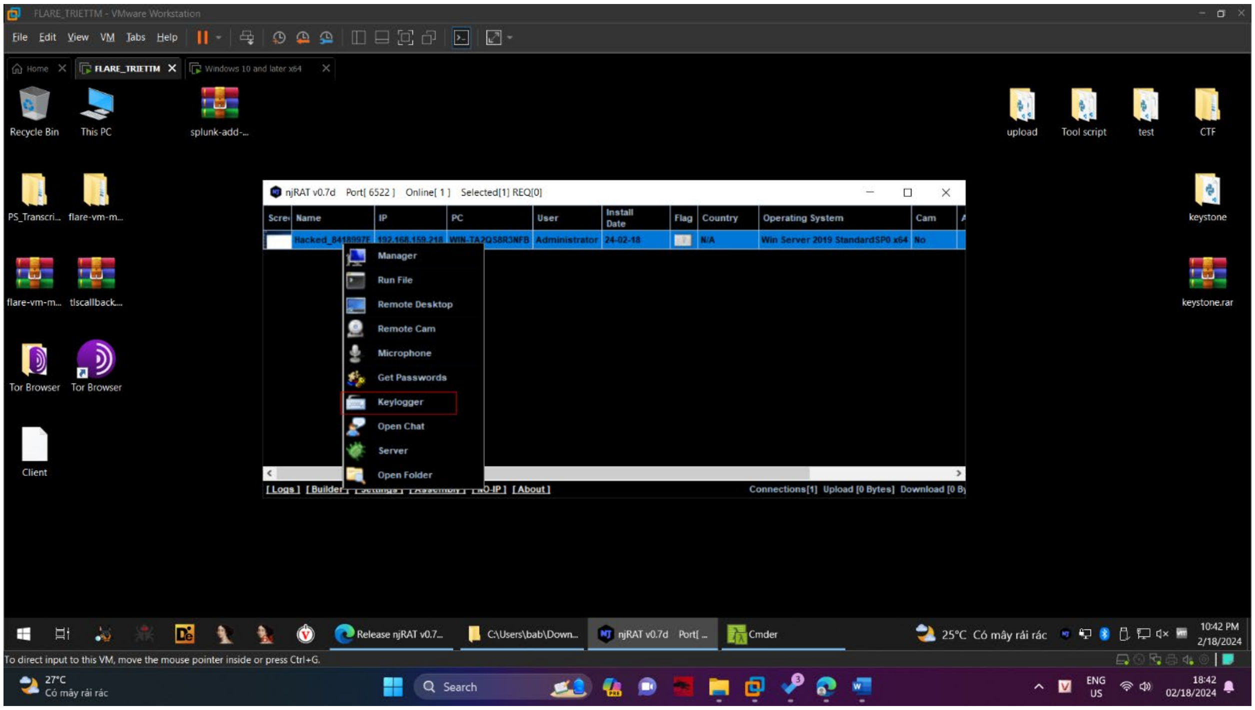
Windows 10 and later x64 - VMware Workstation

Test - Notepad

```
My name iss Triettm. i am very handsome
```

Windows (CRLF) Ln 1, Col 40 100%

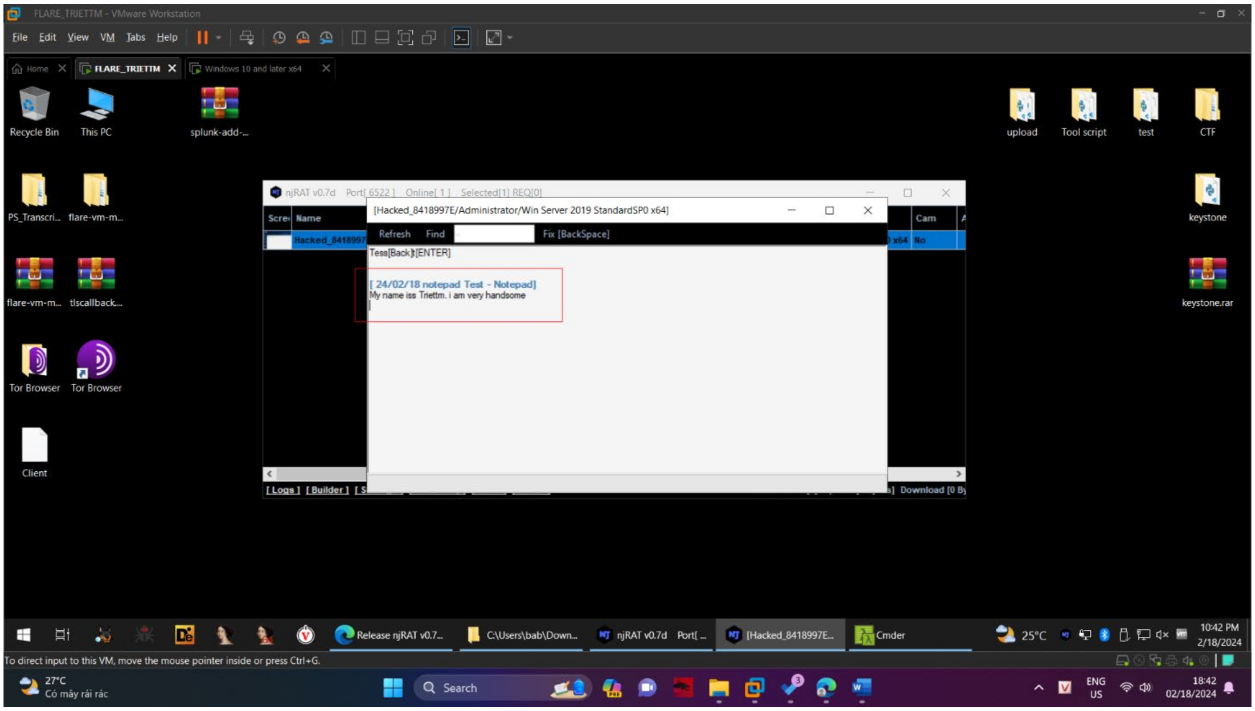
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



njRAT v0.7d Port[6522] Online[1] Selected[1] REQ[0]

Scre	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam
	Hacked_8418997E	192.168.159.218	WIN-TA2QS8R3NFB	Administrator	24-02-18		N/A	Win Server 2019 StandardSP0 x64	No

