K logix

BE CONFIDENT.

DECEMBER 2023 | THREAT INTEL NEWSLETTER

NoEscape and GhostLocker Ransomware

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

K logix has observed an increase in ransomware-as-a-service (RaaS) threat actors. RaaS is when threat actors sell the use of their ransomware to other actors. The service typically offers technical functionality as well as strategic support. RaaS contributes to the spread of ransomware as it makes it easier for middle and lower-tier actors to conduct successful ransomware attacks.

NoEscape Ransomware:

NoEscape ransomware is a RaaS operation that emerged in May 2023. Affiliates have targeted organizations in the professional services, manufacturing, telecommunications, and healthcare industry. It is most actively deployed against organizations in North America, Europe, and Southeast Asia. Threat analysts are exploring a possible link between NoEscape and Avaddon, a RaaS that ceased operations in 2021. Both NoEscape and Avaddon ransomware have built-in mechanisms to avoid attacking the Commonwealth of Independent States (CIS).

GhostLocker Ransomware:

GhostSec is known as a hacktivist group that is a descendant of Anonymous, a decentralized international group of hacktivists. The group recently released a RaaS called GhostLocker, indicating that the group is shifting from hacktivism to financially motivated activity.

NoEscape Ransomware

Threat Level: Medium

Attack:

NoEscape Ransomware tends to infect systems via dropper malware or user execution (MITRE T1204.002). Upon execution, the ransomware variant will seek to inhibit system recovery by deleting Windows Shadow Volume copies and backup catalogs (MITRE T1490). It will also terminate processes related to security software, backup applications and web and database servers (MITRE T1489 and T1562.001). The RaaS includes functionality that avoids detection. For example, it can utilize Windows safe-mode operations to disable endpoint protection software more easily (MITRE T1562.009). It also uses Windows Restart Manager to ensure files are unlocked for encryption. The ransomware executes on Windows devices, moves laterally across the organization, and encrypts files on Windows, Linux, and VMware ESXI servers (MITRE T1486). The RaaS offers shared encryption functionality, which means a single encryption key is shared across all infected files, enabling efficient encryption and decryption. It also supports multiple encryption modes. In addition to the ransomware's technical functionality, it offers 27/7 customer support, private chat functions and a Tor admin panel.

Remediation:

- Network security controls that monitor and regulate incoming traffic should be in place and reviewed periodically.
- Security personnel should be prepared to immediately act during a ransomware attack to minimize damage. One key measure to ensure this is to have a documented and well-understood Incident Response Plan in place and periodically tested.
- Regularly backup critical data, test the backup and recovery process periodically and ensure backups are stored in a secure location.

GhostLocker Ransomware

Threat Level: Low

Attack:

GhostLocker is a python-based ransomware and the executable contains all necessary dependencies, meaning it can run on computers that do not have python installed (MITRE T1059.006). GhostSec markets the RaaS as having complete undetectability. It does appear to offer defense evasion capabilities. For example, it compiles with PyInstaller and Nuitka, which anti-virus solutions struggle to properly scan (MITRE T1027). It is advantageous for the threat actor to augment capabilities of known tools rather than create ones from scratch. This is not, however, a novel technique. GhostSec also markets the GhostLocker Ransomware as having military-grade encryption. However, according to an analysis conducted by Rapid7 on GhostLocker samples, the ransomware's encryption capabilities appear to still be under development.

Remediation:

- K logix monitored threat actor activity throughout 2023. The top initial access technique utilized by threat actors is phishing. To combat this, organizations should regularly conduct security awareness training and role-based security training.
- Ransomware actors commonly utilize email phishing as an initial access vector. Organizations should invest in a robust email security solution.
- Implement a proactive security posture by acquiring and/or developing cyber threat intelligence capabilities.

NoEscape Ransomware Details:

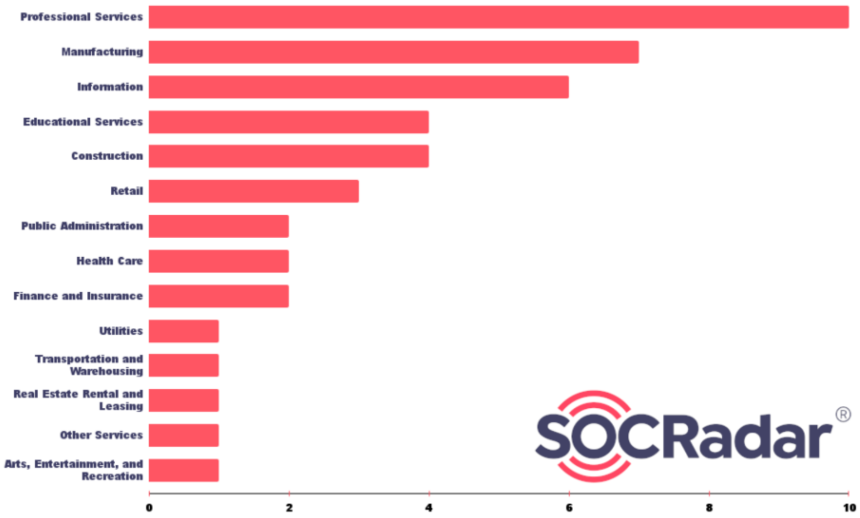
- **Overview of the threat:** https://www.hhs.gov/sites/default/files/noescape-ransomware-analyst-note-tlpclear.pdf
- **Additional insight into its capabilities:** https://socradar.io/dark-web-profile-noescape-ransomware/

GhostLocker Ransomware Details:

- **Thorough analysis of capabilities:** https://www.rapid7.com/blog/post/2023/11/08/ghostlocker-a-work-in-progress-raas/
- **High-level overview:** https://socradar.io/ghostlocker-a-new-generation-of-ransomware-as-a-service-raas/

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



Distribution of Industries targeted by NoEscape Ransomware

Source: https://socradar.io/dark-web-profile-noescape-ransomware/

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs to strategically align with the business to reduce risk.