Trustwave SpiderLabs

Financial Services
Deep Dive

Phishing-as-a-Service

Contents

Note: All the phishing examples in this document were sent to organizations from the financial services sector and the statistics apply to this sector only.

Phishing-as-a-Service (PaaS) has emerged as a significant cybersecurity threat to the financial sector. This "Cybercrime-as-a-service" model provides sophisticated packaged phishing tools and services to threat actors that can be availed via underground forums and is easily accessible through Telegram marketplaces. What this means is virtually anyone with only basic technical skills can access PaaS frameworks and launch sophisticated phishing attacks. Today, many phishing emails arriving in corporate networks are related to campaigns driven by PaaS platforms.

How PaaS works

As a potential phisher, all you need to do is find a PaaS platform and subscribe. There are different subscription levels offering varying features and support for different durations. The costs vary depending on the platform and the length of time you subscribe for. The infamous and now defunct Lab Host offered a basic monthly subscription of US $179/month. ONNX's MFA module costs US$400/month. Raccoon365 has options ranging from US $150 for 11 days to US$450 for 35 days and includes Microsoft 365 features.

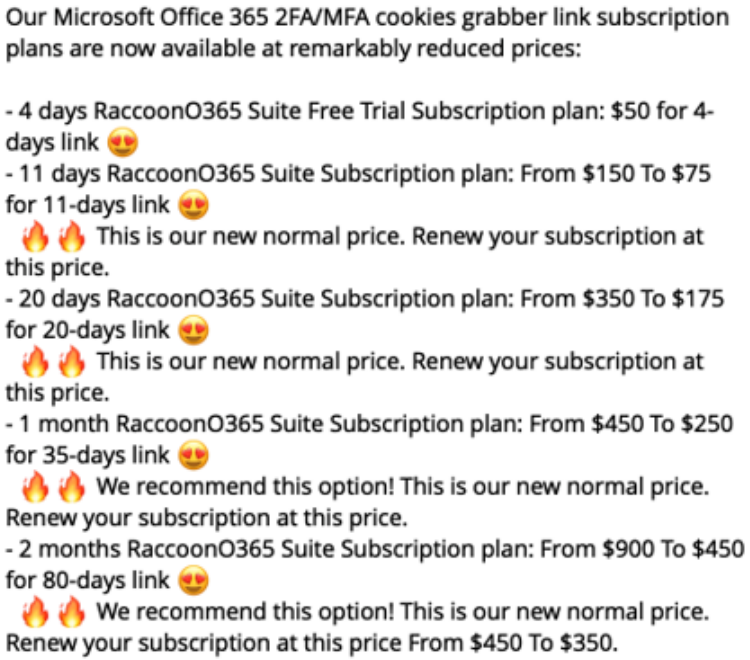


Figure 1: Racoon365 PaaS subscription options

PaaS Features

PaaS platforms typically include features such as:

- **Phishing Templates:** Pre-designed phishing landing page templates mimicking reputable organizations (e.g., banks, tech companies, Microsoft 365) to deceive recipients.
- **Website Cloning/Generator Tools:** Tools to create near-exact replicas of legitimate credential login pages.
- **Real-time Dashboards:** Provide insights into the performance of phishing campaigns, including open rates, click-through rates, captured credentials, and session cookies.
- **Multi-Factor Authentication (MFA) Bypass:** Tools to capture MFA sessions, allowing attackers to gain full access to accounts even with MFA enabled.
- **CAPTCHA Authentication:** PaaS platforms such as Tycoon2FA, DadSec, ONNX, and RaccoonO365 use Cloudflare's Turnstile – a free CAPTCHA service to authenticate that the link is legitimately clicked by a human.
- **Obfuscation Techniques:** Encode and obfuscate email and web page content to evade detection by spam filters and security software.
- **Mass Email:** Tools to send out mass phishing emails to targets.
- **Help and Support:** Tutorials and support to help customers use the platform.

