**SOC Investigation Report – Phishing & Malware Campaign – March 2025**

**Authors:** Nelson P. **Date:** 24/03/2025

**Key Findings**

**Indicators to Block**

**Malicious Domains Identified from Investigation**

These domains were discovered **through WHOIS, passive DNS, PCAP analysis, SSL certificate research, and AlienVault OTX**, all linked to the original IOCs.

* kvckz[.]engineercoin[.]xyz (Initial phishing domain)
* wgcuwcgociewewoo[.]xyz (Command and Control domain found in PCAP)
* ockimqekmwecocug[.]xyz (Linked to MetaStealer infrastructure)
* iqaeaoeueeqouweo[.]xyz (Linked to MetaStealer infrastructure)
* ywsogsasmecsemsy[.]xyz (Sinkholed domain previously used for malicious purposes)
* us-vpn02[.]yethoro[.]xyz (Associated with a VPN service used for obfuscation)
* safeworld08[.]info (Resolved to 185.172.129.192 in 2019)
* blackdiamond-promo[.]site (Resolved to 185.172.129.192 in 2020)
* play-dino-game[.]com (Resolved to 185.172.129.192 multiple times from 2022 to 2023)
* mmswgeewswyyywqk[.]xyz (Resolved to multiple IPs, including 185.172.129.192, 172.234.25.151, and 162.249.67.151)

**Malicious IPs Identified for Blocking (Total: 18)**

These IP addresses were found to be **associated with malware infrastructure** and pose security risks. Many malicious IPs listed here were found from WhoisXMLAPI by searching all the IPs associated with the malicious domains found previously.

* 185.172.129.192 (Command and Control infrastructure linked to VPN obfuscation)
* 199.21.76.77 (Previously linked to malicious domains)
* 34.174.78.212 (Historical association with malicious domains)
* 54.80.154.23 (IP found hosting malicious domains in mid-2024)
* 18.208.156.248 (Recent associations with malicious domains)
* 34.227.7.138 (Active malicious domain hosting in early 2025)
* 34.229.166.50 (AWS-hosted infrastructure linked to discovered domains)
* 35.205.61.67 (Passive DNS history showing activity linked to malicious domains)
* 104.155.138.21 (Previously associated with malicious infrastructure)
* 107.178.223.183 (Linked to attacks using iqaeaoeueeqouweo[.]xyz)
* 44.221.84.105 (Historical link to iqaeaoeueeqouweo[.]xyz)
* 172.234.25.151 (Recent resolution of mmswgeewswyyywqk[.]xyz)
* 162.249.67.151 (Actively hosting mmswgeewswyyywqk[.]xyz in late 2024)

**Tools Used in Investigation**

**Threat Intelligence and Domain Analysis**

* WHOIS Lookup – Checking domain registration details and ownership
* VirusTotal – Checking domain reputation and malware classifications
* FortiGuard – Web filtering classification
* AbuseIPDB – Searching abuse reports for malicious IPs
* AlienVault OTX – Reviewing open threat intelligence sources
* Passive DNS Analysis – Identifying historical associations

