Phishing-as-a-Service Profile: LabHost Threat Actor Group

By Cybersecurity Experts at Fortra

Published: 2024-02-15 · Archived: 2026-04-25 02:00:35 UTC

Fortra continues to monitor malicious activity targeting Canadian banks by the Phishing-as-a-Service (PhaaS) group known as LabHost. Throughout 2022 and 2023, phishing campaigns linked to PhaaS platforms have surged, as threat actors increasingly rely on subscription-based services to execute attacks. These platforms offer a range of features, including stolen industry branding, real-time monitoring tools, and techniques to bypass security measures.

Canadian Phishing-as-a-Service Background

In 2022 and 2023, Fortra monitored threat actors targeting Canadian banks as they adopt the use of Phishing-as-a-Service platforms. Initially, the dominant provider for these services was Frappo. Frappo's launch in late 2021 resulted in an explosion of multi-branded phishing attacks capable of targeting numerous Canadian financial institutions simultaneously.

After the initial spike in activity in the first half of 2022, Frappo users reported that phishing pages made through the service were being blocked and mitigated at faster rates. In September 2022, Frappo promised that an improved second version of the service would be launched.

Over the course of 2023, Fortra observed phishing content families grow in popularity which shared many similarities with existing Frappo campaigns but included minor changes. Originally thought to be possible candidates for "V2", over time it became evident that the campaigns were sourced from a different distinct PhaaS platform. Communication in Canada-centric threat actor channels suggested that phishers had pivoted to using LabHost instead of Frappo for phishing campaigns.

The phishing kits used by LabHost and Frappo don't feature many indicators that make distinguishing between the two easy. However, a LabHost service outage in October and the resulting drop in phishing volume provided strong evidence for the attribution of LabHost to specific tracked phishing content families. This new information confirmed Fortra's suspicion that LabHost had overtaken Frappo in popularity in the first half of 2023.

LabHost Threat History

LabHost began publicly operating in Q4 2021, only a month after Frappo first became available to paying customers. Threat actors did not immediately take to using LabHost. Compared to Frappo, LabHost was considerably more expensive to subscribe to and initially developed a reputation among threat actors for "taxing" their users' successful campaigns or outright stealing from their customers.

LabHost's original multi-branded phishing kit featured full multi-factor authentication phishing for only three Canadian banks. LabHost added a more robust Canadian inter-bank network scam kit in June 2022 which

expanded this capability to ten Canadian banking institutions. Fortra first detected a significant increasing trend in phishing threats originating from LabHost compared to Frappo in the fourth quarter of 2022. In April 2023, Canadian financial phishing activity spiked following the release of LabHost's latest multi-branded page offering.

Multi-branded phishing attacks generated by PhaaS platforms, 2023.

After the release of the most recent Canadian inter-bank network kit, phishing remained at an elevated level through spring and summer until October. On October 4, 2023, LabHost experienced a major outage which prevented the creation of new phishing pages and locked threat actors out of any stolen information they had stored in the platform. This outage coincided with the disappearance of multiple tracked phishing content families from the threat landscape, providing strong evidence for attributing specific kits to the LabHost threat group.

Week-to-week PhaaS activity targeting Canadian Banks, Q3-Q4 2023.

Communication from the LabHost support team claimed that server maintenance had corrupted their installation and that a partner of the group sabotaged their systems, and as a result the recovery of the platform would be delayed. LabHost remained completely out of service until November 20, when users were allowed back onto the website to view their information stored on the platform. The functionality to purchase and host new phishing pages was not made available until the service was fully restored on December 6.

PhaaS Analysis

LabHost divides their available phishing kits between two separate subscription packages: a North American membership covering US and Canadian brands, and an international membership consisting of various global brands (and excluding the NA brands). While the international service is only offered through a single $300 per month subscription, the North American service is available in either a standard or premium package. LabHost's standard membership limits the threat actor to only Canadian brands and three concurrently active phishing pages. Premium membership grants phishers access to kits targeting US banks and increases the concurrent page count to 20 active phish.

Monthly subscriptions offered by LabHost phishing service.

The phishing kits most utilized by LabHost's customers are the Canadian inter-bank network kits targeting a wide array of Canadian banks. Other Canadian-targeted phishing kits target regional telecom providers and postal delivery services. Premium kits include phishing pages for 13 US banks, Spotify, and DHL.

LabHost ad for new and updated phishing pages, June 2022.

Several variations of the popular multi-brand scam pages are offered, each tailored to work with phishing lures targeting various industries including telecommunications, postal services, retail stores and more.

These kits include detailed installation options which allow threat actors to choose what banks will be actively targeted and what personal information will be requested.

Sample of multi-branded phishing kit setup and customization.

Live Phishing Capabilities

All scam kits available from LabHost work alongside a real-time campaign management tool named LabRat. LabRat allows the phisher to control and monitor their active attacks. This functionality is leveraged in man-in-the-middle style attacks to obtain two-factor authentication codes, authenticate valid credentials, and bypass additional security checks.

Demonstration of 2FA code interception. Left – Victim View. Right – Threat Actor Panel.

LabSend Phishing Lures

Alongside LabHost's relaunch in December, The Lab released a new SMS lure and campaign manager named LabSend. This new SMS spamming tool provides a sophisticated automated method for sending links to LabHost phishing pages. As described by The Lab team, the LabSend tool can coordinate an automated smishing campaign across multiple SIDs, randomizing portions of text messages to evade detection of catalogued malicious spam messages. After sending an SMS lure, LabSend will auto-reply to victims' responses using customizable message templates.

LabSend features detailed in launch ad, December 2023.

LabSend service home page.

LabHost services allow threat actors to target a variety of financial institutions with features ranging from ready-to-use templates, real-time campaign management tools, and SMS lures. In order to protect against attacks targeting their organizations, security teams should be aware of the spaces these attacks are occurring and monitor for activity targeting their brands. Fortra will continue to provide updates on any LabHost developments as they occur.