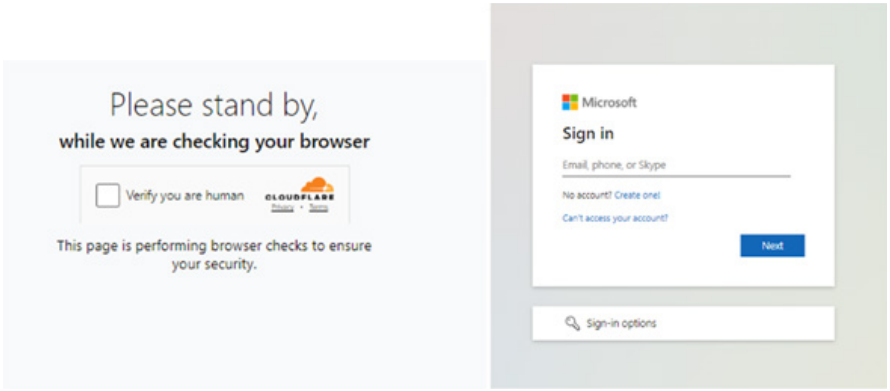


Figure 2: A Tycoon2FA phishing attack where a user is directed to a CAPTCHA landing page and then to a final landing page used by the attackers to harvest credentials. In the background, this phishing platform steals session tokens to be used later by the threat actors.

PaaS Platforms

There are different PaaS platforms available on the market. They are in constant flux, as their developers morph, change branding, and introduce new features to stay ahead of the game. The platforms change quickly when they get unwanted exposure from cybersecurity and law enforcement agencies.

Lab Host

- Launched in 2021
- Is tailored to different regions
- Targets customers of financial institutions
- Its operations and users around the world were interrupted by law enforcement in April 2024

W3LL

- Advanced phishing service designed specifically to hijack corporate Microsoft 365 accounts
- Exposed by Group-IB in 2023
- Had over 500 active users at the time of exposure

Caffeine

- Exposed by Mandiant in 2022
- Provides intuitive dashboard for phishers
- Facilitates credential theft targeting Microsoft 365 accounts

ONNX

- Exposed by EclecticIQ June 2024
- Performs specific targeting of financial sector customers
- Has anMFA bypass feature
- Is the probable evolution of the Caffeine platform

Greatness

- In use since 2022
- Has an MFA bypass feature
- A discussion of its key features and tactics can be found in a Trustwave blog entry

DadSec/Phoenix

- Active since July 2023
- Performs Microsoft 365 credential stealing
- Has an MFA bypass feature
- Rebranded to Phoenix in late 2023

Tycoon2FA

- Active since August 2023
- A possible clone of the DadSec platform
- Has an MFA bypass feature
- Features a Cloudflare security challenge
- A technical analysis of this platform can be found in the Trustwave blog

RacoonO365

- Active since May 2024
- Targets Microsoft 365 users
- Has an MFA bypass feature

V3B (Vssrtje Panel)

- Designed to capture sensitive information, such as credentials and one-time passcodes (OTPs).
- Targets banking customers in the EU

Interac

- Active since mid-2024
- Targets Canadian tech and finance sectors
- Has 35 different phishing page templates

Tycoon PaaS Phishing Example

Figure 3 illustrates a PDF attachment with an embedded QR image, which contains a link to a credential phishing page. Two steps are involved before the final phishing page is presented:

- Check with Tycoon C2 server whether the session is allowed, if not, redirect the session to a legitimate site.
- If the session is allowed, show a CAPTCHA challenge, then redirect to the phishing page.

