ThreatMon
Under Cyber Wings

HELLCAT RANSOMWARE

HELLCAT RANSOMWARE GROUP
DEFINITION OF HELLCAT

Hellcat is a recently emerged ransomware group that surfaced in late 2024, quickly establishing itself as a significant threat actor in the global cyber threat landscape. The group is characterized by its aggressive targeting of high-profile entities, including government agencies, critical infrastructure, and large corporations. Hellcat employs sophisticated tactics, such as double-extortion schemes, where they not only encrypt sensitive data but also exfiltrate it, threatening to publicly release the stolen information if their ransom demands are not met.

What sets Hellcat apart is its unique approach to communication, often blending humor and cultural references into their ransom notes and public announcements. For instance, in one attack, the group demanded a ransom denominated as "baguettes," a humorous nod to the French origin of their victim. This unorthodox style is part of a broader strategy to draw media attention and distinguish themselves in a crowded field of ransomware operators.

Hellcat leverages advanced cyberattack methodologies, including exploiting niche vulnerabilities and weak credentials, to infiltrate their targets. Their operations are global, with victims spanning multiple industries and regions. Despite their newness, Hellcat has demonstrated rapid adaptability, evolving their tactics to bypass modern security defenses and amplify the impact of their attacks.

MAJOR ATTACKS OF THE HELLCAT RANSOMWARE GROUP

Hellcat Attack Timeline: November 2024

Schneider Electric Attack

- Date: November 2024
- Target: Schneider Electric, a French energy management company.
- Incident: Hellcat claimed to have infiltrated Schneider Electric's Atlassian Jira system and stole 40+ GB of data.
- Demand: USD 125,000 worth of “baguettes” (a humorous reference to the company’s French origin).
- Impact: Pending public confirmation.

Jordanian Ministry of Education & Tanzania Business College Attacks

- Date: November 2024
- Targets:
  - Jordanian Ministry of Education.
  - Tanzania Business College.
- Incident: Hellcat claimed to have leaked sensitive data belonging to both organizations.
- Reason/Impact: Specific details remain unclear.

Pinger Attack

- Date: November 2024
- Target: Pinger, a US telecom provider offering free texts, images, calls, and voice messaging.
- Incident: Hellcat claimed to have stolen 111+ GB of data.
- Demand: USD 150,000 in Monero (XMR) or Bitcoin (BTC) in exchange for deleting the stolen data and preventing its public release.
- Impact: Awaiting updates from Pinger or official confirmation.

SUMMARY

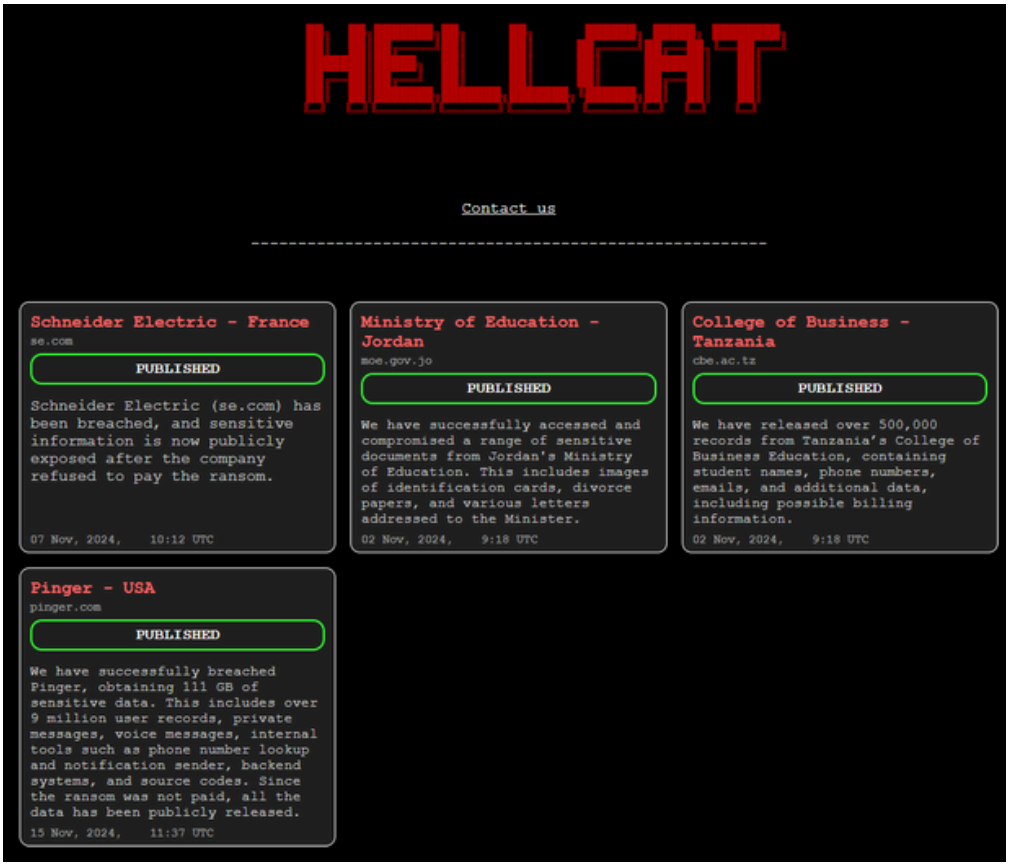
Hellcat, an emerging threat actor group, conducted a series of high-profile attacks in November 2024, targeting organizations across various sectors and regions:

- Schneider Electric in France.
- Jordanian Ministry of Education and Tanzania Business College in the Middle East and Africa.
- Pinger, a major US telecom provider.

