

Forum:[Hack Forums](#)

Thread: [How to hide RAT from task manager?](#)

Cyamic - March 21, 2019, 6:19 pm

Hello. I am fairly new to ratting and I only know the basics to it like crypting and port forwarding to setup the rat. I am wondering if there is any way to hide the rat I have created from the victims task manager. I am trying to not let my rat show up so its not obvious. Is there anything I can do to hide this? Anything would help me, thanks :).

I.M.P - March 21, 2019, 6:24 pm

I assume that

- A. You have the source code (or can edit the stubs code in some way) to this rat
- B. Your okay with loosing the client every time they open task manager
- C. Have some FUD watchdog program to keep the task alive after they close task manager

Assuming all these conditions are met it should be fairly simple

SoonTM - March 21, 2019, 8:22 pm

A rootkit would do the trick.

Silent hill - March 23, 2019, 2:56 am

(Mar 21, 2019 06:24 PM)Atroxcity Wrote: [\[CITE\]](#) I assume that

- A. You have the source code (or can edit the stubs code in some way) to this rat
- B. Your okay with loosing the client every time they open task manager
- C. Have some FUD watchdog program to keep the task alive after they close task manager

Assuming all these conditions are met it should be fairly simple
100% d) also you can inject it into any legit process.

NYANxCAT - March 23, 2019, 4:25 am

the simplest solution is to make your RAT kill itself every time task manager is open.
then start your RAT again using windows task schedule.
It's very simple and basic.

iCoreX - March 23, 2019, 6:58 am

(Mar 23, 2019 04:25 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) the simplest solution is to make your RAT kill itself every time task manager is open.
then start your RAT again using windows task schedule.
It's very simple and basic.
What do you mean with "using windows task schedule"? How can it detect that taskmanager is closed?

Onireves - March 23, 2019, 7:12 am

You can always give it a legit name and icon, and no one will suspect :)

iCoreX - March 23, 2019, 7:18 am

(Mar 23, 2019 07:12 AM)Onireves Wrote: [\[CITE\]](#) You can always give it a legit name and icon, and no one will suspect :)

True, I always name my stub "svchost" and everytime they look in taskmanager they never find it lol

Goku - March 23, 2019, 7:21 am

you guys make me paranoid...

int - March 23, 2019, 7:26 am

the real chads name their stub some fishy shit and then make it unkillable in tskmgr

WhatTheLeak - March 23, 2019, 3:01 pm

(Mar 23, 2019 04:25 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) the simplest solution is to make your RAT kill itself every time task manager is open.

then start your RAT again using windows task schedule.

It's very simple and basic.

Does any RAT has this feature? Or is it more like a crypter feature?

Zecture - March 23, 2019, 3:02 pm

The rat should be programmed as a driver

Exodus - March 23, 2019, 3:05 pm

(Mar 23, 2019 03:02 PM)Zecture Wrote: [\[CITE\]](#) The rat should be programmed as a driver

Drivers can't be installed without being digitally signed.

Zecture - March 23, 2019, 3:16 pm

(Mar 23, 2019 03:05 PM)Exodus Wrote: [\[CITE\]](#) Drivers can't be installed without being digitally signed.

Ahh Thanks never knew that. But I believe you can disable it

NYANxCAT - March 23, 2019, 3:20 pm

(Mar 23, 2019 03:01 PM)WhatTheLeak Wrote: [\[CITE\]](#) Does any RAT has this feature? Or is it more like a crypter feature?

It's just an idea, you can code it as a rat feature or crypter feature. It's simple yet efficient

RCE - March 23, 2019, 3:27 pm

(Mar 23, 2019 03:05 PM)Exodus Wrote: [\[CITE\]](#) Drivers can't be installed without being digitally signed.

Are you sure ?

Exodus - March 23, 2019, 3:30 pm

(Mar 23, 2019 03:27 PM)Shad0Byte Wrote: [\[CITE\]](#) Are you sure ?

Yes.

In windows 10 atleast unless you have testsigning on.

RCE - March 23, 2019, 3:32 pm

(Mar 23, 2019 03:30 PM)Exodus Wrote: [\[CITE\]](#) Yes.

In windows 10 atleast unless you have testsigning on.