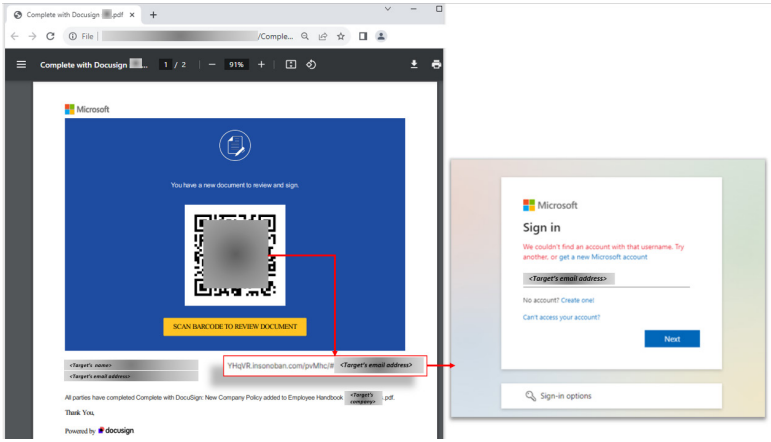


Figure 3: A Tycoon PDF attachment with a QR code that leads to a Microsoft 365 credential phishing page, when scanned and if the session is allowed.

Services Offered by Phishing-as-a-Service Platforms

PaaS platforms offer a range of services and tools designed to simplify and enhance the way threat actors execute phishing campaigns. PaaS platforms feature tools that allow threat actors to easily craft convincing fake emails and websites that mimic legitimate financial services, tricking customers into revealing sensitive information such as account credentials and personal identification details.

PaaS platforms typically include features such as:

- **Phishing Templates:** Pre-designed phishing landing page templates that mimic reputable organizations (e.g., banks, tech companies, Microsoft 365) to deceive recipients.

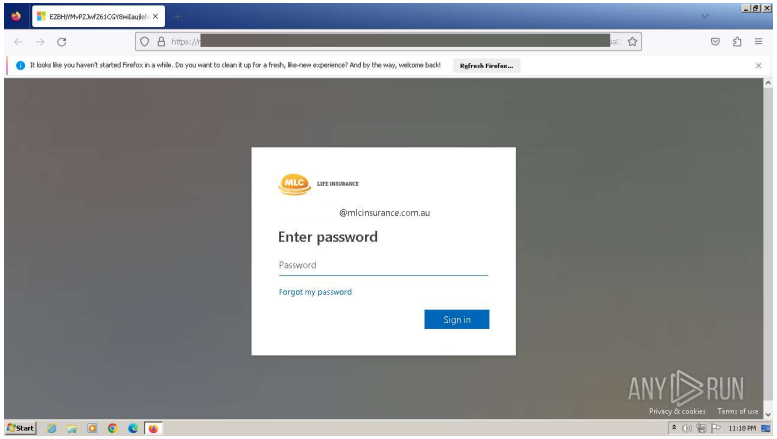


Figure 4. An example of a DadSec PaaS phishing campaign using a Microsoft 365-page template with the user's email address pre-populated and including the recipient's company logo.

- **Website Cloning/Generator Tools:** Tools to create near-exact replicas of legitimate websites to trick users into entering their credentials.

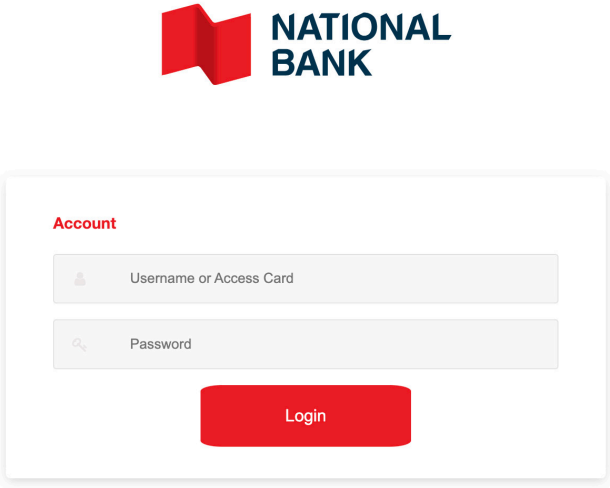


Figure 5. Sample of a phishing landing page generated by the Interac PaaS platform.

- **Dashboards:** Real-time dashboards provide insights into the performance of phishing campaigns, including open rates, click-through rates, captured credentials, and session cookies.
- **Reports:** Provide detailed reports on campaign success, including the number of valid and invalid accounts, two-factor authentication (2FA) login sessions, and the number of bots blocked.

