

Forum:[Hack Forums](#)

Thread: [Better RAT coming to HF \[REAL HVNC, REAL BOOTKIT, REAL RING0 ROOTKIT, REAL UAC BYPASS](#)

rathvncgod - March 21, 2022, 1:06 pm

Unlike the RATs on HF that utilize public code like tinynuke's dogshit HVNC... (for one, it doesn't implement any compression algorithms for streaming data across the network thus increasing the network utilization more and bottlenecking I/O even further, for two it doesn't manage all windows properly and doesn't handle drawing of specific windows correctly, and lastly it doesn't handle user input properly. At least zeus implements some OKAYISH algorithm to determine changes in a 2D array)

So all the RATs you see being sold right now are copy pasted trash.

This RAT I am designing will contain the following:

- the core which utilizes I/O completion ports for handling clients, and managing threadpools
- the plugin manager which is an interface used both by the core and plugins
- the plugin feature enables anyone to create features for the rat, whether they are serversided plugins, or clientsided plugins, or both.

This rat is designed with a loosely coupled modular design pattern.

Plugins that will be available for the RAT created by me:

- USB Persistence (works by copying a boot segment to the usb drive, and changing the boot order to USB, this will also act as a bootkit and load the malware before windows even loads, Note: that the malware being loaded is an arbitrary driver that will execute the user mode code upon WinLogon)

- UEFI Bootkit (with secure boot disabled, which will be trivial on windows 7 > windows 10 we can replace the original uefi bootloader with a custom one and load your malware before the system even loads)

- UAC Bypass/Escalation (no trash betabot social engineering, we use exploits that allow us to obtain write primitives in the kernel, we will gain NT_Authority privileges from a limited user)

- A complete ring0 rootkit (file minifilter, documented callbacks, and undocumented practices), or even a ring-1 (hypervisor) which allows users to hook anything in memory using EPT page splitting, or other techniques.

- Reverse Socks

- HVNC (a proper HVNC, think of using REALVNC except with an invisible session & reverse connect, not that trash you see in market place. Implements latest RFB protocol)

- UPNP Mapper (map your own ports, and host services on your victims system & network)
(Other features can't be listed here)

*Using injection techniques never before seen by any skids on these forums

*Completely subverting any antiviruses during runtime using ring0 evasion techniques that allow us to hide from the antivirus, an example would include manually allocating memory for everything we do, system-wide-injection through modifying page tables directly and abusing CoW

*Processes use kernel memory within ring3 (Think of your process accessing an address > mmuserprobeaddress)

*The stub is written in 32 bit assembler that determines what payload to inject (x86,x64) and uses heaven's gate to inject into the appropriate process(es)

*All memory is allocated as Read Only, will be able to write and execute on these pages. VAD will return as READONLY.

*Anti dump measures taken place ; Encrypted .text section, guarded .text sections, integrity checks, anti debug, anti VM analysis

*Client stub is generated using an LLVM backend with obfuscation passes and mutation passes(peep hole optimization) that allow for unique builds to avoid signature detection and code obscurity

Cost: \$5000/month for the RAT with the features above + plugin SDK

runs3c - March 21, 2022, 3:22 pm

Its not first april yet, isnt it ?

rathvncgod - March 21, 2022, 4:35 pm

(Mar 21, 2022 03:48 PM)Dyne Wrote: [\[CITE\]](#) You had me in the first half, not gonna lie.

Alright.

Imao.

It's real. Hypervisors are a real thing when it comes to malware and game cheat development.

(Mar 21, 2022 03:22 PM)runs3c Wrote: [\[CITE\]](#) Its not first april yet, isnt it ?

HF skids can't even believe that the mentioned features are real.

It's not a joke

Silkroad - March 21, 2022, 4:44 pm

(Mar 21, 2022 01:06 PM)rathvncgod Wrote: [\[CITE\]](#) Unlike the RATs on HF that utilize public code like tinynuke's dogshit HVNC...

Cost: \$5000/month for the RAT with the features above + plugin SDK

It's always the new members with 5 posts ?

Join Date: Today

Can't wait to see the "progress" on this ?

rathvncgod - March 21, 2022, 4:46 pm

(Mar 21, 2022 04:44 PM)Silkroad Wrote: [\[CITE\]](#) It's always the new members with 5 posts ?

Join Date: Today

Can't wait to see the "progress" on this ?

Do you think this is a progress thread? no. It'll just pop up in the marketplace under some ub3r account that doesn't log in

rathvncgod - March 21, 2022, 8:54 pm

(Mar 21, 2022 05:42 PM)Check The Name Wrote: [\[CITE\]](#) ?

This is APT group level malware

Kr0n0s - March 21, 2022, 9:25 pm

pics, videos?

kinda mandatory.

Verra - March 21, 2022, 11:45 pm

Yeah you can't really blame anyone for flaming you. Proof is always neat!

NotKover - March 22, 2022, 12:07 am

Some big claims you have there, lets hope you can back them up

Ph4n70M Phr34K - March 22, 2022, 1:28 am

(Mar 21, 2022 01:06 PM)rathvncgod Wrote: [\[CITE\]](#) -A complete ring0

you are incompetent and uneducated. good developers hide malware under ring-1(ring minus one)

- a place somewhere between CPU PCB(printed circuit board) and IHS(integrated heat spreader).