



| Flash |

Hunters International Increases Ransomware Activity

F-2024-02-26a

Classification: TLP:CLEAR

Criticality: Medium

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

February 26, 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 (EST) on February 26, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | Hunters International Increases Ransomware Activity

› Key Findings

- Ransomware and digital extortion (R&DE) collective Hunters International has significantly increased its operational tempo, having so far conducted at least 29 attacks in February 2024.
- Hunters International is a ransomware-as-a-service (RaaS) operation that was first observed in October 2023. Over the following quarter, affiliates leveraged the ransomware against a diverse set of global targets from an array of industries.
- Since Q4 2023, over 60 percent of R&DE attacks leveraging Hunters International ransomware targeted organizations based in North America. The most targeted industries are manufacturing, construction, and healthcare.

Details

R&DE collective Hunters International has significantly increased its operational tempo, having so far conducted at least 29 attacks in February 2024. This is more than twice the amount observed during January—and second only to prominent threat collective and ransomware strain LockBit.

Hunters International is a RaaS operation that was first observed in October 2023. Over the following quarter, affiliates leveraged the ransomware in attacks against a diverse set of global targets from an array of industries.

- Hunters International often forgo the double-extortion method that is popular amongst many R&DE threat actors. Instead, the collective opts to directly exfiltrate valuable data after gaining initial network access.¹ This is likely to increase attack simplicity and reduce both exploit costs and the risk of decryption.
- The group is widely thought to be associated with the Hive ransomware collective, which suffered severe disruption at the hands of law enforcement (LE) in Q1 2023.² Hunters International has denied any direct descent, though there is a roughly even chance that it is associated with developers that previously operated as a part of Hive.

Speculations About Us

We started to see that someone falsely decided that we are successors of the Hive ransomware group based on a 60% similarity of encryption code.

All of the Hive source codes were sold including the website and old Golang and C versions and we are those who purchased them.

Unfortunately for us, we found a lot of mistakes that caused unavailability for decryption in some cases. All of them were fixed now.

As you may see here, encryption is not our primary goal, that's why we didn't do it by ourselves.

Share on:



Hunters International statement posted to an open source website

Source:

<https://www.bitdefender.com/blog/businessinsights/hive-ransomwares-offspring-hunters-international-takes-the-stage/>

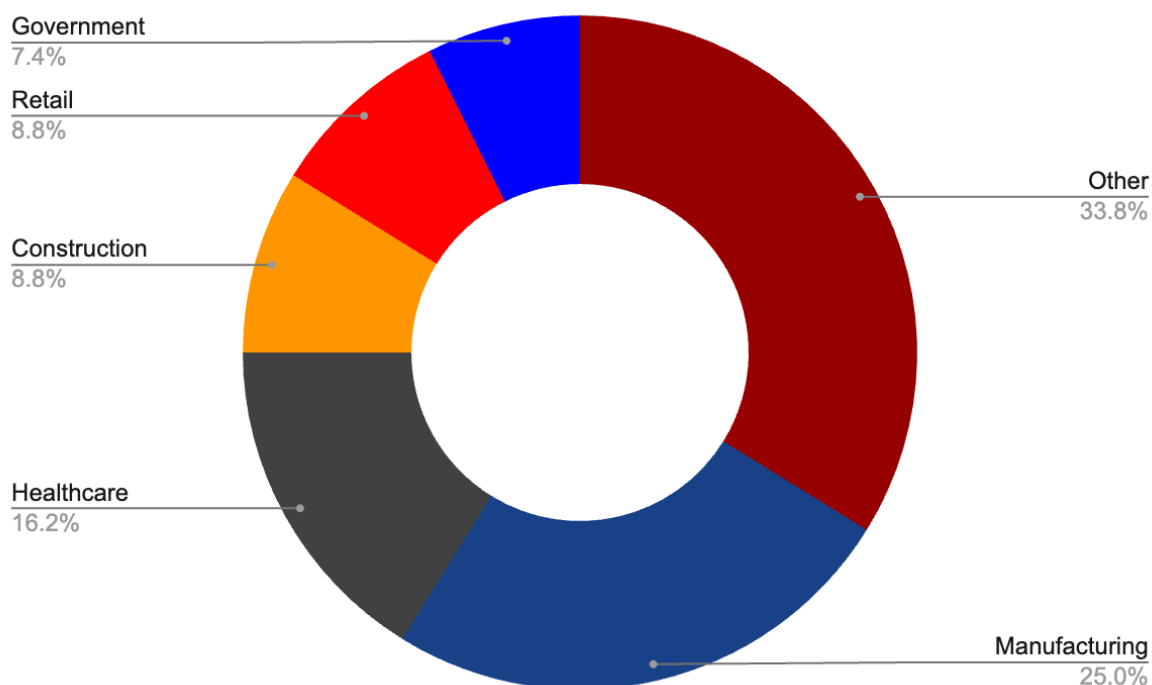
Since Q4 2023, over 60 percent of R&DE attacks leveraging Hunters International ransomware targeted organizations based in North America, the vast majority of which are in the United States. This is slightly higher than the 55 percent of global R&DE that

¹ <https://www.privacyaffairs.com/hunters-international-ransomware-targets-two-more-in-the-us/>

² <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>

target the same region. The most targeted industries are manufacturing, construction, and healthcare, with the latter accounting for over 15 percent of Hunters International's attacks—significantly higher than the global average of 8.5 percent.

- The observed targeting of the healthcare sector is likely due, in part, to the industry's association with sensitive patient information and proprietary data related to governmental and academic partnerships. Furthermore, the industry's criticality very likely makes organizations rendered inoperative by ransomware attacks more likely to submit to extortion demands.



Top five industries targeted by Hunters International ransomware

Source: ZeroFox Intelligence

There is a likely chance that the recent increase in Hunters International's activity can be attributed to the garnering of additional affiliates, some of which may have recently departed more prominent RaaS services, such as ALPHV and LockBit.

- ALPHV and LockBit, the two most prominent R&DE RaaS collectives of 2023, have been subjected to LE disruption over the past three months. The extent of the

disruption is not yet clear, though it is likely that some affiliates are seeking other RaaS operations to avoid LE attention.

There is a likely chance that the increased attack tempo from Hunters International will continue throughout Q1 2024, particularly if the operation has obtained a significant number of skilled affiliates. This is very likely further dependent on the extent to which the ALPHV and LockBit operations remain hindered—and the appeal of their operations to newer, would-be ransomware affiliates.

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 deep and dark web 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: Indicators of Compromise

SHA-256

- 94b6cf6c30f525614672a94b8b9788b46cbe061f89ccbb994507406404e027af
- c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e

MD5

- 46fc4776db5e40ee5e0341746ddd3443

SHA-1

- 0fc1feaef2b32fa7b77af80f729c761c600ef71f

Domains

- hunters33mmcwww7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd[.]onion
- hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid[.]onion

| Appendix B: 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 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%