SECURITY ADVISORY

CYBER STASH

November, 2024

Xiū gou Phishing Kit

A Rising Cyber Threat to Users and Businesses

Context

The Xiū gou phishing kit represents a newly uncovered, highly sophisticated and global phishing threat, designed to deceive and exploit unsuspecting users across diverse sectors. Derived from Mandarin internet slang for "doggo," this toolkit is distinguished by its refined branding and advanced evasion techniques, which collectively enhance its efficacy in targeting individuals across a wide array of industries, including public services, postal systems, banking, and digital platforms.

Since its emergence in September 2024, the Xiū gou phishing kit has proliferated across over 2,000 known malicious websites, primarily affecting users in the UK, US, Spain, Australia, and Japan. The kit harnesses Rich Communication Services (RCS) messaging to distribute malicious, shortened URLs, which lure recipients with fraudulent alerts concerning government payments, postal fines, and other urgent notifications. These deceptive messages direct victims to counterfeit websites that closely mimic legitimate institutions, such as the UK Government, USPS, and Lloyds Bank.

Once victims are compelled to enter sensitive personal or financial information, it is surreptitiously exfiltrated via a Telegram bot controlled by the attackers. Furthermore, the Xiū gou phishing kit leverages sophisticated anti-detection measures, including Cloudflare’s obfuscation technologies, to mask the malicious nature of the campaign and circumvent traditional security mechanisms, rendering it an exceptionally potent and evasive threat.

Mitigation

Defending against Xiū gou requires proactive measures, including:

User Education: Regularly train employees and users on recognizing phishing tactics and unusual sender behaviors.

User Education: Regularly train employees and users on recognizing phishing, including unusual messages from Rich Communications Services (RCS) message service.

Restrict Network Traffic: Limit outbound traffic to high-risk infrastructures, including specific TLDs, ASNs, and countries, to reduce exposure to potential threats.

Technical Details

The Xiū gou phishing campaign employs a sophisticated and multi-layered infrastructure designed to maximize its effectiveness while evading detection. The attack follows a precise sequence of steps:

Initial Attack via RCS Messages: The campaign begins with the delivery of Rich Communication Services (RCS) messages containing shortened URLs. These messages are designed to deceive recipients by claiming urgent matters such as package deliveries or outstanding fines, prompting victims to click the link.

Obfuscated Payload Delivery: Upon clicking the link, victims are redirected to phishing websites that closely resemble legitimate services. These sites are constructed using Vue.js for a realistic user interface, while the backend is powered by Golang via SynPhishServer, which ensures smooth and covert delivery of malicious payloads.

Credential Harvesting & Data Exfiltration: Once victims land on the spoofed site, they are prompted to input personal information, including payment details. This data, along with metadata such as IP addresses and browser information, is harvested and exfiltrated to the attackers via Telegram bots, providing continuous access to stolen data even if the phishing sites are taken down.

Domain Naming & Hosting Tactics: Attackers utilize anti-bot technologies and services like Cloudflare to obscure their phishing infrastructure, preventing automated detection. Domains are typically registered with the .top TLD, often using keywords related to government fines, parking violations, or other urgent matters to enhance the site's legitimacy.

Detection Evasion: To further evade detection, the phishing sites employ advanced evasion tactics, including anti-bot scripts that redirect non-human traffic to benign websites. This ensures that only legitimate users, not automated security bots, are exposed to the phishing attempt.

Persistence Mechanisms: The Xiū gou kit incorporates mechanisms for sustained operation:

- **Domain Obfuscation** using Cloudflare’s services helps avoid automatic detection by security systems.

- **Campaign Customization** via an admin panel allows attackers to adapt the phishing campaign to specific targets, ensuring ongoing engagement and reducing the chances of detection.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to Xiū gou phishing kit:

Initial Access | Technique: Phishing via Rich Communication Services (RCS) (T1566.002)

Xiū gou initiates attacks by sending phishing messages through RCS instead of SMS, using shortened URLs to redirect victims to spoofed websites that impersonate government agencies or service providers.

Defense Evasion | Technique: Obfuscated Files or Information (T1027)

To bypass detection, Xiū gou employs Cloudflare's anti-bot services and redirects bot traffic to benign websites, masking its phishing pages from automated security systems.