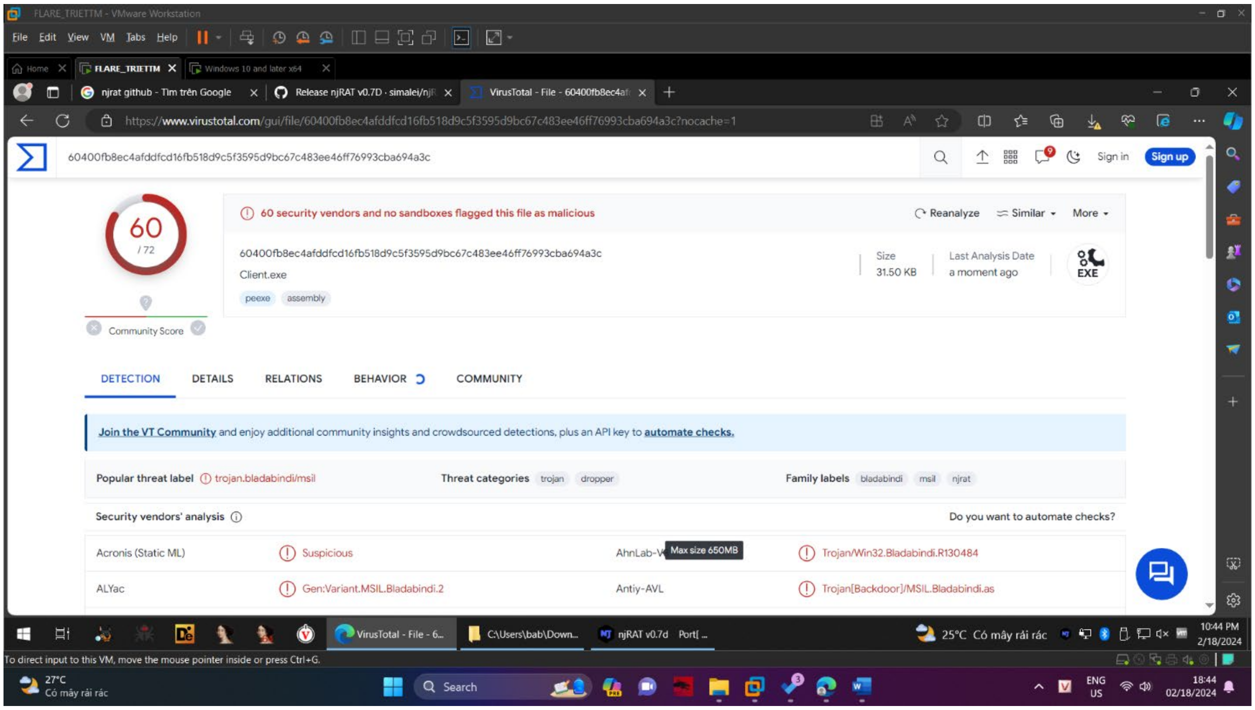
Connections[1] Upload [0 Bytes] Download [0 B



[Hacked_8418997E/Administrator/Win Server 2019 StandardSP0 x64]

```
Tess[Back]t[ENTER]

[ 24/02/18 notepad Test - Notepad]
My name iss Triettm. i am very handsome
```

Hide a Trojan using SwayzCryptor and Make it Undetectable to various AV Programs



https://www.virustotal.com/gui/file/60400fb8ec4afddfcd16fb518d9c5f3595d9bc67c483ee46ff76993cba694a3c?nocache=1

60400fb8ec4afddfcd16fb518d9c5f3595d9bc67c483ee46ff76993cba694a3c

60 / 72

Community Score

60 security vendors and no sandboxes flagged this file as malicious

60400fb8ec4afddfcd16fb518d9c5f3595d9bc67c483ee46ff76993cba694a3c
Client.exe
peexe assembly

Size 31.50 KB

Last Analysis Date a moment ago

EXE

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.bladabindi/msil

Threat categories trojan dropper

Family labels bladabindi msil njrat

Security vendors' analysis

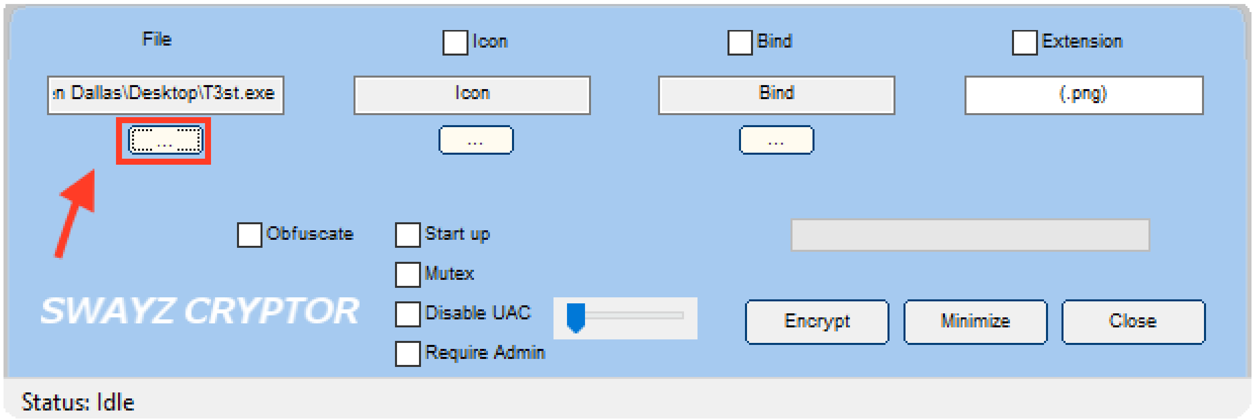
Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V Max size 650MB	Trojan/Win32.Bladabindi.R130484
ALYac	Gen:Variant.MSIL.Bladabindi.2	Antiy-AVL	Trojan[Backdoor]/MSIL.Bladabindi.as

25°C Có mây rải rác 10:44 PM 2/18/2024

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

27°C Có mây rải rác 18:44 02/18/2024



File | □ Icon | □ Bind | □ Extension

:n Dallas\Desktop\T3st.exe | Icon | Bind | (.png)

□ Obfuscate

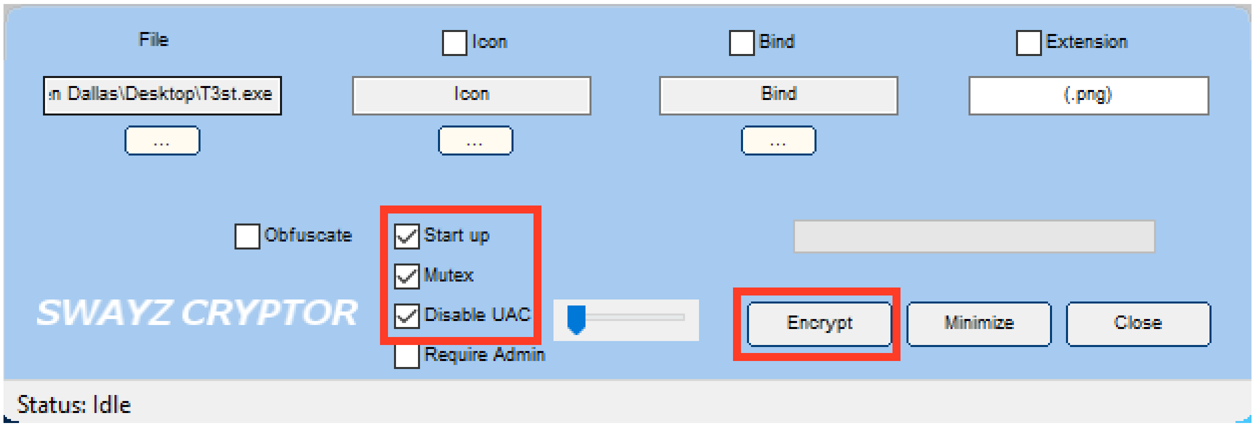
□ Start up

□ Mutex

□ Disable UAC

□ Require Admin

Status: Idle



File | □ Icon | □ Bind | □ Extension

:n Dallas\Desktop\T3st.exe | Icon | Bind | (.png)