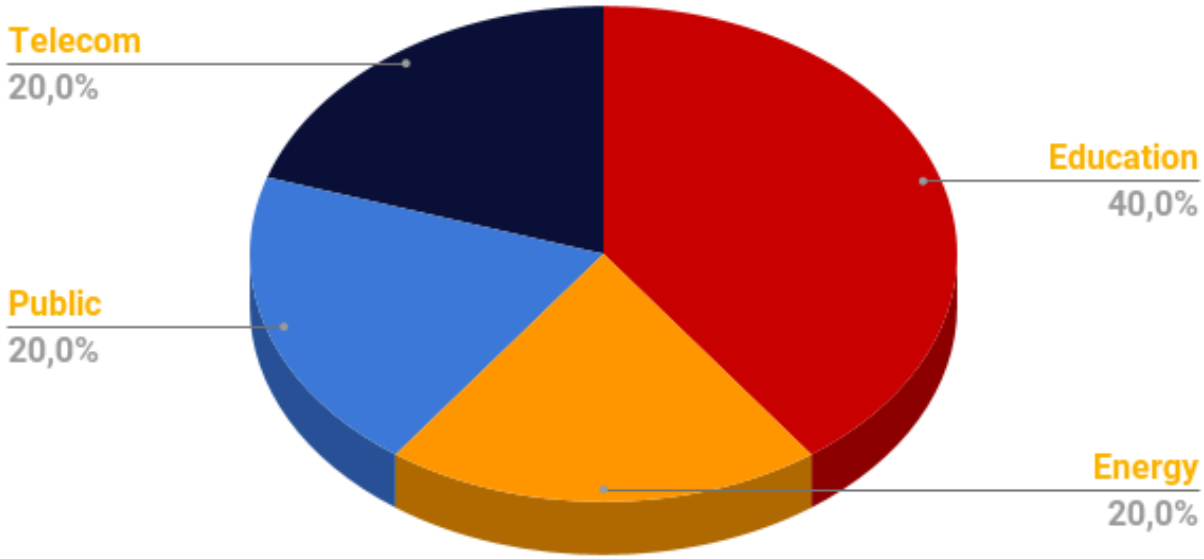
Their demands and messaging often included notable themes:

- Use of humor and regional references (e.g., “baguettes” for Schneider Electric).
- Payment requests in cryptocurrency, particularly Monero and Bitcoin.

The scale and nature of these incidents suggest a sophisticated and coordinated operation by Hellcat.



SECTORS TARGETED BY HELLCAT



Hellcat ransomware group adopted a multi-pronged attack strategy targeting various sectors. When the sectoral distribution is analyzed, the education sector has the highest attack rate with 40%. After the education sector, the energy, public and telecom sectors are targeted at equal rates of 20%.

This multi-sectoral targeting approach shows that Hellcat aims to neutralize or compromise critical assets and sensitive data in different sectors, not just a specific area.

UNIQUE CHARACTERISTICS OF THE HELLCAT RANSOMWARE GROUP

Humor in Communications

- Cultural References in Ransom Notes: Hellcat's ransom demands often include humorous or culturally specific references. For example, in the Schneider Electric attack, they demanded "baguettes" instead of traditional currency, a nod to the French origin of the company.
- Taunting Victims: The group uses humor to taunt victims, which sets them apart from the typically somber tone of ransomware negotiations.
- Public Announcements: Their announcements on leak sites or communication channels often contain jokes or sarcastic remarks, giving them a distinct personality among ransomware actors.

Aggressive Target Selection

- High-Value Targets: They prioritize attacks on government agencies, large corporations, and critical infrastructure.
- Focus on International Targets: Hellcat appears to avoid a regional focus, targeting entities from Europe, Africa, and the Middle East.
- Sensitive Data Emphasis: They are known for exfiltrating and threatening to leak highly sensitive data, aiming to maximize their leverage.

Sophistication in Execution

- Precision Attacks: Their operations demonstrate advanced planning and reconnaissance. The breach of Schneider Electric’s Atlassian Jira system indicates expertise in exploiting niche software vulnerabilities.
- Selective Encryption: Instead of encrypting entire systems, Hellcat targets critical files to avoid detection and speed up the process.

Use of Psychological Pressure

- Dual Extortion Tactics: They not only encrypt files but also threaten to release stolen data publicly if demands are not met.
- Deadlines and Escalation: Hellcat uses strict deadlines and incremental ransom increases to pressure victims.
- Reputation Damage Threats: By targeting government and educational institutions, they exploit the fear of public scandal to push for compliance.

Sophisticated Branding

- Distinctive Group Identity: Hellcat has worked to establish itself as a recognizable entity in the cybercrime ecosystem, distinguishing itself from other ransomware groups through branding.
- Leak Site Aesthetics: Their data leak site features a polished design, and their announcements are formatted to draw attention from media and cybersecurity professionals alike.
- Dark Web Recruitment: They actively promote their activities on dark web forums to recruit affiliates or collaborators.

Rapid Adaptation

- Tactics Evolution: Despite being a relatively new group, Hellcat has quickly adapted to new trends, such as the shift from encryption-only attacks to sophisticated double-extortion campaigns.
- Awareness of Security Trends: They seem to be aware of how cybersecurity defenses evolve and actively adjust their methods to bypass new security measures.

Global Footprint

- Multinational Impact: Hellcat's operations span across multiple countries and industries, indicating they have the resources and network to operate on a global scale.
- Target Diversity: They do not limit themselves to specific sectors but aim for varied victims, from energy management companies to educational institutions.

