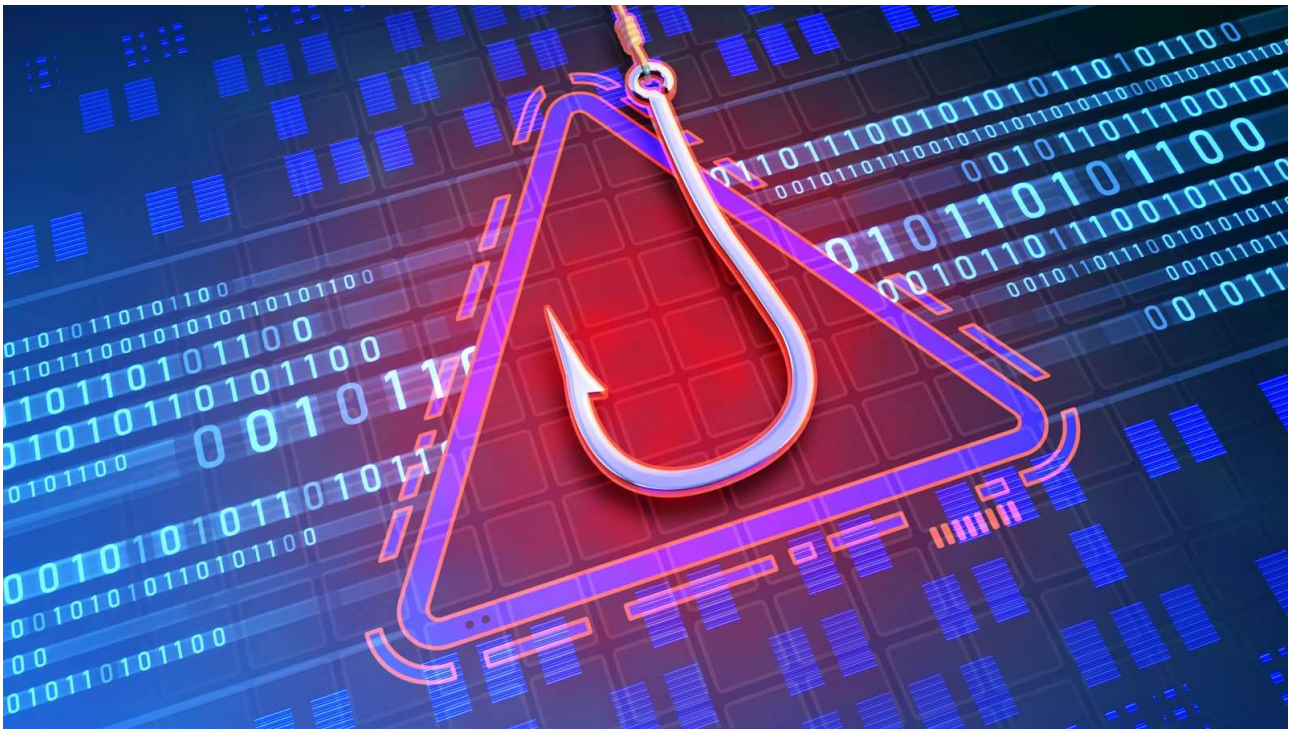


LabHost cybercrime service lets anyone phish Canadian bank users



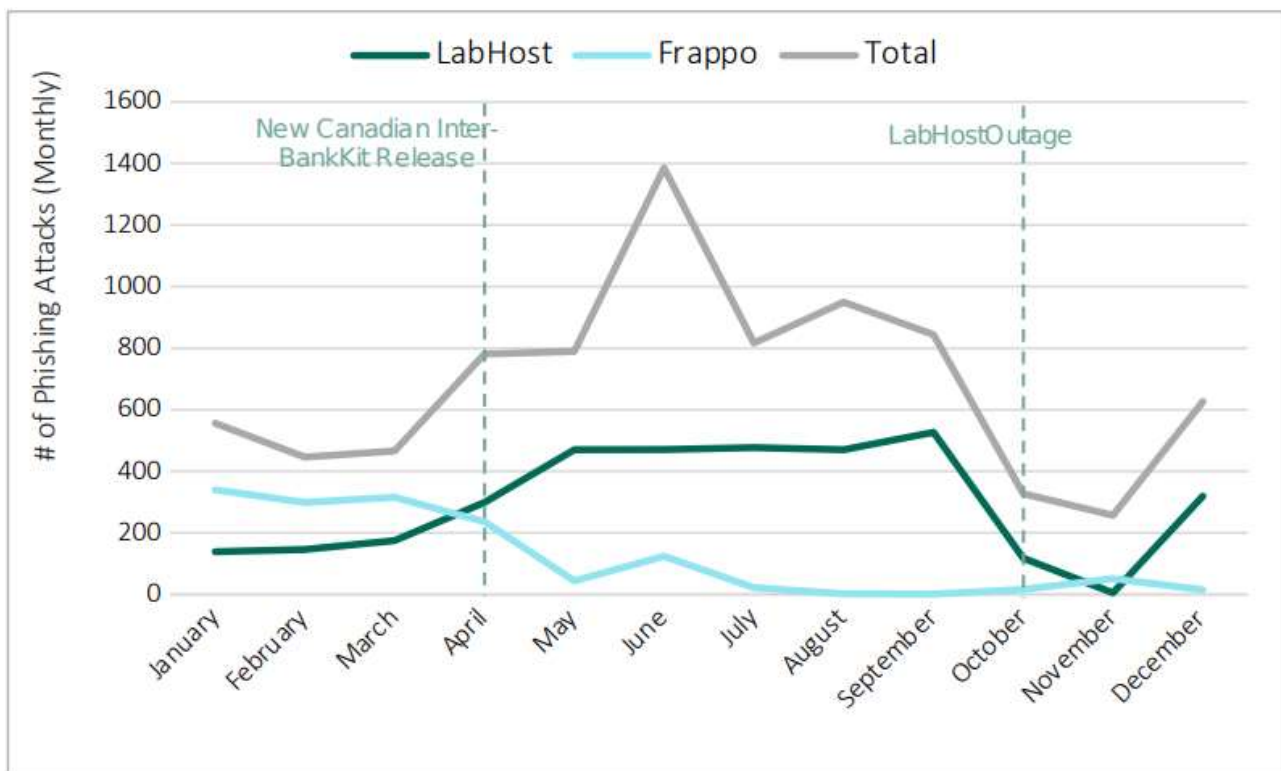
The Phishing as a Service (PhaaS) platform 'LabHost' has been helping cybercriminals target North American banks, particularly financial institutes in Canada, causing a notable increase in activity.

PhaaS platforms provide turnkey phishing kits, infrastructure for hosting the pages, email content generation, and campaign overview services to cybercriminals in exchange for a monthly subscription.

LabHost isn't a new provider, but its popularity surged after introducing custom phishing kits for Canadian banks in the first half of 2023.

Fortra, following the cybercriminal's activity, reports that LabHost has overtaken cybercriminals' previous favorite PhaaS platform, Frappo, and is now the primary driving force behind most phishing attacks targeting Canadian bank customers.

Though LabHost suffered a disruptive outage in early October 2023, it has restored its activity to notable levels, counting several hundreds of attacks per month.



Observed PhaaS activity (Fortra)

Fortra first published a post on its blog section two weeks ago to alert about the emerging threat but added many more details about LabHost and its internal workings yesterday, after presumably infiltrating the operation with an account of their own.

A look inside LabHost

LabHost offers three membership tiers: the Standard (\$179/month), Premium (\$249/month), and World (\$300/month).

