



| Flash |

GhostSec Announces Return to Hacktivism

F-2024-05-22a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Ransomware, Threat Group

May 22, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on May 22, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | GhostSec Announces Return to Hacktivism

› Key Findings

- On May 15, 2024, the threat group “GhostSec” announced on its official Telegram channel its intention to abandon financially motivated cybercrime and resume hacktivism activities.
- GhostSec is a member of the Five Families, a collective of hacking groups that has conducted financially, ideologically, and politically-motivated attacks against industries across the globe.
- GhostSec's renewed focus on hacktivism is very likely enabled by its financial success in leveraging GhostLocker ransomware-as-a-service (RaaS) in ransomware and digital extortion (R&DE) activity. In the short to medium term, GhostSec is likely to attempt disruptive and undermining attacks against the Israeli government, as well as other state institutions that are politically and ideologically misaligned with the group.

| Details

On May 15, 2024, GhostSec announced on its official Telegram channel its intention to abandon financially motivated cybercrime and resume hacktivism activities. According to the statement, the group's current “services” and Telegram channel will be closed, as it has “obtained enough funding” to enable future hacktivism operations.

- GhostSec first came to prominence in 2015 as an offshoot of the “Anonymous” collective, with an initial aim of combating Islamic State of Iraq and Syria (ISIS). GhostSec has almost certainly been focused primarily on politically and ideologically-motivated hacktivism activity since 2015.
- Since approximately Q3 2023, GhostSec has been conducting financially motivated cybercrime activities leveraging GhostLocker malware. This temporary shift in focus and tactics was almost certainly undertaken to amass enough funding to enable the group to eventually shift back to focusing on politically-motivated activity and resume targeting of its ideological opposition.
- In the statement, GhostSec alluded to its intention to provide an educational hacking course to forum members but appeared undecided on the content.

GhostSec

We'd like to announce GhostSec's leave from the financial motivation "CyberCrime" Scene. We as Ghosts have obtained enough funding through our times to continue funding our operations for a while we deem the cybercrime and ransomware we once promoted no longer necessary and will shift back to pure hacktivism what does this mean?

All this means is that we will not be providing services anymore therefore the Ghostsec services channel and services once provided will be closed, The ransomware Ghostlocker will be closed Though we will provide the entire code of V3 to Stormous and shift all buyers from GL to the new Stormous locker making it a clean exit without any exit scam. Five families will be taken over and Stormous will be in charge with the new associates involved in that organization resulting in our complete retirement from the "cybercrime" and ransomware scene!

What will remain? At the moment we will continue to keep our private channel and chat room available and will be running a discount from today until may 23rd, Get lifetime access to the private channel and chat room for \$400 \$250 ONLY until may 23rd. We may also plan soon to make and provide a hacking course/package though we are still debating on making this hack like a ghost course.

Thank you for your constant support, love and understanding. We are very excited to continue and put all focus into our work in changing the world to becoming a better place!

Fight for something you believe in and truly find it for yourself. Chase your own freedom, dreams and goals. Then Pass it on to the future.

Hack the planet!!

We Run Shit Cause We Can!

~GhostSec0

GhostSec announcement on its Telegram channel

Source: ZeroFox Intelligence

Since the outbreak of the Israel-Hamas war, GhostSec has been vocal in its support for Palestine, targeting Israeli critical national infrastructure and organizations.

- GhostSec conducted its first attack intended to harm Israel back in May 2022. Attacks have continued since then to the present.
- GhostSec has also conducted attacks against nations such as Russia, Iran, and France. The array of nations GhostSec has targeted shows no geopolitical trend, and it is very unlikely the group has any wider allegiance.



GhostSec announcing attacks conducted against Israel

Source: [hXXps://www.uptycs\[.\]com/blog/ghostlocker-ransomware-ghostsec](https://www.uptycs[.]com/blog/ghostlocker-ransomware-ghostsec)

GhostSec is a member of the Five Families, a collective of hacking groups that has conducted financially, ideologically and politically motivated attacks against industries

across the globe. Aside from GhostSec, the Five Families collective consists of the hacktivist groups “ThreatSec” and “SiegedSec” and the ransomware group “Stormous,” as well as Blackforums, a deep and dark web (DDW) forum used for illicit discussion and trading. In December 2023, SiegedSec was allegedly removed from The Five Families following the post of a statement appearing to promote paedophilia.

- The Five Families has conducted attacks against a diverse array of organizations across regions and industries. Despite their collaboration, the individual collectives are unlikely to be geopolitically or ideologically aligned.



GhostSec announce its intention to focus on hacktivism activities

Source: ZeroFox Intelligence

In the statement, GhostSec alleged that the GhostLocker malware, along with all associated affiliates, will be taken over by fellow Five Families member Stormous. According to GhostSec, this approach will ensure a “clean exit”, with no exit scam activity.

- GhostLocker is a RaaS operation that came to prominence in late 2023 and is reportedly available for USD 269.99 per month. GhostLocker versions 2.0 and 3.0 have almost certainly been leveraged by the Stormous ransomware collective in past digital extortion attacks.

GhostSec's resumed focus on hacktivism is very likely enabled by its financial success in leveraging GhostLocker in R&DE activity. In the short to medium term, GhostSec is likely to attempt disruptive and undermining attacks against the Israeli government, as well as other state institutions that are politically and ideologically misaligned with the group.

Recommendations

- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Configure ongoing monitoring for Compromised Account Credentials.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of R&DE threats; their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise (IOCs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system, and ensure all business IT assets are updated with the latest software as quickly as possible.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%