ultraviolet

THREAT REPORT:

Hunters International Prioritizes Data Over Ransom with SharpRhino Tool

Services Performed By:
UltraViolet Cyber
Johnathon Moyer
(443) 351-7630
info@uvcyber.com

Published Date:
August 06, 2024

Contents

1 Executive Summary

'Hunters International' runs a Ransomware-as-a-Service (RaaS) organization, with a focus on exfiltrating data over ransom extortion. 'Hunters International' (HI) know that most organizations do not pay ransoms and instead focus on gathering marketable data they can broker to interested parties. If HI believes they have a good chance of extorting a ransom from a target, HI will deploy ransomware to the target environment. While their ransomware shares over half of its codebase with the 'Hive' ransomware strain, 'Hunters International' denies any affiliation with Hive.

2 Technical Analysis

Currently, 'Hunters International' attempts to stay out of the spotlight by avoiding large-scale ransomware activities. HI prefers to exfiltrate data, extort victims for money, then post the data on their website after a long period of time. HI's new tool, 'SharpRhino', was written in C# and acts as both an initial infection vector and as a remote access trojan. 'Hunters International' was first spotted in late October of 2023 and their activity online has grown sharply over 2024.

HI will exfiltrate data first, then encrypt endpoint files to the '.locked' extension, then leave a ransom note instructing the victim to contact the group via a TOR link. The encryption mechanism operates on Rust code, rather than C#, due in part to the difficulty in reverse-engineering the codebase. This activity is eerily similar to how Hive and BlackCat tools were developed. The initial file poses as a signed, legitimate tool 'AngryIP'. 'AngryIP' is an OpenSource tool, which lends to the ease of 'Hunters International' repackaging the tool with their own malware embedded. Once the file is unzipped and executed, the tool establishes persistence by modifying the Windows registry 'Run\UpdateWindowsKey' to point to the file 'Microsoft.AnyKey', mimicking a legitimate Windows filename.

Once the malware has installed on the endpoint, it will beacon out to a Command-and-Control server (C2) via HTTP POST with base64 encrypted text which itself is further encrypted. The tool will then wait approximately 26 hours before beaconing out again for instructions.

3 What UltraViolet Cyber is Doing

- Monitoring for registry modifications on endpoints through the use of our agent
- Network monitoring tools to alert on traffic to known malicious sites
- Monitoring for commands associated with malicious activity from threat actors

4 What Customers Can Do

- Ensure your endpoint security tools are up to date with the latest malware signatures
- Train users to only download tools from trusted sites
- Given the shared codebase with Hive, any detections previously created for the Hive strain should help with detection of 'SharpRhino' to some extent

5 References

Forret, M. (2024, August 06). SharpRhino – New Hunters International RAT identified by Quorum Cyber. Quorum Cyber. Retrieved from https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/

(2024, August 06). Threat Intelligence Hunters International Ransomware. Quorum Cyber. Retrieved from https://www.quorumcyber.com/wp-content/uploads/2023/11/QC-Hunters-International-Ransomware-Report-TI.pdf