Provocative Public Image

- Taunting Security Researchers: Hellcat occasionally mocks cybersecurity experts on forums, signaling confidence and attempting to build a bold image.
- Media Attention: Their humorous and provocative communications are designed to attract media coverage, amplifying their presence and creating additional pressure on victims.

HELLCAT MEMBERS HELLCAT MEMBERS AND HISTORICAL CHANGE IN MEMBERSHIP

According to information obtained from Onion websites, known members of the Hellcat group include people operating in various roles. All members of the team use login addresses, and Rey, Miyako and Gwap also use these login addresses on BreachForums.

In general terms, Pryx was responsible for all operations, Rey was the Group Administrator, Grep and Gwap handled development, and Miyako and AnonBF handled initial access sales. Hellcat Ransomware Group, which received external help in the development of the ransomware malware, also received support from names such as SoupsInSuits, SMeu, Sukob at this stage.

IntelBroker is described as a prominent figure in the world of cybercrime and has recently been associated with the Hellcat Ransomware group. IntelBroker has attracted attention with his posts and targeting globally recognised companies. This may have contributed to the increased influence and visibility of the Hellcat Ransomware group. However, it is claimed that IntelBroker is not an official member of this group, but only in co-operation.

IntelBroker's activities are particularly focused on high-profile targets. Its data leak posts on various platforms attracted attention. It is assessed that this co-operation may expand the group's reach and pave the way for more sophisticated attacks.

IntelBroker's online presence is particularly concentrated on dark networks and platforms such as Telegram. His posts on these platforms show that he is a figure with technical know-how, but it remains unclear whether his connection with Hellcat is a strategic partnership or a deeper co-operation.

DOX CASE

Hellcat Ransomware group, which started with 7 members since its establishment, lost members and power after a dox case involving one of its members, Pryx. Rey and Miyako also left the group, bringing the number of members down to 5.

A member of a popular dark web forum published a post claiming that on December 8, 2024, Hellcat ransomware group member Pryx exposed a member named “netnsher”. Pryx later denied on his social media account that the doxing was his and then targeted and exposed threat actor Emo. While Emo's past is associated with serious crimes and manipulations, Pryx shared this information with the community and used it as an effective tool to target those around Emo.

Pryx's move is believed to have caused “Rey” and “Miyako”, members of the Hellcat ransomware group, to leave the group. Investigations show that the person Pryx exposed had a direct relationship with these two group members, which upset the group's dynamics. Tensions within the group increased after Rey and Miyako's departure, and Pryx's revelation seemed to be a turning point that caused the split.

In addition, Pryx's subsequent attempt at self-pity is also noteworthy. His statement on his Telegram account, “I am a 17-year-old boy, a fascist waiting to be deciphered”, can be considered as an attempt to deflect the backlash caused by the disclosure. Pryx's statements stand out as both a personal defense mechanism and a move to turn the incident in his favor.

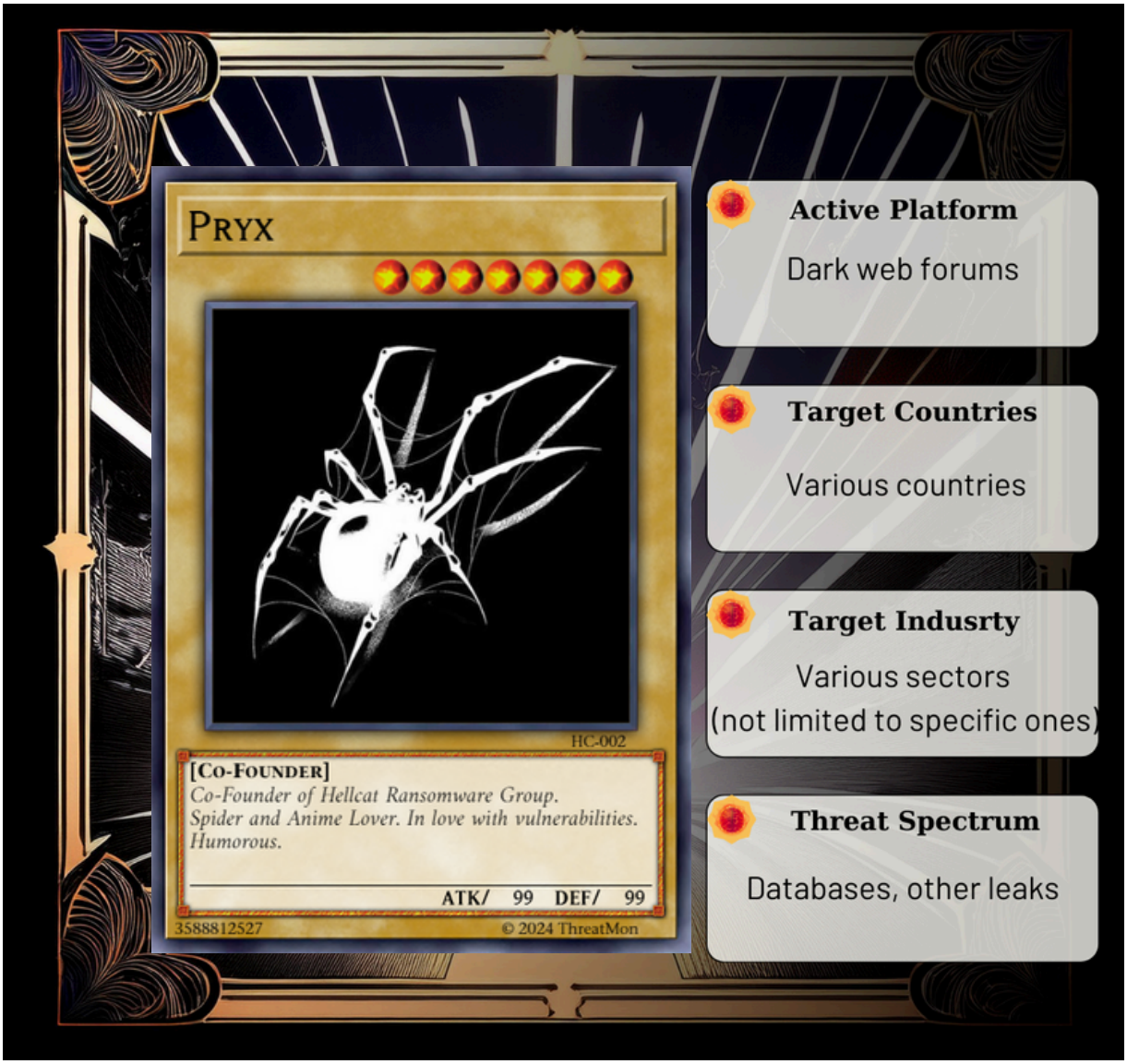
During this process, our team analyzed the ransomware site belonging to the Hellcat group and observed that “Rey” and “Miyako” were removed from the membership. Pryx's denial of the disclosure must have worked because Rey and Miyako were reinstated shortly afterwards and the team became 7 people again.