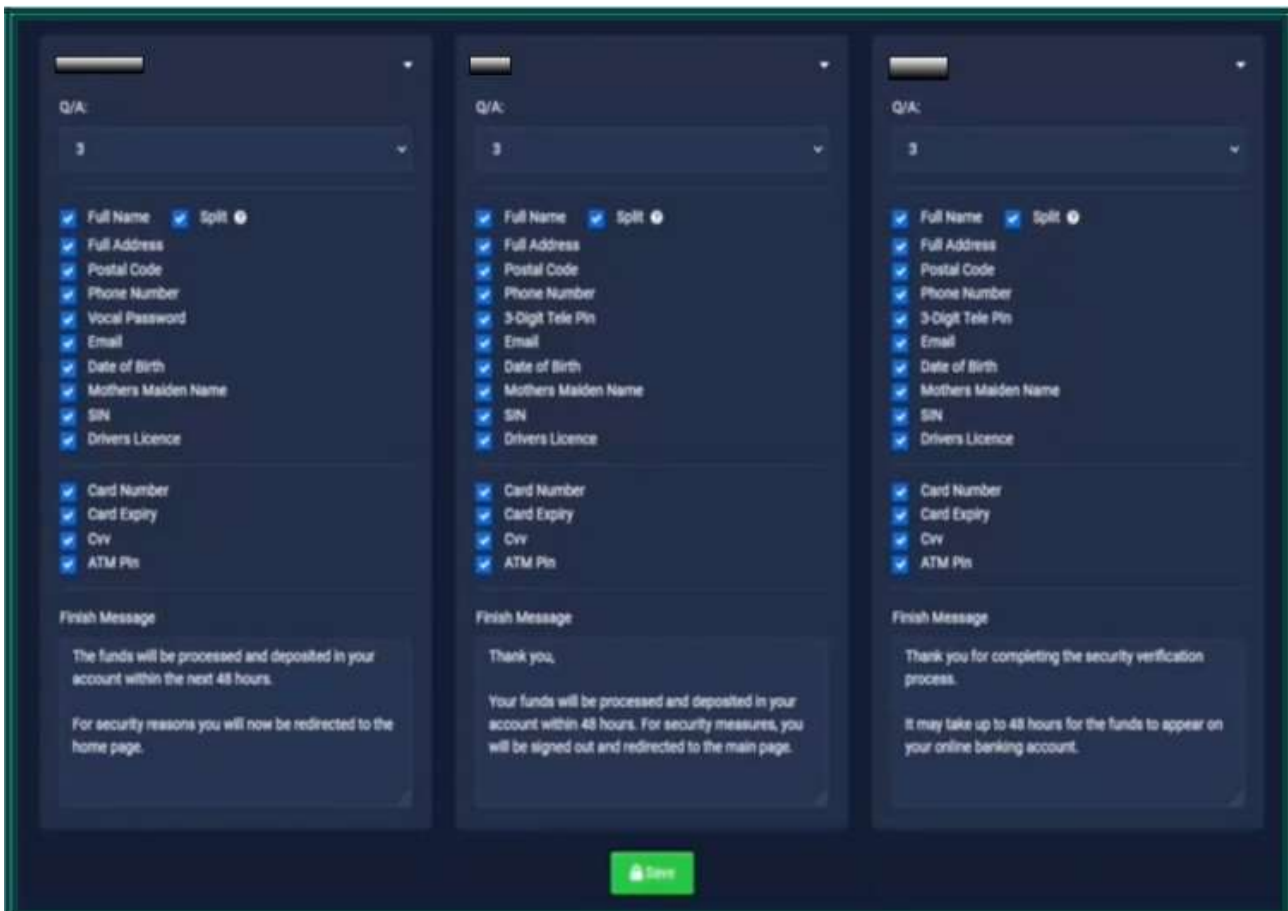
The first focuses on Canadian banks, the second includes U.S. banks, and the third targets 70 institutions worldwide, excluding North America.