Command and Control | Technique: Exfiltration Over Alternative Protocol (T1041)

The kit uses Telegram bots for real-time exfiltration of victim data, transmitting stolen information immediately to attackers, which also enables continuous access if the phishing site is taken down.

Credential Access | Technique: Input Capture via Web Page Spoofing (T1056.004)

Xiū gou mimics login and payment forms on fake websites resembling legitimate entities (e.g., USPS, gov.uk) to harvest sensitive information such as login credentials and payment details from victims.

Persistence | Technique: Domain Generation Algorithm (DGA) and Obscured Domains (T1568.002)

The phishing kit registers numerous domains using the ".top" TLD and generates URLs that include keywords like "parking" or "gov," enhancing persistence and allowing for quick re-deployment after takedowns.

Impact | Technique: Financial Impact and Data Manipulation (T1499)

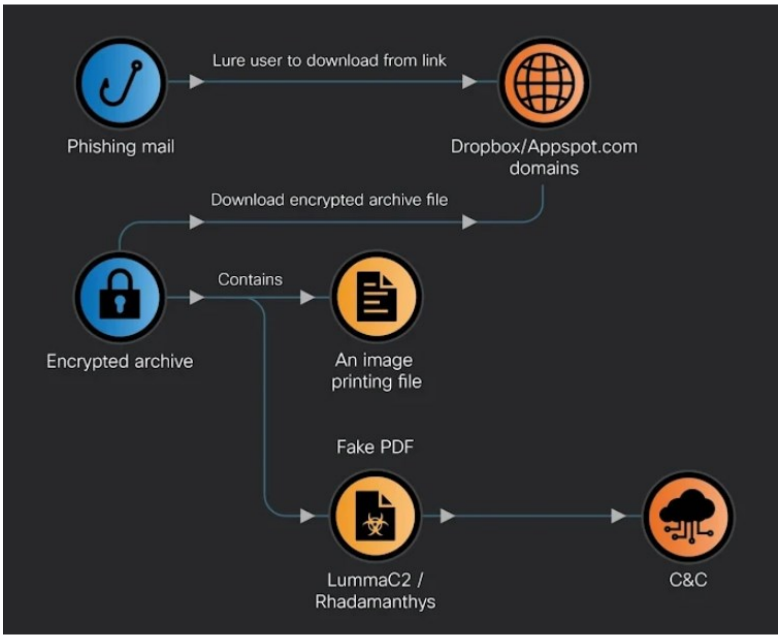
Xiū gou manipulates victims into paying fake fines or fees, leading to financial loss and the unauthorized disclosure of personal information, which directly impacts individuals and organizations financially and operationally.

Cyber Threat Intelligence

The Xiū gou (修狗) phishing kit, attributed to a Chinese-speaking cybercriminal group, has been used in global phishing campaigns since September 2024, targeting the US, UK, Spain, Australia, and Japan. The kit primarily focuses on public services, banking, and postal services, using fake charges and government payment scams to harvest credentials. Built with Golang and Vue.js, it features an admin panel for easy campaign management and integrates advanced evasion techniques like Cloudflare anti-bot protection and obfuscated hosting. The kit also employs Telegram for exfiltrating stolen data. While there is no direct link to state-sponsored actors, the sophisticated design and global targeting suggest potential connections to economic espionage or large-scale financial fraud. Given its capabilities, CyberStash predicts that Xiū gou will continue to expand, targeting additional sectors with increasingly refined social engineering tactics. As attackers evolve, organizations must strengthen their defenses to mitigate this growing and persistent threat.

References

Attack Chain Graph: Malware Infection | Source: Cisco TALOS



Public Intelligence:

- https://thehackernews.com/2024/11/new-phishing-kit-xiu-gou-targets-users.html
- https://hackread.com/gou-phishing-kit-hits-uk-us-japan-australia-sectors
- https://www.scworld.com/brief/novel-xiu-gou-phishing-kit-has-global-reach
- https://insight.scmagazineuk.com/global-scams-used-xiu-gou-phishing-kit
- https://www.netcraft.com/blog/doggo-threat-actor-analysis

Act now to protect your business!

Contact CyberStash today to learn about eclipse.xdr and our round-the-clock managed detection and response service.