Good Game, Gone Bad: Xeno RAT Spread Via .gg Domains and GitHub

Published: 2024-06-25 · Archived: 2026-04-05 17:33:38 UTC

TABLE OF CONTENTS

Introduction

XenoRAT, an open-source malware available on GitHub, has been linked to a North Korean hacking group and unnamed threat actors preying on the gaming community. Recently, Hunt's Research Team discovered the remote access tool (RAT) spreading through .gg domains, a term synonymous with "good game" in esports, and a GitHub repository portraying its software as scripting engine tools for the popular game Roblox.

In this post, we'll explore the specific **.gg domains hosting Xeno RAT**, the GitHub account, and a possibly linked YouTube account and provide insight into how this emerging threat targets gamers and developers.

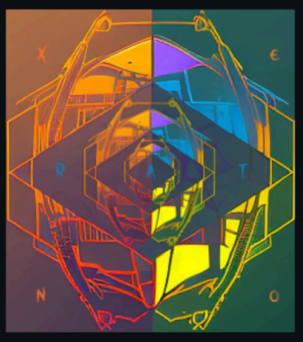
Xeno RAT in the Wild

Most recently, AhnLab's ASEC reported on a likely North Korea-linked group using Dropbox to deliver Xeno RAT to victim networks. In late April, a third-party researcher on X posted on an open directory likely administered by the Kimsuky threat group, hosting a copy of the tool in a folder titled "/rat."

The tools GitHub page boasts several advanced features, including **HVNC, real-time audio surveillance, and a SOCKS5 reverse proxy**. The README, detailing these capabilities, is pictured below in Figure 1.

README MIT license

Xeno Rat



Xeno Rat is a remote access tool (RAT) that is used to control a computer remotely. It is written in C# and is compatible with Windows 10, 11. It is meant to stable, completely open source, easy to use and has a lot of features.

What Sets Xeno Rat Apart

Xeno Rat stands out from the crowd for several reasons:

- **HVNC (Hidden Virtual Network Computing)**: Xeno Rat offers HVNC, which is typically a paid feature in other RATs, but here, it's freely available to enhance your remote access experience.
- **Live Microphone**: Enjoy real-time audio surveillance with Xeno Rat, which provides a live microphone feature.
- **Socks5 Reverse Proxy**: Xeno Rat includes a Socks5 reverse proxy, allowing you to bypass network restrictions and access remote systems with ease.
- **Regular Updates and Much More**: We are committed to keeping Xeno Rat up to date and continually improving its features and functionality to better meet your needs.
- **Built Completely from Scratch**: Xeno Rat is developed entirely from scratch, ensuring a unique and tailored approach to remote access tools.

Figure 1: Screenshot of Xeno RAT README

A Closer Look at Xeno RAT Network Traffic

Communication between the controller and Xeno RAT clients occurs over TCP sockets, as illustrated in Figure 2. The initial exchange follows a recognizable pattern, which can help identify malicious activity.

Additionally, C2 servers respond to requests in the same pattern as the one seen below. For an in-depth talk on detecting malware infrastructure according to controller responses, we recommend Greg Lesnewich's LABScon23 talk.