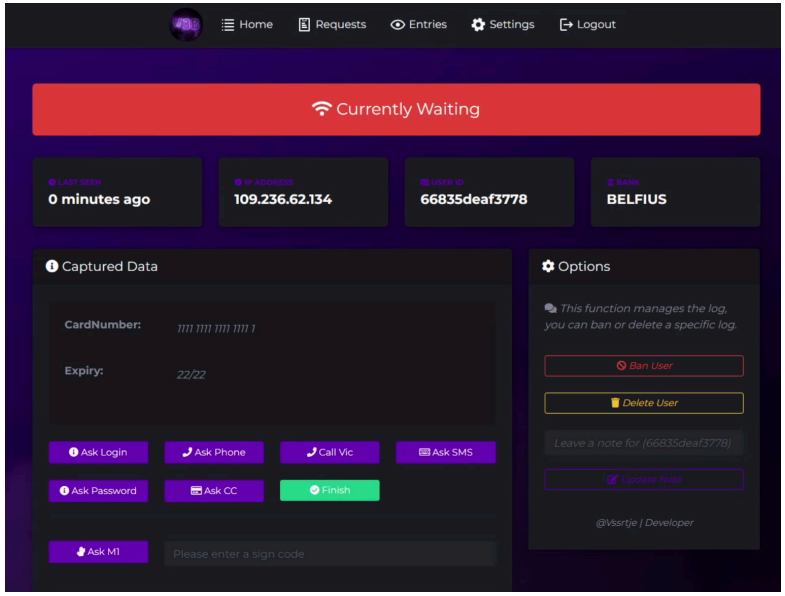


Figure 6. A phishing panel offered by the V3B PaaS platform showing real-time feedback and a panel to interact with the potential victim.

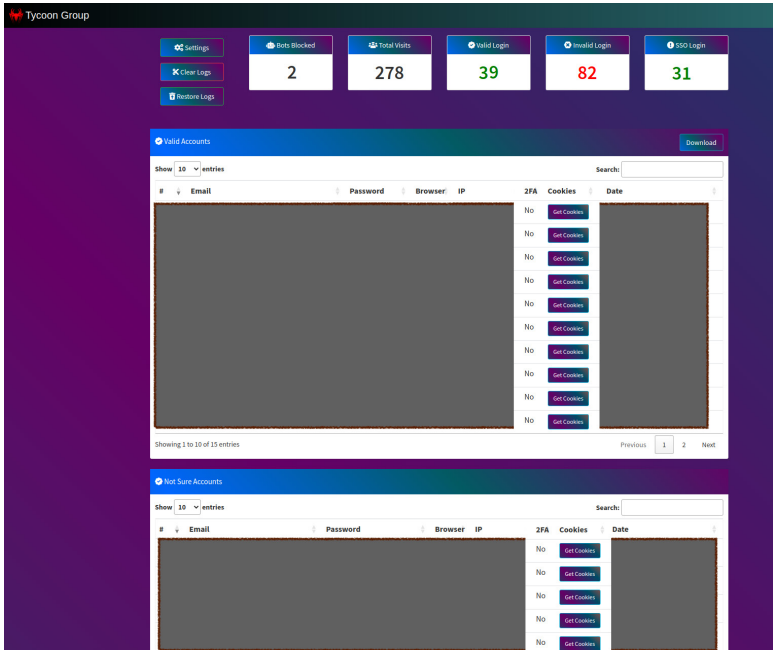
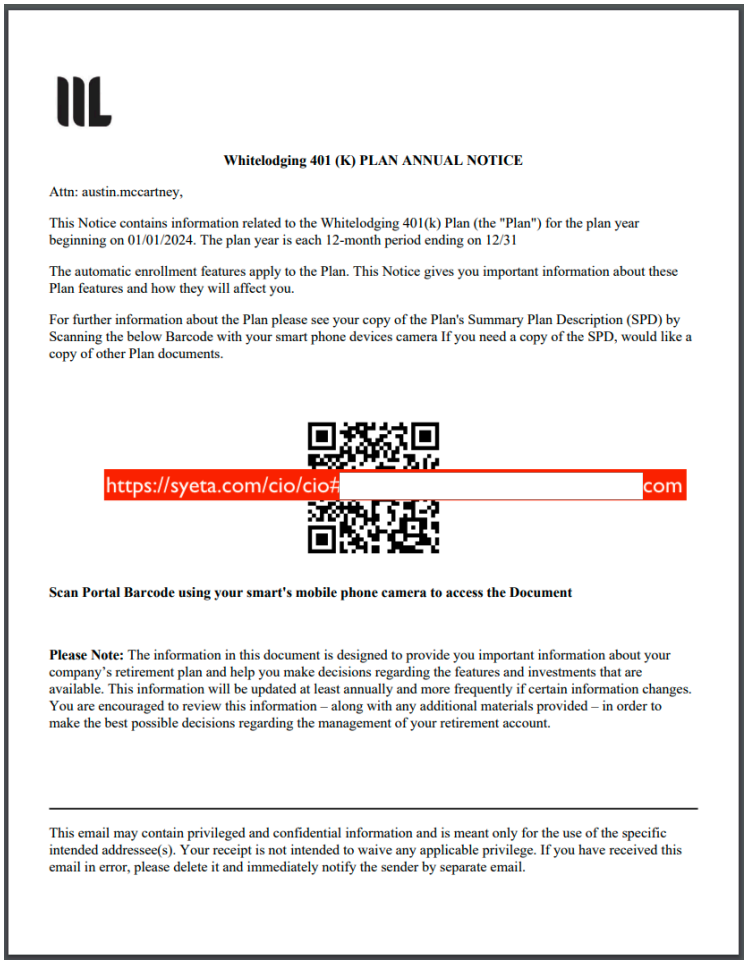


