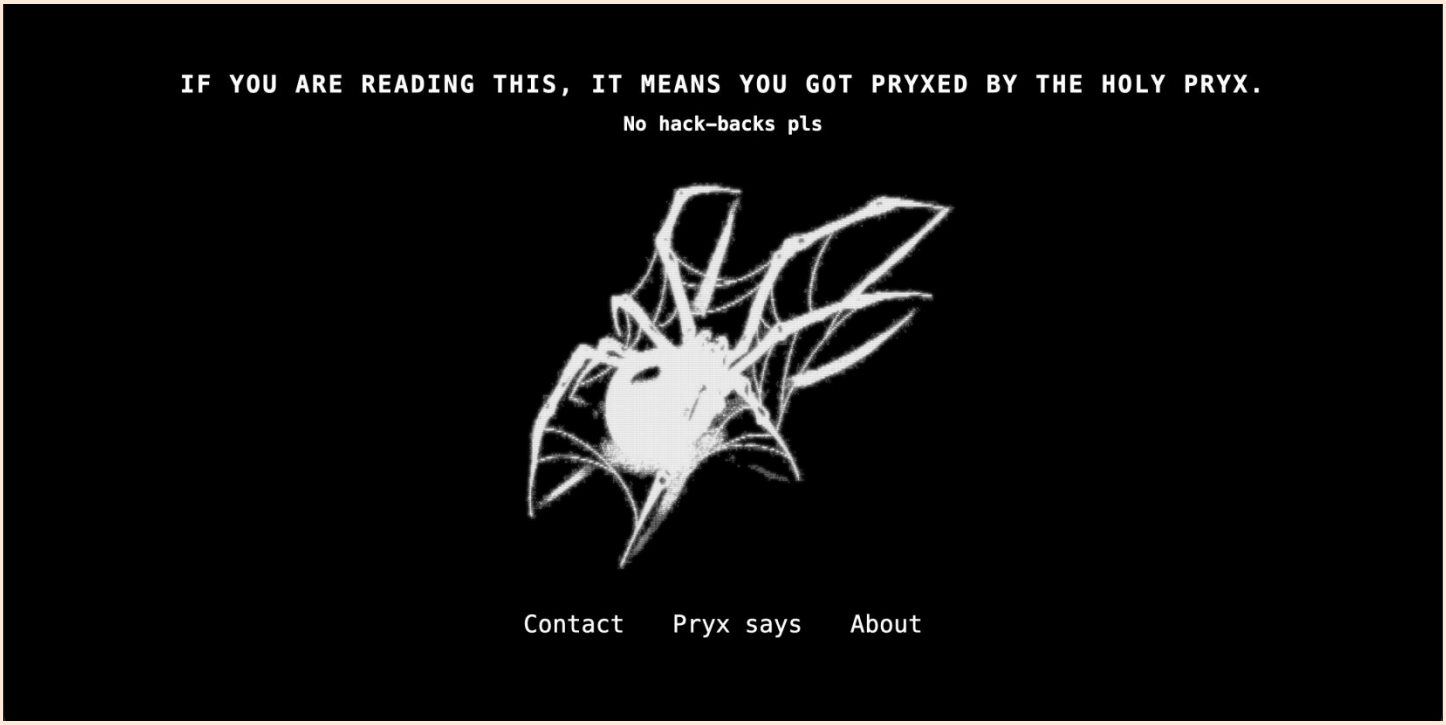
Threat Actor Profile: Pryx

By: Mohamed Galal Hashem



Source:

1- Morado Report (link to report)

2- bridewell Hellcat Report (link to report)

3- KelaCyber Report (link to report)

4- Threat Actor Interview: Spotlighting on Pryx (Link)

Introduction about Pryx

- Pryx is a cybercriminal active since around June 2024 across multiple platforms including XSS, BreachForums, Dread, Telegram, and X (Twitter), and engages deeply in technical discussions and competitions. Before joining Hellcat, he started with solo data leaks from educational institutions before escalating to government systems in UAE, Saudi Arabia, and Barbados. He later expanded to targeting private companies, while also selling malware such as AES256-based crypter. He also maintained a personal blog (pryx.pw, formerly pryx.cc).
- Pryx is a threat actor who engages in malware/ransomware development and identity access brokering. Active on XSS since June 2024, Pryx has made notable contributions to the cybercrime community, particularly in his write-ups on server-side information stealers and silent Tor servers. Outside of these novel developments in malware, he has led the charge in creating a new ransomware group named Hellcat that already has four claimed victims on their data leak site (DLS). In addition, Pryx has operated in circles that create and maintain cybercrime forums including BreachForums, BlackForums, and most recently, DangerZone.
- The threat actor known as Pryx has recently escalated their activities, forming a new ransomware group and potentially developing a novel family of information-stealing malware. Pryx, who claims to be 17 years old, is an access broker and malware developer who primarily operates on the XSS cybercrime forum, with occasional activity on BreachForums. This actor has also operated under the aliases “HolyPryx” and “Sp1d3r” (not to be confused with a different threat actor who used the aliases “Sp1d3r” and “Sp1d3rhunt3rs” when advertising stolen data from the Snowflake breaches on BreachForums). He also worked on the DangerZone project, a cybercrime forum that started in November. Pryx is associated with prominent threat actors such as IntelBroker and members of the “Five Families” hacking alliance, highlighting a well-established network of collaborators and influence within the cybercrime community.
- Pryx submitted a write-up about a piece of malware he calls “the first server-side stealer in the world.” As described by Pryx, the new malware inverses the established behavior of information stealers. Rather than dropping the stealer malware on the victim’s machine, it operates by setting up a secret Tor service directly on the compromised machine. This covert service functions as a lightweight server that quietly hosts stolen data. Instead of maintaining persistent connections or generating noticeable activity on the victim's machine, the malware allows the attacker to retrieve the stolen files through discrete GET requests. This reduces the chances of security researchers detecting the threat before sensitive information is stolen.

