مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Banshee Stealer Targets macOS Users

Tracking #:432316724

Date:10-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new version of the Banshee macOS Stealer has been detected, posing a significant threat to macOS users worldwide.

TECHNICAL DETAILS:

A new variant of the Banshee macOS Stealer malware has been identified by Security researchers, with significant updates to its functionality and distribution methods. This sophisticated malware is designed to steal sensitive data such as browser credentials, cryptocurrency wallets, and macOS passwords. Notably, Banshee now uses string encryption derived from Apple's own XProtect antivirus engine, allowing it to evade detection by antivirus solutions for over two months. The malware has been distributed via phishing websites and fake GitHub repositories, often impersonating legitimate software like Chrome, Telegram, and TradingView.

Key Details:

- Malware Name: Banshee macOS Stealer
- Target Platform: macOS (also targets Windows via a different malware variant, Lumma Stealer)
- Key Targets:
  - Browser credentials (Chrome, Brave, Edge, Vivaldi)
  - Cryptocurrency wallets and Two-Factor Authentication (2FA) credentials
  - macOS system passwords
  - Software and hardware details
- Malware Behavior:
  - Data Theft: Banshee steals sensitive data from browsers and wallet extensions, exploiting 2FA extensions to capture credentials.
  - Anti-Analysis: The malware employs techniques to avoid detection by antivirus software and evades debugging tools.
  - Exfiltration: Stolen data is encrypted and sent to command-and-control servers for unauthorized use.
  - Deceptive Tactics: Banshee uses convincing pop-ups to trick users into entering their macOS passwords.
- Distribution Channels:
  - Phishing Websites: Banshee was distributed through fake websites that masquerade as legitimate software, targeting users looking for tools like Chrome, Telegram, and TradingView.
  - GitHub Repositories: Malicious GitHub repositories, often with user reviews and stars to appear legitimate, were used to distribute the malware.
- Key Update (November 2024):
  - The malware's developers removed a language check for Russian, broadening the malware's target audience and indicating a move towards a more global distribution.
- **Impact**
  - Data Breach Risks: Unauthorized access to sensitive information, such as browser credentials, cryptocurrency wallet data, and macOS passwords, putting users and organizations at risk for identity theft and financial losses.
  - Undetected Malware: The use of string encryption based on Apple's XProtect allowed Banshee to avoid detection for over two months, demonstrating the sophisticated nature

of modern malware.

- Business Disruption: The malware's stealthy nature could lead to long-term operational disruptions as it silently exfiltrates data, potentially compromising company systems before detection.
- Cryptocurrency Risks: Targeting cryptocurrency wallets increases the financial threat posed by Banshee, especially for businesses dealing in digital currencies.
- Reputation Damage: Successful infections leading to data exfiltration can result in publicized breaches, tarnishing the reputation of businesses and eroding consumer trust.

RECOMMENDATIONS:

- Ensure that all systems, especially macOS devices, are running the latest antivirus software capable of detecting advanced threats like Banshee.
- Enable Gatekeeper, XProtect, and System Integrity Protection (SIP) for macOS systems to create additional barriers against unauthorized malware installation.
- Use Endpoint Detection and Response (EDR) tools to detect and mitigate threats in real-time, preventing malware from exfiltrating data.
- Train users on the dangers of phishing websites and encourage caution when downloading software from untrusted sources.
- Deploy web filtering and DNS security solutions to block access to known malicious websites and prevent malware distribution.
- Enforce the use of multi-factor authentication (MFA) for accessing sensitive systems, particularly cryptocurrency wallets and accounts containing confidential information.
- Regularly review and update password policies to ensure strong, unique credentials are used across all user accounts.
- Educate employees and users on the risks associated with downloading software from unofficial sources, including GitHub repositories.
- Regularly back up all critical data to reduce the impact of data exfiltration or loss in case of a successful malware attack.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://blog.checkpoint.com/research/cracking-the-code-how-banshee-stealer-targets-macos-users/