FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

29 APR 2025

FLASH Number

FLASH-20250429-001

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

**Note: By reporting any related information to FBI Cyber Squads, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

Phishing Domains Associated with LabHost PhaaS Platform Users

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate 42,000 phishing domains linked to the LabHost phishing-as-a-service (PhaaS) platform between November 2021 and April 2024. Prior to being disabled by law enforcement in April 2024, LabHost was one of the world's largest PhaaS providers, offering a range of illicit services for approximately 10,000 users. The platform enabled cyber criminals to impersonate more than 200 organizations, including major banks and government institutions, in an effort to collect personal information and banking credentials from unsuspecting victims worldwide. The FBI is releasing this information to maximize awareness and provide indicators of compromise that may be used by recipients for research and defense.

Technical Details

Overview

LabHost provided numerous phishing services to their customers including, but not limited to: infrastructure configuration/support, customized phishing pages, adversary-in-the-middle proxy connections to obtain two-factor authentication (2FA) codes, smishing services, and stolen credential management.

LabHost's infrastructure stored over one million user credentials and nearly 500,000 compromised credit cards, enabling financial theft, various fraud schemes, and money laundering by its users.

LabHost offered a variety of phishing pages and, for an additional cost, creation of bespoke pages. Once a victim clicked a phishing page link and entered their details, LabHost servers received the captured information and delivered it to the LabHost customer. LabHost collected personally identifiable information (PII), credentials, and credit card information.

LabHost phishing domains were configured to impersonate over 200 trusted sites, including spoofed pages for banks, online streaming platforms, government agencies, postal services, and more. Law enforcement action identified over 42,000 unique domains associated with the platform, impacting over a million victims worldwide.

Indicators

FBI obtained these 42,000 domain names and creation dates associated with LabHost from the backend server of the platform. FBI has not validated every domain name, and the list may contain typographical or similar errors from LabHost user input. The information is historical in nature, and the domains may not currently be malicious. The full list of domain names used by Labhost users can be found at https://www.ic3.gov/CSA/2025.

Recommended Mitigations:

Though the LabHost domains are historical in nature, this list of over 42,000 domains may provide insight for network defenders and cyber threat intelligence personnel on adversary tactics and techniques. Historical research that identifies connections to any of these domains should prompt additional response and follow up with the impacted user(s). FBI recommends organizations that identify any activity related to these indicators of compromise within their networks act to mitigate or minimize the impact and prepare their environment for incident response. Additional research into these domains may identify other malicious domain names or infrastructure.

Organizations may also consider taking forward-looking steps to protect their environments, such as blacklisting domains or configuring alerts for connections made to domains that they have vetted and deemed to be malicious.

Reporting Notice

FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

The specific indicators that appear in this communication, which are of non-deterministic or ephemera nature, may not alone be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Administrative Note

This product is marked **TLP:CLEAR**. Subject to standard copyright rules, the information in this product may be shared without restriction.