The Five Families: Hacker Collaboration Redefining the Game

socradar.io/the-five-families-hacker-collaboration-redefining-the-game/

November 3, 2023

At the end of the Summer of 2023, five hacker groups, including **ThreatSec, GhostSec, Stormous, Blackforums, and SiegedSec**, have collectively formed an entity known as “The Five Families.” The name ‘Five Families’ potentially draws its inspiration from the influential Italian-American families engaged in the New York mafia during the 1950s and 1960s. However it may also draw inspiration from the renowned **“Five Eyes”** intelligence alliance, an international intelligence-sharing partnership between five English-speaking countries: the United States, the United Kingdom, Canada, Australia, and New Zealand. This collaboration signified a pivotal shift in cybersecurity as these groups united to maximize their reach and impact. In our interconnected digital world, this cooperative initiative enables the seamless exchange of knowledge, resources, and skills among the collectives, creating a potent force. As a result, The Five Families anticipate exerting a lasting influence on the digital sphere, shaping the direction of online activities in the times to come.

The Five Families

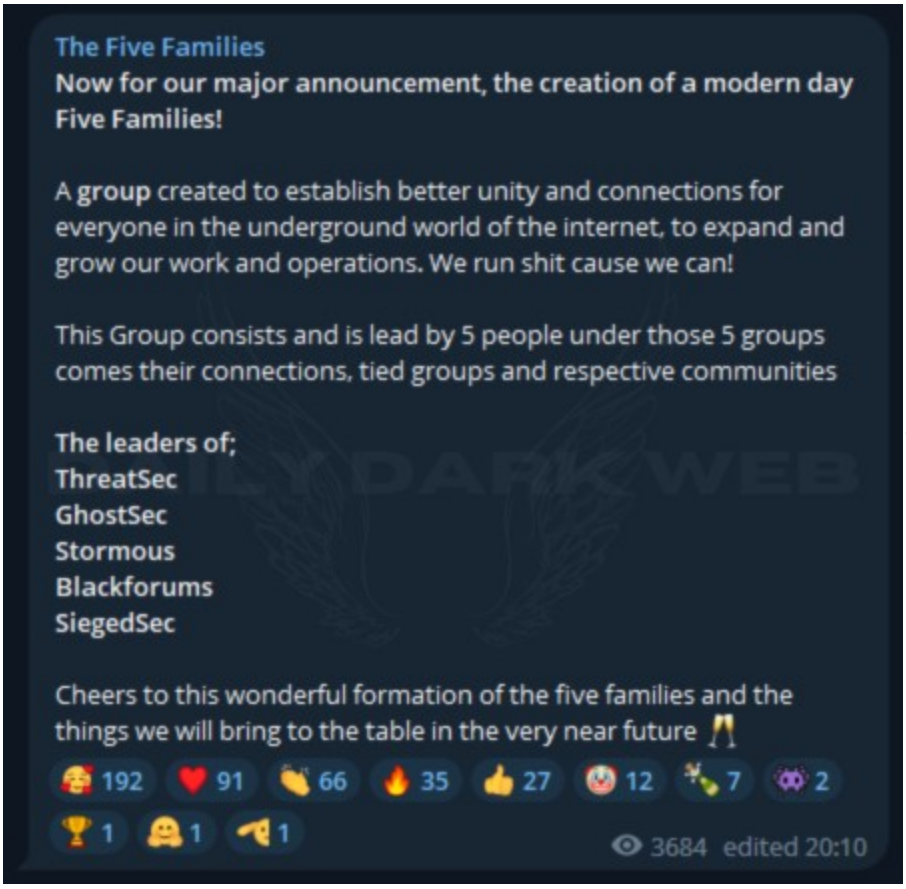
One instance illustrating this scenario is the participation of certain members from the Five Families in the cyber conflict between pro-Israelis and pro-Palestinians, which resulted in an expansion of hacktivists’ cyber arsenals and numbers. The introduction of GhostLocker Ransomware, previously covered in a distinct article and developed by pro-Palestinian

GhostSec, could potentially be a game-changer in digital warfare. By revealing that the Stormous Ransomware group, a constituent of the Five Families hacker consortium, intends to incorporate GhostLocker into their operations, we have witnessed how these groups can mutually assist and exert influence on each other.

