CYBERFORCE

THREAT BULLETIN:

APRIL 2025

CREDENTIAL PHISHING USING SVG FILES

OVERVIEW

CyberForce|Q's Security Operation Center has identified an emerging trend where threat actors are increasingly exploiting Scalable Vector Graphics (SVG) files as part of credential phishing attacks. Unlike traditional image formats, SVG files are XML-based and capable of embedding JavaScript (JS), which has led to the abuse of this file type for malicious purposes. This technique bypasses traditional email security controls and poses a significant risk to organizations, particularly those with users who may interact with unsolicited file attachments.

This bulletin provides a detailed analysis of the attack tactics, techniques, and procedures (TTPs) leveraged in SVG-based credential phishing campaigns, along with detection and mitigation strategies.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

1

Initial Access (T1071.001)

The attackers use phishing (T1071.001) to gain initial access. A highly social-engineered email is sent to the target, impersonating as a legitimate notification (e.g., a voicemail or an important document). The email typically uses legitimate-looking senders and trusted logos, thereby enhancing the likelihood that the target will open the email and interact with the attachment.

2

Execution (T1203)

The malicious attachment is an SVG file (T1203), which, while usually considered harmless, can contain executable JavaScript code. The SVG file typically disguised as an image (e.g., a blue checkmark or voicemail icon), encourages the target to open it. Once opened, the JavaScript code embedded in the SVG file is automatically executed within the browser or the default viewer.

3

Command and Control (C2) Communication (T1071.001, T1102)

The embedded JavaScript code initiates communication with an external Command and Control (C2) server (T1071.001). After the SVG file is processed, the victim is redirected to a malicious phishing site that imitates legitimate web pages, often featuring a spoofed Microsoft login page that includes the victim's corporate logo to enhance legitimacy. This redirection (T1102) establishes communication between the victim's system and the attacker's server, facilitating the credential harvesting process.

4

Credential Dumping (T1003)

Upon entering their credentials into the fake login page, the user's credentials are harvested by the attacker. The credentials are automatically transmitted (T1003) to a backend server controlled by the attacker for further abuse. These credentials are then used in a later stage of the attack to gain access to corporate systems or services.

5

Persistence (T1071.001)

If the attacker successfully harvests valid credentials, they may use them to establish a foothold in the victim's environment and persist through legitimate access points. For example, the attacker may attempt to use these credentials for lateral movement (T1071.001), escalating privileges or accessing additional systems across the organization.

MITIGATION RECOMMENDATIONS:

Email Filtering and Sandboxing:

Use advanced email filtering solutions that inspect all incoming file attachments for suspicious content, particularly JavaScript in SVG files. Incorporate sandboxing techniques to evaluate the behavior of any attachment before it reaches the end user.

Network Defense:

Deploy network-level defenses such as DNS filtering and C2 detection tools to block communication with known malicious infrastructure. Ensure proper segmentation to limit lateral movement should credentials be compromised.

Authentication and Session Security:

Enforce strong session management policies, including short session timeouts and session re-authentication on critical systems. Apply Zero Trust principles to ensure that access controls are in place even for authenticated users.

ETERNAL TREND:

INCREASE IN GENERATIVE AI SCRAPER BOT ACTIVITY

OVERVIEW

Generative AI scraper bots, such as ClaudeBot and Bytespider, are rapidly increasing in the web landscape. These AI-driven bots are consistently targeting web applications, scraping vast amounts of data at an unprecedented scale. Unlike traditional bots that operate in bursts, these bots maintain persistent traffic patterns, leading to significant operational challenges for web applications. Their activity, although not overtly malicious, can overwhelm systems, distort data, and increase compliance risks.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

Persistent Bot Traffic (T1071.001)

Generative AI bots maintain continuous scraping behavior, generating millions of requests daily. This results in constant traffic that overwhelms web application resources.

1

Data Scraping and Resource Exhaustion (T1071.001, T1071.003)

These bots scrape large-scale datasets, often violating data ownership rights. The aggressive scraping increases CPU utilization, bandwidth consumption, and cloud hosting costs while distorting business analytics.

2

Legal and Compliance Risks (T1081)

Web scraping by AI bots raises compliance concerns, particularly for PII and sensitive data in regulated industries. Unauthorized data scraping leads to potential violations of GDPR and other data protection laws.

3

MITIGATION STRATEGIES:

- **AI-Powered Bot Defense:**

  Deploy AI-driven bot detection systems that utilize machine learning to analyze traffic patterns and block malicious bots in real-time.

- **Rate Limiting and CAPTCHA:**

  Implement rate limiting to mitigate high-frequency requests and deploy CAPTCHA to prevent automated scraping.

- **Web Application Firewall (WAF):**

  Use WAFs to inspect traffic for suspicious patterns (e.g., bots with high request rates, odd User-Agent headers) and block scraper bots.

- **Network Defense:**

  Deploy network-level defenses such as DNS filtering and C2 detection tools to block communication with known malicious infrastructure. Ensure proper segmentation to limit lateral movement should credentials be compromised.

- **Authentication and Session Security:**

  Enforce strong session management policies, including short session timeouts and session re-authentication on critical systems. Apply Zero Trust principles to ensure that access controls are in place even for authenticated users.

How CyberForceQ Can Help

For 29 years, CyberForceQ has been a trusted name in advancing cybersecurity programs. Our expertise lies in designing and executing measurable cybersecurity strategies tailored to organizations of all sizes. With a track record of proven results, we offer services such as customized security assessments, robust security operations centers, and comprehensive strategic guidance. Let us assist your organization in prioritizing its goals, elevating your cybersecurity capabilities, and providing meaningful measurements of progress. Our participants are innovative leaders who share optimal strategies to implement and advance a proven cybersecurity program. CyberForceQ, in collaboration with our participants, is protecting the cyber realm.

CONNECT WITH US

www.cyberforceq.com 248.837.1400 solutions@cyberforceq.com