Published on *The National Law Review* https://natlawreview.com

SharpRhino Malware Targeting IT Professionals

Article By:

Linn F. Freedman

Information technology professionals—beware of SharpRhino—a malware variant attributed to threat actor cybercriminals associated with Hunters International. It is being reported that Hunters International is the "10th most active ransomware group in 2024." Hunters International has "claimed responsibility for 134 attacks in the first seven months of 2024." It has been linked to the defunct Russian-based Hive ransomware group. Hunters International is known as a Ransomware-as-a-Services provider, which increases the risk other threat actors will use its techniques.

The Quorum Cyber Incident Response Team has identified the SharpRhino malware, which is a Remote Access Trojan (RAT) that uses C# programming language "delivered through a typosquatting domain impersonating the legitimate tool Angry IP Scanner." This allows the threat actor with remote access to the device to obtain escalated privileges to proceed with the attack without detection.

Quorum Cyber has outlined the tools, techniques, and procedures of SharpRhino and Hunters International in its post, including samples, hashes, signing information, how it is installed, the C# code, IOCs, and Mitre ATT&CK mapping. Since this malware is targeted at IT professionals, you may consider giving a heads up to your IT professional staff.

National Law Review, Volume XIV, Number 221