Medusa Ransomware and MedusaLocker Ransomware

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

Medusa Ransomware and MedusaLocker Ransomware share similar names, making it appear as though the two threat actors are linked, but it is believed that the two operations are separate. Sharing a name has led to confusion in technical analyses and attribution, making it more difficult to track their activity and assess each of their separate capabilities. MedusaLocker Ransomware emerged in 2019 while Medusa Ransomware emerged in 2021. The two threat actors could have chosen their names out of an interest in Greek mythology, but it is also possible that Medusa Ransomware chose its name as an obfuscation tactic, intentionally trying to muddle analysis and attribution.

Medusa Ransomware:

Medusa Ransomware ramped up its malicious activity in 2023 making it a looming threat for 2024. According to Palo Alto's threat intelligence, it operates as a ransomware-as-a-service (RaaS). The threat actor and its affiliates appear to be financially motivated, targeting organizations worldwide. Top affected industries are technology, education, manufacturing, and healthcare. Targets are primarily located in the United States and Europe. The ransomware is designed to target Windows environments.

MedusaLocker Ransomware:

MedusaLocker Ransomware operates as a RaaS and is thought to be based in Russia as it leverages Russian infrastructure. While this threat actor and its adversaries target an array of industries, a core target is the healthcare industry. This ransomware variant is designed to target Windows environments.

Medusa Ransomware

Threat Level: Medium

Attack:

Medusa Ransomware actors gain initial access into organizations through two primary techniques. The first technique is by exploiting a vulnerability in a public-facing asset (MITRE T1190). The second technique is to engage initial access brokers for valid credentials (MITRE T1078). Once inside, the threat actors have been observed uploading a web shell to a Microsoft Exchange server, establishing persistence (MITRE T1505.003). The adversary may then install a remote monitoring and management software to further interact with the target system (MITRE T1219). Capabilities also include terminating or deleting security processes and tools to obscure detection (MITRE T1562.001). Of note, this threat actor has been observed using NetScan, a network monitoring and discovery tool, along with software that strengthens NetScan's functionality (MITRE T1046) and ultimately deploys the ransomware. The ransomware will encrypt and exfiltrate data as well as hinder recovery activities (MITRE T1490).

Remediation:

- Strengthen detection and visibility capabilities with a next generation firewall (NGFW).
- Assess your organization's security controls through penetration testing, risk assessments and MITRE ATT&CK evaluations.
- Conduct vulnerability scanning on external-facing assets at a defined cadence and swiftly remediate identified vulnerabilities.

MedusaLocker Ransomware

Threat Level: Medium

Attack:

MedusaLocker Ransomware threat actors gain initial access to their targets through phishing, exploiting vulnerable remote desktop protocol (RDP) services, and valid accounts (MITRE T1566.001, T1133, T1078). Valid accounts are acquired through brute-force attacks on RDP services (MITRE T1110). Once the ransomware is deployed to the victim's environment, it thwarts detection by disabling security and forensic tools and restarting the device in safe mode (MITRE T1562.001 and T1562.009). It also creates a scheduled task to run the ransomware every 15 minutes (MITRE T1053). MedusaLocker ransomware will encrypt data and prevent data recovery by deleting shadow copies and local backups (MITRE T1490).

Remediation:

- Use multi-factor authentication for remote service accounts.
- Assess remote services to ensure only necessary RDPs are in use.
- Ensure users are trained at a defined cadence to identify phishing emails.

Medusa Ransomware Details:

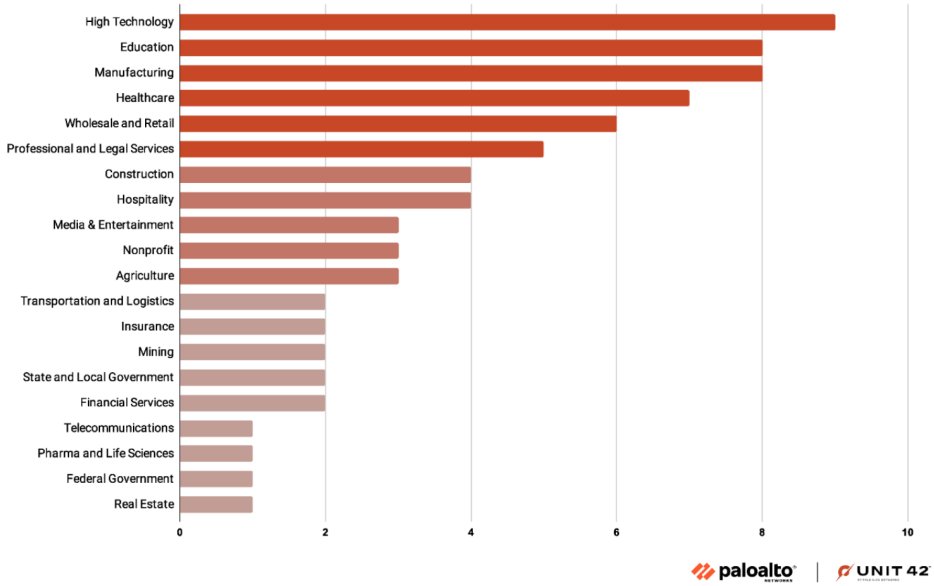
- **Technical analysis of Medusa Ransomware's capabilities:** https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/
- **News report on Medusa Ransomware activity:** https://www.bleepingcomputer.com/news/security/medusa-ransomware-gang-picks-up-steam-as-it-targets-companies-worldwide/

MedusaLocker Ransomware Details:

- **Technical analysis by the U.S. Department of Health and Human Services:** https://www.hhs.gov/sites/default/files/medusalocker-ransomware-analyst-note.pdf
- **Government advisory:** https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-181a

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
- Threat Intelligence
  - Notification to customers of threats
  - On-demand briefings
  - Threat exposure workshops
  - User awareness training seminars
  - Monthly and quarterly threat intelligence reports



Industries Impacted by Medusa Ransomware

Source: https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/