Formation of The Five Families

On August 28, three hacker groups, a ransomware group, and a malware forum joined forces to create a unified hacker collective, naming themselves “The Five Families.” The alliance aimed to “forge stronger unity and connections for all within the underground realm of the internet.”

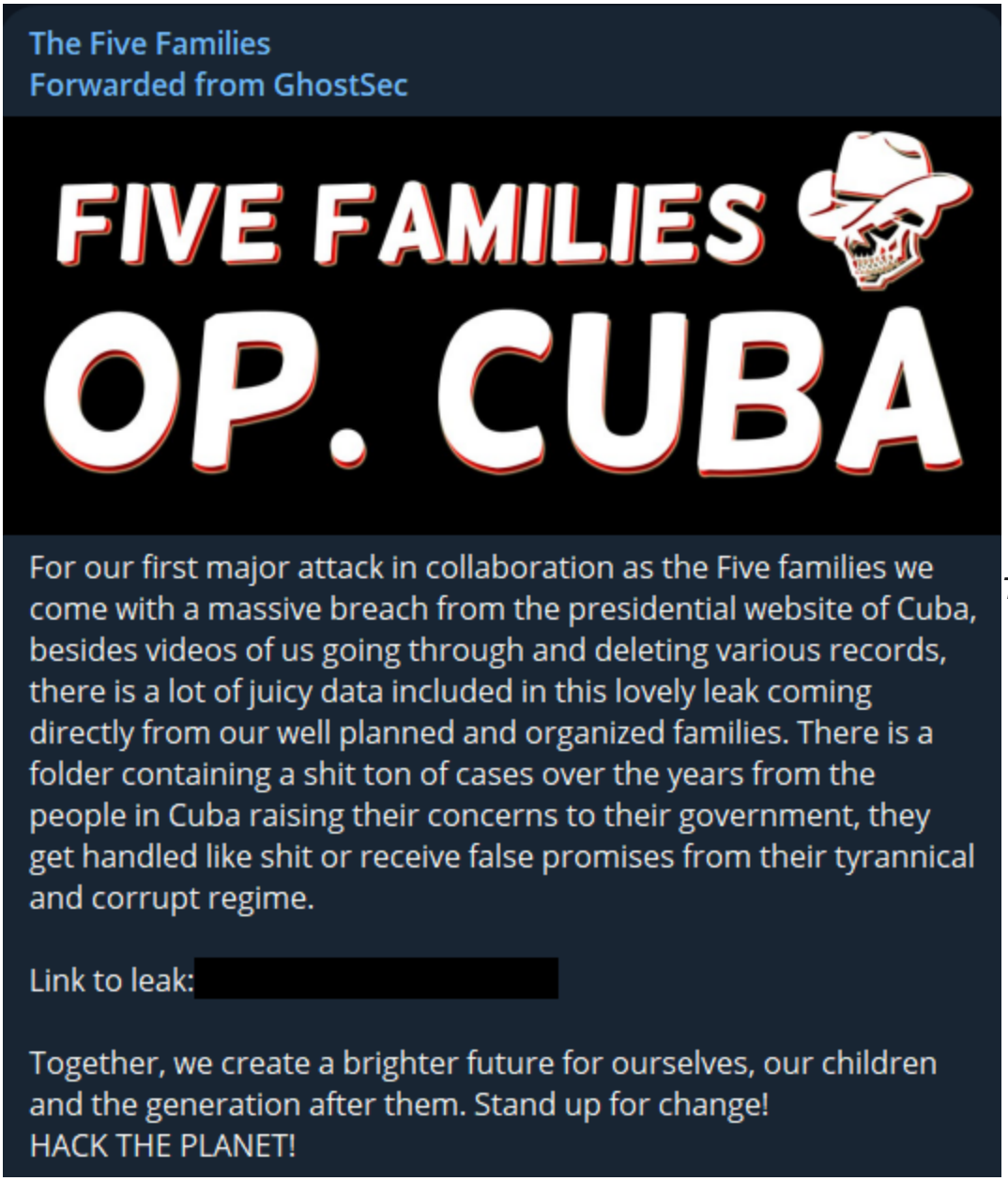
The existing alliance boasts a robust and intricate leadership framework where every member is on equal footing and mutually answerable. The coalition is led by leaders from the five groups, potentially implying that each leader assumes responsibility for decision-making and other pivotal functions.



