From Hunters to Hunted: Quorum Cyber Exposes New Hunters International Remote Access Malware

Remote Access Trojan (RAT) Represents an Evolution in the Tactics, Techniques, and Procedures (TTP)

TAMPA, FLORIDA, UNITED STATES, August 6, 2024 /EINPresswire.com/ -- Quorum Cyber, a global cybersecurity firm, today announced that it has identified a novel new malware named SharpRhino. The malware, utilized by the threat actor as an initial infection vector and subsequent Remote Access Trojan (RAT), represents an evolution in the tactics, techniques, and procedures (TTP) of Hunters International, a prominent threat actor group believed to be affiliated with Russia.

Quorum Cyber's Threat Intelligence team discovered previously unknown malware during a ransomware investigation. Based on the TTPs observed and the identification within the ransom note itself, the malware was attributed to Hunters International. This research demonstrates that, despite a clampdown by international law enforcement agencies this year, Ransomware-as-a-Service (RaaS) threat groups continue developing their capabilities.

Named SharpRhino due to its use of the C# programming language, the malware is delivered through a typosquatting domain impersonating the legitimate networking tool Angry IP Scanner, which is popular with IT professionals. On execution, it establishes persistence and provides the attacker remote access to the device, which is then utilized to progress the attack. Using previously unseen techniques, the malware can obtain a high level of permission on the device to ensure the attacker can further their targeting with minimal disruption and gain sufficient control to conduct sophisticated ransomware operations.

"Typosquatting and watering hole attacks are just one tool in the threat actor's arsenal, used to prey on organizations. SharpRhino serves as a reminder that threat actors, particularly ransomware groups, given the financial gain they seek, are constantly developing new capabilities and identifying new ways to infiltrate their victims," said James Allman-Talbot, Head of Incident Response and Threat Intelligence at Quorum Cyber.

First observed in October 2023, Hunters International became the 10th most active ransomware group globally in 2024. Due to compelling similarities in the ransomware source code, the group has been attributed to the now defunct, Russia-based ransom group known as the Hive. Hunters International, which claimed responsibility for over 130 attacks in 2024, has positioned itself as a

RaaS provider, enabling other potentially less sophisticated threat actors with the tooling required to conduct additional attacks.

About Quorum Cyber
Founded in Edinburgh in 2016, Quorum Cyber is one of the fastest-growing cybersecurity companies in the UK and North America, with over 150 customers on four continents. Its mission is to help good people win by defending teams and organizations worldwide and all industry sectors against the rising threat of cyber-attacks, enabling them to thrive in an increasingly hostile, unpredictable, and fast-changing digital landscape. Quorum Cyber is a Microsoft Solutions Partner for Security, a Microsoft Intelligent Security Association (MISA) member, and a Microsoft Security Partner of the Year 2024 finalist. For more information, please visit Quorum Cyber or contact us at info@quorumcyber.us.

###

Source: BridgeView Marketing PR Services

Betsey Rogers
Bridgeview Marketing
betsey@bridgeviewmarketing.com
Visit us on social media:
X
LinkedIn
YouTube