HELLCAT MEMBERS

Rey, the Hellcat ransomware group administrator, is also known by the aliases Hikkl-Chan and Wristller.
In addition, as a result of the information obtained through various open source intelligence methods, various social media accounts were identified. Rey is also a serious anime fan and loves to play valorant.

An intelligence investigation by our team revealed that Rey has several social media accounts. From these accounts, it appears that Rey is a serious anime fan and likes to play the game Valorant. In addition, as a result of the research conducted by our team, a private channel with Hellcat group and Breachforum members was detected on the Discord platform. Another noteworthy point in the channel is the presence of a profile that identifies itself as “Rei” and is very similar to the nickname Wristller. Although the similarity between the usernames Rei and wristller and the presence of some other members on the discord channel raise the possibility that they may be the same person, no definitive conclusion has been reached on this matter. Rei's social media posts also include the information that he as a black cat named Bumi .

On the channel, it was seen that there was a user who identified herself as “Rei” and whose username was very similar to the nickname Wristller. Although Rei has publicly stated that he is not Rey, the similarity in usernames, the presence of some other members on the Discord channel and other details shared raise the possibility that they could be the same person. But is all of this together just a coincidence?



Pryx is a 17-year-old spider lover and one of the young genius (!) founders of Hellcat. He is also a member of the Dangerzone team. His motto is #Get_Pryxed. He posts this slogan on his Darkweb profiles.

He has a humorous personality and loves vulnerabilities. He likes to follow and exploit current vulnerabilities. It can be said that Pryx's love for vulnerability made these attacks successful in many attacks they carried out as a group.

Pryx is originally from Morocco and later immigrated to USA. He is ethnically Rufian.

Grep, a key developer for the Hellcat ransomware group and a former member of the CyberNiggers threat group, is a prominent figure in the world of digital crime. Known for his controversial online persona, he calls himself "Arkan's Tiger," a clear reference to Željko Ražnatović, the Serbian paramilitary leader infamous for his war crimes during the Yugoslav Wars. Grep's admiration for Ražnatović is evident in his actions, such as using this title on a popular dark web forum and featuring Ražnatović's image on his Twitter profile. These choices have fueled speculation that Grep may be aligned with Serbian nationalism, suggesting an ideological dimension to his criminal activities.

Arkan’s legacy, marred by war crimes, appears to influence Grep's behavior in the cybercrime world, where he has carved a similarly dark and dangerous path. His digital presence further amplifies his notoriety; he is highly active on social media, consistently engaging with other figures in the criminal underworld. This relentless activity, combined with his symbolic associations, portrays Grep as not just a technical threat actor but also a potentially ideologically driven figure, adding another layer of complexity to his role in the cybercriminal landscape.

Miyako is a figure operating in the depths of the cyber world, notable for her title of “First Access Broker”. The fact that she has the rank of “GOD” on BreachForums shows her power and reputation in this field. Miyako often sells access to various companies' systems on forums.

The information in her profile makes her even more mysterious. For example, even though his location is listed as “Korea” and his gender as “Female”, profiles like these are always surrounded by a veil of uncertainty.

Miyako has always said that classic ransomwares are boring(!) and that there is a need for better, newer and more fun ransomwares. She pointed out that this ransomware is Hellcat Ransomware.

The Telegram channel “FreshAccess” seems to be the center of Miyako's activities. It is also noteworthy that she changed her username several times.

AnonBF is an anime-profiled threat actor who operates under the alias “AnonBF” on BreachForums and “Death” on Dangerzone. As an Initial Access Broker (IAB) for the Hellcat ransomware group, he’s the guy opening the digital doors for cyber mayhem.

With a self-proclaimed love for “pwning,” AnonBF thrives on finding and exploiting vulnerabilities. His activity on BreachForums is a catalog of sales threads for first access—think of it as a darkweb shopping spree for cybercriminals. It wouldn’t be wrong to say that AnonBF’s knack for “pwning” has made him a significant asset to the Hellcat group’s operations.