The Five Families’ first post on their Telegram channel

Operations of The Five Families

The Collective announced its first operations a day later. Hacker groups that infiltrated the **Presidential website of Cuba** carried out their first major attack, claiming to have leaked many government data to the public and deleted various data from government systems.

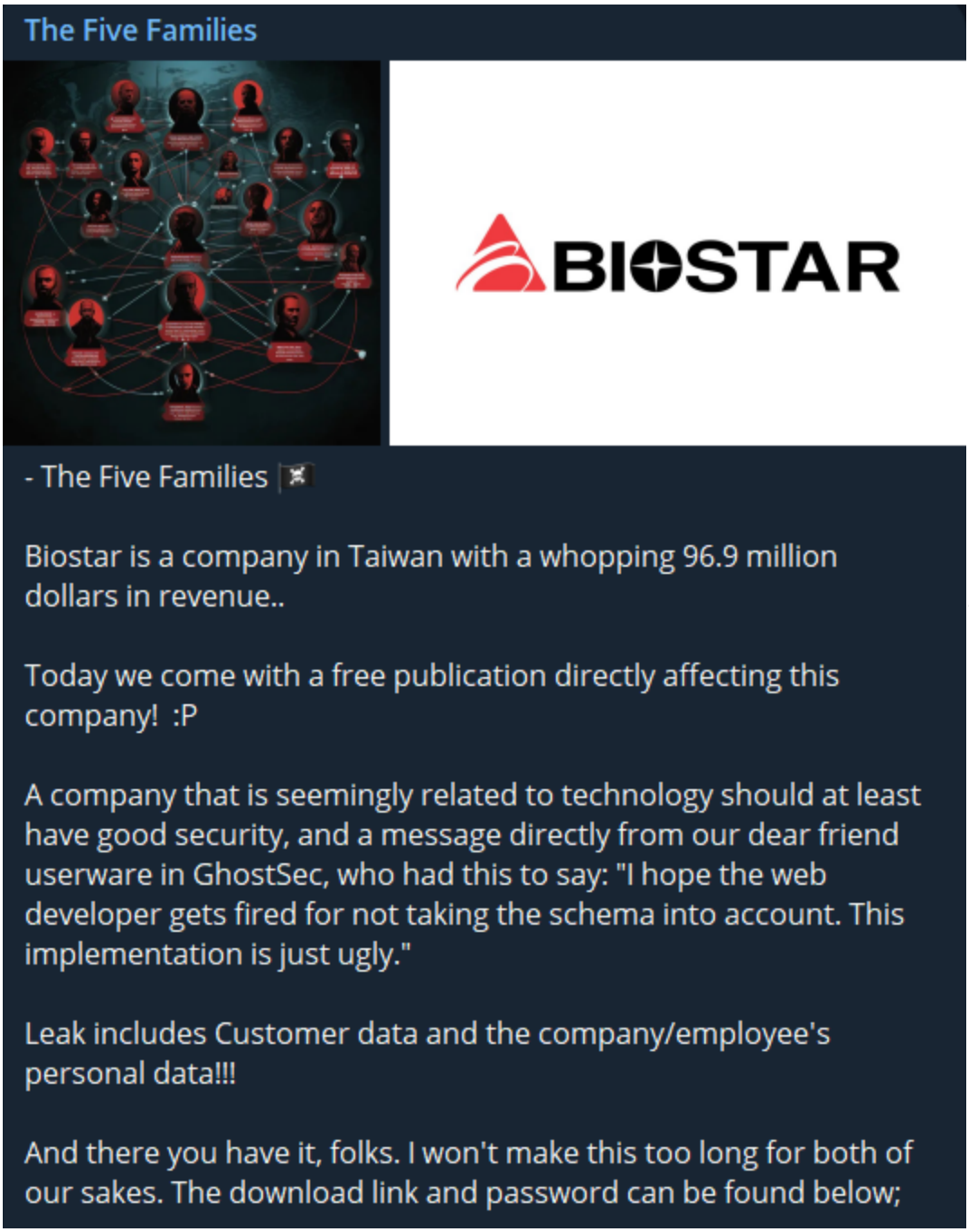


The Five Families' first major attack OpCuba

The next day, they targeted an organization in Brazil, a target from a similar geography. The group, which claimed to have breached the company called **Alfa Comercial**, provided the company with a Session ID to extort 230 GB of data. They also provided an e-mail address for those who would like to receive the data in case a scenario occurs where the company does not contact them. They uploaded sample data to their channel as a Torrent file.

