AvosLocker and Rhysida Ransomware

C-Suite level threat review by applicable business area addressing active threats.

A dual ransomware attack occurs when threat actors target the same organization with two different ransomware variants over a short period of time, putting further strain on organizations' defenses. The FBI recently issued a warning on dual ransomware attacks, noting that this was an emerging trend in the threat landscape. AvosLocker, a ransomware variant described in this report, has been used in dual ransomware attacks. Organizations can strengthen their defenses by conducting tabletop exercises that account for dual ransomware attacks and update response and recovery plans accordingly.

AvosLocker:

AvosLocker is a ransomware-as-a-service operation that was first detected in July 2021. AvosLocker ransomware variants can compromise Windows, Linux, and VMware ESXI environments. Among the industries targeted are financial services, critical infrastructure, and government bodies. In a campaign that has been ongoing since May 2023, AvosLocker ransomware has been used to target critical infrastructure across the United States.

Rhysida Ransomware:

The Rhysida ransomware group emerged in May 2023. The group has compromised victims in Western Europe, North and South America, and Australia. Since it emerged, Rhysida ransomware has been observed targeting education, manufacturing, government, and technology sectors. Most recently, the ransomware group has turned its attention to healthcare organizations, claiming responsibility for the ransomware attacks on the Singing River Health System and Prospect Medical Holdings.

AvosLocker Ransomware

Threat Level: Medium

Attack:

AvosLocker leverages remote administration tools, such as AnyDesk, to connect to a victim's machine and gain initial access into an organization (MITRE T1133). AvosLocker can then restart a compromised machine in safe mode, impairing defenses (MITRE T1562.009). Affiliates are known to use living off the land techniques (i.e., use legitimate system functions) to aid in compromise. Examples of this include using native Windows tools such as PsExec and Nltest. Affiliates are also known to utilize open-source tools to support their attacks. Tools include Mimikatz and LaZagne for credential harvesting (MITRE T1555), Chisel and Ligolo for protocol tunneling (MITRE T1572), Cobalt Strike and Sliver for command and control, and FileZilla and Rclone for data exfiltration. The group employs double extortion ransomware, which is when the data is both encrypted and exfiltrated.

Remediation:

- Prevent an attacker from leveraging remote administration tools by disabling or blocking unnecessary remote services and/or limiting access to remote services.
- Implement network segmentation to prevent the spread of ransomware across your organization.
- Test and validate your organization's security controls against the MITRE ATT&CK techniques utilized by this threat actor.

Rhysida Ransomware

Threat Level: Medium

Attack:

Rhysida threat actors gain initial access into organizations through phishing emails (MITRE T1566). Upon compromise, the threat actors have been observed deploying Cobalt Strike for command and control (MITRE T1071). The malicious actors then utilize Cobalt Strike and PsExec to deploy PowerShell scripts and the ransomware payload itself (MITRE T1059.001). It can also deploy SILENTKILL, a malware that is able to terminate AV processes (MITRE T1562.001), delete shadow copies (MITRE T1490) and modify active directory passwords (MITRE T1098). The threat actor will encrypt and exfiltrate data, which is known as a double extortion ransomware attack.

Remediation:

- Conducting phishing simulations quarterly to ensure users are trained to be vigilant of phishing attempts.
- Implement email phishing protection.
- Acquire an Endpoint Detection and Response (EDR) tool to help detect and prevent the spread of ransomware.

AvosLocker Ransomware Details:

- **Joint cybersecurity advisory:** https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-284a
- **News coverage of AvosLocker Ransomware:** https://www.darkreading.com/ics-ot/feds-beware-avoslocker-ransomware-attacks-critical-infrastructure

Rhysida Ransomware Details:

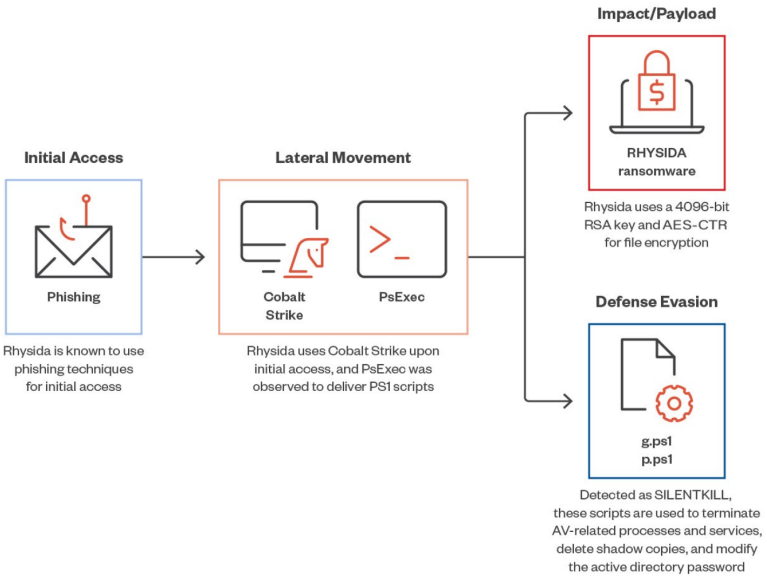
- **U.S. Department of Health and Human Services (HHS)'s report on Rhysida Ransomware:** https://www.hhs.gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf
- **An analysis of Rhysida ransomware:** https://www.trendmicro.com/en_za/research/23/h/an-overview-of-the-new-rhysida-ransomware.html

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)

- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
  - Penetration testing
  - Tabletop exercises
  - Threat Intelligence Program Maturity
  - Develop playbooks of adversary TTPs

Rhysida Ransomware Attack Chain:



Source: https://www.trendmicro.com/en_za/research/23/h/an-overview-of-the-new-rhysida-ransomware.html