Figure 7. The dashboard of the Tycoon PaaS platform shows reports of valid captures, including session cookies that can be later imported by threat actors onto their browsers and use those sessions to access user accounts.

- **MFA Bypass and CAPTCHA Human Authentication:** Tools and techniques to capture MFA sessions, allowing attackers to gain full access to accounts even with MFA enabled. PaaS platforms such as Tycoon2FA, DadSec, ONNX, and RaccoonO365 also integrate the Cloudflare's turnstile service to authenticate that the link is legitimately clicked by a human.
- **Advanced Attack Vectors:** Provide support for various attack vectors, including malicious attachments, QR codes, and embedded links.



Whitelodging 401 (K) PLAN ANNUAL NOTICE

Attn: austin.mccartney,

This Notice contains information related to the Whitelodging 401(k) Plan (the "Plan") for the plan year beginning on 01/01/2024. The plan year is each 12-month period ending on 12/31

The automatic enrollment features apply to the Plan. This Notice gives you important information about these Plan features and how they will affect you.

For further information about the Plan please see your copy of the Plan's Summary Plan Description (SPD) by Scanning the below Barcode with your smart phone devices camera If you need a copy of the SPD, would like a copy of other Plan documents.

https://syeta.com/cio/cio#[redacted]com

Scan Portal Barcode using your smart's mobile phone camera to access the Document

Please Note: The information in this document is designed to provide you important information about your company's retirement plan and help you make decisions regarding the features and investments that are available. This information will be updated at least annually and more frequently if certain information changes. You are encouraged to review this information – along with any additional materials provided – in order to make the best possible decisions regarding the management of your retirement account.

This email may contain privileged and confidential information and is meant only for the use of the specific intended addressee(s). Your receipt is not intended to waive any applicable privilege. If you have received this email in error, please delete it and immediately notify the sender by separate email.

Figure 8. An example of a Greatness PaaS spam campaign attachment that includes a QR code generated from the Greatness panel.