Standard For the Common Users	Premium For Top & Knowledge Users	World Membership Access to rest of the World
\$179/month	\$249/month	\$300/month
<ul style="list-style-type: none"> ✓ *DOESN'T INCLUDE WORLD MEMBERSHIP* ✓ Access to Standard Features ✓ Access to Standard Pages (18 Pages) ✓ Protection from Lab Host Antibots ✓ Access to Future Updates ✓ Allowed 3 Captcha & 3 Page Active ✓ NO RESULTS TAX 	<ul style="list-style-type: none"> ✓ *DOESN'T INCLUDE WORLD MEMBERSHIP* ✓ Includes All Standard Features ✓ Access to LABRAT ✓ Access to USA Pages (13 Pages) ✓ Access to Premium Pages (19 Pages) ✓ Access to Future Features ✓ Allowed 20 Captchas & 20 Pages Active ✓ NO RESULTS TAX 	<ul style="list-style-type: none"> ✓ *DOESN'T INCLUDE CANADA/USA* ✓ Access to 70+ bank panels ✓ Access to LABRAT ✓ Comes with multi banks for multiple countries ✓ Allowed 10 Captchas & 10 Pages Active
Buy now	Buy now	Buy now
		NO REFUNDS

Membership tiers (Fortra)

Apart from phishing kits for banks, the templates include phishing pages for online services like Spotify, postal delivery services like DHL, and regional telecommunication service providers.

Cybercriminals buying access to the LabHost panel are given multiple installation options to craft custom attacks quickly.

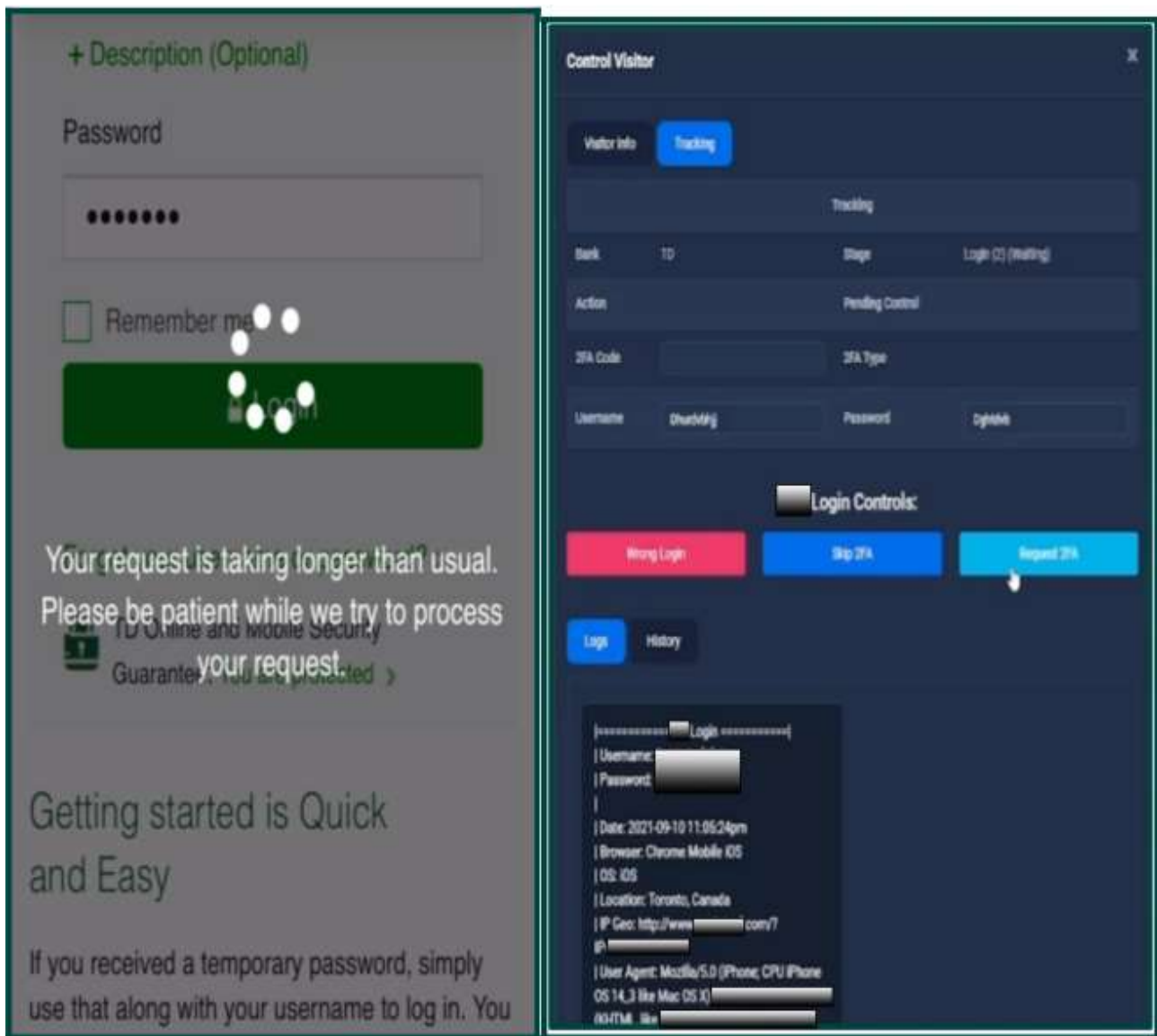
The image displays three side-by-side panels of a phishing kit interface, each representing a different phishing page template. Each panel has a dark blue background with a lighter blue header area containing a 'Q/A:' dropdown menu set to '3'. Below the header, there are two sections of checkboxes, each preceded by a blue checkmark icon. The first section includes: Full Name, Split (with a small circular icon), Full Address, Postal Code, Phone Number, Vocal Password, Email, Date of Birth, Mothers Maiden Name, SIN, and Drivers Licence. The second section includes: Card Number, Card Expiry, Cvv, and ATM Pin. At the bottom of each panel is a 'Finish Message' section with a light blue background and a rounded rectangle border. The first panel's message states: 'The funds will be processed and deposited in your account within the next 48 hours. For security reasons you will now be redirected to the home page.' The second panel's message states: 'Thank you, Your funds will be processed and deposited in your account within 48 hours. For security measures, you will be signed out and redirected to the main page.' The third panel's message states: 'Thank you for completing the security verification process. It may take up to 48 hours for the funds to appear on your online banking account.' A green 'Save' button with a white floppy disk icon is centered at the bottom of the three panels.

