Report

Phishing Off a Peer

How Threat Actors Use Third Parties to Execute Advanced Phishing Campaigns

BlueVoyant

Overview

Phishing is already a headache for businesses, but threat actors are constantly finding new ways to carry out increasingly sophisticated attacks that circumvent the various cyber defense protocols security teams have in place. In the first half of 2023, BlueVoyant's expert cyber threat analysts began investigating one such tactic that they first identified in 2020 but has now dramatically increased in volume: third-party phishing. The scale, complexity, and successful deployment of advanced evasion mechanisms make this phishing technique far more efficient and effective than traditional standalone phishing sites.

Third-party phishing is a phenomenon targeting hundreds of global financial institutions using intermediary sites that redirect victims to a phishing site impersonating a brand they trust. By impersonating an ostensibly unrelated brand, threat actors can better evade detection, while collecting credentials and PII from customers of a wider array of companies.

More than 100 Financial Institutions targeted

Tens of new impersonating websites per day

10-20 targeted brands in each website

Over twenty countries across various sectors

Our expert cyber threat analysts have seen a significant rise in the popularity and reach of this tactic among threat actors. It now permeates across a number of sectors: e-commerce, logistics and shipping, mobile carriers, government institutions, payment transaction platforms, and more.

This report offers an inside look at the sophisticated schemes attackers have cooked up to carry out third-party phishing campaigns, as well as best practices for defending against this type of attack that your users may not recognize, even if they are security-savvy.

Traditional Phishing vs. Third-Party Phishing

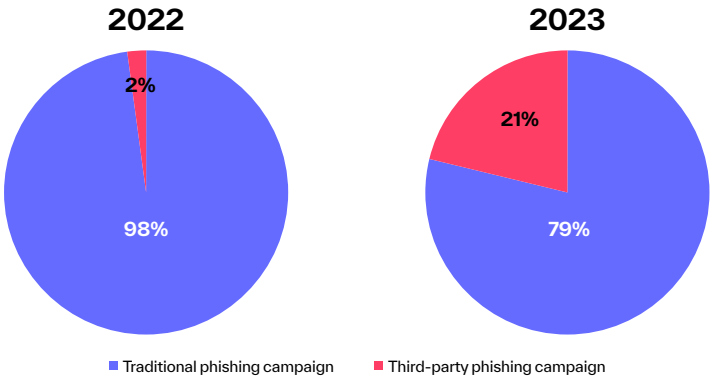
Phishing is one of the oldest – and certainly one of the most common – types of cyberattack. Traditionally, phishing websites exclusively target users of one organization, whether they be employees or customers. These websites tend to follow a similar cadence: attackers deploy a phishing kit to create a near-identical (or convincing enough) spoofed website of a corporate brand, using a lookalike domain to further a sense of legitimacy.

While phishing scammers use different distribution methods to lure in unsuspecting victims – phishing emails with links to their sites, links posted on social media platforms, etc. – the end goal of tricking a user into entering their login credentials, payment card information, or other personally identifiable information (PII) is always the same. Later, the threat actor collects these credentials and sells them or uses them to defraud the victim.

Third-party phishing sites, on the other hand, will include some characteristics of the original flow, with an added step – the initial impersonation that establishes credibility to the end user is a service that is not connected to the targeted organization. Furthermore, the third-party phishing page itself won't ask the victim to submit their personal credentials. The fraud occurs in the final phishing page to which the client has been redirected, impersonating the chosen financial institution.

Targeting Vendors
↓
SMS/Email Distribution
↓
Intermediary Impersonating Page
↓
Selecting a Financial Institution
↓
Phishing Page

Third-party phishing websites are spread on a massive scale across the internet. Over the past year, BlueVoyant has witnessed a major increase in the number of phishing sites originating in third-party phishing campaigns. One major European client saw an increase from just 2% of all detected phishing attacks in 2022 to 21% in 2023, as is depicted in the chart below.



A Phishing Trip Around the World

The third-party phishing trend is not necessarily confined to a specific geographic area. As seen below in the world map, we have detected evidence of third-party phishing campaigns in many regions across the globe.

Third-party phishing campaigns

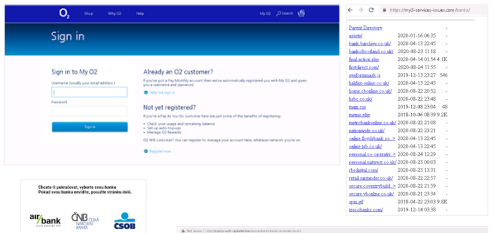
Attackers are also targeting multiple business sectors: financial institutions, governments, delivery services, e-commerce sites, payment platforms, and more.

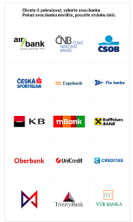
Below are three examples of third-party phishing campaigns targeted at different sectors around the globe:

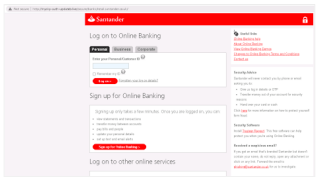
In **Europe and the UK**, BlueVoyant has detected third-party phishing sites targeting dozens of financial institutions via intermediary websites impersonating postal services, e-commerce platforms, tax payment platforms, mobile carriers, and government services.