□ Obfuscate

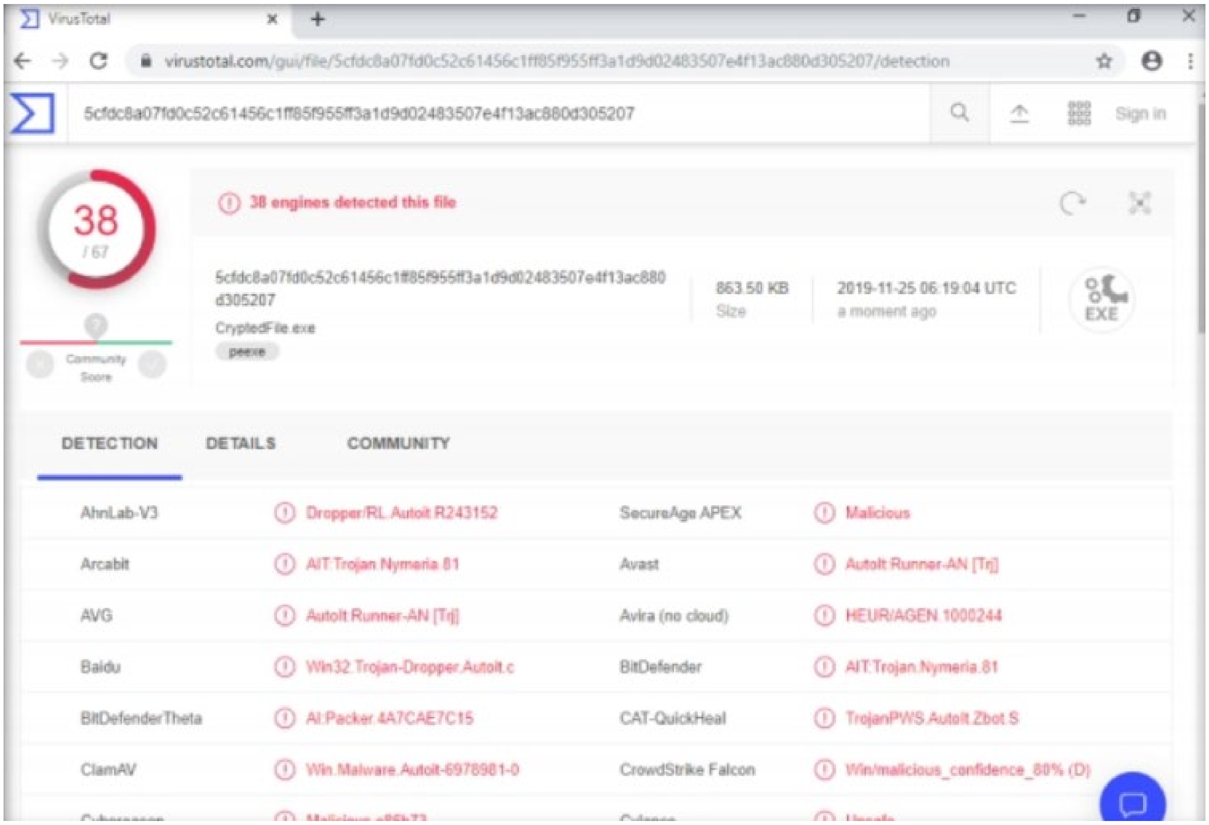
☑ Start up

☑ Mutex

☑ Disable UAC

□ Require Admin

Status: Idle



virustotal.com/gui/file/5cfdc8a07fd0c52c61456c1ff85f955ff3a1d9d02483507e4f13ac880d305207/detection

5cfdc8a07fd0c52c61456c1ff85f955ff3a1d9d02483507e4f13ac880d305207

38 / 67

38 engines detected this file

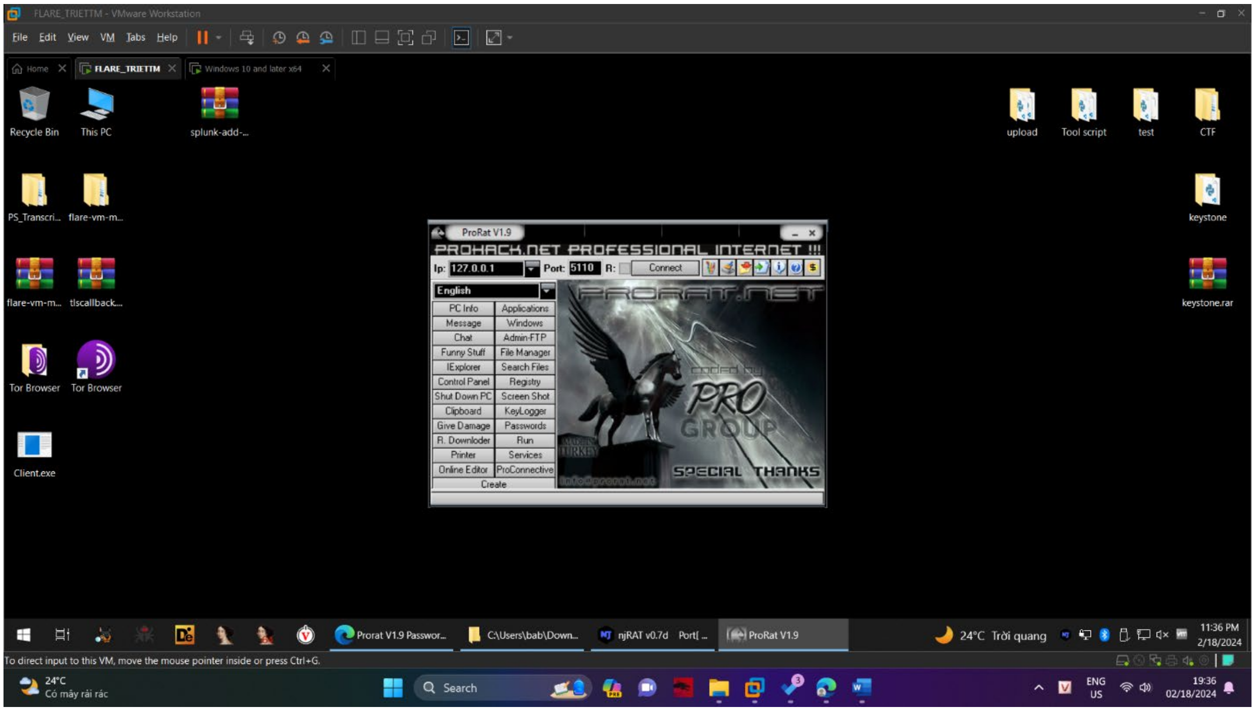
5cfdc8a07fd0c52c61456c1ff85f955ff3a1d9d02483507e4f13ac880d305207
CryptedFile.exe
peexe

