THREAT BULLETINS

VoidProxy: A New and Evasive Phishing-as-a-Service Framework

TLP:WHITE

Sep 18, 2025

On September 11, 2025, Okta discovered a sophisticated Phishing-as-a-Service framework named VoidProxy. Due to its evasive capabilities and modular design, it has emerged as a significant threat. Cybercriminals use it to conduct Adversary-in-the-Middle (AitM) phishing attacks, which allow them to intercept and manipulate communications between users and legitimate services. The attacks target Microsoft and Google accounts and can redirect accounts secured by identity providers, such as Okta, to malicious websites.

As phishing remains one of the most common attack vectors for the health sector, Health-ISAC is providing this information to increase situational awareness and share details about the recent Phishing-as-a-Service framework, its security implications, and recommendations for defending against malicious activity.

VoidProxy features a modular architecture that allows cybercriminals to easily tailor phishing campaigns to specific targets. The framework employs sophisticated evasion techniques such as residential proxy usage, dynamic content injection, and session hijacking to bypass traditional security measures and steal authentication tokens. Once they manage to gain access to the system, cybercriminals can engage in various malicious activities, including Business Email

Compromise (BEC), financial fraud, data exfiltration, and lateral movement.

Its stealthy nature makes it difficult to detect, underscoring the need for identity-centric security strategies, adaptive risk-based policies, and robust multi-factor authentication.

Reference(s)	oktasecurity, bleepingcomputer, hackread

Sources
https://sec.okta.com/articles/uncloakingvoidproxy/

https://www.bleepingcomputer.com/news/security/new-voidproxy-phishing-service-targets-microsoft-365-google-accounts/

https://hackread.com/voidproxy-phishing-service-bypasses-mfa-microsoft-google/

Recommendations
Health-ISAC recommends organizations review and assess their level of risk to this activity and implement the following:

- Implement strong authentication methods such as passkeys, hardware security keys, and smart cards, and ensure that policies enforce resistance to phishing attacks. Limit access to critical applications to devices managed through endpoint management systems and protected by endpoint security tools. For less sensitive applications, allow access only from registered devices that meet basic security hygiene standards.
- Block or require additional verification for access attempts from unfamiliar or rarely used networks. Monitor for access requests that deviate from typical user behavior patterns, and configure policies to either escalate authentication requirements or deny access based on this context.
- Educate users to recognize signs of phishing emails, malicious websites, and common social engineering tactics. Enable

notification and reporting mechanisms to make it easy for users to report suspicious activity.
- Enable real-time responses to interactions with suspicious infrastructure by automating remediation workflows. Apply IP session binding to administrative applications to prevent session hijacking and enforce re-authentication whenever an administrator initiates sensitive actions.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patient Resources.

Alert ID 34be8062

This Alert has 3 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Share Feedback

was this helpful?  | 

Tags VoidProxy, Phishing-as-a-service

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits

https://h-isac.org/events/

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**