New Hunters International RAT identified by Quorum Cyber

Archived: 2026-04-05 19:48:25 UTC

Introduction

During a recent ransomware incident investigated by the Quorum Cyber Incident Response team, a malware variant linked to the ThunderShell malware family was identified. The incident was attributed to Hunters International, based on tactics, techniques, and procedures (TTPs) observed during the investigation, as well as identification within the ransom note itself. It is highly likely that this is the first time Hunters International has been reported deploying this Remote Access Trojan (RAT), based on there being no indicators of previous use.

This malware, dubbed SharpRhino by Quorum Cyber, utilised by the threat actor as an initial infection vector and subsequent RAT, represents an evolution in the tactics, techniques, and procedures (TTPs) of Hunters International, demonstrating the continuous advancement and adaption of capabilities by Ransomware-as-a-Service (RaaS) threat groups.

The malware, named SharpRhino due to its use of the C# programming language, is delivered through a typosquatting domain impersonating the legitimate tool Angry IP Scanner. On execution, it establishes persistence and provides the attacker with remote access to the device, which is then utilised to progress the attack. Using previously unseen techniques, the malware is able to obtain a high level of permission on the device in order to ensure the attacker is able to further their targeting with minimal disruption.

This post outlines the Quorum Cyber Threat Intelligence team’s analysis of the malware and its capabilities, including a strategic outline of Hunters International as a prominent ransomware group. Also provided is a MITRE ATT&CK mapping, as well as Indicators of Compromise (IoCs) related to SharpRhino and Hunters International.

Source: https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/