863.50 KB
Size

2019-11-25 06:19:04 UTC
a moment ago

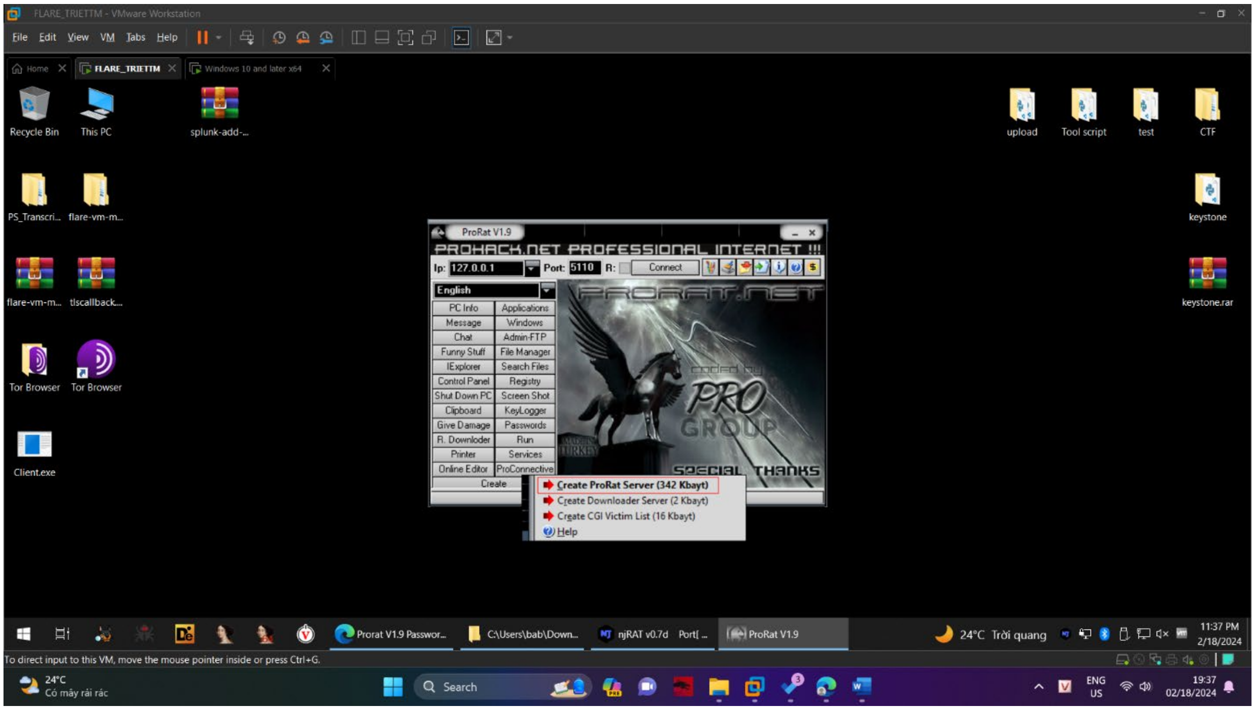
AhnLab-V3	Dropper/RL.AutoIt.R243152	SecureAge APEX	Malicious
Arcabit	AIT:Trojan.Nymeria.81	Avast	AutoIt:Runner-AN [Trj]
AVG	AutoIt:Runner-AN [Trj]	Avira (no cloud)	HEUR/AGEN.1000244
Baidu	Win32.Trojan-Dropper.AutoIt.c	BitDefender	AIT:Trojan.Nymeria.81
BitDefenderTheta	AI:Packer.4A7CAE7C15	CAT-QuickHeal	TrojanPWS.AutoIt.Zbot.S
ClamAV	Win.Malware.Autoit-6978981-0	CrowdStrike Falcon	Win/malicious_confidence_80% (D)

Create a server using Prorat tools

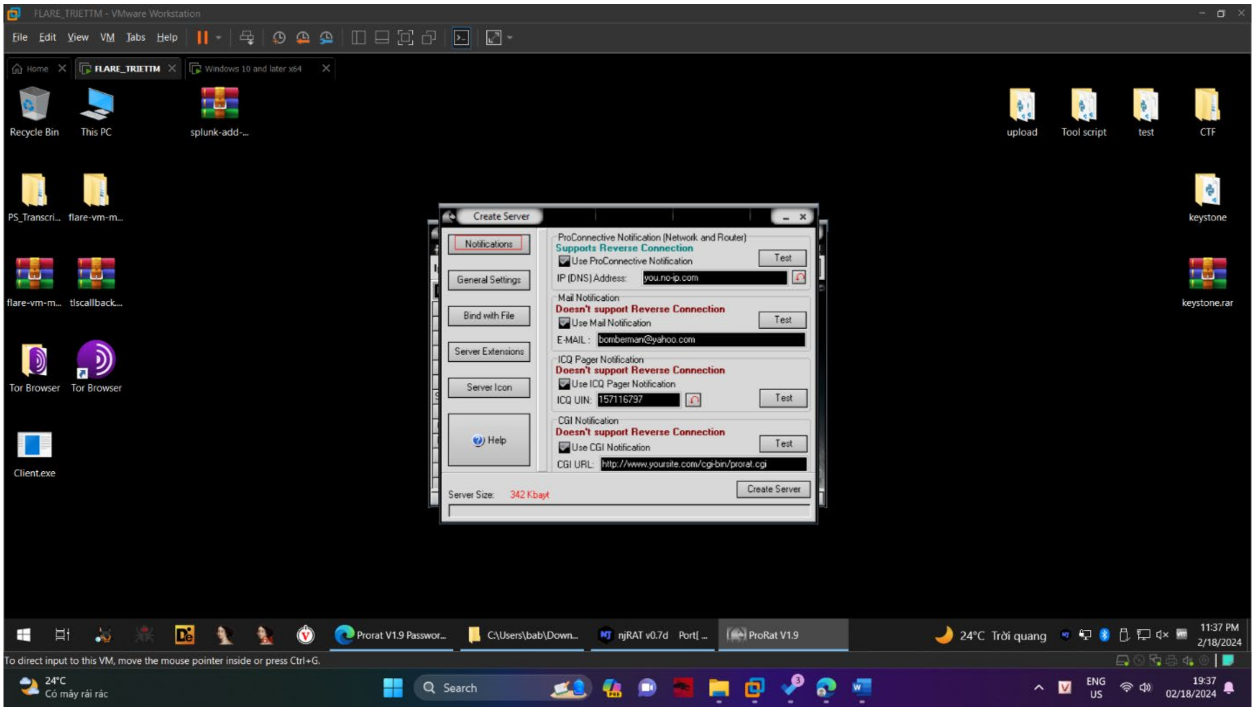


Ip: 127.0.0.1 Port: 5110 R:

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Ip: 127.0.0.1
Port: 5110
R:
English