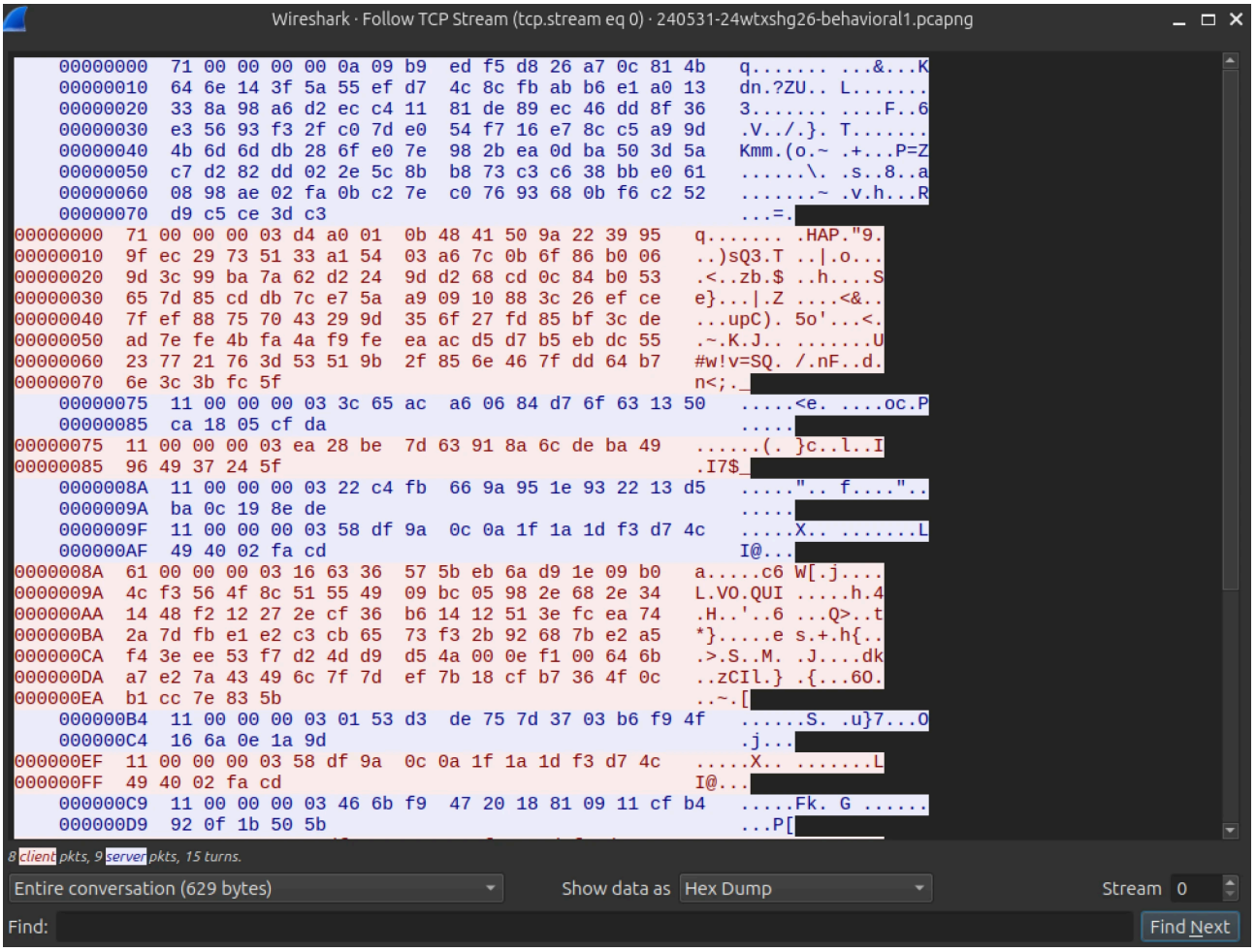


Figure 2: Xeno RAT Client -> Controller Communication (Source Hatching Triage)

If you're in need of robust network IDS rules (Suricata/Snort) to detect these servers, check out @Jane0sint's contributions on the Emerging Threats website.

Discovery of Xeno RAT C2s on .gg Domains

Xeno RAT infrastructure hosted on .gg domains spotlights a troubling trend in malware distribution as the top-level domain (TLD) is popular in the esports community and is now being exploited to spread malware.

This section will provide an overview of controller domains and the associated clients.

Examples

The following section provides a detailed list of identified .gg domains hosting XenoRAT controllers, the resolving IP addresses, and the sandbox analysis results.

Domain	people-weekend.gl.at.ply_gg:5719
IP	147.185.221_20
Filename	Client.exe

SHA1	38ce2a41d59a1bf0f3332fb867f43794c39577af
Triage Link	Link

Domain	anyone-blogging.gl.at.ply_gg:22284
IP	147.185.221_20
Filename	SynapseX.revamaped.V1.2.rar
SHA1	2051551c6c0f18eaf3c4cf45ffe6119e582c19ae
Triage Link	Link

Domain	performance-ha.gl.at.ply_gg:33365
IP	147.185.221_19
Filename	4d820f671919b3029173d8659aa59600_NeikiAnalytics.exe
SHA1	af68a0b9e9c58dcbdd2ede205c30537bca39650c
Triage Link	Link

Domain	character-acquisitions.gl.at.ply_gg:5050
IP	147.185.221_17
Filename	a3254b90b2c6e12c29f7d9f538087da2d4bb7f64d003c591c8936cee7dd74b39.exe
SHA1	029f3396c39f543dd984031eb82edcc035ed0a25
Triage Link	Link

Domain	related-directed.gl.at.ply_gg:3403
IP	147.185.221_20
Filename	testingrat.exe
SHA1	e9251ef1dd3ebe4f17acf0b3552e22751009c8c1
Triage Link	Link

Domain	david-login.gl.at.ply_gg:54479
IP	147.185.221_19

Filename	WavePreTest.rar
SHA1	5e7138c7ee8a1de9d041804fd11ac0ba63cb1f34
Triage Link	Link
Domain	taking-headquarters.gl.at.ply_gg:3069
IP	147.185.221_20
Filename	xeno.exe
SHA1	707c68257c2ea97fa4591f58be326e1308fd1106
Triage Link	Link

Each domain was hosted on one of **three shared IP addresses belonging to the Developed Methods LLC** ASN in the U.S. Notably, IP 147.185.221_19 also served as controller infrastructure for **DcRAT and VenomRAT**, as seen in Figure 3. Additionally, this same IP hosted a C2 server for Redline Stealer just last month.

Last Seen	First Seen	IP	Ports	SubjectCommonName	IssuerOrganization	
2024-06-16 3 days ago	2024-05-29 3 weeks ago	147.185.221.19	37434	ninizazar		Certificate Details Certificate IPs
2024-06-16 3 days ago	2024-05-01 1 month ago	147.185.221.19	9550	omegaserver	20516d010de7432ba637283cb6687f25	Certificate Details Certificate IPs
2024-06-16 3 days ago	2024-05-08 1 month ago	147.185.221.19	30248	solardarkglass.hopto.org	Let's Encrypt	Certificate Details Certificate IPs
2024-06-16 3 days ago	2024-05-15 1 month ago	147.185.221.19	50580	DESKTOP-J92461D		Certificate Details Certificate IPs
2024-06-16 3 days ago	2024-06-16 3 days ago	147.185.221.19	44905	do-not-trust.citizenfx.tls.invalid		Certificate Details Certificate IPs
2024-06-16 3 days ago	2024-05-15 1 month ago	147.185.221.19	48154	pop-os	Crafty Controller	Certificate Details Certificate IPs
2024-06-16 3 days ago	2024-06-16 3 days ago	147.185.221.19	37300	DcRat	DcRat By qwqdanchun	Certificate Details Certificate IPs
2024-06-16 3 days ago	2024-06-16 3 days ago	147.185.221.19	50397	DESKTOP-3UAEEH5		Certificate Details Certificate IPs
2024-06-16 3 days ago	2024-05-08 1 month ago	147.185.221.19	43771	DESKTOP-FF40NAT		Certificate Details Certificate IPs
2024-06-16 3 days ago	2024-05-29 3 weeks ago	147.185.221.19	50378	*.a6046ab21be64810849e8b686de1dc48.plex.direct	Let's Encrypt	Certificate Details Certificate IPs
2024-06-16 3 days ago	2024-05-29 3 weeks ago	147.185.221.19	54766	Steven_pc		Certificate Details Certificate IPs
2024-06-16	2024-05-22	147.185.221.19	53544	WIN-62VAHFNPJUC		Certificate Details