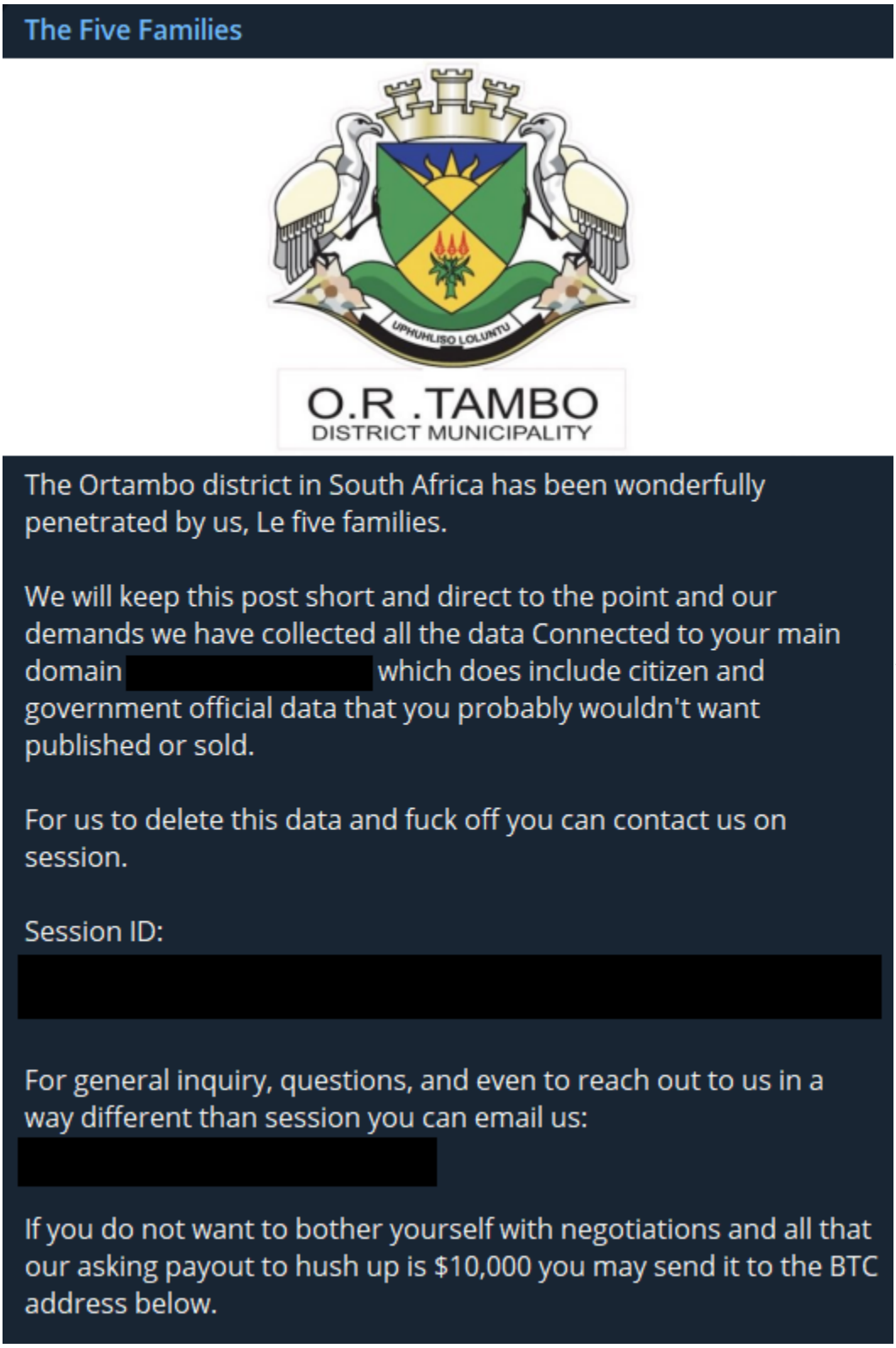
Second attack of The Five Families

Their third operation, a data leak, targeted a Taiwanese computer hardware company. The leaked data shared on Telegram channels was claimed to be customer data and company/employee's personal data.



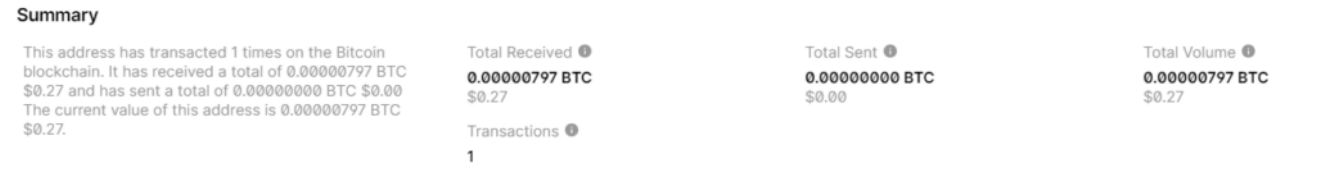
Third attack of The Five Families

The collective, which remained inactive for about a month after its first three attacks, announced its fourth attack in late September 2023, targeting **Ortambo District Municipality**.



The fourth attack by The Five Families on September 29, 2023

The group, which shared a session ID, also shared a BTC address. However, for now, there were no transactions in the wallet.



A screenshot of the wallet from blockchain.com

Lastly, on October 15, while they shared 85 GB of data from a Chinese chip company called Unisoc with a Torrent file on their Telegram channel, they said that this data was only a small part and tried to extort it again with a session ID.

Members of The Five Families

ThreatSec

According to an interview of Cybertecwiz with ThreatSec, under the leadership of its founder known as Wiz, it identifies itself as a group fighting for the rights and freedom of the oppressed. Wiz expressed their mission in the interview: *"We're here to fight for everyone's freedom and rights, and everyone should have their world to live in."* The group primarily targets corrupt governments, emphasizing that monetary gain is not their main motive.

Allegedly, ThreatSec distinguishes itself as a unique breed of hacktivists. Unlike many groups focused on monetary gain, they carefully select victims based on their potential to help local populations. Wiz stated that their goal is to set an example for others to better themselves and be free individuals.

ThreatSec utilizes various attack methods like Cross-Site Scripting (XSS), XML External Entity (XXE), and SQL Injection (SQLi), and is open to employing tactics such as ransomware and social engineering. The group also appears to be one of the rare groups declaring their **neutrality** in the Israel-Hamas conflict scorching the cyber world.

GhostSec

GhostSec, a prominent member of The Five Families, garnered considerable notice from both experts and the general public, particularly in light of their recent action involving **GhostLocker**. Altimetrik claims that this group, purportedly affiliated with **Anonymous** and often self-identifying as vigilante hackers, has assumed the responsibility of combating extremist content and activities on the internet.

GhostSec first came to light in 2015, originating from the remnants of the renowned hacktivist collective Anonymous. While Anonymous was known for its diverse operations, GhostSec adopted a more specific mission – countering online terrorism and violent extremism. With a skilled team of hackers and cybersecurity enthusiasts, they rapidly gained recognition for their unconventional approach to tackling extremist groups on the internet.