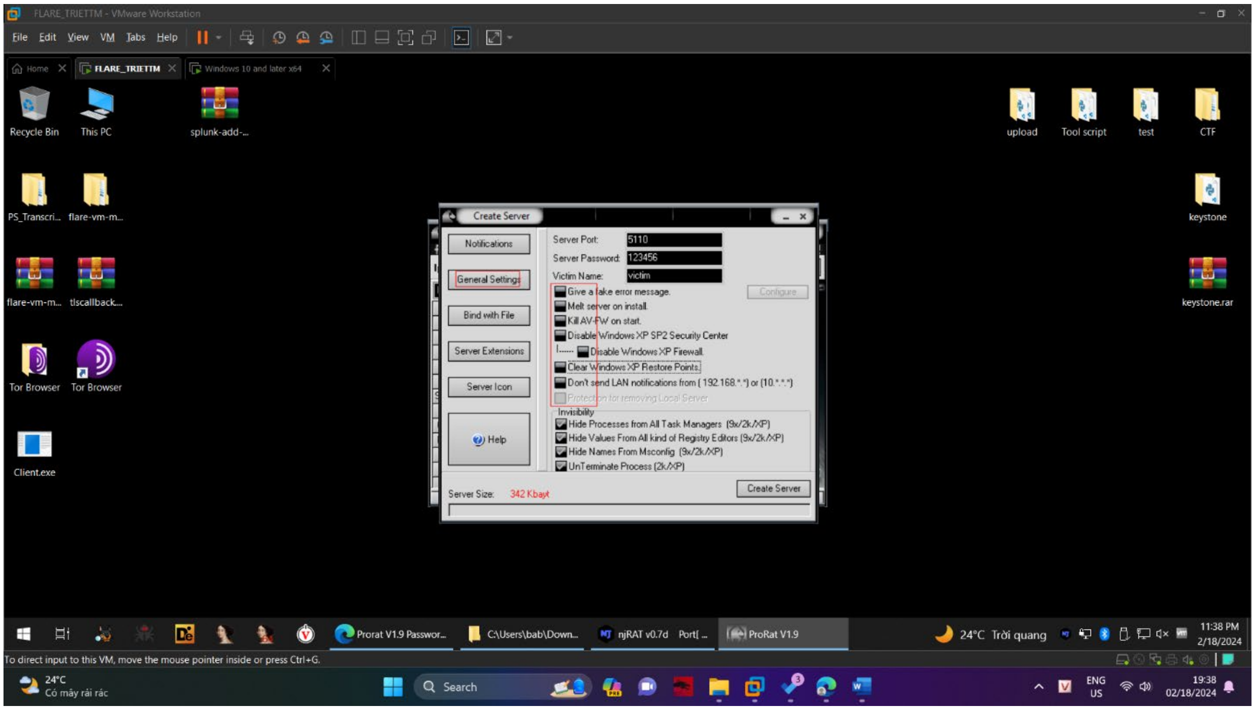
ProConnective Notification (Network and Router)
Supports Reverse Connection
☑ Use ProConnective Notification
IP (DNS) Address: you.no-ip.com

Mail Notification
Doesn't support Reverse Connection
☑ Use Mail Notification
E-MAIL : bomberman@yahoo.com

ICQ Pager Notification
Doesn't support Reverse Connection
☑ Use ICQ Pager Notification
ICQ UIN: 157116797

CGI Notification
Doesn't support Reverse Connection
☑ Use CGI Notification
CGI URL: http://www.yoursite.com/cgi-bin/prorat.cgi

Server Size: 342 Kbayt



Create Server

Server Port: 5110

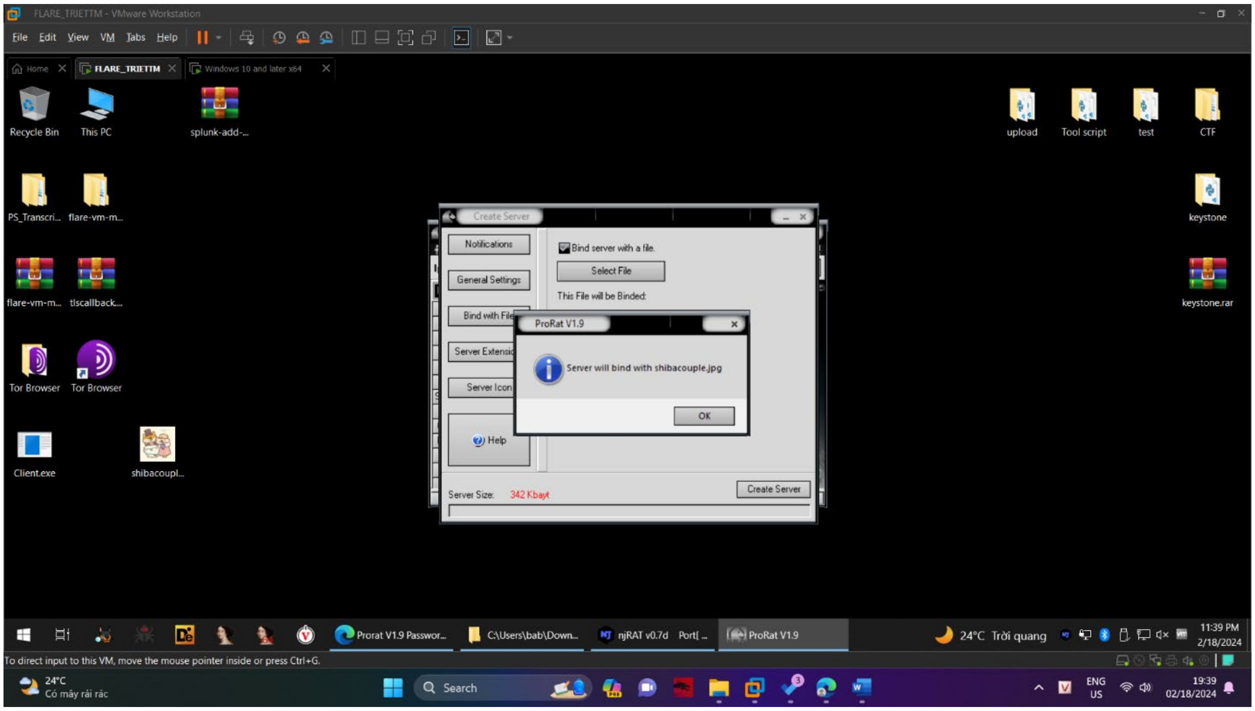
Server Password: 123456

Victim Name: victim

☐ Give a fake error message.
☐ Melt server on install.
☐ Kill AV-FW on start.
☐ Disable Windows XP SP2 Security Center
|...... ☐ Disable Windows XP Firewall.
☐ Clear Windows XP Restore Points.
☐ Don't send LAN notifications from (192.168.*.*) or (10.*.*.*)
☐ Protection for removing Local Server

Invisibility
☑ Hide Processes from All Task Managers (9x/2k/XP)
☑ Hide Values From All kind of Registry Editors (9x/2k/XP)
☑ Hide Names From Msconfig (9x/2k/XP)
☑ UnTerminate Process (2k/XP)