Figure 3: Historical Certificate Data in Hunt for 147.185.221_19

The GitHub Repo

During our analysis, one file name stood out among those communicating with the .gg domains: **SynapseX.revamped.V1.2.rar.** This file led us to a GitHub repository (Figure 4) under an account claiming to own Synapse X Revamp, a scripting engine for Roblox. The account hosts 10 repositories, most disguised as gaming-related executors and named loader.exe.

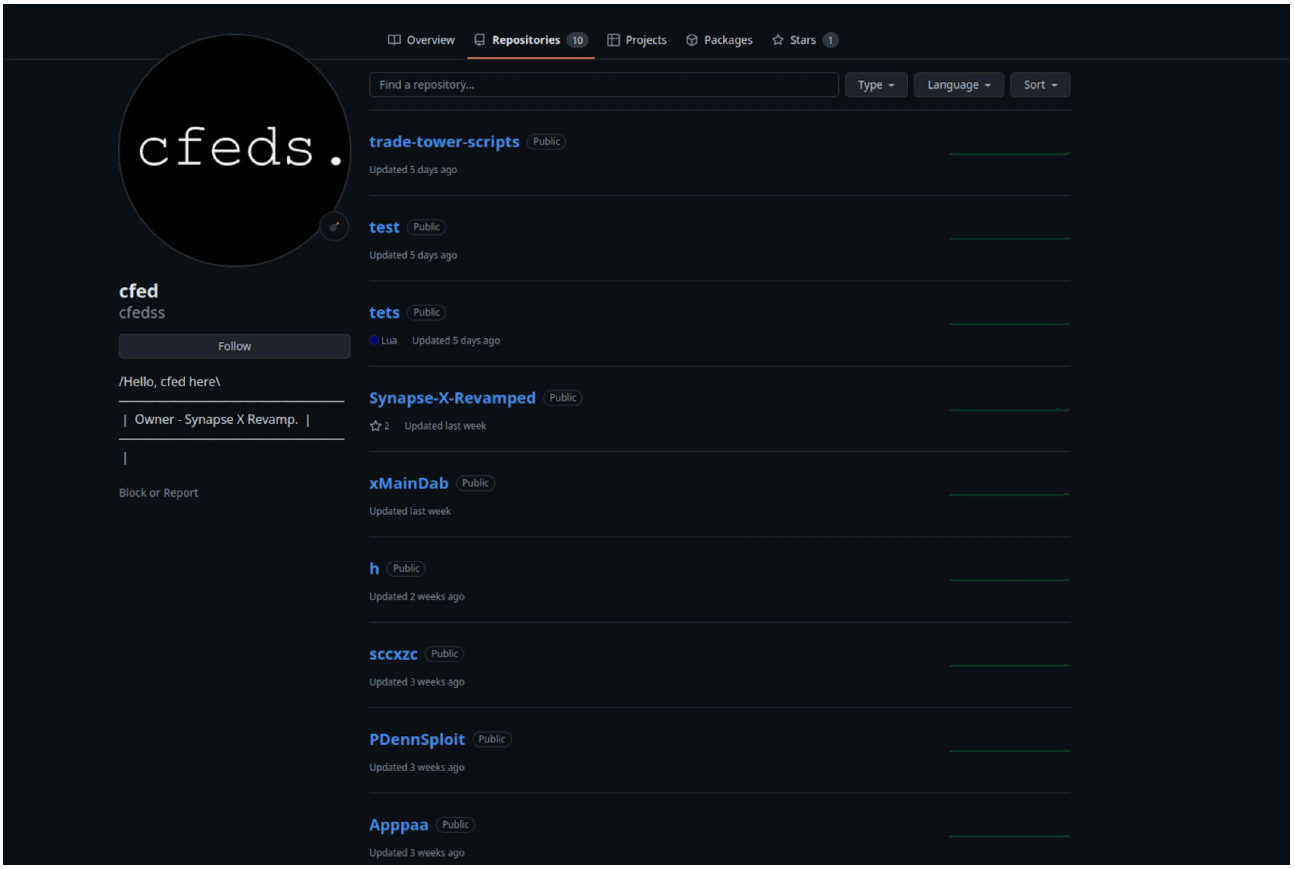


Figure 4: GitHub repository containing malicious files, including Xeno RAT.

When extracted, the .rar file, as mentioned above, contains two executables: Synapse X Launcher.exe.exe and Synapse X Launcher.exe. The first file is identified as XenoRAT, while the latter is **detected as Quasar**, a well-known malware family also written in .NET. Sandbox results for both files are displayed below.

