RansomHub Affiliates: NONAME and Velvet Tempest

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

RansomHub, a notable Ransom-as-a-Service (RaaS) provider, highlighted in K logix's June newsletter, is set to be a significant player in the ransomware landscape, providing affiliates, hackers who subscribe and buy RaaS, with ready-made tools and infrastructure. Since its debut in February 2024, RansomHub has quickly gained prominence, particularly due to the FBI actions against RaaS providers LockBit and BlackCat/ALPHV. These shutdowns drove affiliates to seek other sophisticated and trustworthy groups. RansomHub has conducted more than 210 attacks affecting countries such as the US, Brazil, Italy, and the UK. Its activity already accounts for 14.2% of ransomware attacks in Q3 2024. RansomHub enables threat actors to employ the double extortion technique, encrypting files and exfiltrating data to demand ransom. This newsletter examines two RansomHub affiliates, NONAME and Velvet Tempest.

NONAME:

NONAME, also known as CosmicBeetle, has been active since at least 2020 and targets small and medium sized businesses worldwide in the government, financial, and healthcare sectors. Recently, NONAME switched from LockBit, as their RaaS provider, to RansomHub, presumably in response to FBI disruptions affecting LockBit. This new affiliation helps elevate their existing capabilities, and significantly enhances their ransomware toolset and operational capacity.

Velvet Tempest:

Velvet Tempest, a prominent user in the RaaS landscape, has transitioned to deploying ransomware from RansomHub, moving on from their past affiliation with BlackCat/ALPHV. This transition likely alleviates technical challenges and resolves financial trust issues associated with BlackCat/ALPHV. Velvet Tempest targets diverse industries, such as energy, fashion, tobacco, IT, and manufacturing, indicating a broad scope of interest.

NONAME

Threat Level: Medium

Attack:

NONAME actors gain initial access to targeted organizations with brute force attacks and by exploiting vulnerabilities in Veeam, FortiOS SSL-VPN, EternalBlue, Microsoft Active Directory, and other public-facing applications (MITRE T1078.001 and MITRE T1190). Once inside, the group seeks to expand access to systems by conducting remote desktop protocol attacks, allowing them to perform actions remotely as the logged-in user (MITRE T1021.001). This threat actor likes to employ its own capabilities, such as the ScRansom payload for file encryption and process termination, while also enhancing their toolkit by leveraging various RaaS offerings (MITRE T1587.001 and MITRE T1588.01). Recently, after failing to infect systems with ScRansom, NONAME successfully utilized RansomHub's capabilities to disable targets' endpoint detection and response (EDR) tools, obscuring their activities. NONAME then executes RansomHub on the compromised machine, encrypting data and rendering it inaccessible (MITRE T1486).

Remediation:

- Prioritize patching critical vulnerabilities that ransomware groups could exploit.
- Regularly back-up data and test the back-ups to ensure availability in the event of a ransomware attack.
- Require strong passwords and limit login attempts to prevent brute-force attacks.

Velvet Tempest

Threat Level: Low

Attack:

Velvet Tempest primarily gains initial access by relying on access brokers (MITRE T1650). Once inside, this attacker tends to utilize PsExec, a command line tool that allows users to run programs, for payload staging and lateral movement. The group's operations often include disabling antivirus solutions lacking tamper protection (MITRE T1562.001). The attackers also implement persistence mechanisms such as scheduled tasks that conceal secure shells in well protected environments or deploy the ExMatter trojan in less secure settings (MITRE T1053). Exmatter, a hallmark of Velvet Tempest's approach, is a tool designed to automate the extraction of targeted directories and file types for effective data theft.

Remediation:

- Acquire intrusion detection systems (IDS) and intrusion prevention systems (IPS) to readily detect PsExec activity in the network.
- Ensure MFA is implemented for remote access tools.
- Implement network segmentation to prevent the spread of ransomware.

NONAME:

- **Overview of NONAME/ComicBeetle's capabilities:** https://www.welivesecurity.com/en/eset-research/cosmicbeetle-steps-up-probation-period-ransomhub/
- **Recent NONAME attack using RansomHub:** https://www.bleepingcomputer.com/news/security/noname-ransomware-gang-deploying-ransomhub-malware-in-recent-attacks/

Velvet Tempest:

- **Velvet Tempest's expansion to RansomHub:** https://www.s-rminform.com/latest-thinking/a-tempest-at-ransomhub-major-new-cyber-threat-group-expands
- **Velvet Tempest Attack Methods:** https://malpedia.caad.fkie.fraunhofer.de/actor/velvet_tempest

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Response (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)
- Program 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

Top 10 Countries Targeted by RansomHub in Q2 2024

Source: https://cyberint.com/blog/research/ransomhub-the-new-kid-on-the-block-to-know/