GhostSec's mission revolves around a somewhat ambiguous goal: disrupting the online presence and communication of terrorist organizations, such as ISIS (Islamic State of Iraq and Syria) and Al-Qaeda. However, although the group initially seemed to remain neutral in the ongoing Israel-Hamas war, it also decided "to support Palestine people against Israel's war crimes," according to its own claims.

Their approach involves identifying social media accounts, websites, and online platforms associated with these extremist groups and then launching precise cyberattacks to take them offline. Utilizing a range of hacking techniques, from Distributed Denial of Service (DDoS) attacks to defacement and data breaches, GhostSec allegedly aims to disrupt the propaganda machinery of these organizations. However, while discussing such noble causes, they did not refrain from developing modular ransomware that they would potentially sell to everyone.

SiegedSec

SiegedSec, a hacktivist collective, emerged coincidentally just days before Russia's invasion of Ukraine. Under the leadership of the hacktivist known as "YourAnonWolf," the group swiftly gained strength, announcing an increasing number of victims after its inception.

The group humorously self-identifies as "gay furry hackers" and is renowned for its comical slogans and the use of vulgar language. SiegedSec has affiliations with other hacker groups like GhostSec and typically consists of members aged between 18 and 26.

On April 3, 2022, the group established its Telegram channel, marking its initial appearance. In addition to carrying out cyber attacks, their chat channel is a hub for casual conversations and sexual humor.

Notably, SiegedSec's Twitter account has remained inactive for an extended period, likely due to frequent suspensions. This is evident from their Telegram posts expressing frustration about these suspensions.

The group's founder and administrator, "YourAnonWolf," currently manages the group under the pseudonym "vio." While there have been posts about vio leaving the group at various times, it remains unclear who took over when vio departed.

Stormous Ransomware

The Stormous Ransomware group has strategically capitalized on the escalating tensions between Russia and Ukraine. SOCRadar analysts suggest they attempt to gain notoriety by aligning with agendas similar to Conti's.

Threat intelligence experts have yet to agree on whether Stormous pursues these actions for political motives or future financial gains. Still, the prevailing belief is that this is primarily an advertising campaign.

Stormous ransomware attacks are often labeled as “scavenger operations” in the realm of cybersecurity. These operations involve targeting companies whose data has **already been compromised** by previous threat actors. However, the general consensus on Stormous leans toward regarding it as a fraudulent enterprise.

As previously mentioned, it appears that the group is striving to establish a prominent identity and may intend to solidify its reputation through actual attacks in the future. Consequently, SOCRadar analysts are closely monitoring the group’s activities.

The group that has remained inactive for a long time recently made a resurgence with their previously inaccessible data leak site, now featuring additional pages and information. These updates include a primary page listing their recent victims, a “Shop” section offering data from specific companies for sale, and a “Job Application” page soliciting individuals skilled in extortion and hacking.

Furthermore, the group has forged a partnership with GhostSec, officially announced on July 13, 2023, via GhostSec’s Telegram channel. Together, they have declared their collaboration to target organizations in Cuba and have identified three Cuban government ministries as their primary targets. GhostSec has also expressed interest in potential joint operations targeting other countries. This situation later evolved into The Five Families Collective.

Despite presenting itself as a ransomware operation, it is uncertain whether Stormous employs ransomware in its attacks. Some of the data they claim to have stolen and shared has been debunked as fake, casting doubt on the credibility of their claims and intrusions. One of their latest announcements was that they will use GhostSec’s modular ransomware GhostLocker in their operations.

BlackForums

BlackForums, a prominent hacker forum and data marketplace, has gained notoriety within the cybercriminal underworld. This covert platform has become a hub for various illicit activities, serving as a rendezvous point for individuals and groups seeking to exchange sensitive data and malware. The group behind BlackForums actively promotes their services, inviting interested parties to engage with them on the platform. This level of openness and activity has attracted numerous cyber criminals, and the forum has established a reputation as a go-to destination for various cyber misdeeds.