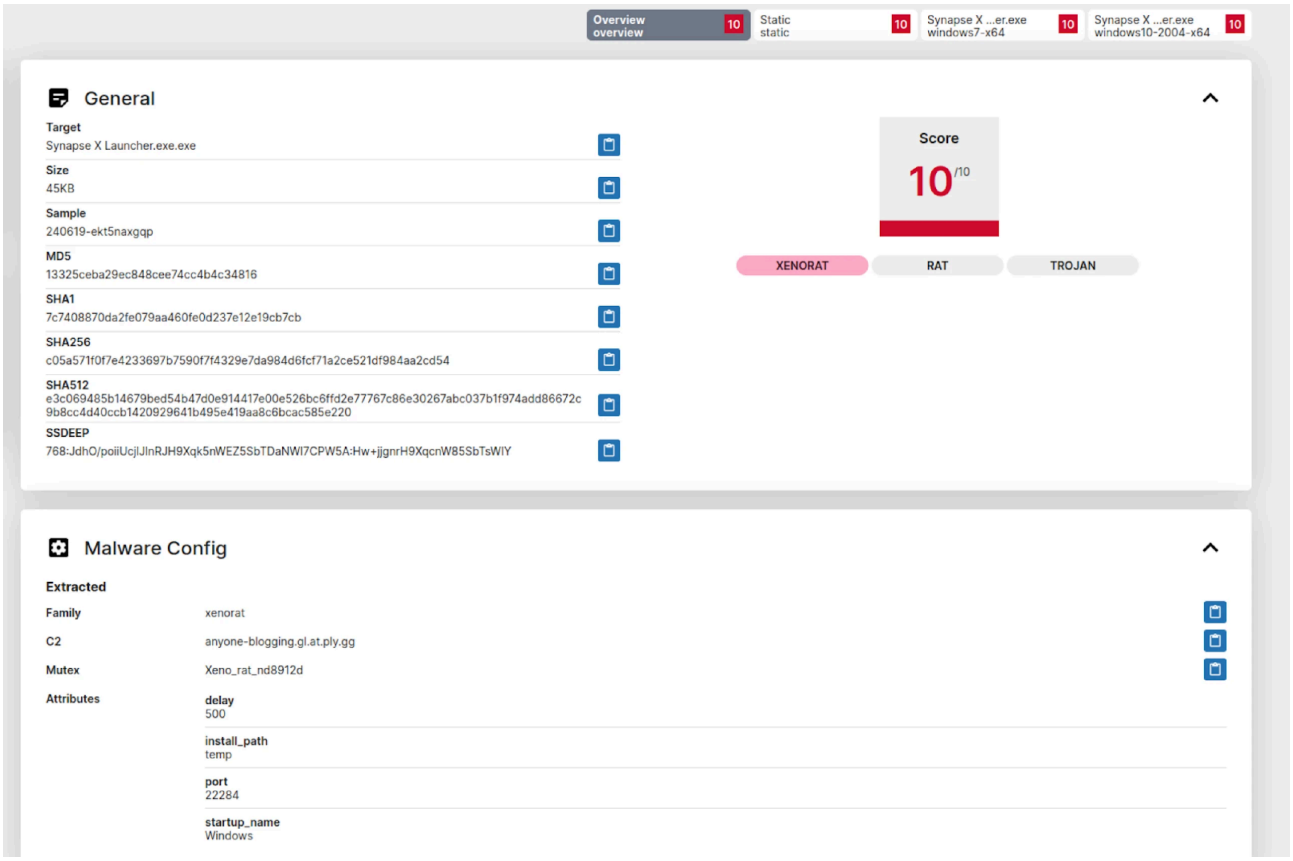


Figure 5: Sandbox Analysis of Synapse X File

The **C2 server for Quasar uses portmap.io**, a free port forwarding service. Interestingly, suppose you're a fan of animated YouTube series or have young children. In that case, you might recognize that the domain name resembles Skibidi Toilet, a popular machinima series featuring videos and shorts.

Details

Domain	anyone-blogging.gl.at.ply.gg
IP	147.185.221_20
Filename	Synapse X Launcher.exe.exe
SHA1	7c7408870da2fe079aa460fe0d237e12e19cb7cb
Triage Link	Link

