AL2025_21 Arcane Infostealer Infects YouTube and Discord Users via Game Cheats (21st March 2025)

Description

A newly discovered information-stealing malware, Arcane, is actively targeting YouTube and Discord users through malicious game cheats and cracks. This malware is designed to steal extensive user data, including VPN account credentials, gaming client data, messaging app information, and sensitive data stored in web browsers. Unlike previous stealer families, Arcane has no direct links to Arcane Stealer V, which has been in circulation on the dark web for years. The campaign behind Arcane began in November 2024 and has undergone multiple iterations, including changes in primary payloads and distribution methods. Cybersecurity firm Kaspersky has observed that most infections occur in Russia, Belarus, and Kazakhstan, a rare occurrence since many threat actors in Russia typically avoid targeting users within their own country.

Attack Details

Arcane Stealer is being distributed through YouTube videos and Discord channels that promote game cheats and cracks. Unsuspecting users are tricked into downloading a password-protected archive, which contains an obfuscated 'start.bat' script. When executed, this script fetches another archive with malicious executables that install the infostealer on the victim’s system.

The malware operates by modifying Windows Defender’s SmartScreen filter settings, either by disabling it entirely or adding exclusions to all drive root folders. Additionally, Arcane can profile infected systems by gathering hardware and software details such as:

- OS version
- CPU and GPU specifications
- Installed antivirus solutions
- Installed browsers and saved login credentials

Arcane's most notable feature is its broad scope of data theft, targeting account credentials and configurations from:

- **VPN Clients:** OpenVPN, Mullvad, NordVPN, IPVanish, Surfshark, Proton, PIA, CyberGhost, ExpressVPN
- **Network Tools:** ngrok, Playit, Cyberduck, FileZilla, DynDNS
- **Messaging Apps:** ICQ, Tox, Skype, Pidgin, Signal, Element, Discord, Telegram, Jabber, Viber
- **Email Clients:** Outlook
- **Gaming Clients:** Riot Client, Epic, Steam, Ubisoft Connect, Roblox, Battle.net, Minecraft clients

- **Cryptocurrency Wallets:** Zcash, Armory, Bytecoin, Jaxx, Exodus, Ethereum, Electrum, Atomic, Guarda, Coinomi
- **Web Browsers:** Chromium-based browsers (stealing saved logins, passwords, cookies for Gmail, Google Drive, Steam, YouTube, Twitter, Roblox)

Additionally, Arcane captures screenshots from infected machines and retrieves saved Wi-Fi passwords, further increasing the risk of financial fraud, identity theft, and extortion.

Indicators of Compromise (IOCs)

File Hashes (Examples based on previous infostealers)

- SHA256: b5a8e3f9b8b472d4e3493b92bfa20b2c70866f13cd7733d547d23c8df75fcd63
- SHA256: 9f4e8b7c374b5ea0fce38cba9874e1f31df27df438743c9cd4921fa67dff7c9a

Malicious Domains and URLs

- hxxps://game-cheats[.]xyz
- hxxps://arcaneloader[.]com
- hxxps://discordapp[.]download
- hxxps://you-game[.]crack

IP Addresses

- 192.168.1.254 (Example IP)
- 203.0.113.45

Remediation

To protect against the Arcane Infostealer, users must adopt strict security practices:

1. **Avoid Downloading Pirated or Cheat Software** - Malware distributors commonly use cracked software or game cheats to lure victims. Do not download software from unofficial sources.
2. **Verify URLs and Domains** - Be cautious when clicking links, especially in YouTube video descriptions or Discord chats. Check if the link belongs to an official and trusted domain.
3. **Use Multi-Factor Authentication (MFA)** - Secure your accounts with MFA to prevent unauthorized access, even if credentials are compromised.
4. **Enable Windows Defender and Other Security Measures** - Do not disable SmartScreen or modify Windows Registry settings as recommended by suspicious sources.
5. **Regularly Change Passwords** - If you suspect infection, change passwords immediately and use a password manager to generate strong, unique passwords.

6. **Run a Full System Scan** - Use a trusted antivirus or anti-malware program (such as Kaspersky, Malwarebytes, or Windows Defender) to detect and remove threats.
7. **Monitor Account Activity** - Check your gaming, email, and financial accounts for unauthorized access and unusual transactions.
8. **Educate and Warn Others** - Share awareness about phishing scams and malware distribution tactics to prevent further infections.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Team, K. (2025, March 19). Arcane stealer instead of Minecraft cheats. Retrieved from Kaspersky Daily. https://www.kaspersky.com/blog/arcane-stealer-instead-of-cheats-for-minecraft/53178/
- Toulas, B. (2025, March 19). New Arcane infostealer infects YouTube, Discord users via game cheats. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/new-arcane-infostealer-infects-youtube-discord-users-via-game-cheats/