Alright , in this week ill post a video as POC registering my kernel driver(not signed) in Win10 x64 b

, keep in touch in SMM botnet thread ?

Exodus - March 23, 2019, 3:33 pm

(Mar 23, 2019 03:32 PM)Shad0Byte Wrote: [\[CITE\]](#) Alright , in this week ill post a video as POC registering my kernel driver(not signed) in Win10 x64 b , keep in touch in SMM botnet thread ? Will do, always exciting to learn something new.

Dendimirror - March 23, 2019, 6:38 pm

(Mar 23, 2019 03:01 PM)WhatTheLeak Wrote: [\[CITE\]](#) Does any RAT has this feature? Or is it more like a crypter feature?

My RAT have this feature, easily implemented

D.N.A - March 28, 2019, 5:13 am

just rename it to Windows.exe or Something like Host.exe .. or COM.exe .. tricks is the best way to confuse ur sheep

I.M.P - March 28, 2019, 7:35 am

(Mar 28, 2019 05:13 AM)D.N.A Wrote: [\[CITE\]](#) just rename it to Windows.exe or Something like Host.exe .. or COM.exe .. tricks is the best way to confuse ur sheep

This is a terrible idea! I can name a completely clean hello world.exe compile it's name as chrome and it will get detected

BTC - March 28, 2019, 7:38 am

(Mar 28, 2019 05:13 AM)D.N.A Wrote: [\[CITE\]](#) just rename it to Virus.exe or Something like VirusWatchDog.exe .. or FOOL.exe .. tricks is the best way to confuse ur sheep

This is a great idea. I second this. Only a true expert with 15+ years of malware experience would understand the sorcery used to disguise these processes :-)

Exodus - March 28, 2019, 7:40 am

(Mar 28, 2019 05:13 AM)D.N.A Wrote: [\[CITE\]](#) just rename it to Windows.exe or Something like Host.exe .. or COM.exe .. tricks is the best way to confuse ur sheep

This is a god awful idea, it's super suspicious to have a process called windows.exe that isn't a system process, it's basically a guarantee that anyone with just the tiniest bit of knowledge will see it as a virus.

Fisher - March 28, 2019, 8:01 am

Good idea is to inject your process

CyberStrike - March 28, 2019, 11:45 am

(Mar 23, 2019 04:25 AM)??` NYAN CAT ?`? Wrote: [\[CITE\]](#) the simplest solution is to make your RAT kill itself every time task manager is open.

then start your RAT again using windows task schedule.

It's very simple and basic.

This is a good idea actually

(Mar 23, 2019 06:58 AM)iCoreX Wrote: [\[CITE\]](#) What do you mean with "using windows task schedule"? How can it detect that taskmanager is closed?

Google Windows schtasks, basically consider it as a persistence method.

frank3 - March 28, 2019, 7:05 pm

Use a root kit.

Example: google: github r77-rootkit

AlibabaMarket - March 28, 2019, 10:13 pm

(Mar 23, 2019 07:18 AM)iCoreX Wrote: [\[CITE\]](#) True, I always name my stub "svchost" and everytime they look in taskmanager they never find it lol
the simplest trick here..

James Burnham - March 28, 2019, 10:17 pm

(Mar 23, 2019 07:21 AM)IKIGAI Wrote: [\[CITE\]](#) you guys make me paranoid...Same. They make me want to ditch windows and go back to linux.

BTC - March 28, 2019, 10:36 pm

(Mar 28, 2019 10:17 PM)Burnham Wrote: [\[CITE\]](#) Same. They make me want to ditch windows and go back to linux.

Do it. Windows is the worst shitware ever created.

I enjoy Debian & Tails they are my favorite distros

helloworld112 - March 28, 2019, 11:29 pm

Usually you would use a rootkit to achieve this, however, that will only bring more attention to your process. I advise you inject into another or simply rename.

iCoreX - March 29, 2019, 12:40 pm

(Mar 28, 2019 10:13 PM)N1ckNam3 Wrote: [\[CITE\]](#) the simplest trick here..
Maybe a simple trick, but it's still efficient :)

GTrails - March 29, 2019, 11:02 pm

Try injecting it as a sub process of another known system process. Modern crypters do support this feature as "inject into" eg svchost.exe