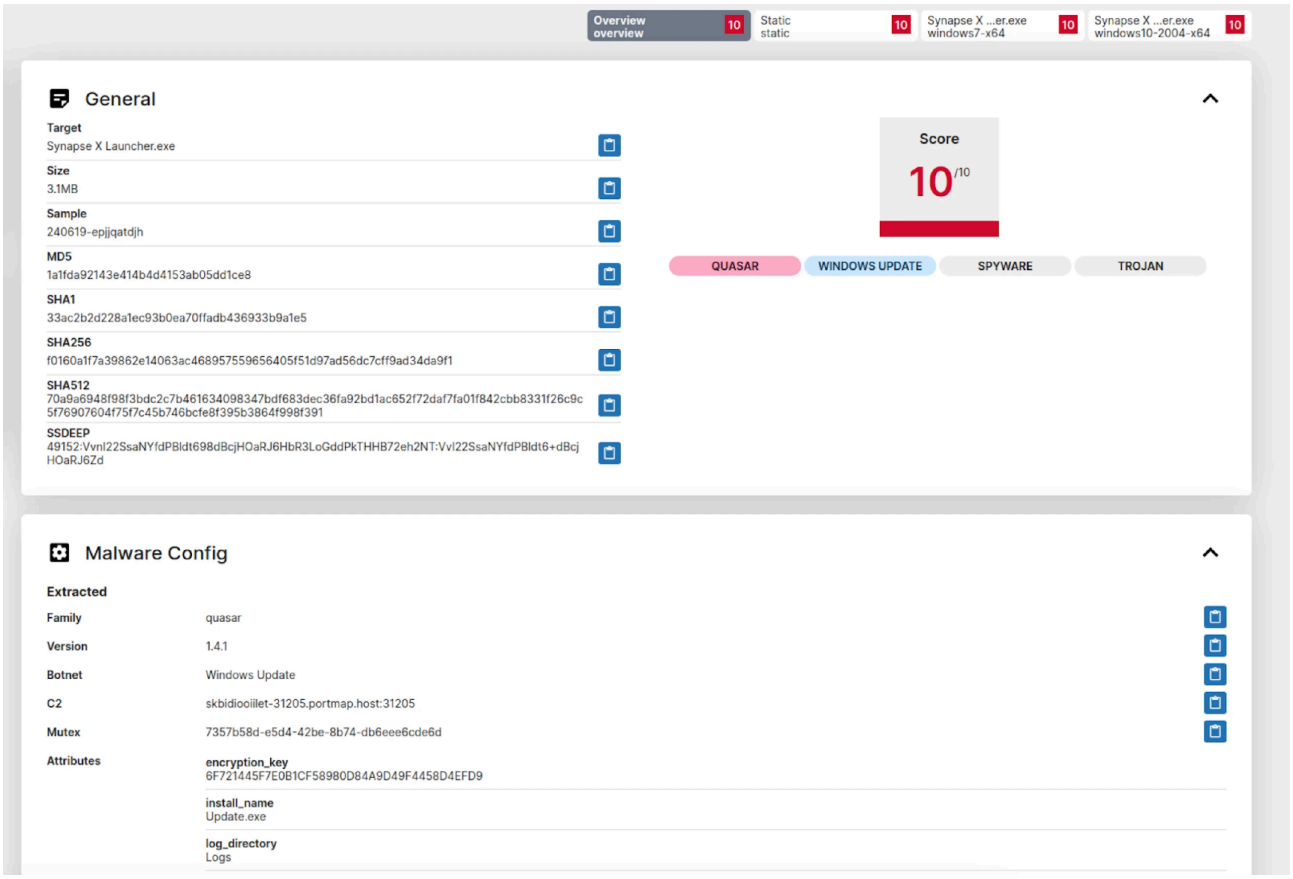


Figure 6: Quasar RAT Sandbox Analysis and Config

Details for the Quasar sample:

Domain	skbidiooiilet-31205.portmap_host:31205
IP	193.161.193_99
Filename	OOO GETWIFI
ASN	OOO GETWIFI
SHA1	33ac2b2d228a1ec93b0ea70ffadb436933b9a1e5
Triage Link	Link

Hunt researchers weren't the first to uncover this repository's malicious nature. Two weeks ago, a GitHub user named ByfronTechnologies submitted an issue, complete with screenshots from Hatching Triage, indicating that the **file in the XMainDab folder was detected as XWorm malware**. Figure 7 includes a screenshot of the comment and the analysis images.

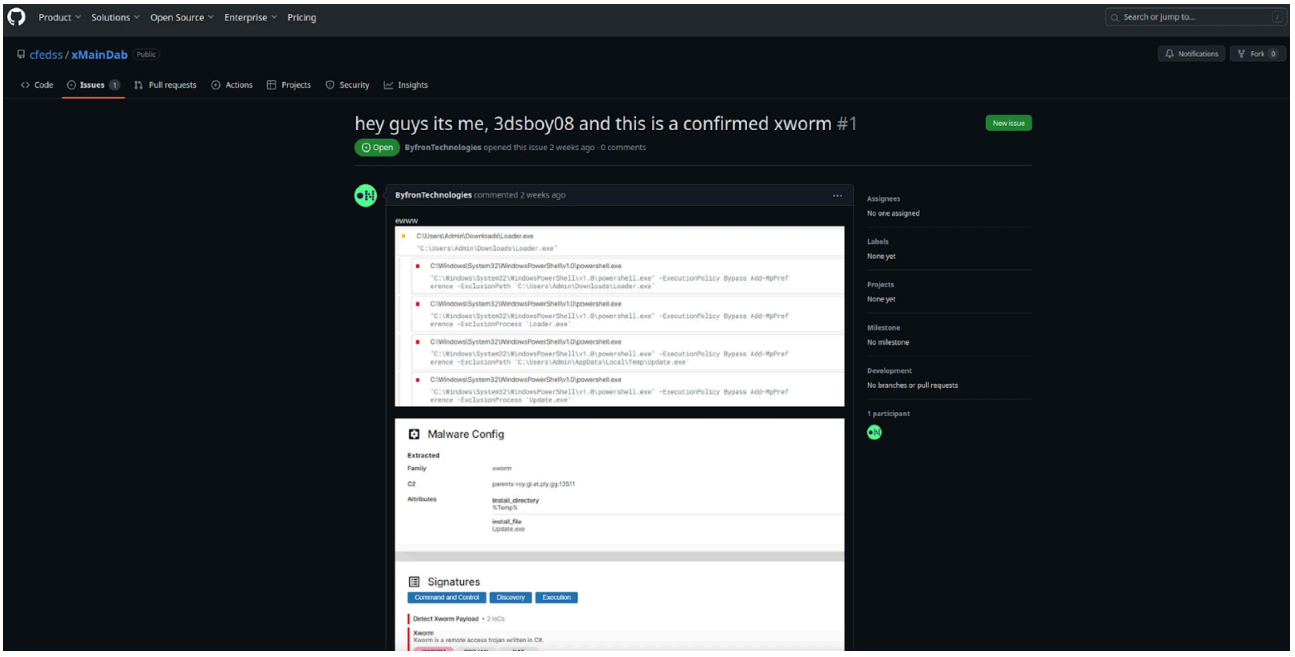


Figure 7: GitHub Issue Identifying Loader.exe as XWorm Malware

By pivoting on the file and folder names in the repository, we discovered what appears to be the YouTube channel associated with this threat actor. The account, named P-Denny Gaming (Figure 8), features several videos related to Roblox. The video titles use similar names to those found in the GitHub account, further linking the two.