- **Obfuscation Techniques:** Encode and obfuscate emails and web content to evade detection by spam filters and security software.
- **Step-by-Step Tutorials:** Detailed guides and video tutorials to help users navigate the platform, set up campaigns, and optimize their phishing tactics.

Figure 9. The FishProxy PaaS platform has documentation, tutorials, and support included in its service.

- **Dedicated Support:** Customer support teams are available to answer questions, resolve issues, and provide personalized assistance.

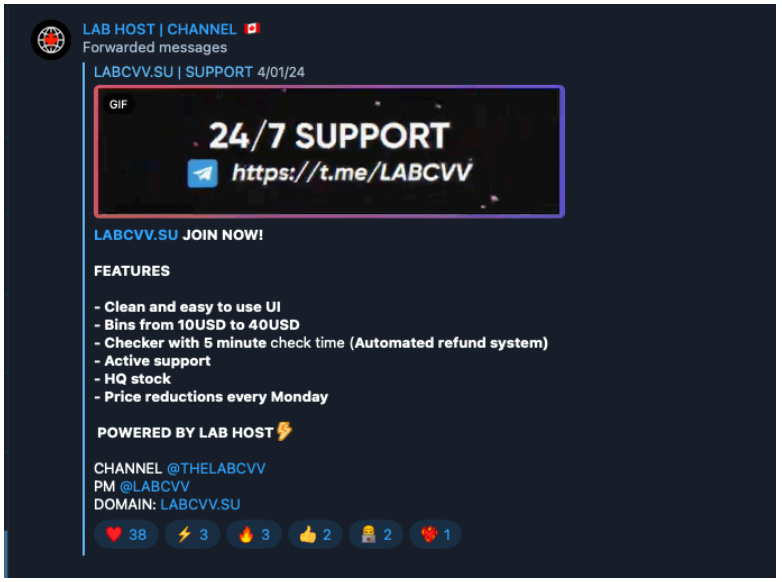


Figure 10. The LabHost PaaS platform offers 24/7 support to its affiliates.

Subscription Model

- **Pricing Tiers:** Different subscription levels offering varying features and support, and varying durations for the subscription to remain active.
- **Payment Methods:** Often require payment in cryptocurrencies such as Bitcoin to maintain anonymity and security.

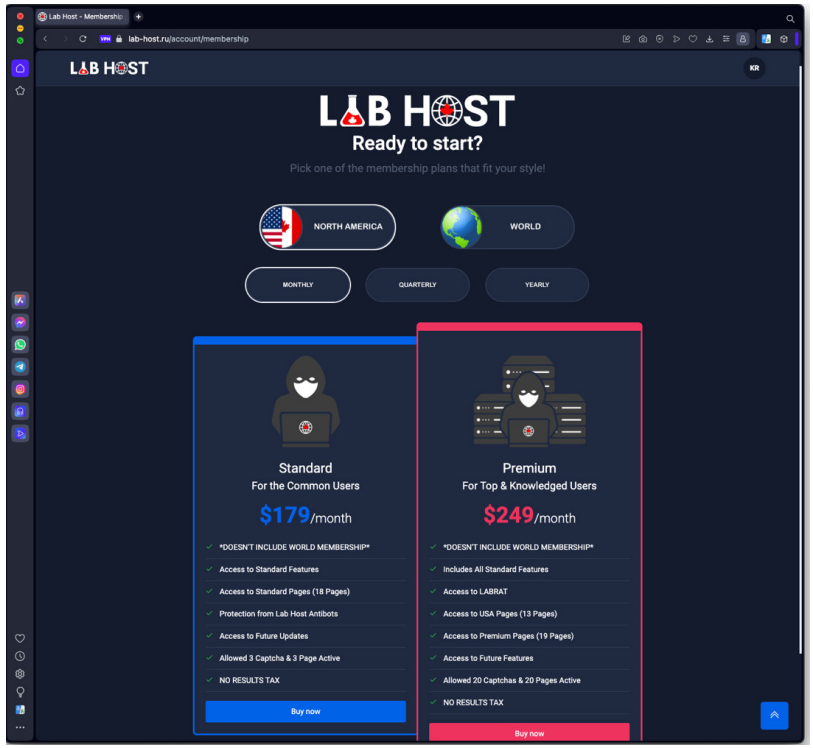


Figure 11. Labhost PaaS pricing tiers.

