FEBRUARY 2025 | THREAT INTEL NEWSLETTER

Infostealer Insights: Lumma and BANSHEE

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

As cyber threats evolve in 2025, Malware-as-a-Service (MaaS) platforms like Lumma Stealer and BANSHEE Stealer are equipping attackers with advanced tools to infiltrate systems and steal sensitive data. By exploiting trusted system processes, Lumma and BANSHEE blend in, making it increasingly difficult for traditional security measures to spot them.

Lumma Stealer:

Lumma Stealer, a Russian-based MaaS, started being used in 2022 and primarily targets the transportation and manufacturing industries in India and the United States. It specializes in stealing sensitive data, such as login credentials and financial information. While initially distributed via traditional phishing tactics, recent campaigns have seen Lumma Stealer delivered through more sophisticated methods, including fake CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) verification pages.

Banshee Stealer:

Banshee Stealer first emerged in August 2024 and is a Malware-as-a-Service (MaaS) developed by a group of Russian cybercriminals. This information-stealing malware offers advanced tools for stealing sensitive data from macOS systems. Despite a shutdown in November 2024, it has made a resurgence with its strong evasion tactics. While no specific industry or country is noted as a target, there is a possible focus on individuals involved in cryptocurrency. This is likely due to the difficulty in tracing the origin of transactions and the potentially high value of crypto assets.

Lumma Stealer

Threat Level: Medium

Attack:

Lumma Stealer has recently made its way onto systems via fake CAPTCHA pages that look like a legitimate human verification form but trick users into executing harmful actions (MITRE T1566). The CAPTCHA pages prompt the user to press a series of keys, such as "Windows+R" and "CTRL +V," which trigger a PowerShell command (MITRE T1204 and MITRE T1059.001). The command leverages mshta.exe, a trusted Windows tool that runs HTML applications (MITRE T1218.005). Since mshta.exe is trusted and frequently employed for legitimate purposes, attackers can install Lumma Stealer without detection by traditional security measures. After installation, Lumma Stealer actively seeks out sensitive information, including login credentials stored in web browsers, cookies, and cryptocurrency wallets. The attackers exfiltrate the stolen data back to themselves through trusted cloud services, disguising the traffic as regular web activity to evade detection (MITRE T1567). Additionally, Lumma Stealer ensures its persistence by scheduling the malware to run automatically at specific times of the day or when the system reboots (MITRE T1053 and MITRE T1547).

Remediation:

- Ensure users are trained and educated on emerging tactics used by threat actors such as CAPTCHA forms.
- Limit access to the Run command in your organization's policy to prevent unknown commands from being executed on systems.
- Monitor system startup entries to detect unusual applications that could indicate malware.

BANSHEE Stealer:

Threat Level: Low

Attack:

BANSHEE Stealer malware spreads through phishing websites and fake software downloads (MITRE T1566). Once executed, it uses credential harvesting to trick users into entering their passwords onto fake login prompts, allowing the malware to capture the passwords for future use (MITRE T1056). BANSHEE targets sensitive information on the system, including passwords saved in browsers like Chrome and Safari, cryptocurrency wallet details, and data stored in Apple's Keychain app. To avoid detection, BANSHEE employs sophisticated tactics. It encrypts itself using the same algorithm as Apple's security system, XProtect, designed to block malicious software (MITRE T1027). This encryption makes it more difficult for anti-malware tools to detect the malware. BANSHEE compresses and encrypts the stolen data into a ZIP archive before sending it to its command-and-control server via HTTP POST requests (MITRE T1071.001). This layered approach ensures that the exfiltrated data remains undetected while reaching the attackers.

Remediation:

- Ensure employees only download software from trusted sites.
- Implement email filtering to detect and block phishing attempts that may contain malware.
- Update all browsers, especially browsers with stored passwords.

Lumma Stealer:

- **Overview of Lumma Stealer Capabilities:** https://blog.qualys.com/vulnerabilities-threat-research/2024/10/20/unmasking-lumma-stealer-analyzing-deceptive-tactics-with-fake-captcha
- **Lumma Stealer Background:** https://darktrace.com/blog/the-rise-of-the-lumma-info-stealer

BANSHEE Stealer:

- **Overview of BANSHEE Stealer Capabilities:** https://cybersecsentinel.com/macos-users-targeted-by-the-new-variant-of-banshee-infostealer/
- **BANSHEE and Apple's XProtect:** https://www.darkreading.com/threat-intelligence/banshee-malware-steals-apple-encryption-macs

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)

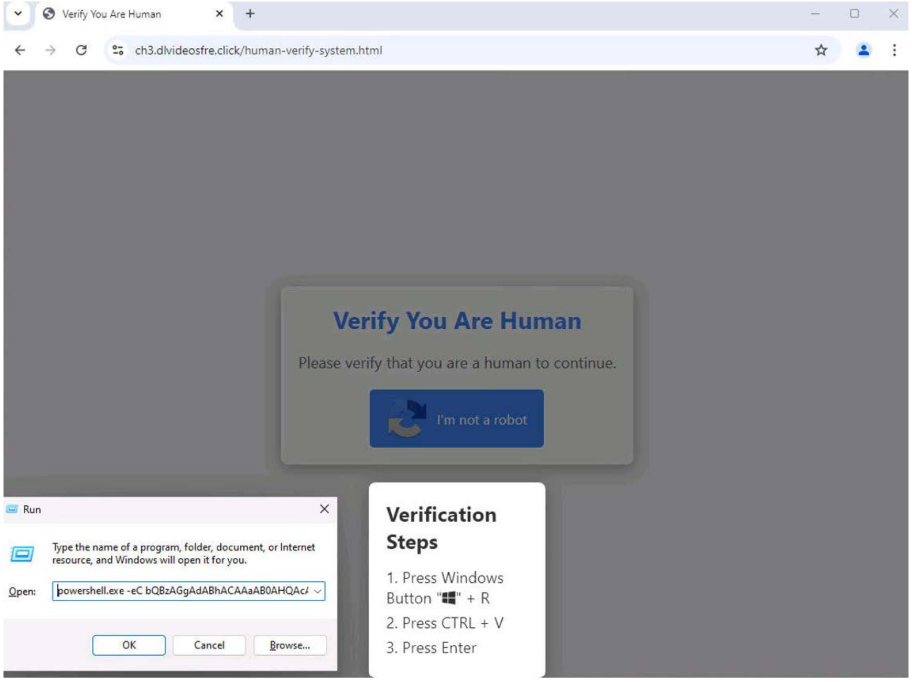
Program Advisory

- 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

Fake Lumma Stealer Malware CAPTCHA Form



ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

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