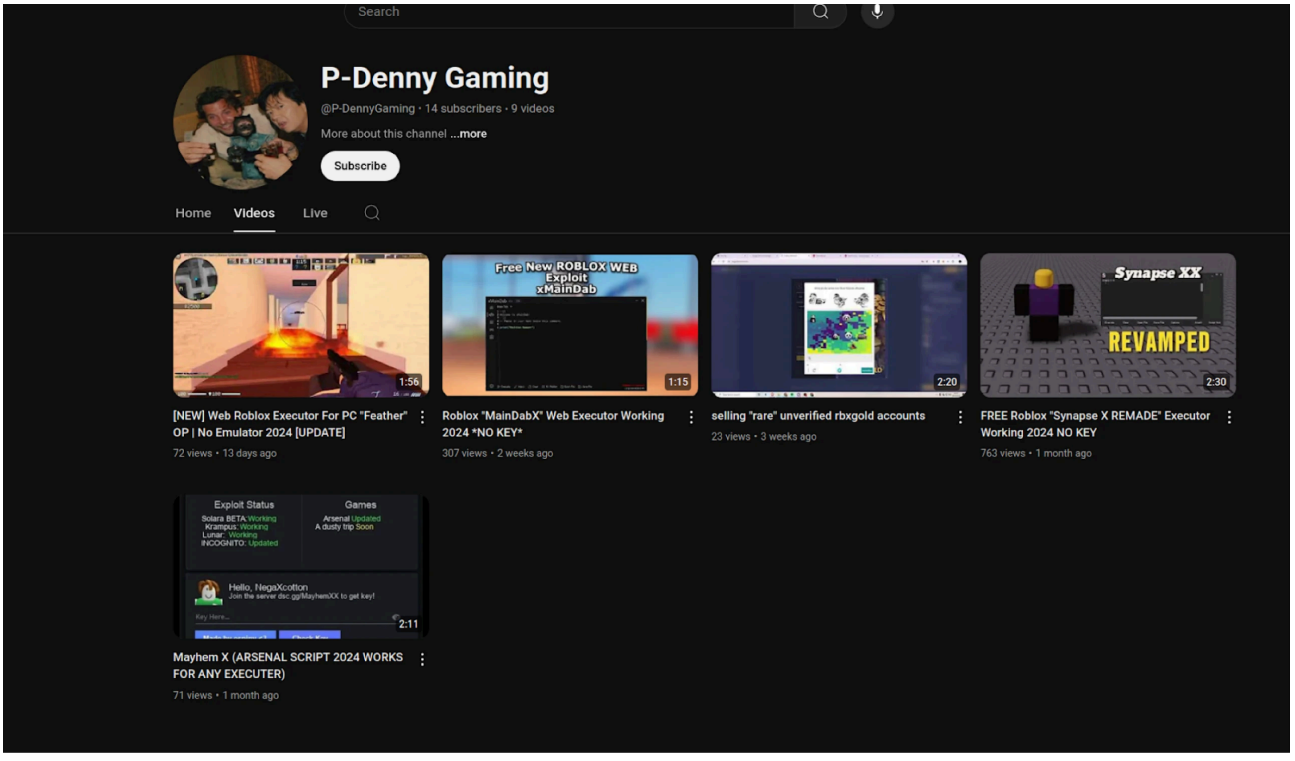


Figure 8: Screenshot of YouTube Account Associated with Xeno RAT & Quasar Distribution

Figure 9 shows a screenshot from one of the videos instructing users to disable Windows Defender before installing the Synapse X RAR file. Notably, the screenshot reveals that the user's Windows desktop uses the Swedish language and includes a **browser bookmark labeled 'Roblox Stealer,'** providing additional context about the actor's intent.

