



| Flash |

GhostSec Hacktivist Group Launches Ransomware-as-a-Service

F-2023-11-14a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Malware, Threat Actor Targeting

November 14, 2023

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 (EST) on November 14, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | GhostSec Hacktivist Group Launches Ransomware-as-a-Service

› Key Findings

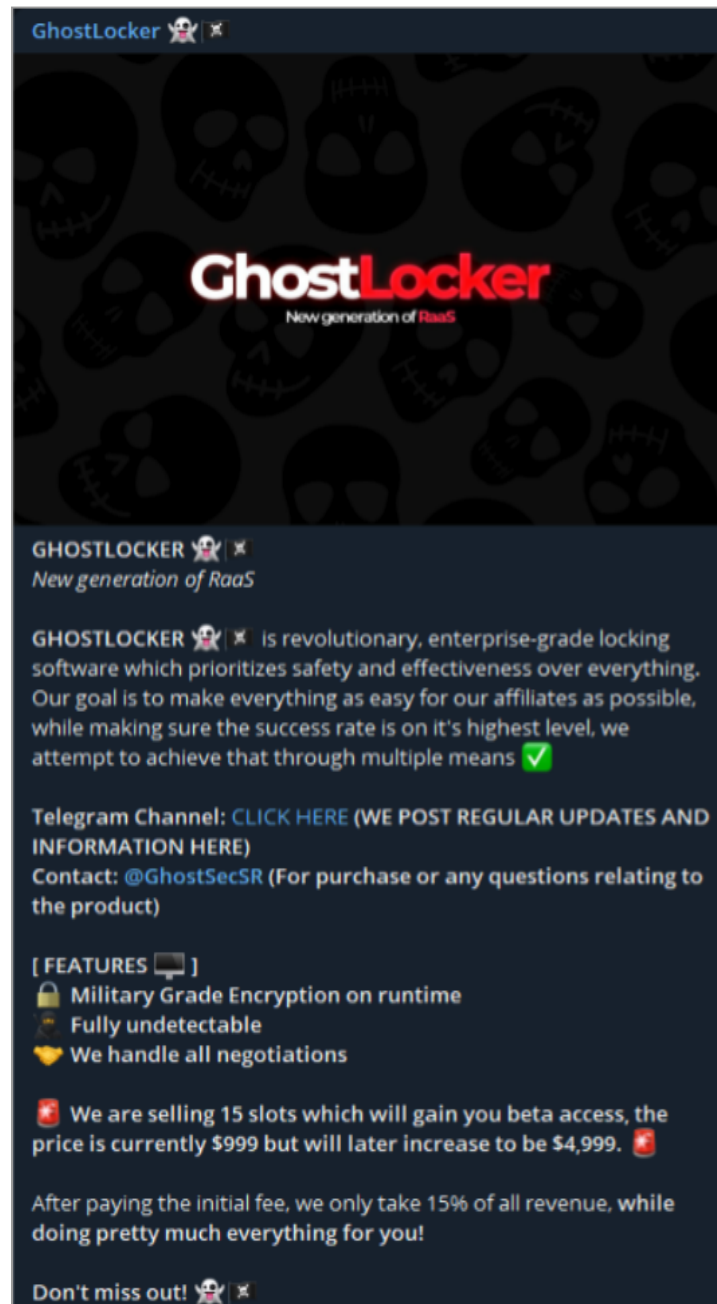
- Hacktivist group GhostSec launched a new generation ransomware-as-a-service (RaaS) called GhostLocker, which it is auctioning through November 18, 2023, or until 20 copies are sold. After that, access to the ransomware will be invite-only.
- GhostLocker ransomware offers alleged military-grade encryption, undetectability, negotiation services, and low fees to affiliates, setting it apart from other similar RaaS offerings.
- Stormous ransomware group has announced it will be incorporating GhostLocker ransomware into its operations.

| GhostLocker RaaS

On October 8, 2023, hacktivist group GhostSec announced the launch of GhostLocker RaaS on its Telegram channel. GhostSec claims that GhostLocker is a “revolutionary, enterprise-grade locking software.” The RaaS has its own Telegram channel for updates, which currently has 830 subscribers.

GhostLocker ransomware offers alleged military-grade encryption, undetectability, negotiation services, and low fees, setting it apart from other similar RaaS offerings.