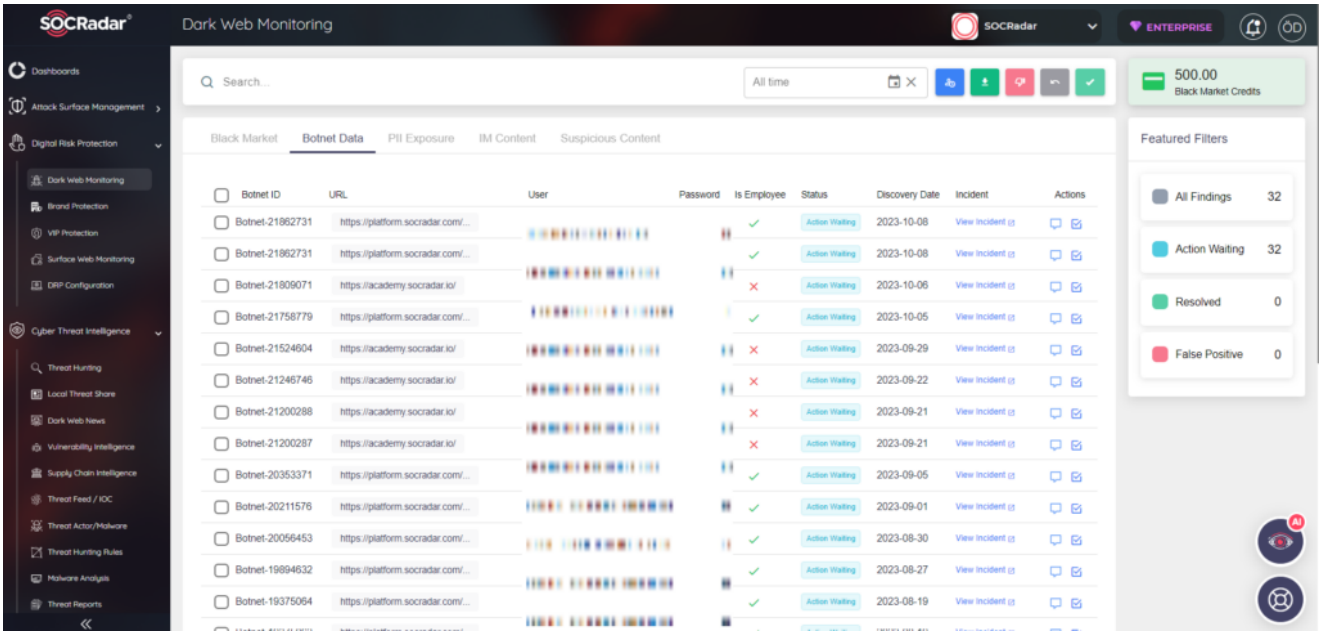
One significant aspect of BlackForums is its connection to ransomware data and malware distribution. Cybercriminals often utilize this platform to trade stolen information, offer malware for sale, and collaborate on various cyber exploits. Remarkably, BlackForums

operates openly on the **clear web**, making it more accessible to a **broader audience**. Its presence on the clear web is a testament to its operators' audacity and confidence in the forum's longevity.

The prominence of BlackForums came to the forefront when a high-profile attack on BreachForums exposed a stolen database. The threat actors behind this breach shared the compromised data on BlackForums.

Conclusion

In conclusion, as The Five Families bring together their diverse interests and capabilities, they find a temporary common ground, although their long-term cohesion remains uncertain. These groups, comprising ransomware operators, hacking forums, and hacktivist factions, have the potential to reinforce each other in various ways. The effectiveness of their collaboration, without specific objectives and rules, remains a question mark, but their collective potential is undeniably significant.



SOCRadar Dark Web Monitoring

In a world where even hackers are collaborating, it becomes imperative for the cybersecurity community to unite and adapt. Monitoring and understanding the actions of such groups is vital, and taking a proactive stance is crucial. SOCRadar's comprehensive Dark & Deep Web Monitoring solution equips organizations to detect and address threats across the surface, deep, and dark web, including platforms like Telegram. With our unparalleled reconnaissance capabilities and threat analysis, we provide actionable insights to empower you in safeguarding your organization proactively. Integrating automated external cyber intelligence with a dedicated team of analysts allows SOC teams to extend their reach beyond their immediate perimeters. It's a new cybersecurity era that demands **collective awareness and action**.