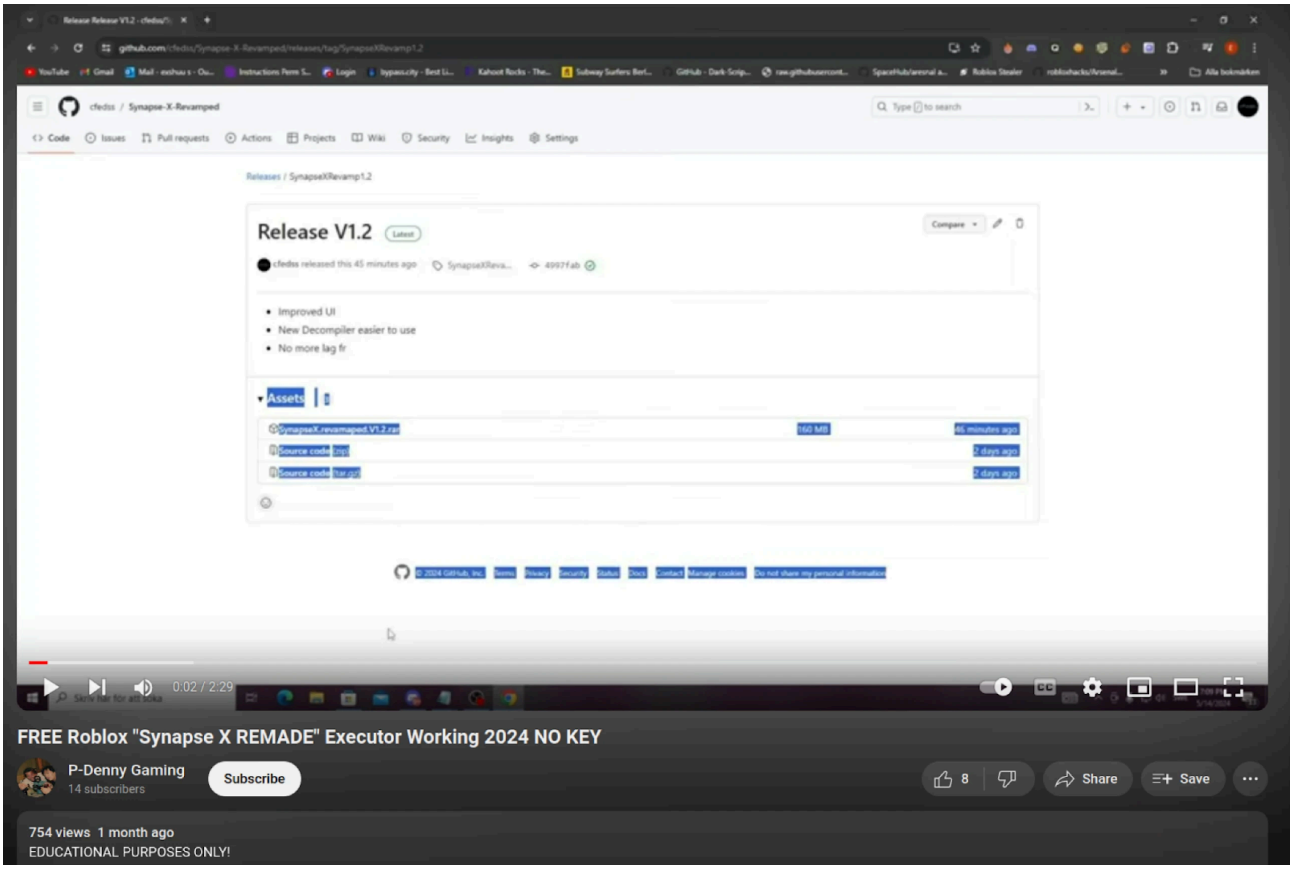


Figure 9: Screenshot of YouTube Video Instructing Users to Install Synapse X File

In the same video, several comments vouched for the legitimacy of the files, dismissing warnings from other users who had correctly identified the software as malicious.

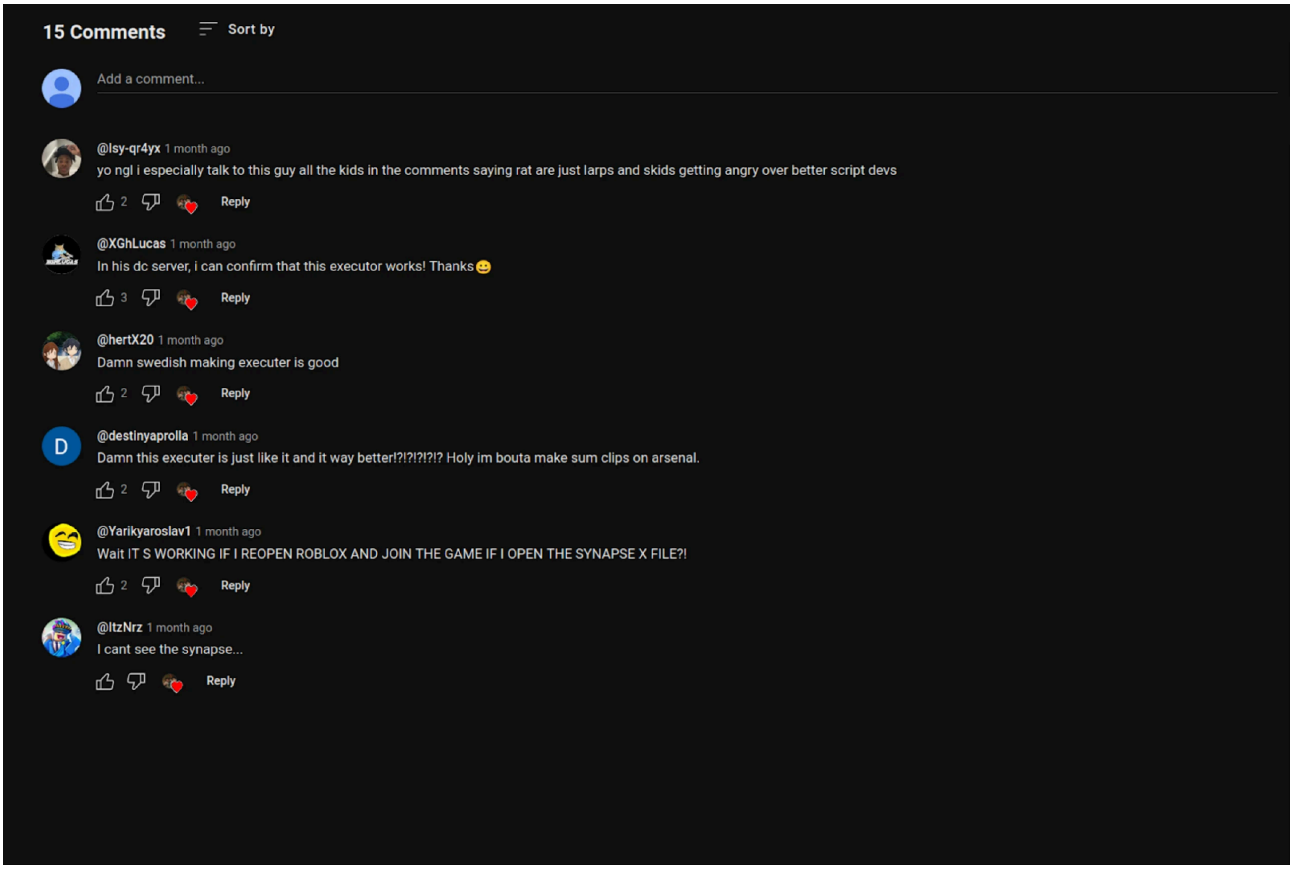


Figure 10: Comments on the video supporting the video uploader and the legitimacy of the files

The presence of XenoRAT and other malware on .gg domains and GitHub poses significant risks to the gaming community. Gamers and developers are particularly vulnerable to these threats due to the seamless integration of malicious software into legitimate-looking tools and resources.