**Network and Infrastructure Analysis**

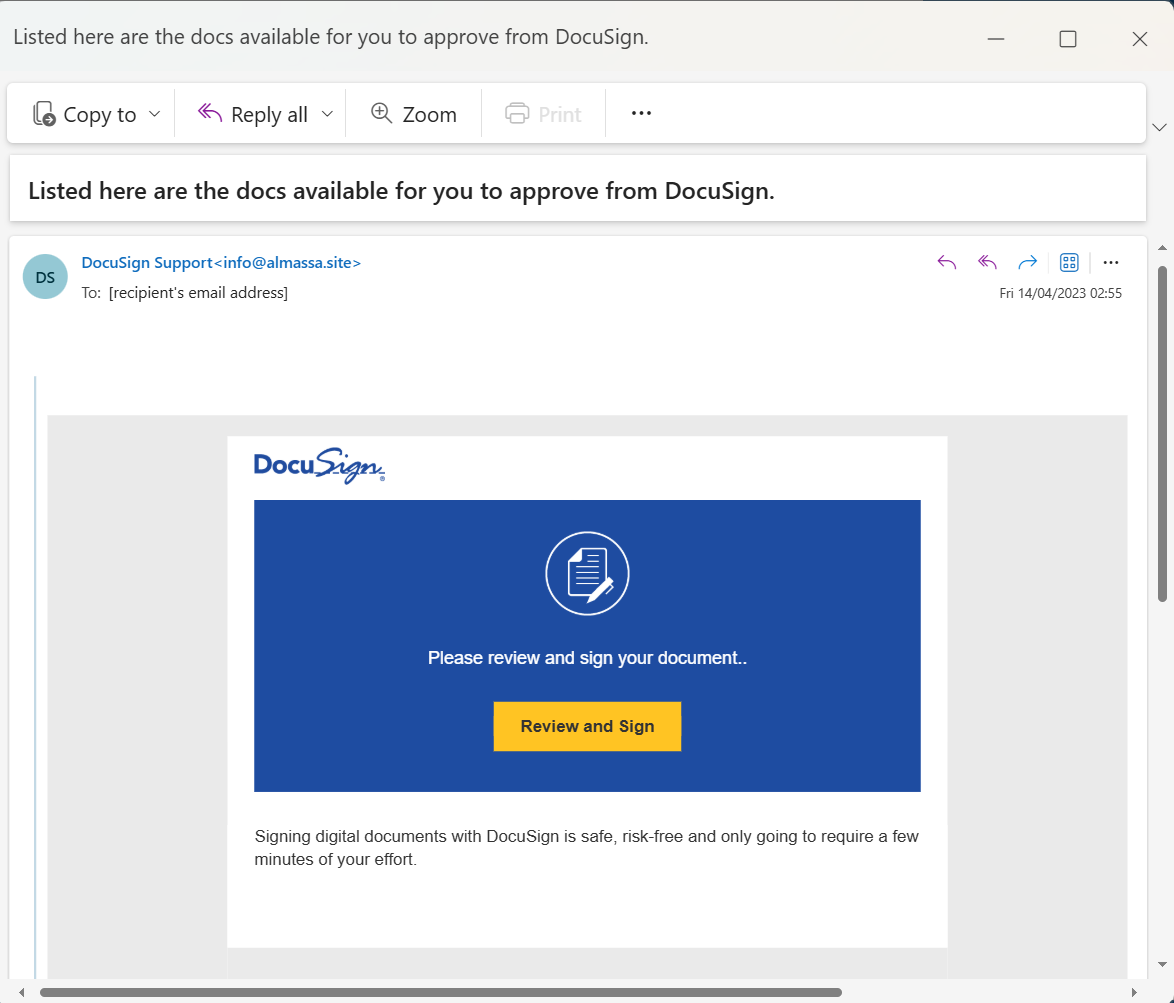
* Wireshark – Packet capture analysis of suspicious network traffic
* Shodan – Identifying open ports, vulnerabilities, and SSL certificates

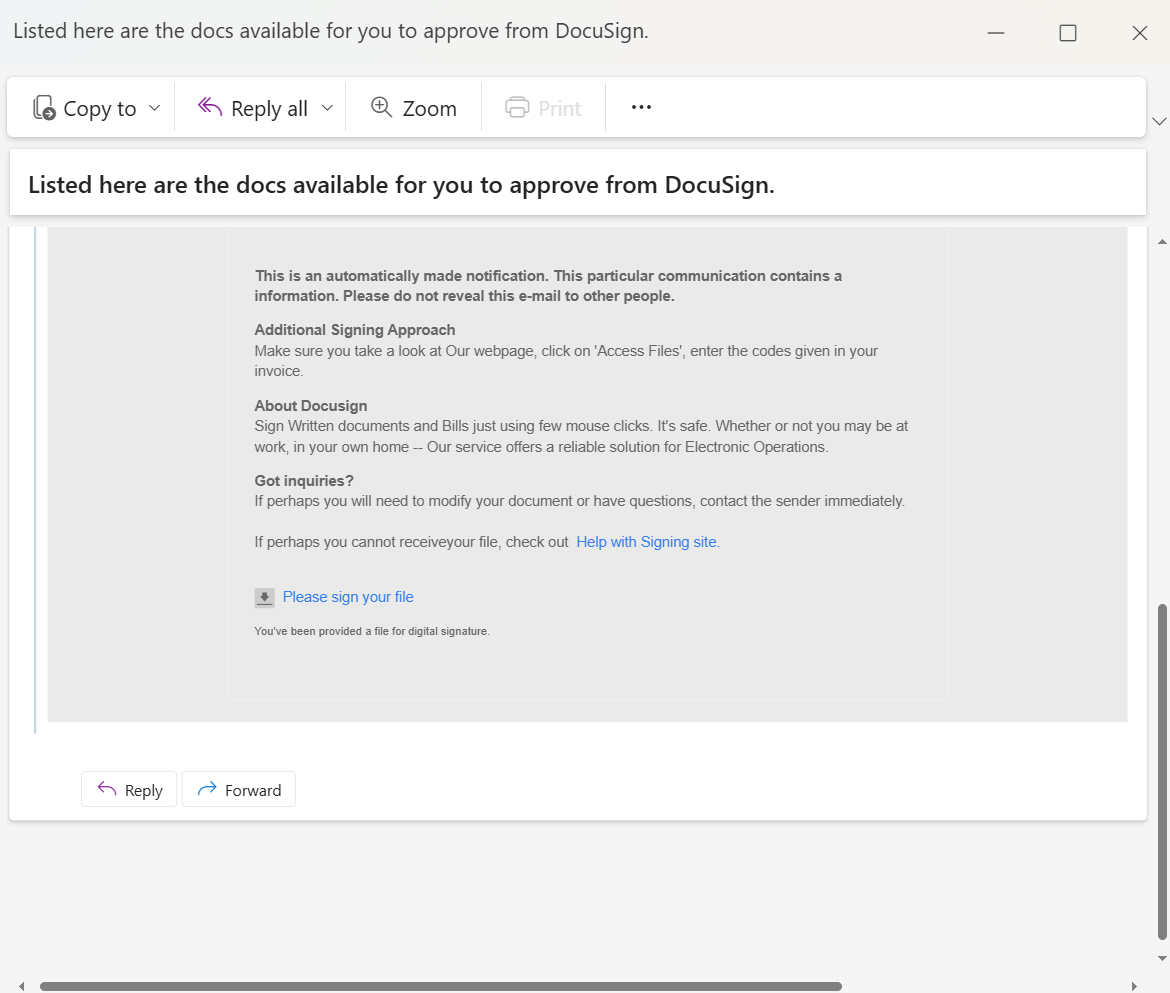
**SSL Certificate and Encryption Research**

