Investigating the New Rhysida Ransomware

fortinet.com/blog/threat-research/investigating-the-new-rhysida-ransomware

November 15, 2023

The goal of the FortiGuard IR team is to provide organizations with valuable insights from threat analysis to bolster their security posture. We recently conducted a comprehensive analysis of an incident involving the Rhysida ransomware group, shedding light on their operations, tactics, and impact, including a novel technique involving ESXi-based ransomware.

The Rhysida Ransomware Group

The Rhysida group was first identified in May 2023, when they claimed their first victim. This group deploys a ransomware variant known as Rhysida and also offers it as Ransomware-as-a-service (RaaS). The group has listed around 50 victims so far in 2023.

The investigation conducted by the FortiGuard IR team and MDR team uncovered some of the techniques and tools used by Rhysida:

The initial detection was identified by the FortiGuard MDR team. The threat actor was observed accessing systems in a victim's network and attempting to create memory dumps and gather user data. FortiEDR detected these events, allowing the MDR team to analyze them further.

Following the initial detection and triage, the FortiGuard IR team was engaged to conduct a complete analysis.

Attack Details

The threat actors abuse legitimate software such as PowerShell to gain information about users and systems within the network, PSExec to schedule tasks and make changes to registry keys to maintain persistence, AnyDesk for remote connections, and WinSCP for file transfers. The threat actors also attempt to exfiltrate data from various systems using MegaSync.

The report also covers the additional malware the FortiGuard IR Team identified, along with a technique we don’t often see where the group deployed Windows and Linux binaries.

Restricting Veeam access to only designated machines hindered the threat actors from gaining access to the backup files. Moreover, the prudent management of passwords for vSphere fortified the victim's defense. The Rhysida ransomware group is known to target vSphere and look for credentials, so the safeguards that the victim implemented were vital to preventing widespread ransomware of the virtual infrastructure.

Staying informed on the landscape of cyber threats is critical. This analysis of the Rhysida group serves as a valuable resource for organizations. By uncovering motives and impact, the FortiGuard IR teams’ findings can guide proactive strategies.

For a comprehensive understanding of our investigation into Rhysida, including a list of Fortinet protections able to safeguard your organization, look at the full intrusion analysis report here.