February 3, 2025

Threat Actors Exploit .gov Domains for Phishing and Malware Operations

Overview

A recent report by Cofense Intelligence has uncovered a growing trend of cybercriminals exploiting government (.gov) top-level domains (TLDs) for phishing campaigns and malware operations. Between November 2022 and November 2024, attackers leveraged vulnerabilities in government websites across multiple countries to host malicious content, establish command-and-control (C2) servers, and redirect victims to phishing pages. The inherent trust users placed in the government domain has been weaponized, enabling these campaigns to bypass security measures and effectively deceive targets. The critical vulnerability, CVE-2024-25608, affecting the Liferay digital experience platform, has played a significant role in these attacks, particularly through open redirect abuse.

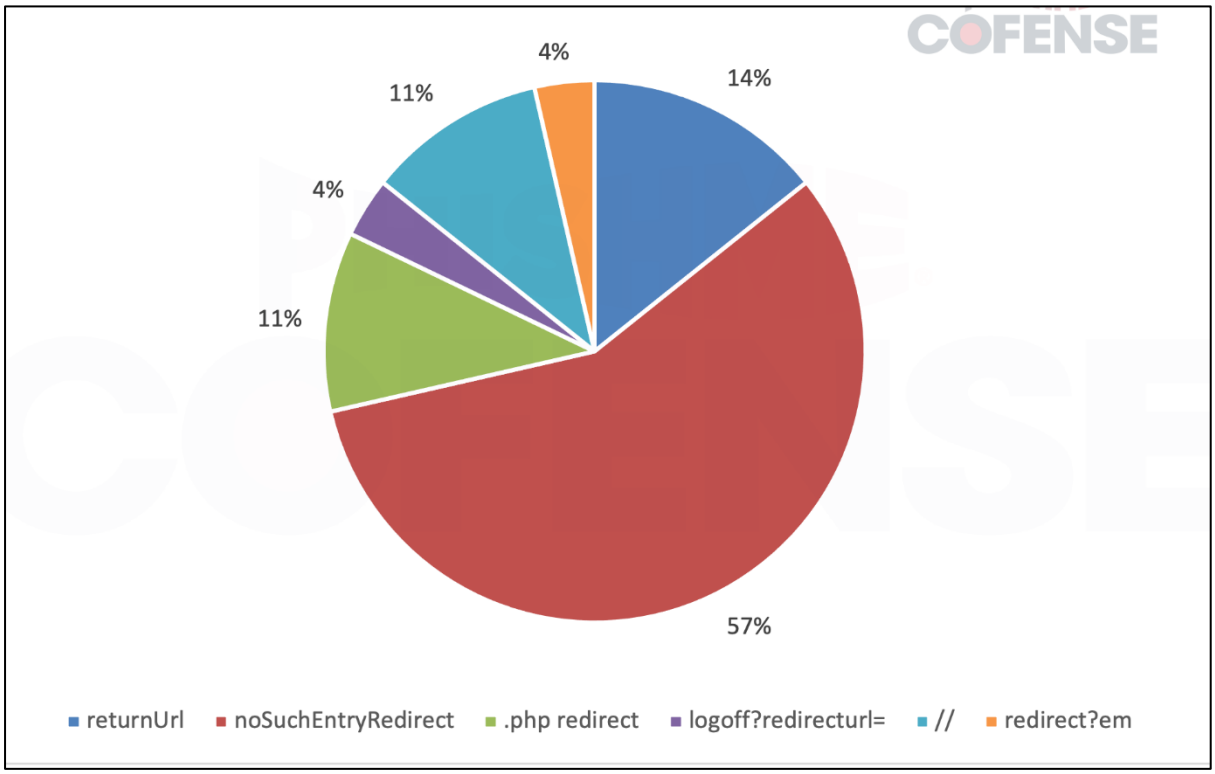

Figure 1: Methods of open redirects observed with abused .gov domains

CTI Analysis

Threat actors primarily rely on open redirect vulnerabilities to deceive users and evade secure email gateways (SEGs). An open redirect occurs when a legitimate website allows user-controlled input to specify an external site, leading unsuspecting victims to credential

phishing pages. Attackers have embedded compromised .gov URLs in phishing emails, impersonating Microsoft login pages and other legitimate services. The exploitation of US-based .gov domains accounted for 9% of all observed cases, making them the third-most targeted worldwide. Notably, 77% of these open redirects contained the "noSuchEntryRedirect" element, indicating a strong connection to CVE-2024-25608. Brazil emerged as the most targeted country, with its *.gov.br* domains contributing to most cases, suggesting repeated exploitation of specific sites rather than widespread vulnerabilities.