The ransomware group charges its affiliates a 15 percent fee, which is lower than most groups. The RaaS was being sold at an initial price of USD 999 for 15 beta phase slots, but the advertisement states the price will later increase to USD 4,999.



GhostLocker RaaS announcement

Source: ZeroFox Intelligence

On October 14, 2023, ransomware group Stormous announced on its Telegram channel that it was incorporating GhostLocker ransomware into its operations. ZeroFox has observed Stormous and GhostSec partnering in the past on Stormous ransomware group's data leak site.

STORMOUS Ransomware

We officially announce that in our upcoming operations, we will be using a ransomware program named "GhostLocker" in addition to our program "StormousX" in collaboration with our allies at "GhostSec."

Stormous ransomware announcing the use of GhostLocker ransomware

Source: ZeroFox Intelligence

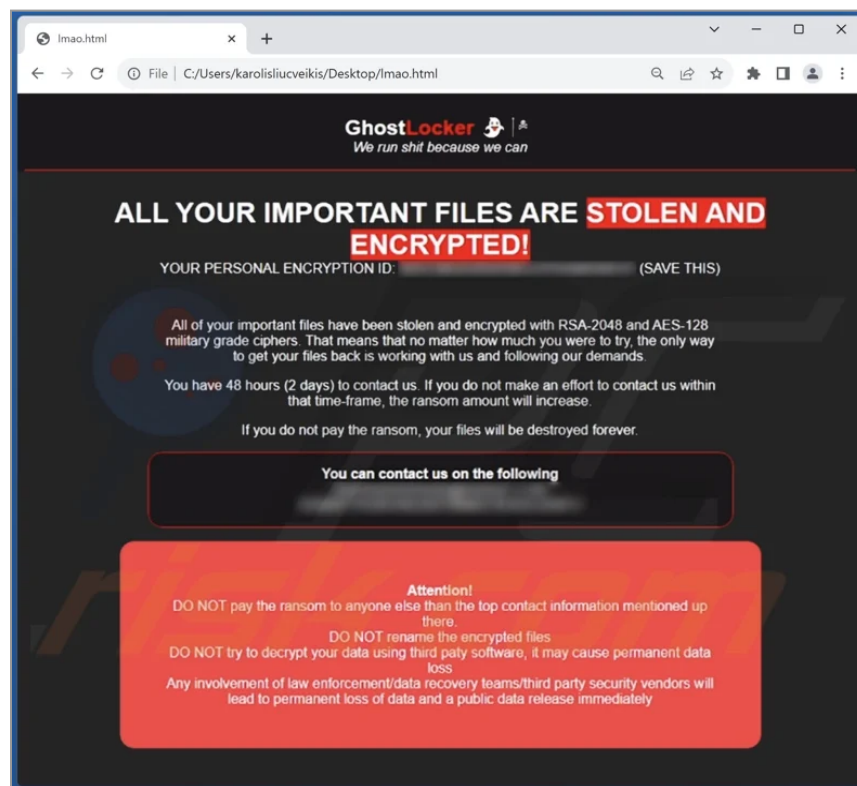
On November 11, GhostSec announced on its Telegram channel that the official sale of GhostLocker ransomware would occur in the next few days. The post specified there would be a one-week period wherein the RaaS could be purchased for the price of .03 BTC (approximately USD 1,099) until 20 copies were sold. Once that occurred, the ransomware would go off-sale while the group continued to enhance its capabilities and update it. From then on, the RaaS would be invite-only to protect the operators and affiliates.

- The following day, GhostSec announced that the GhostLocker rewrite was complete and ready for sale. The group reiterated that sales would be open for one week (closing on the 18th at 00:00 UTC) or until 20 copies were sold. GhostSec advertised some of the features, including, but not limited to:
 - Panel statistics to track locker launches, number of builds, and earnings
 - Enhanced builder capabilities to enable automatic privilege escalation for potential admin permissions, as well as an option to remove the background
 - Option for affiliates to lead negotiations via built-in chat or delegate negotiations to GhostLocker operators
 - Fast encryption and locker persistence that helps prevent stoppage of the locker encryption even if a machine is turned off in the process
 - No additional cost for the sale of breaches on member channels
 - Rewritten, metamorphic engine to increase stealth

- SmartCrypt option allowing GhostLocker to decide what to encrypt on its own
- Victims tab to see detailed information about victims targeted

| GhostLocker Encryption

During encryption, GhostLocker ransomware appends encrypted files with a “.ghost” extension.¹ After the encryption process is finished, a ransom note labeled “lmao.html” or “readme.html” is dropped onto the machine. The ransom note states that the victim’s files were encrypted using RSA-2048 and AES-128 algorithms and that sensitive data was exfiltrated. A ransom is required for decryption, and the victim is given 48 hours to contact the attackers, or the ransom price will increase. The note also states that if the victim does not pay the ransom, then data will be destroyed.