* SSL Checker – Reviewing certificate validity and ownership
* Censys – Investigating historical certificates and TLS usage

1. **Phishing Email Investigation**

Figure 1. DocuSign Phishing Email (screenshot across two images)





**Phishing email details:**

* The phishing email impersonated **DocuSign** using **kvckz[.]engineercoin[.]xyz**, leading to a malicious website
* WHOIS revealed the domain was **registered under GMO Internet Group**, currently in **server hold status**
* VirusTotal flagged the domain for **hosting malware**
* FortiGuard classified the domain under **Malicious Websites**

**2. Network Traffic Analysis (PCAP Review)**

* Wireshark revealed **Command and Control interactions** with **wgcuwcgociewewoo[.]xyz**
* Frequent TCP SYN packets targeted **185.172.129.192**, indicating repeated backdoor connections
* API calls observed included **/tasks/collect** and **/tasks/get\_worker**, suggesting remote malware execution
* Unencrypted HTTP traffic showed **potential data exfiltration attempts**

**Expanded Infrastructure Analysis**

* **185.172.129.192** is linked to a **VPN provider (FIRST SERVER LIMITED)**
* Hostnames include **github.com** and **us-vpn02[.]yethoro.xyz**
* Open ports include **SSH (22), HTTP (80), HTTPS (443), RDP (3389), Windows services (135, 139, 445, 5357, 5985, 47001)**

**3. Malware Sample Analysis**

VirusTotal scans confirmed malicious attributes across multiple hashes.

**Mapped MITRE ATT&CK Techniques:**

* T1071 – Application Layer Protocol (HTTP used for malware communication)
* T1078 – Valid Accounts (Credential harvesting attempts)
* T1140 – Obfuscated Files (Evidence of MSI-based evasion)

**4. Attack Chain Correlation**

The malware campaign follows a **phishing-to-execution flow**:

1. Phishing email delivers **kvckz[.]engineercoin[.]xyz**, leading victims to an infected site
2. Malicious binary establishes **C2 communication** via **wgcuwcgociewewoo[.]xyz**
3. Network logs confirm repeated exfiltration attempts, particularly targeting **185.172.129.192**

**5. Conclusion and Security Recommendations**

**Immediate Actions**

* **Blacklist all identified domains and IPs** to prevent future interactions
* **Monitor outbound traffic** to detect unauthorized data exfiltration attempts
* **Block MSI wrappers** using endpoint security to prevent silent payload installations
* **Strengthen phishing awareness programs** focusing on the building awareness of campaigns that use methods like false DocuSigns to gain user trust.

This report outlines an **organized malware campaign** leveraging **phishing, C2 persistence, obfuscation techniques, and possible infrastructure misuse**.