FINISHED INTELLIGENCE REPORTS

Phishing Guidance - Stopping the Attack Cycle Phase One

○○○ TLP:WHITE

Oct 19, 2023

Social engineering is the attempt to trick someone into revealing information (e.g., a password) or taking an action that can be used to compromise systems or networks. Phishing is a form of social engineering where malicious actors lure victims (typically via email) to visit a malicious site or deceive them into providing login credentials. Malicious actors primarily leverage phishing for:

- Obtaining login credentials. Malicious actors conduct phishing campaigns to steal login credentials for initial network access. Malware deployment. Malicious actors commonly conduct phishing campaigns to deploy malware for follow-on activity, such as interrupting or damaging systems, escalating user privileges, and maintaining persistence on compromised systems.

- The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint guide to outline phishing techniques malicious actors commonly use and to provide guidance for both network defenders and

> software manufacturers. This will help to reduce the impact of phishing attacks in obtaining credentials and deploying malware. Health-ISAC is distributing this report for your situational awareness. To view the full report, please see the attached document.

The guidance for network defenders is applicable to all organizations but may not be feasible for organizations with limited resources. Therefore, this guide includes a section of tailored recommendations for small-and medium-sized businesses that may not have the resources to hire IT staff dedicated to a constant defense against phishing threats.

The guidance for software manufacturers focuses on secure-by design and -default tactics and techniques. Manufacturers should develop and supply software that is secure against the most prevalent phishing threats, thereby increasing the cybersecurity posture of their customers.

Alert ID 3bd8c502

This Alert has 2 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags MS-ISAC, CISA, FBI, Phishing

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

Share Threat Intel

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP “Share Threat Intel” Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Knowledge Base

Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/

CISA CISA is the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.

Access the Health-ISAC 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 Cyware.

Download Health-ISAC’s Information Sharing App.

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

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.