Lazarus and Royal Ransomware

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

Third-party vulnerabilities are a common attack vector and, given that multiple organizations will share these vulnerabilities, enable adversaries to scale operations. The two adversaries in this report are notable examples of this, with both having recently utilized third-party vulnerabilities to gain initial access into their targeted organizations. In both cases, patches exist for the exploited vulnerabilities. To mitigate this type of threat, it is recommended to have a documented and well-understood patch management process.

Lazarus:

Lazarus is a North Korean advanced persistent threat (APT) actor. Lazarus is an umbrella term, and it is thought that several subgroups operate under it. Generally, Lazarus is financially motivated, but in a recent campaign, called 'No Pineapple!', where Lazarus extracts data from its targets without disrupting operations, the objective appears to be intelligence gathering. The campaign targeted chemical engineering, defense, energy, healthcare, medical research, and education organizations.

Royal Ransomware:

The Royal ransomware group first emerged in January 2022 and includes skilled personnel, some of which are likely ex-Conti members. Other aliases could include Dev-0569, which is a threat actor Microsoft tracks that uses the royal ransomware strain. The adversary is known to target window systems but recently implemented a Linux-based version of its ransomware to target ESXi specifically. This adversary targets a range of industries, a large portion of which are based in the United States.

Lazarus

Threat Level: High

Attack:

In the 'No Pineapple!' campaign, Lazarus exploited two known vulnerabilities in unpatched Zimbra devices to gain initial access and escalate privileges via remote code execution (CVE-2022-27925) and authentication bypass (CVE-2022-37042). Lazarus then used Plink and 3Proxy (MITRE T1090.001) to connect its infrastructure to its target's internal network. Notable techniques include account creation and modification to facilitate persistent access and privilege escalation (MITRE T1136 and T1078), and the use of Mimikatz for credential harvesting (MITRE T1003.001). New versions of the Dtrack information-stealer and GREASE malware were also observed in this campaign.

Remediation:

- Ensure Zimbra devices are patched to prevent an adversary's ability to exploit the CVE-2022-27925 and CVE-2022-37042 vulnerabilities. Remediation details can be found here.
- It is recommended for a defined and documented patch management process to be in place. Typically, patches are handled within 30-90 days, depending on the criticality level.
- Regularly leverage vulnerability scanning tools to identify vulnerabilities for remediation.
- Consider implementing an Endpoint Detection and Response (EDR) tool to detect threats.

Royal Ransomware

Threat Level: High

Attack:

The Royal Ransomware group deploys an array of techniques to gain initial access into an organization, including targeted callback phishing campaigns, malicious advertisements and exploiting existing vulnerabilities. Notably, Royal Ransomware was the first observed group exploiting the Citrix vulnerability CVE-2022-27510 for initial access. Once inside an organization's network, the threat actor has been observed deploying Cobalt Strike for persistence, harvesting credentials, and circumventing EDR tools (MITRE T1562.001). Initially, the group used BlackCat's encryptor but soon transitioned to their own encryptors, one of which, called Zeon, generates similar ransomware notes to Conti.

Remediation:

- Organizations with Citrix products in their environment should ensure the necessary patches are implemented to mitigate the CVE-2022-27510 vulnerability. Remediation details are found here.
- VMware ESXi servers should be patched to secure them against the CVE-2021-21974 vulnerability. Remediation details can be found here. While the Royal ransomware group has not been observed exploiting this vulnerability, it is actively being exploited in a campaign called ESXiArgs.
- Maintain and periodically review a Software Bill of Materials (SBOM).
- Ensure data is backed up in a separate location to facilitate business continuity.

Lazarus Details:

- **Analysis of the 'No Pineapple!' campaign:** https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Lazarus-No-Pineapple-Threat-Intelligence-Report-2023.pdf
- **Synopsis of the 'No Pineapple!' campaign:** https://www.bleepingcomputer.com/news/security/north-korean-hackers-stole-research-data-in-two-month-long-breach/

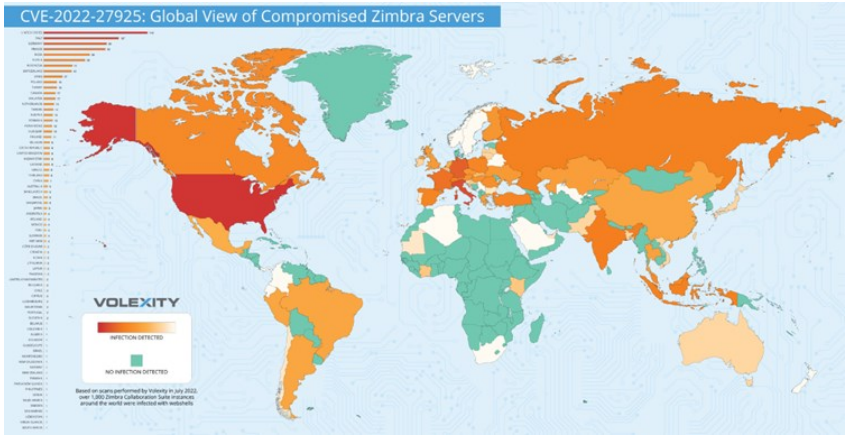
Royal Ransomware Details:

- **The U.S. Department of Health and Human Services put out an advisory on Royal Ransomware in December 2022:** https://www.hhs.gov/sites/default/files/royal-ransomware-analyst-note.pdf
- **Deep Dive into Royal Ransomware's tactics and techniques:** https://www.kroll.com/en/insights/publications/cyber/royal-ransomware-deep-dive

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

Geographical distribution of Zimbra devices compromised by the CVE-2022-27925 and CVE-2022-37042 vulnerability as of July 2022. This is based on an analysis conducted by Volexity.



Source: https://www.volexity.com/blog/2022/08/10/mass-exploitation-of-unauthenticated-zimbra-rce-cve-2022-27925/