Malicious software like those mentioned above can lead to the theft of personal information, in-game assets, and financial data, severely impacting users' digital lives. Furthermore, using open-source platforms like GitHub to distribute malware disguised as game scripts or executors increases the likelihood of widespread infection.

Note: Hunt is actively scanning for XenoRAT infrastructure using its default port, 4444. Our detection methods for these servers have proven effective; we plan to expand our monitoring to include all ports, ensuring comprehensive coverage in identifying and tracking C2 servers. Stay tuned for updates on our progress.

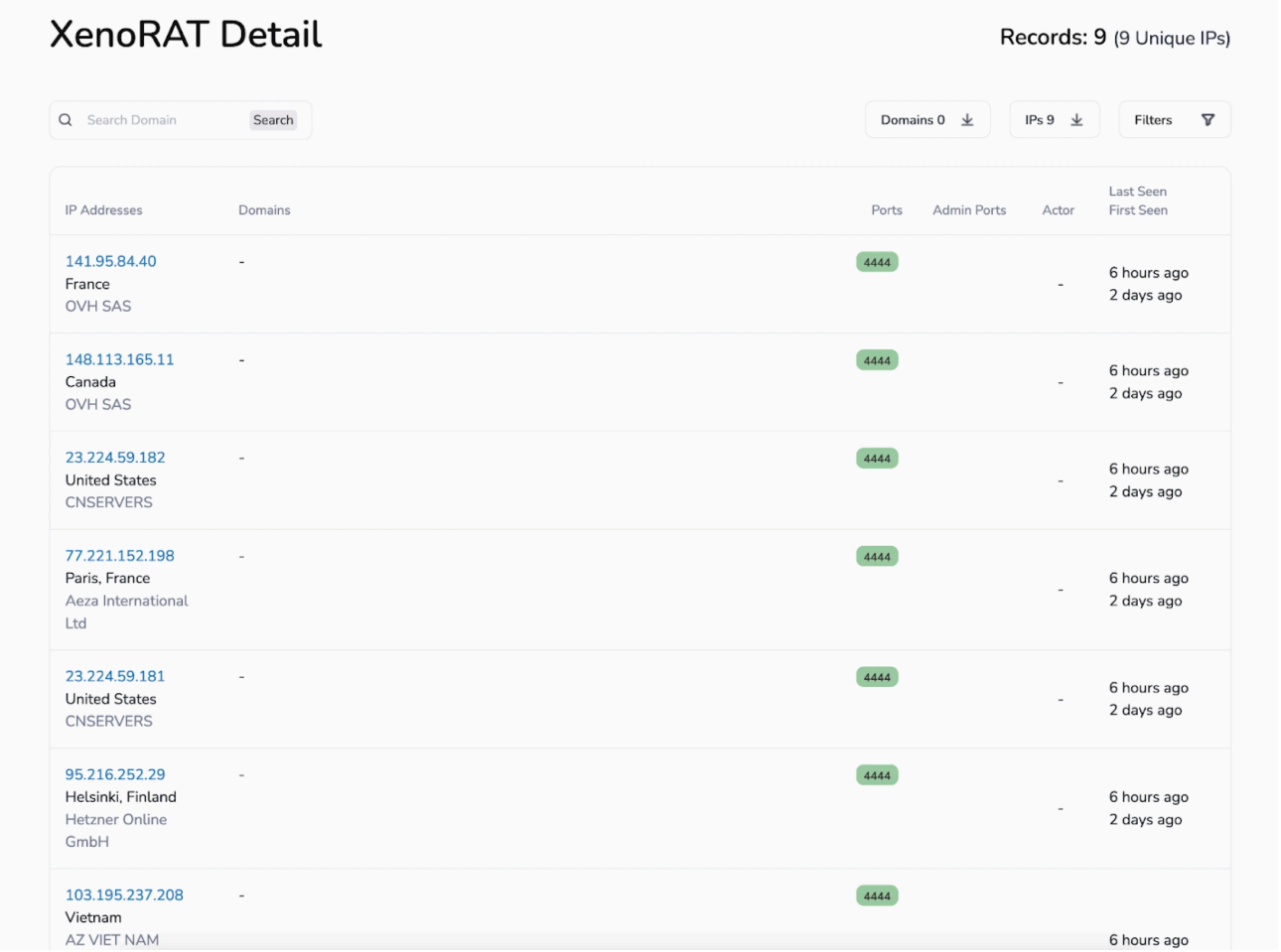


Figure 11: Xeno RAT Detections in Hunt

Conclusion

Hunt has identified several Xeno RAT samples that distribute malware by leveraging .gg domains and a GitHub account. Both pieces of malicious software pose a significant threat to the gaming community.

Users must remain vigilant and exercise caution when downloading and installing software, regardless of the platform. A healthy dose of caution can help mitigate the risks associated with these threats, ensuring a safe online gaming environment.

Contact us for a demo today, and join a community committed to seeking out and exposing malicious infrastructure wherever it may rear its ugly head.