Server Size: 342 Kbayt



Create Server

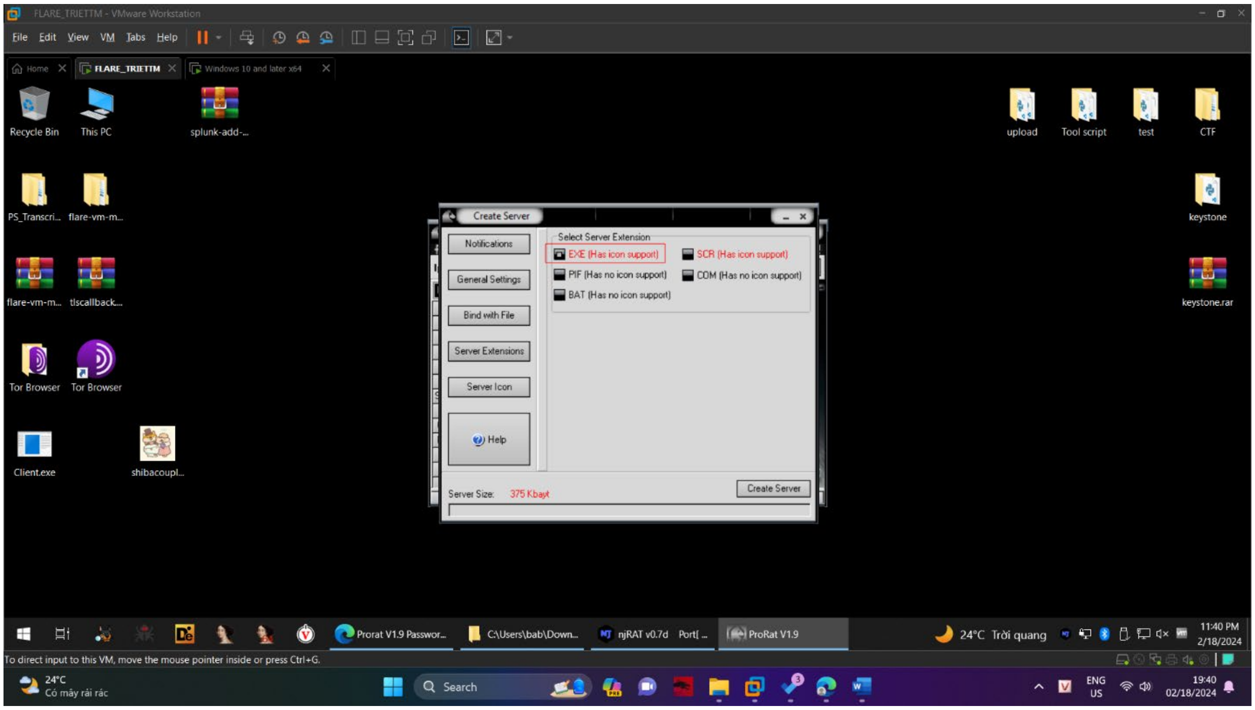
☑ Bind server with a file.

This File will be Binded:

ProRat V1.9

Server will bind with shibacouple.jpg

Server Size: 342 Kbayt



Create Server

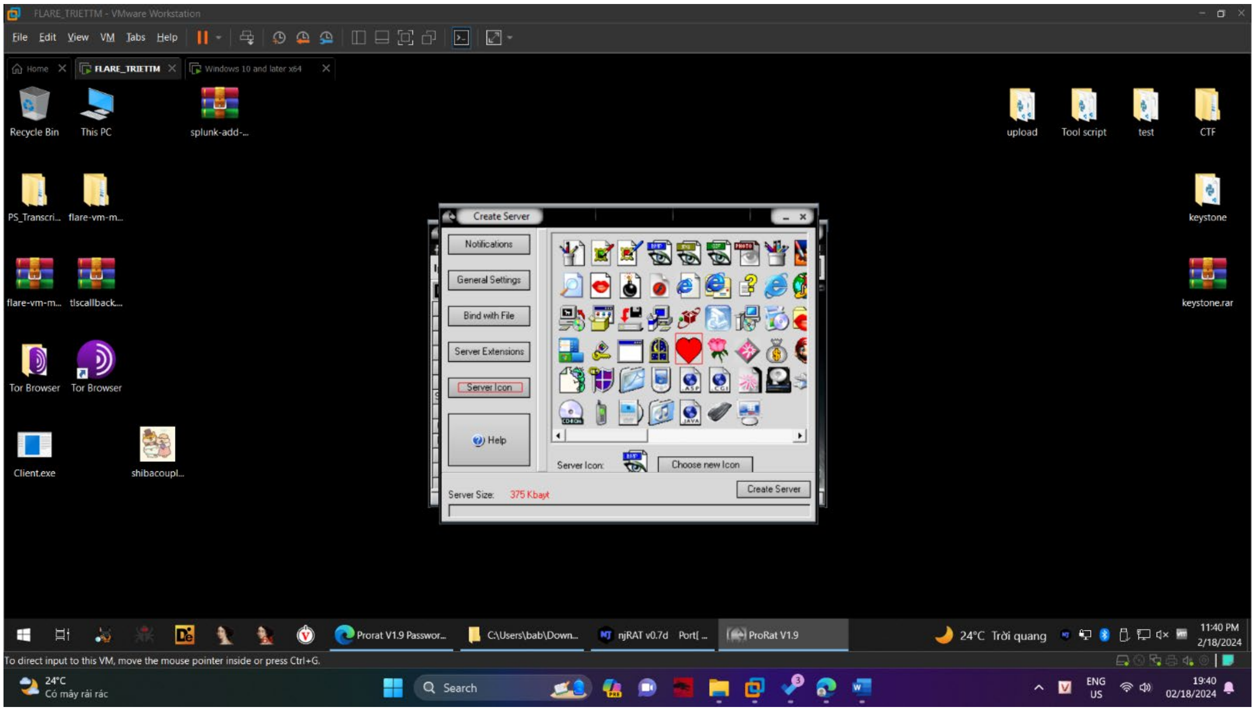
Select Server Extension

● EXE (Has icon support)   ○ SCR (Has icon support)

○ PIF (Has no icon support)   ○ COM (Has no icon support)

○ BAT (Has no icon support)