GhostLocker ransom note

Source: [hXXps://www.pcrisk\[.\]com/removal-guides/28068-ghostlocker-ransomware](https://www.pcrisk[.]com/removal-guides/28068-ghostlocker-ransomware)

¹ [hXXps://www\[.\]pcrisk\[.\]com/removal-guides/28068-ghostlocker-ransomware](https://www[.]pcrisk[.]com/removal-guides/28068-ghostlocker-ransomware)

| Analyst Commentary

Ransomware continues to be a persistent threat to organizations worldwide. There has been evidence over the last year of GhostSec targeting Israel in support of Palestine.² ZeroFox has observed recent posts on the GhostSec Telegram channel also targeting Israeli organizations, suggesting that GhostLocker ransomware may be used in future attacks against Israel.

GhostLocker ransomware's advanced capabilities show that ransomware is constantly evolving, which may make it harder to detect. It is likely that other ransomware groups will adopt certain features of GhostLocker ransomware to make their own more advanced as well. Based on GhostSec's previous partnerships, such as with Stormous ransomware, and its reach on the underground as an established group, ZeroFox assesses that GhostLocker copies will sell out in the one-week timeframe. It is likely that GhostLocker ransomware will gain traction and become more widely used over time, especially as affiliates bring in more members on the invite-only operation.

| Recommendations

- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Implement secure password policies with phishing-resistant MFA, complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform the detection of R&DE threats and 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.
- 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.

² [hXXps://www\[.\]uptycs\[.\]com/blog/ghostlocker-ransomware-ghostsec](https://www[.]uptycs[.]com/blog/ghostlocker-ransomware-ghostsec)

- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| Appendix A: Indicators of Compromise (IOCs)³

Sha256

- 0e484560a909fc06b9987db73346efa0ca6750d523f2334913c23e061695f5cc
- 4844f44c9de364377f574e4d6a8a77dc0b4d6a67f21ccbf693ac366e52eaa8cb
- 65d3a922754af96d8d722859ac31f3de96522d50659c67607021f2ac728f9630
- 15d874e24caf162bc58597ac5f22716694b5d43cf433bee6a78a0314280f2c80
- 663ac2d887df18e6da97dd358ebd2bca55404fd4alc8c1c51215834fc6d11b33
- a98f8468d70426ba255469a92d983d653f937d954e936e0ff5d9a0f44f1bdf70
- ee227cd0ef308287bc536a3955fd81388a16a0228ac42140e9cf308ae6343a3f
- 7d37eddf0b101ff2b633b2ffe33580bdb993a97fecc06874d7b5b07119b9ec99
- 7e14d88f60fe80f8fa27076566fd77e51c7d04674973a564202b4a7cbfaf2778
- 9b6be74c2c144f8bcb92c8350855d35c14bb7f2b727551c3dd5c8054c4136e3f
- abac31b5527803a89c941cf24280a9653cdee898a7a338424bd3e9b15d792972
- 4c09a012efff318b01a72199051815c5a7b920634fb6c76082673681f54f2ec3

URL

- hxxp://88.218.62[.]219/download
- hxxp://88.218.62[.]219/
- hxxps://88.218.62[.]219/download/
- hxxp://88.218.62[.]219/downloadp
- hxxp://88.218.62[.]219/downloadastatus_codel
- hxxp://88.218.61[.]141/addaCrypticMastera__main__a__module__auserConfiga__qualname__uchrome.exeapoces
- hxxp://88.218.61[.]141/adda__main__a__module__auserConfiga__qualname__uchrome.exeapocesuC:/Users/%25
- hxxp://88.218.61[.]141/
- hxxp://88.218.61[.]141/addp
- hxxp://88.218.61[.]141/incrementLaunchesT
- hxxp://88.218.61[.]141/incrementLaunches
- hxxp://88.218.61[.]141/add
- hxxp://195.2.79[.]117/

³ Ibid.

| Appendix B: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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 C: 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%