Communication channel:

- Signal: @prx.01
- Tox: 141C8F13F4B7A4C2EED05A29186AE10F8E849AE4AC2C3E7B167FD27B316E026A42B75D5AE83C
- Twitter | X: @holypryx
- Wire: @pryx

Hellcat Ransomware

- Pryx started the Hellcat ransomware group in October 2024. The group uses a double-extortion tactic, stealing sensitive data before encrypting it. This method allows them to threaten the release of the stolen information so that they can demand a higher ransom from the victim.
- The Hellcat ransomware group consists of nine members who are all active on BreachForums and other cybercrime forums. The most notable member of the group is IntelBroker, a notorious threat actor responsible for multiple high-profile breaches and also the current owner of BreachForums.
- Hellcat had not been seen facilitating any ransomware attacks since November 15th. It seemed like the group had gone defunct, but on December 25th, the group posted two new victims to their data leak site; a Turkish vehicle warranty company and the Blora Regency of Indonesia.

DangerZone

- Pryx is also a moderator of a new cybercrime forum called DangerZone. Operating under the domain dangerzone[.]cx, the forum is accessible on both the dark and clear web. Like other cybercrime forums, DangerZone has a multitude of sections relating to different topics and illicit activities where users can contribute to the community and engage in discourse. Notable sections include leaked databases, malware, and software vulnerabilities.
- The site appears to be fairly active for a new forum boasting over 100 users with almost every available section having posts in them. The forum operators have shared their forum in multiple threat actor group chats on Telegram and Discord and have also advertised on BreachForums.

Main Interview questions with Pryx with the Osint10x

Below we have presented the questions and answers with no modification:

[Q1] can you please tell us about yourself and your work?
[A1] I'm Pryx, known on X as @holypryx. I'm currently a 17-year-old teenager. I entered the cybercrime world when I was 12 or 13 years old. Back then, I was mostly trolling and doing funny things. Now, I am interested in malware development and initial access. I plan to keep improving at what I do and have no intention of stopping anytime soon.

[Q2] What were your aliases in the past? Which all groups did you collaborate with so far?
[A2] From what I can share, I've used the aliases "holypryx" and "sp1d3r" in the past. No other specific past aliases are worth mentioning since I switch aliases whenever I feel the heat.
I never worked with any group other than hellcat after creating the alias "pryx"

[Q3] What are the most common security flaws you have witnessed so far?
[A3]IDORs. Literally, 60% of the corps I target are vulnerable to them in some way. Even the Saudi government breach was caused by poor cookie management, leading to an IDOR that exposed 40 GB of citizen data and private email attachments. This included ID cards, driver's licenses, and even work CVs.

[Q4] Which geo and sector interests you as a target, and why? Is there a broader motive or philosophy behind target selection?
[A4] I'm most interested in U.S. and Israeli targets. U.S. data is highly valuable in the market, and I target Israel simply because I hate the Jews. My main focus is on the government sector.

[Q5] Can you share an example of a time when one of your projects or tactics failed? What lessons did you take away from that experience?
[A5] We had RDP access to a company with $118 billion in revenue, It was China Life Insurance. We were in their systems for a week, fully prepared with the locker and backend server, ready to encrypt over 5TB of data. But when we tried to log in to execute the ransomware, our access was revoked. Worst timing ever.
What I learned from this experience is that we need to move fast and have everything fully prepared before trying to fuck with the target servers.
Not going to lie, we're all still pissed about this incident, it was caused by stupid laziness.

[Q6] What combination of techniques would you employ, and why?
[A6] I'd go with a mix of ETW patching and IAT hooking. ETW patching screws with the telemetry that EDRs rely on, so they can't flag anything. IAT hooking lets you mess with API calls to make the malware look like a legit process. Throw in some obfuscation and sandbox evasion, and you've got something that'll slip right through even high-security setups.

[Q7] Share some of your TTPs you have used for attacks.

[A7] Well, based on a threat intelligence report by an OSINT company analyzing my activities, they outlined the following TTPs, and honestly, I find it impressive how accurate they are:

TA0001: Initial Access

T1566: Phishing

T1078: Valid Accounts

TA0003: Persistence

T1078: Valid Accounts

TA0004: Privilege Escalation

T1078: Valid Accounts

TA0005: Defense Evasion

T1078: Valid Accounts

TA0040: Impact

T1486: Data Encrypted for Impact

[Q8]What tools do you typically use in your operations?

[A8]BurpSuite, Netcat, Netscan. I can't think of anything else for now. I don't really need a massive toolkit—most tasks don't require anything too specific. If I do, I'll script something myself or use whatever gets the job done.

[Q9]How do you maintain your OPSec?

[A9] Not committing human mistakes is the best way to keep your operational security tight. VPNs are just one piece of the puzzle. I encrypt all my hard drives and keep air-gapped systems for the more sensitive stuff. For communication, I stick to XMPP, Tox, and Session, which don't leak metadata and use proper encryption. I also rent VPS servers anonymously, paying with crypto or whatever keeps me untraceable.