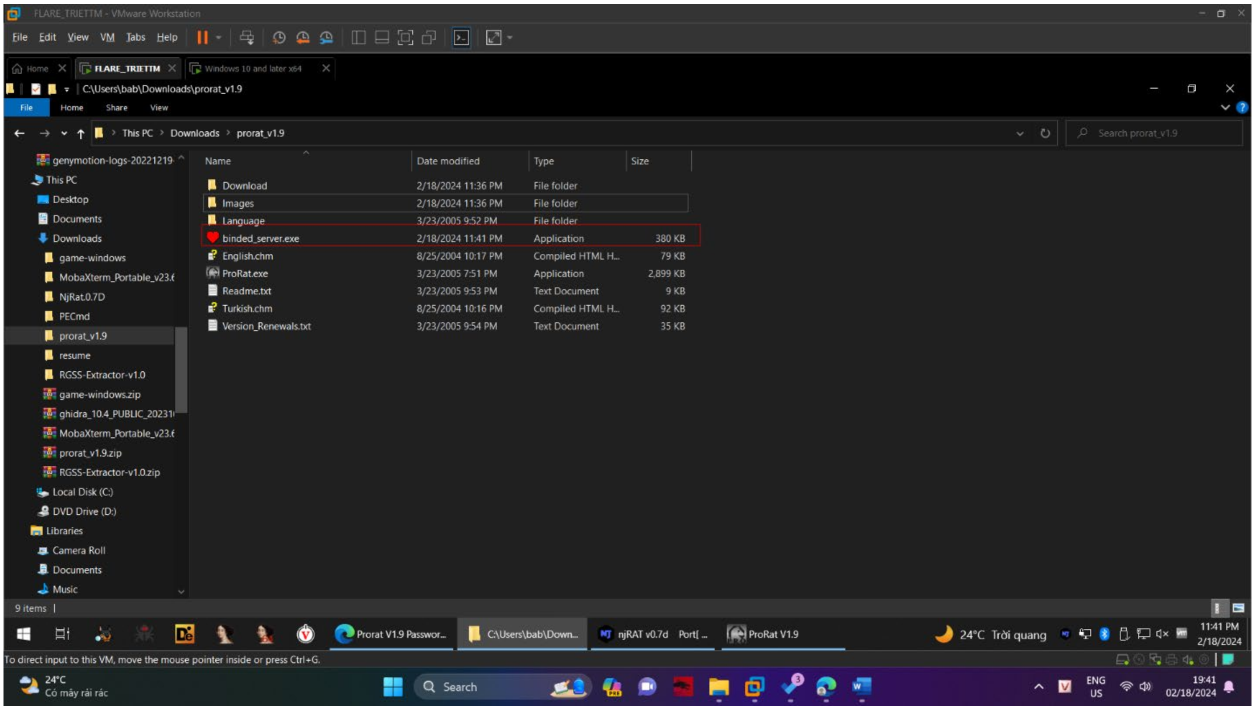
Server Size: 375 Kbayt



Create Server

Server Icon:

Server Size: 375 Kbayt

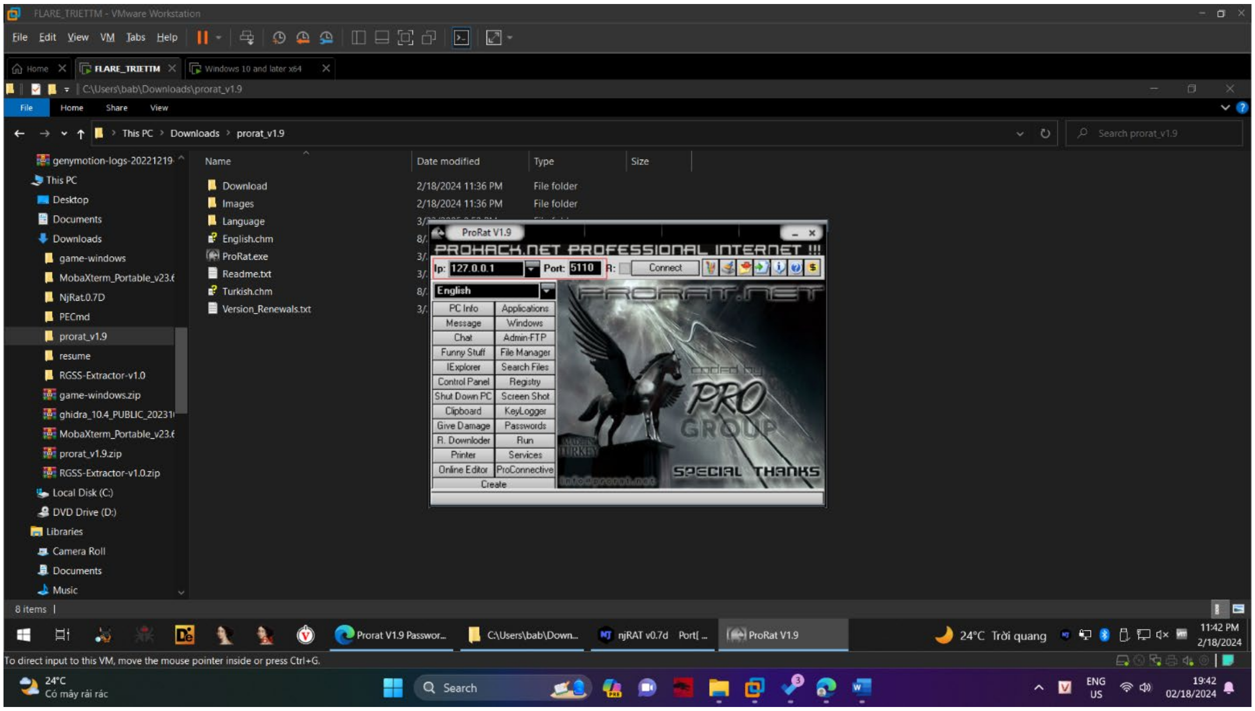


C:\Users\bab\Downloads\prorat_v1.9

This PC › Downloads › prorat_v1.9

Name	Date modified	Type	Size
Download	2/18/2024 11:36 PM	File folder	
Images	2/18/2024 11:36 PM	File folder	
Language	3/23/2005 9:52 PM	File folder	
binded_server.exe	2/18/2024 11:41 PM	Application	380 KB
English.chm	8/25/2004 10:17 PM	Compiled HTML H...	79 KB
ProRat.exe	3/23/2005 7:51 PM	Application	2,899 KB
Readme.txt	3/23/2005 9:53 PM	Text Document	9 KB
Turkish.chm	8/25/2004 10:16 PM	Compiled HTML H...	92 KB
Version_Renewals.txt	3/23/2005 9:54 PM	Text Document	35 KB

9 items



C:\Users\bab\Downloads\prorat_v1.9

This PC › Downloads › prorat_v1.9

Name	Date modified	Type
Download	2/18/2024 11:36 PM	File folder
Images	2/18/2024 11:36 PM	File folder
Language		
English.chm		
ProRat.exe		
Readme.txt		
Turkish.chm		
Version_Renewals.txt		