- **Bulletproof Hosting Service:** This ensures phishing operations aren't interrupted by takedowns, as well as provides remote desktop protocol (RDP) services for managing campaigns securely.

Figure 12. Onnx PaaS platform advertising a bulletproof RDP hosting feature.

Common Phishing Themes

There are many different types of phishing messages, with the most prevalent themes currently being:

- Account and password-related alerts
- HR communications
- Email alerts from document sharing and e-signature platforms
- Missed communications

Attackers have shifted to the widespread use of HTML and PDF attachments to transport, hide, and obfuscate their phishing URLs. These attachment types are ubiquitous and are not usually filtered by email scanning gateways.

- HTML attachments can be self-contained phishing pages, redirectors to phishing pages, or perform HTML smuggling to drop malware.
- PDF attachments can contain links that redirect to phishing pages or malware downloads or contain QR codes.

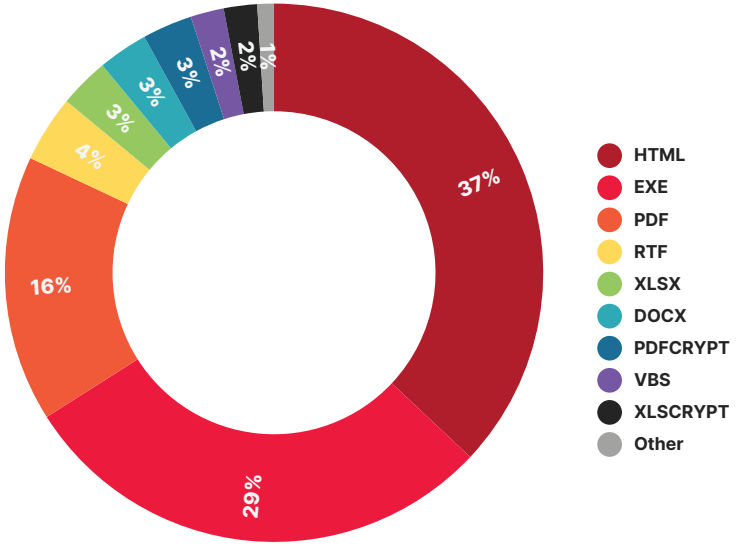


Figure 13: Based on Trustwave telemetry of malicious email attachments, HTML and PDFs are prominent.

The use of **QR codes** in phishing warrants a special mention. QR codes hide the URL from security scanners. They also tend to be scanned using employee's personal phones, which may not be scanned with corporate security tools.

Mitigations

1. **Advanced Training and Awareness Programs:** Continuously updating training programs to educate employees about the latest phishing tactics and preventive practices is crucial.
2. **Email Filtering and Analysis:** Deploying advanced email filtering solutions that use machine learning technologies to detect anomalies in email properties, including header analysis and sender reputation.
3. **Regular Audits and Simulations:** Conducting regular security audits and phishing simulations can help assess the readiness of an organization against phishing attacks and refine response strategies.
4. **Collaboration and Intelligence Sharing:** Participating in industry-wide collaborations can help institutions stay ahead of emerging phishing trends and share critical security intelligence.
5. **Hardware-based Authentication:** An effective mitigation to MFA bypass attacks is implementing Fast IDentity Online 2 (FIDO2) authentication, which uses cryptographic keys stored on hardware devices. This method ensures secure authentication, as private keys never leave the user's device, making it nearly impossible for attackers to intercept or manipulate the process.
6. **Layered Email Security:** Tools like Trustwave MailMarshal provide layered protection against email-based threats, capturing all forms of threats to protect an environment and reduce the burden on security teams.

For all of Trustwave SpiderLabs' research on the Financial Services sector, please see the full series here.


Trustwave
SpiderLabs