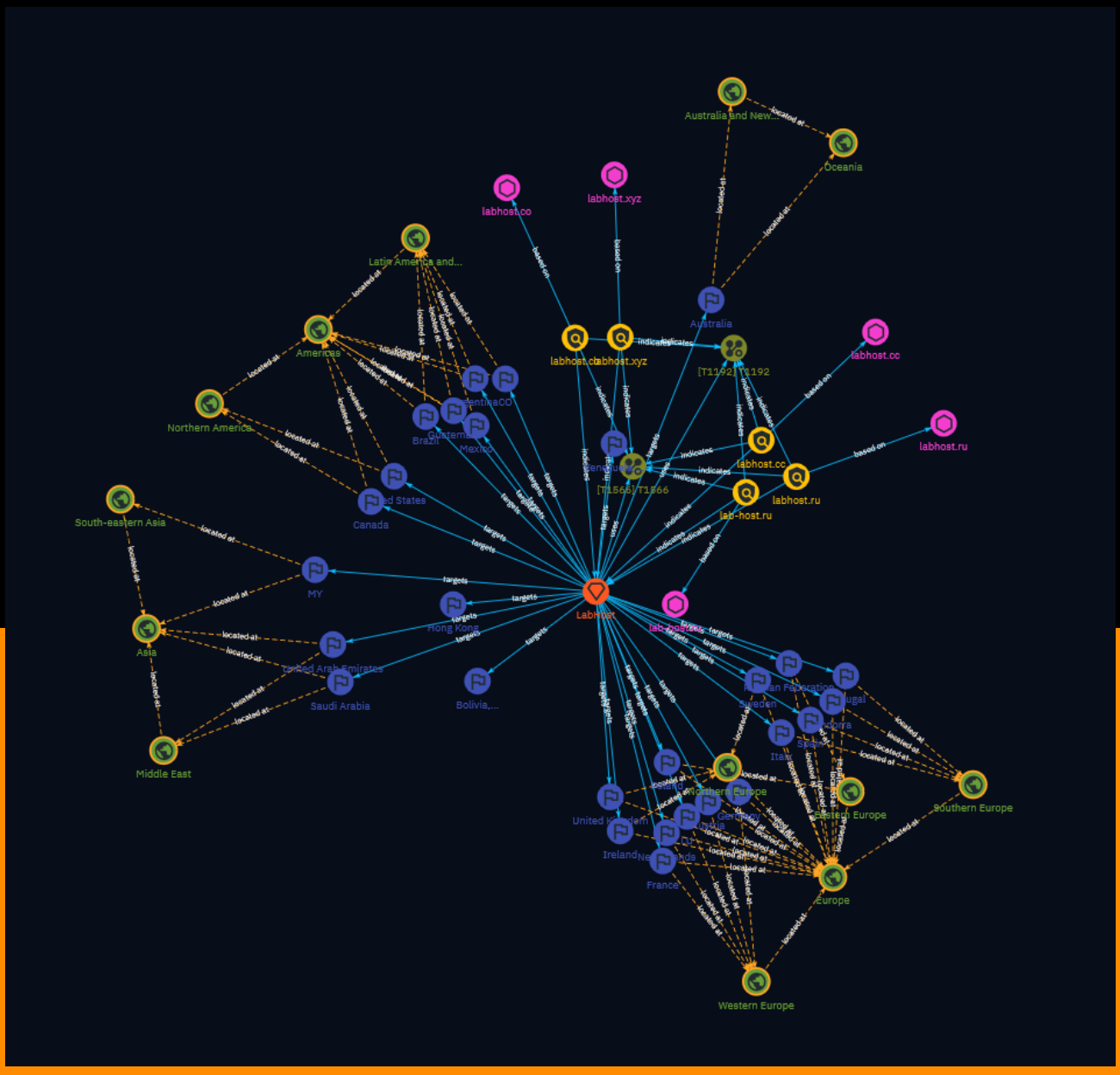
Apr 19 2024

NETMANAGEIT

# Intelligence Report

# The Fall of LabHost: Law Enforcement Shuts Down Phishing Service Provider



# Table of contents

## Overview



## Entities



## Observables

# External References

# Overview

## Description

The report details the takedown of the LabHost phishing-as-a-service (PhaaS) platform by law enforcement agencies. LabHost, active since 2021, offered various phishing tools and templates targeting banks, organizations, and service providers worldwide. With over 2,000 criminal users, it was responsible for deploying over 40,000 fraudulent sites that victimized hundreds of thousands of individuals. The report outlines LabHost's features, subscription tiers, an example attack flow, and the collaborative operation that led to its seizure and arrests of key users.