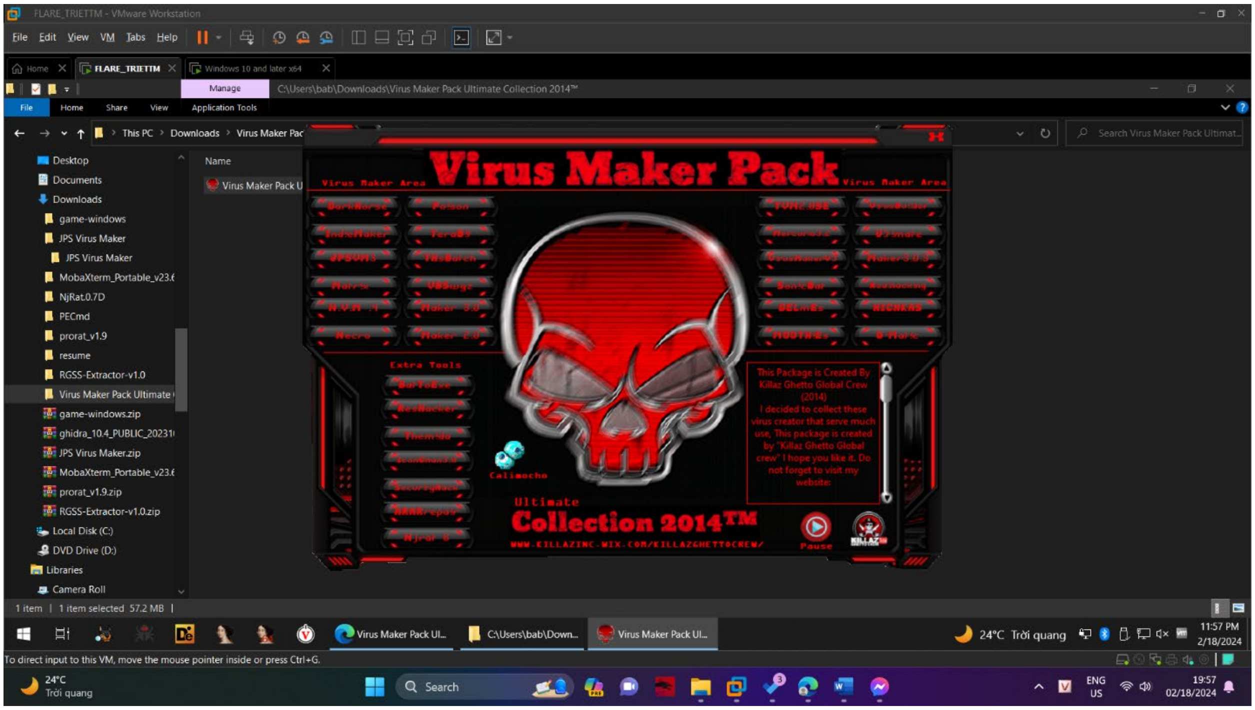
8 items

ProRat V1.9

Ip: 127.0.0.1 Port: 5110

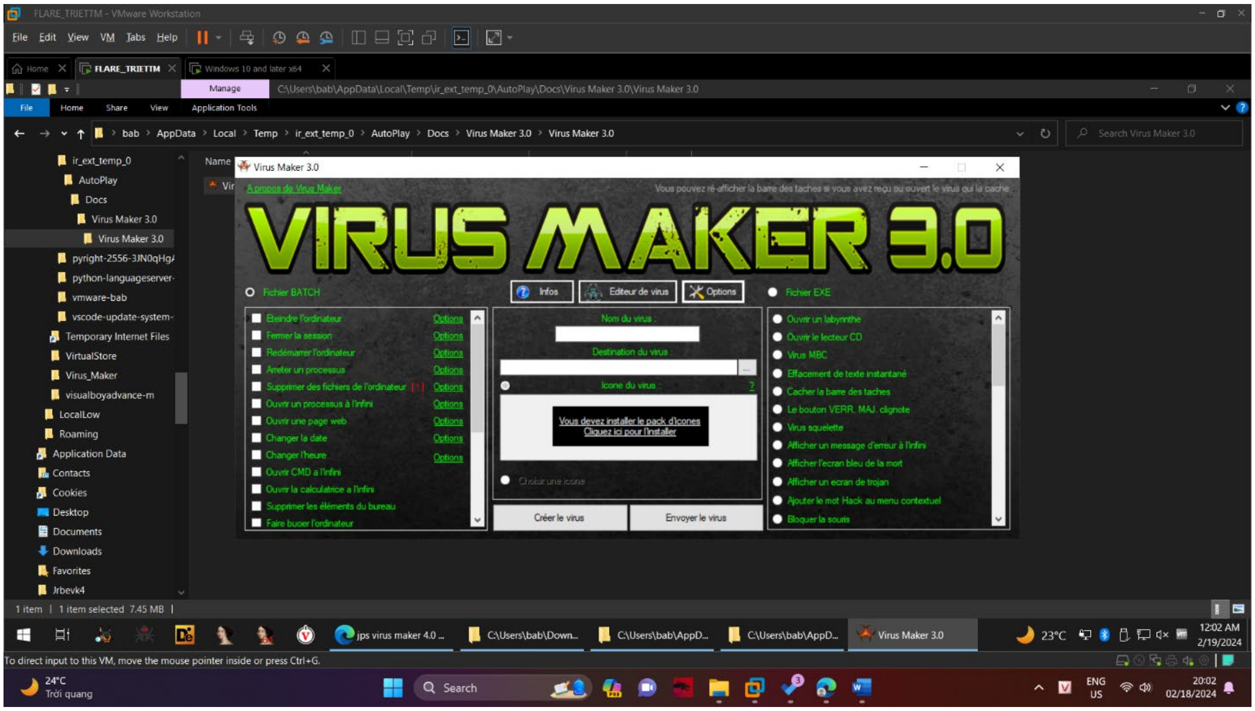
Infected the target system using a virus

Create a Virus using the JPS Virus Maker Tool and infect the target system



C:\Users\bab\Downloads\Virus Maker Pack Ultimate Collection 2014™

This Package is Created By Killaz Ghetto Global Crew (2014)
I decided to collect these virus creator that serve much use, This package is created by "Killaz Ghetto Global crew" I hope you like it. Do not forget to visit my website:



C:\Users\bab\AppData\Local\Temp\ir_ext_temp_0\AutoPlay\Docs\Virus Maker 3.0\Virus Maker 3.0

A propos de Virus Maker

Vous pouvez ré-afficher la barre des taches si vous avez reçu ou ouvert le virus qui la cache

○ Fichier BATCH | Infos | Editeur de virus | Options | ● Fichier EXE

- □ Eteindre l'ordinateur — Options
- □ Fermer la session — Options
- □ Redémarrer l'ordinateur — Options
- □ Arreter un processus — Options
- □ Supprimer des fichiers de l'ordinateur [!] — Options
- □ Ouvrir un processus à l'infini — Options
- □ Ouvrir une page web — Options
- □ Changer la date — Options
- □ Changer l'heure — Options
- □ Ouvrir CMD a l'infini
- □ Ouvrir la calculatrice a l'infini
- □ Supprimer les éléments du bureau
- □ Faire buoer l'ordinateur

Nom du virus :

Destination du virus :

○ Icone du virus : ?

Vous devez installer le pack d'icones
Cliquez ici pour l'installer

○ Choisir une icone

Créer le virus | Envoyer le virus

- ○ Ouvrir un labyrinthe
- ○ Ouvrir le lecteur CD
- ○ Virus MBC
- ○ Effacement de texte instantané
- ○ Cacher la barre des taches
- ○ Le bouton VERR. MAJ. clignote
- ○ Virus squelette
- ○ Afficher un message d'erreur à l'infini
- ○ Afficher l'ecran bleu de la mort
- ○ Afficher un ecran de trojan
- ○ Ajouter le mot Hack au menu contextuel
- ○ Bloquer la souris