Gwap, a member of the Hellcat ransomware group, is notable for his admiration of Debian. Towards the end of 2024, he posted content on social media claiming that the world was about to change. At the time of writing, Gwap was increasing his activity on the underground crime forum by sharing access sales, leaks and cracked accounts.

We see that SMeu has changed its name from ZMeu before and brought it to the new format. ZmEu is a computer vulnerability scanner software. The software was developed in Romania and was widely used, especially in 2012. Its name comes from Zmeu, a dragon-like being from Romanian mythology. Zmeu usually symbolizes evil, destruction and egoism and is defeated by heroes in fairy tales. Looking at the image of SMeu on the Onion website of the Hellcat ransomware group, it's hard not to notice the ZMeu fascination.

COMMON RESULT OF HELLCAT VS HELLDOWN COMPARISON

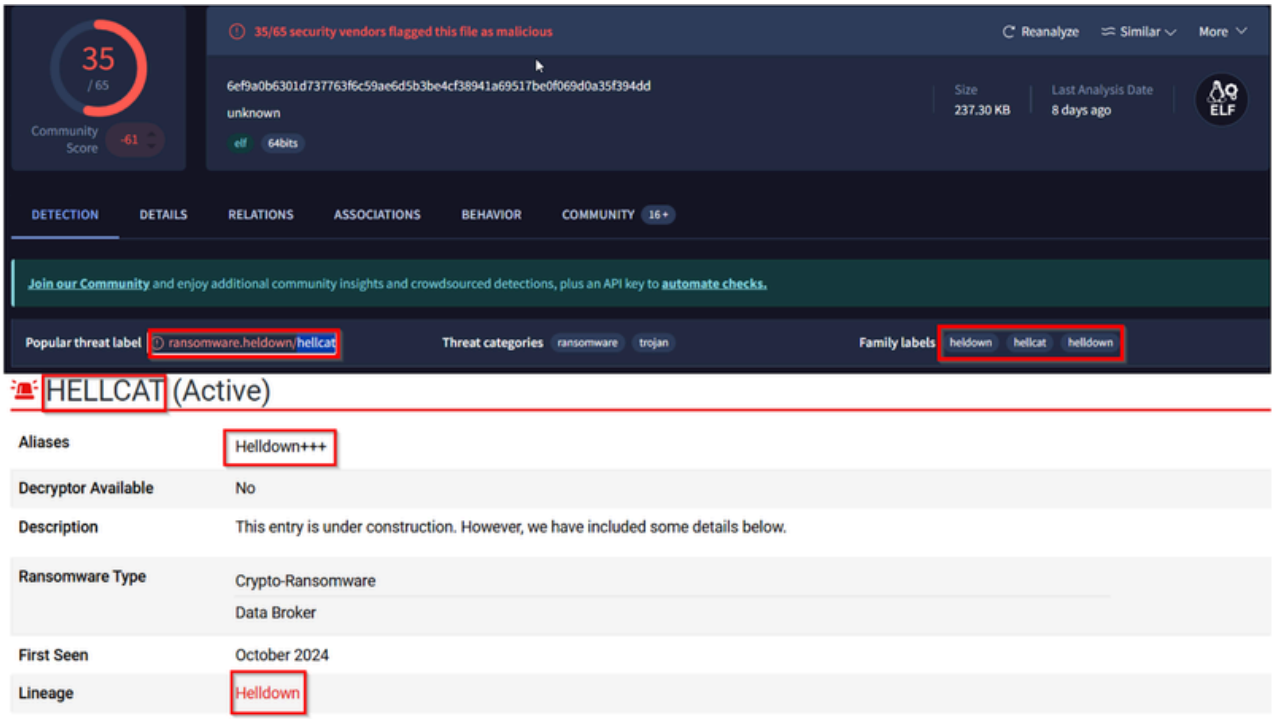


Image of Ransomware Threat Label from Virustotal and Group Overview from Watchguard

Hellcat and Helldown are often confused with each other due to the similarity of their names and dates of operation. Some intelligence sources consider the Helldown group to be of the same origin as an earlier version of the Hellcat. This title discusses the intelligence gathered and the conclusions reached.

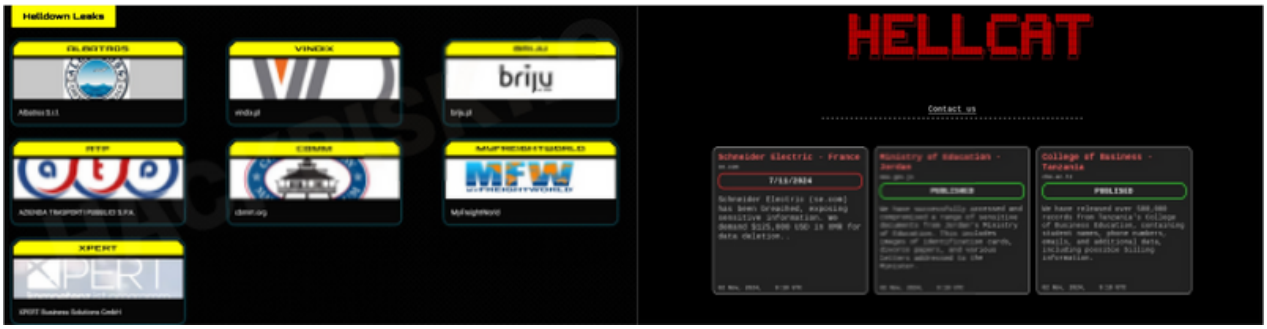


Image of Helldown and Hellcat Websites

The sites from which the two groups published data leaks on the Darkweb are completely different and independent of each other. They also have their own unique and independent designs.