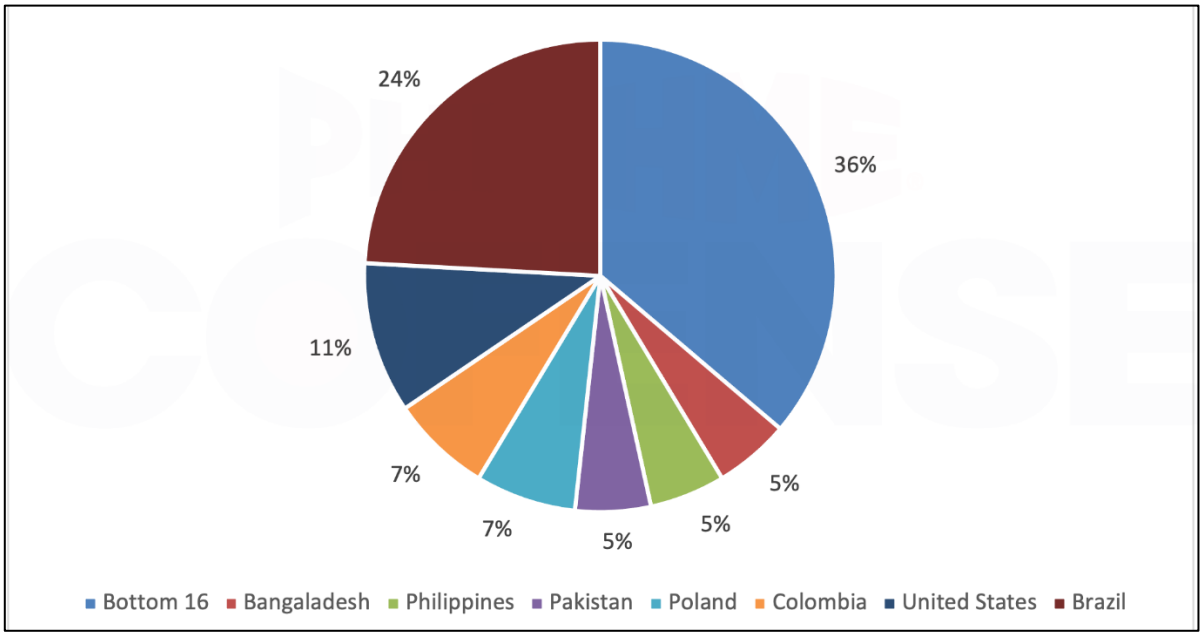

Figure 2: Government domains abused by country based on unique domains

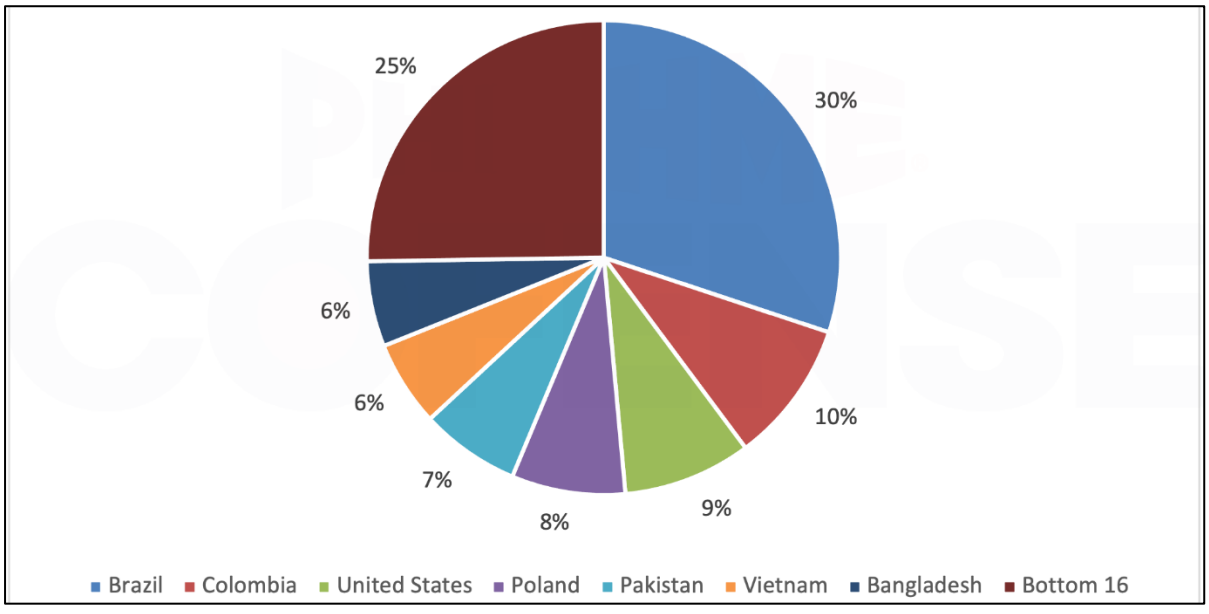

Figure 3: Government domains abused by country based on the frequency of URLs

Impact Analysis

The ability of *.gov* domains to bypass SEGs poses a significant security risk. Prominent email security solutions such as Microsoft ATP, Proofpoint, Cisco IronPort, Symantec MessageLabs, and Mimecast failed to filter phishing emails exploiting government open redirects. As a result, users were more likely to click on malicious links embedded within phishing emails that appeared trustworthy due to the *.gov* domain association. Additionally, in mid-2023 and early 2024, cybercriminals were found to have compromised government email addresses to serve as C2 infrastructure for malware such as Agent Tesla Keylogger and StormKitty. While only two government email addresses were exploited in this manner, the findings highlight persistent vulnerabilities in government digital security.

Mitigation

- Government agencies should implement stricter validation processes to prevent open redirects.
- Regular patching software vulnerabilities, including CVE-2024-25608, are crucial to reducing attack surfaces.
- Increased cybersecurity awareness and phishing training can help individuals and organizations recognize and mitigate threats.

Conclusion

The exploitation of *.gov* domains for phishing and malware operations underscores the urgent need for enhanced security measures in government digital infrastructure. Cybercriminals are deliberately targeting trusted domains to maximize the effectiveness of their campaigns, successfully bypassing traditional security defenses. By addressing vulnerabilities, strengthening security protocols, and promoting awareness, organizations can better defend against these evolving threats.

Source:

https://securityonline.info/gov-no-more-government-domains-weaponized-in-phishing-surge/

https://cofense.com/blog/threat-actors-exploit-government-website-vulnerabilities-for-phishing-campaigns
https://www.infosecurity-magazine.com/news/threat-actors-exploit-gov-websites/