Phish customization options (Fortra)

LabHost enables attackers to steal 2FA protection on targeted accounts by linking the phishing process to 'LabRat,' a real-time phishing management tool that lets cybercriminals monitor and control an active phishing attack.

"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," explains Fortra.

"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."

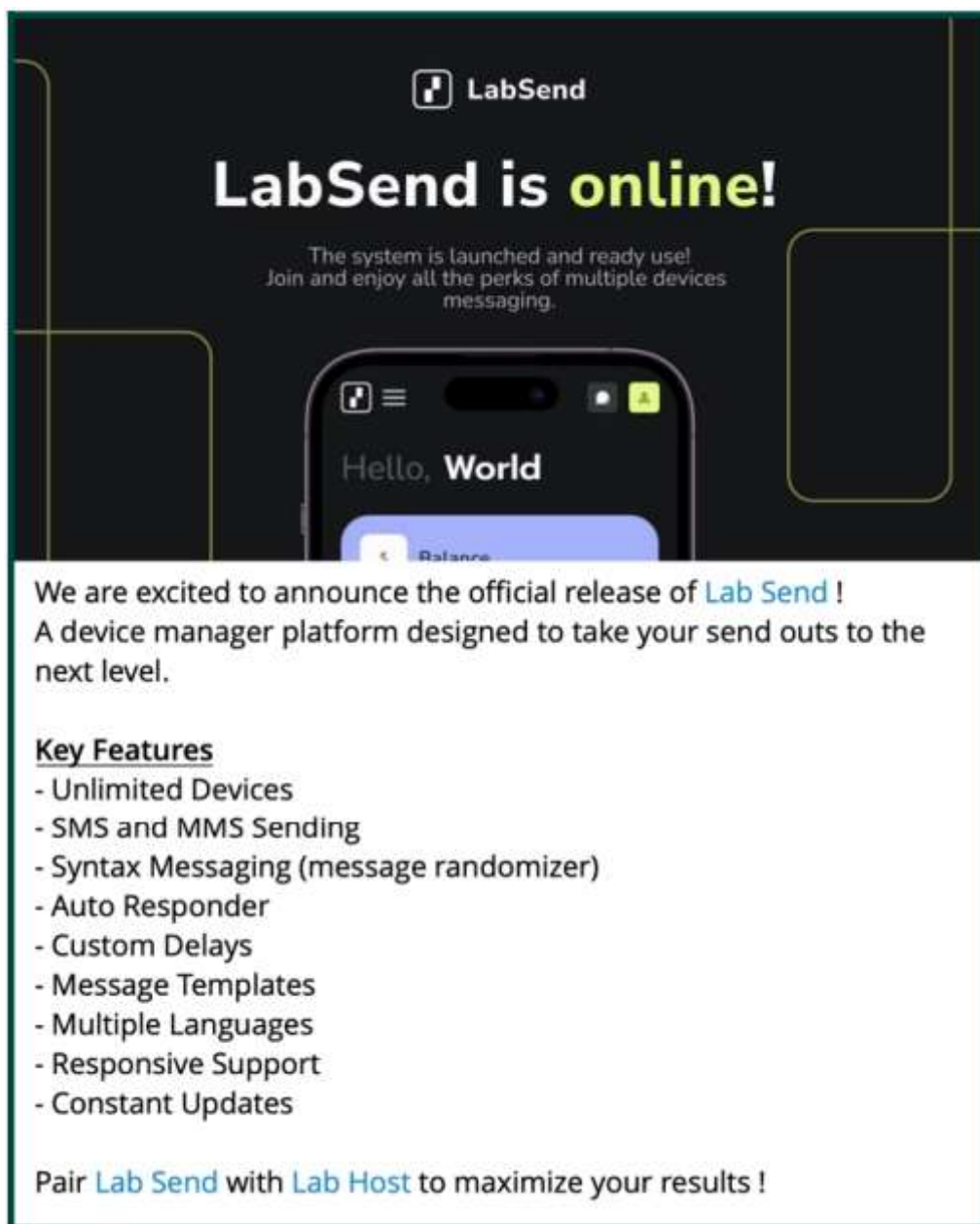


The LabRat tool used for conducting the attack (Fortra)

In addition to the above, when LabHost relaunched following the October disruption, it introduced a new SMS spamming tool named 'LabSend,' which embeds links to LabHost phishing pages on SMS messages.

"The LabSend tool can coordinate an automated smishing campaign across multiple SIDs, randomizing portions of text messages to evade detection of cataloged malicious spam messages," [reads Fortra's report](#).

"After sending an SMS lure, LabSend will auto reply to victims' responses using customizable message templates."

A promotional graphic for LabSend. At the top, the LabSend logo is displayed. Below it, the text 'LabSend is online!' is written in a large, bold font, with 'online!' in green. Underneath, a smaller line of text says 'The system is launched and ready use! Join and enjoy all the perks of multiple devices messaging.' In the center, there is an image of a smartphone screen showing a 'Hello, World' message. Below the phone image, there is a white box containing text that reads: 'We are excited to announce the official release of Lab Send ! A device manager platform designed to take your send outs to the next level.' This is followed by a section titled 'Key Features' with a bulleted list of capabilities. At the bottom of the white box, it says 'Pair Lab Send with Lab Host to maximize your results !'.

LabSend

LabSend is online!

The system is launched and ready use!
Join and enjoy all the perks of multiple devices messaging.

Hello, World

We are excited to announce the official release of **Lab Send** !
A device manager platform designed to take your send outs to the next level.

Key Features

- Unlimited Devices
- SMS and MMS Sending
- Syntax Messaging (message randomizer)
- Auto Responder
- Custom Delays
- Message Templates
- Multiple Languages
- Responsive Support
- Constant Updates

Pair **Lab Send** with **Lab Host** to maximize your results !

New LabSend feature promoted on Telegram (Fortra)

Phishing-as-a-Service platforms make cybercrime more easily accessible for unskilled hackers, significantly expanding the pool of threat actors and impacting cybersecurity on a broader scale.

Other notable PhaaS platforms researchers have warned about recently are '[Greatness](#)' and '[Robin Banks](#),' both launched in mid-2022, featuring MFA bypassing, custom phishing kits, and admin panels.