DATE	VICTIM	ATTACKER	COUNTRY
2024-11-06	COMPASSFS	HELLDOWN	USA
2024-11-06	LACLINIQUEDUCOUREUR	HELLDOWN	FRANCE
2024-11-06	TIVOLI-33	HELLDOWN	FRANCE
2024-11-06	QUALIFORM.CZ	HELLDOWN	CZECHIA
2024-11-06	SMARTS-ENGINEER	HELLDOWN	GERMANY

DATE	VICTIM	ATTACKER	COUNTRY
2024-11-15	PINGER	HELLCAT	USA
2024-11-04	COLLEGE OF BUSINESS	HELLCAT	TANZANIA
2024-11-04	MINISTRY OF EDUCATION	HELLCAT	JORDAN
2024-11-04	SCHNEIDER ELECTRIC	HELLCAT	FRANCE
2024-10-25	THE KNESSET	HELLCAT	ISRAEL

It is observed that the two groups carried out attacks on similar dates. The last detected attack of the Helldown group was on 2024-11-06, while the last detected attack of the Hellcat group was on 2024-11-15. In the meantime, 2 days before the last attack of the Helldown group, it is observed that the Hellcat group carried out a detected active attack.

Image of a part of Hellcat website which Grep Threat Actor Takes Place

In the continuation of the research, it is observed that the threat actor “Greppy”, abbreviated as “Grep”, is included in the Hellcat group.

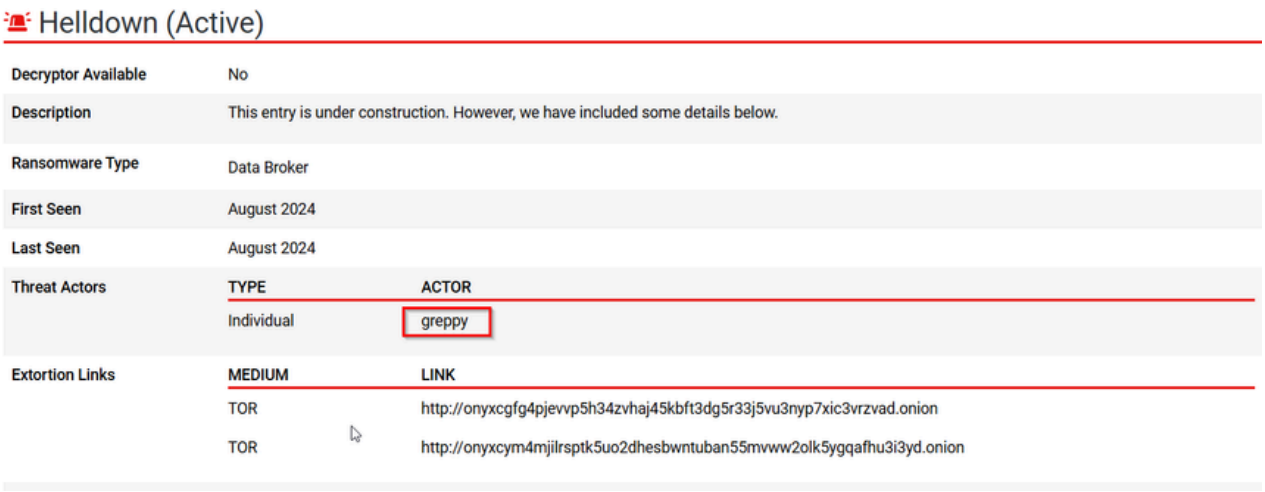


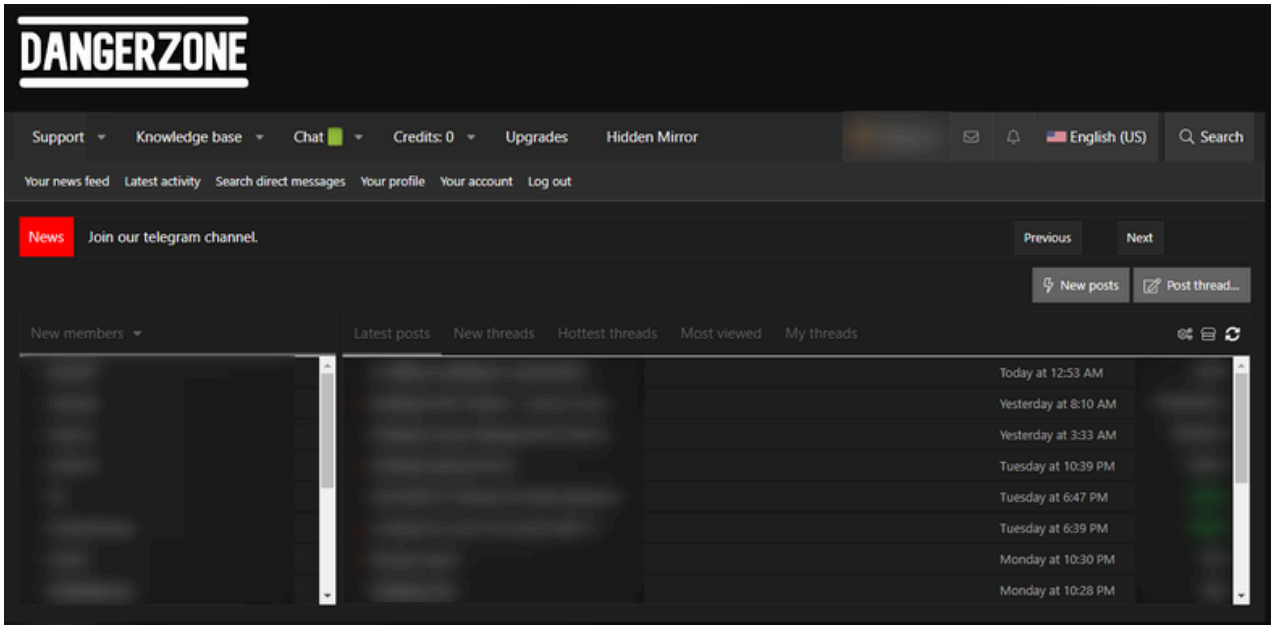
Image of Watchguard Helldown Group Overview From Watchguard