## Confidence

*This value represents the confidence in the correctness of the data contained within this report.*

100 / 100

# Content

N/A

# Indicator

**Name**

labhost.xyz

**Description**

- **Unsafe:** False - **Server:** ope - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '23 hours ago', 'timestamp': 1713345203, 'iso': '2024-04-17T05:13:23-04:00'} - **IPQS: Domain:** labhost.xyz - **IPQS: IP Address:** 34.120.137.41

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'labhost.xyz']

**Name**

labhost.ru

**Description**

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 238 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & Internet - **Domain

Age:** {'human': '2 years ago', 'timestamp': 1637340852, 'iso': '2021-11-19T11:54:12-05:00'} - **IPQS: Domain:** reg.ru - **IPQS: IP Address:** 194.67.72.31

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'labhost.ru']

**Name**

labhost.co

**Description**

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '7 minutes ago', 'timestamp': 1713429108, 'iso': '2024-04-18T04:31:48-04:00'} - **IPQS: Domain:** labhost.co - **IPQS: IP Address:** N/A

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'labhost.co']

**Name**

labhost.cc

**Description**

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1666944110, 'iso': '2022-10-28T04:01:50-04:00'} - **IPQS: Domain:** labhost.cc - **IPQS: IP Address:** 103.224.212.210

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'labhost.cc']

**Name**

lab-host.ru

**Description**

- **Unsafe:** False - **Server:** ddos-guard - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '11 months ago', 'timestamp': 1684967293, 'iso': '2023-05-24T18:28:13-04:00'} - **IPQS: Domain:** lab-host.ru - **IPQS: IP Address:** 91.215.43.219

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'lab-host.ru']

# Intrusion-Set

| Name |
| --- |
| LabHost |

# Country

| Name |
| --- |
| Venezuela, Bolivarian Republic of |
| **Name** |
| Bolivia, Plurinational State of |
| **Name** |
| Hong Kong |
| **Name** |
| Australia |
| **Name** |
| Netherlands |
| **Name** |
| LU |
| **Name** |
| Germany |

| Name |
| --- |
| France |
| **Name** |
| Austria |
| **Name** |
| Spain |
| **Name** |
| Portugal |
| **Name** |
| Italy |
| **Name** |
| Andorra |
| **Name** |
| United Kingdom |
| **Name** |
| Sweden |
| **Name** |
| Ireland |

| Name |
| --- |
| Russian Federation |
| **Name** |
| Poland |
| **Name** |
| United Arab Emirates |
| **Name** |
| Saudi Arabia |
| **Name** |
| MY |
| **Name** |
| United States |
| **Name** |
| Canada |
| **Name** |
| CO |
| **Name** |
| Brazil |

| Name |
| --- |
| Argentina |
| **Name** |
| Mexico |
| **Name** |
| Guatemala |

# Attack-Pattern

| Name |
| --- |
| T1192 |
| **ID** |
| T1192 |
| **Name** |
| T1566 |
| **ID** |
| T1566 |
| **Description** |
| Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft |

OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

# Region

| Name |
| --- |
| Australia and New Zealand |
| **Name** |
| Oceania |
| **Name** |
| Western Europe |
| **Name** |
| Southern Europe |
| **Name** |
| Northern Europe |
| **Name** |
| Eastern Europe |
| **Name** |
| Europe |

| Name |
| --- |
| Middle East |
| **Name** |
| South-eastern Asia |
| **Name** |
| Asia |
| **Name** |
| Northern America |
| **Name** |
| Latin America and the Caribbean |
| **Name** |
| Americas |

# Domain-Name

| Value |
| --- |
| labhost.xyz |
| labhost.ru |
| labhost.co |
| labhost.cc |
| lab-host.ru |

# External References

- https://www.trendmicro.com/en_us/research/24/d/labhost-takedown.html
- https://otx.alienvault.com/pulse/6620d6e79506f0a1144a66ab