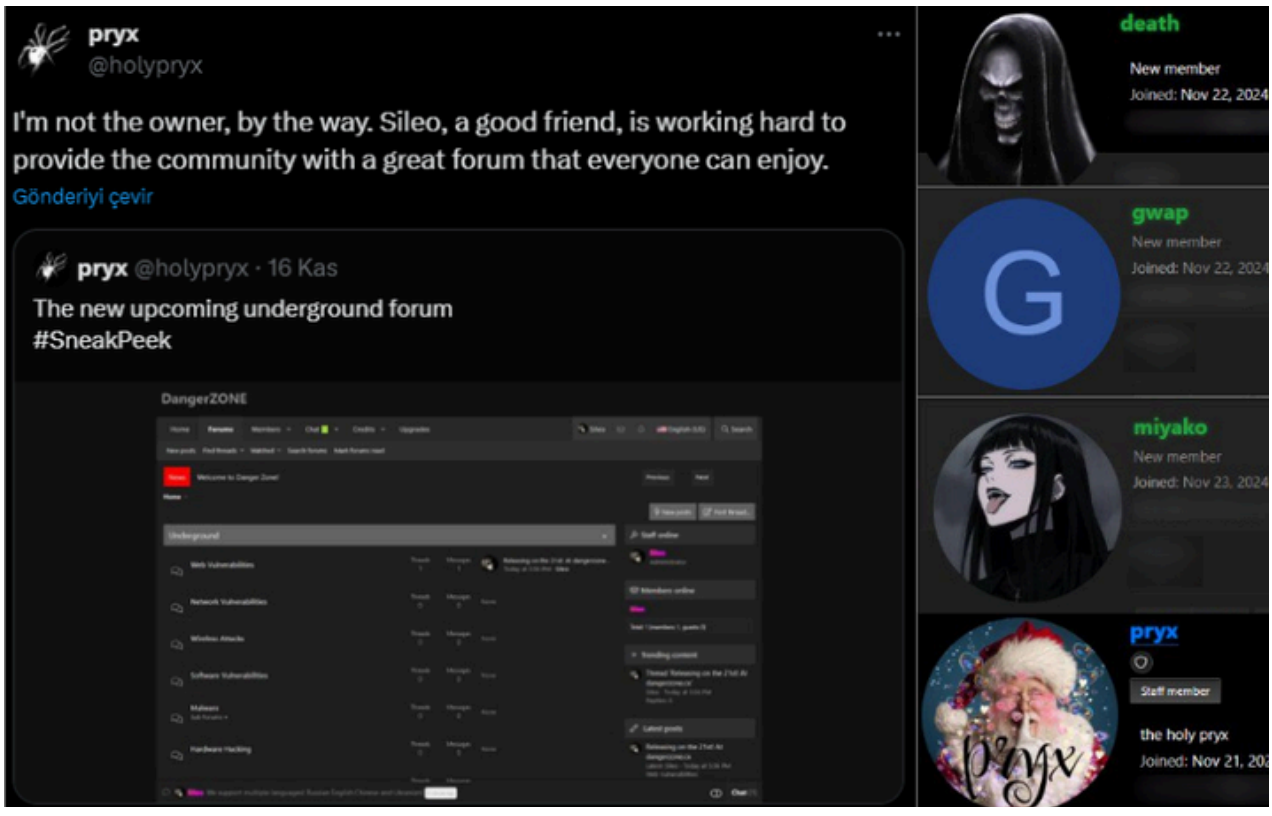
In the research carried out for the Helldown group, it was observed that the threat actor of the group was “Greppy”, as in Hellcat.

According to the conclusions drawn from the intelligence gathered, the Helldown and Hellcat group are two different groups. However, the threat actor “Greppy” is active both in his own group, Helldown, and in the “Hellcat” group, which he later joined. This threat actor, who is also known as the malware developer of the team, actively uses the products he developed for the Helldown group in the Hellcat group. For this reason, there may be cases where the two groups can be confused with each other.

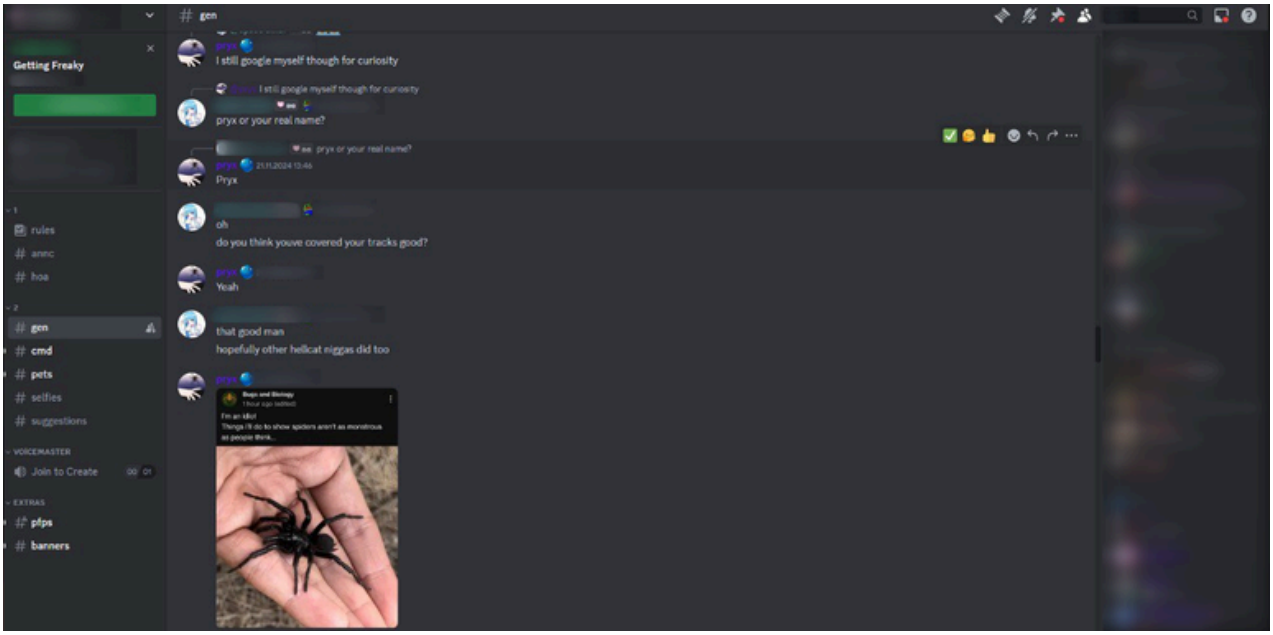
CONNECTION BETWEEN DANGERZONE FORUM AND HELLCAT

In mid-November, Pryx announced a new underground forum on Twitter. Our team investigated this forum and found that some members of the Hellcat group were active on the forum. According to another tweet by Pryx, the original founder of this new forum, Dangerzone, was Sileo, a friend of Pryx. Pryx's purpose in sharing the announcement was to show support for this project.

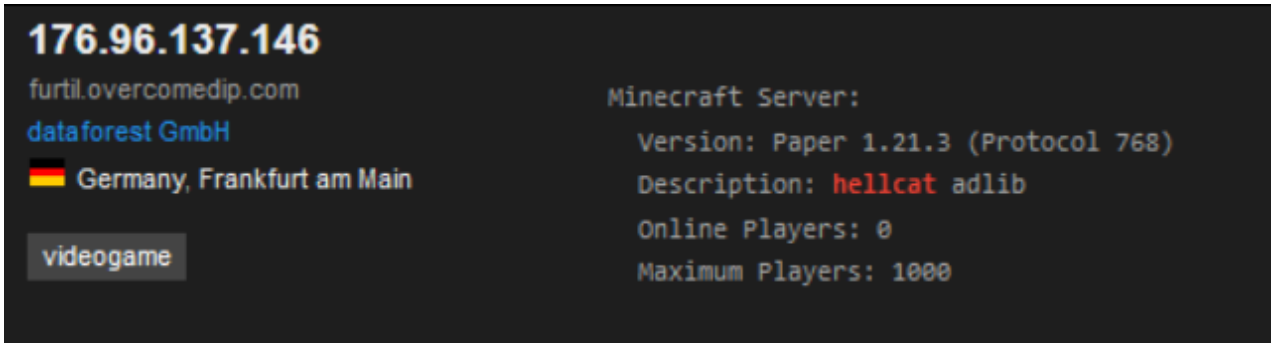




Investigations into the Hellcat ransomware group reveal that the group is active not only on dark web forums, but also on various messaging and group chat platforms. In particular, Hellcat members were found to communicate through groups created on popular platforms such as Discord and Telegram.



IP ADDRESSES ASSOCIATED WITH HELLCAT



After extensive scans, 176[.]96[.]96[.]137[.]146 IP addresses were found to be associated with Hellcat. Further investigation reveals that this IP address belongs to a Minecraft server. The server was found to be hosted by dataforest GmbH based in Frankfurt, Germany. The server is running on Paper version 1.21.3 and is registered with the description 'hellcat adlib'.

CONCLUSION

The Hellcat ransomware group has rapidly emerged as a prominent player in the global cyber threat landscape, leveraging psychological manipulation and striking branding. Their use of double extortion tactics and focus on high-value targets across various sectors highlight the group’s adaptability and potential danger as a threat actor.
The group's humorous and culturally nuanced communication style, while unconventional, serves as an effective psychological tool to amplify media attention and pressure victims. However, internal tensions, such as those stemming from the doxing incident involving key members, reveal vulnerabilities within their organizational structure. These dynamics may impact their operational stability and long-term cohesion.

Hellcat's targeting of diverse industries and global operations underscores the necessity for robust and adaptive cybersecurity measures. The group's rapid adaptation to emerging security trends and their focus on exploiting niche vulnerabilities emphasize the importance of proactive threat intelligence and continuous system hardening.

As Hellcat continues to refine its tactics and expand its reach, organizations must remain
vigilant, leveraging threat intelligence insights to anticipate and mitigate potential risks posed by this group. Collaborative efforts between cybersecurity professionals, government entities, and private organizations are essential to counteract the threats posed by advanced ransomware groups like Hellcat.