Sectors that are being impersonated as intermediary phishing sites

Targeted geographies

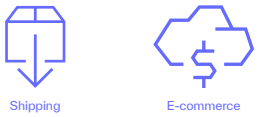






In **North America**, BlueVoyant has identified third-party phishing sites targeting financial institutions, shipping and logistics companies, and e-commerce retailers. One specific campaign targeted Interac, a Canadian interbank network offering online payments. The campaign often used Amazon to initiate the phishing chain, leading victims to a spoofed Interac intermediary site, and finally to the destination phishing page impersonating the victim's selected financial institution.

Sectors that are being impersonated as intermediary phishing sites

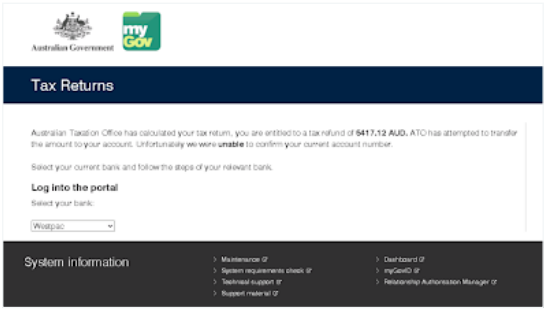


Targeted geographies

In the **Asia-Pacific region**, BlueVoyant has detected third-party phishing campaigns targeting various shipping and logistics companies as well as government services. The example below displays a third-party phishing site masquerading as a government tax payment site, which then redirects users to a phishing page impersonating the financial institutions of their choice – designed to collect the victim's PII and credentials.

Sectors that are being impersonated as intermediary phishing sites

Targeted geographies

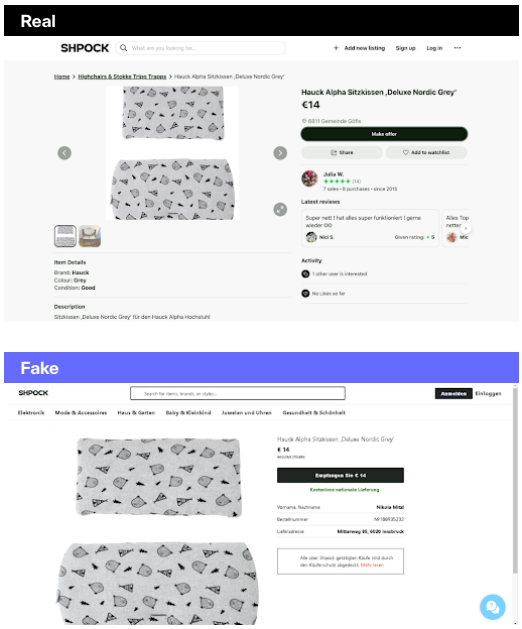


Case Study E-commerce Website

This section illustrates the process that a third-party phishing victim goes through, demonstrated via a campaign targeting an Austrian e-commerce retailer.

Step1: Targeting Vendors on E-commerce Platforms and Marketplaces

Third-party phishing campaigns targeting e-commerce platforms often rely on legitimate listings made on the platforms. Threat actors will create spoofed versions of the platform to deceive sellers into believing that their products have sold and that they are entitled to receive funds for them. In the first screenshot below you can see a legitimate listing of an item posted for sale on the Shpock platform. The second screenshot presents a site impersonating Shpock, claiming that the product shown in the first screenshot has been sold, and the seller is entitled to collect their payment.



Step 2: Distribution Using SMS or Email

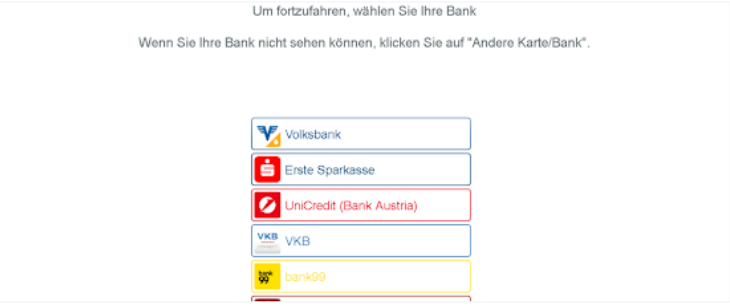
In most cases, the victim will receive a smishing message stating that their listed product was sold and urging them to claim their payment. The message also includes a short link, which upon clicking, redirects the victim to the intermediary phishing page.

Step 3: Intermediary Impersonation Site

The victim will be met with a page mirroring Shpock's official website, with all the details of the original legitimate posting. When clicking to proceed and claim the funds, the victim is redirected to the next step in the phishing chain, where they will be asked to choose the financial institution they bank with.

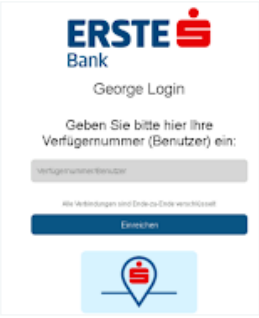
Step 4: Financial Institution Selection

The financial institution selection page is often a separate web page with a separate URL. The screenshot below displays the selection page that the Shpock third-party phishing site leads to, listing several major banks in Austria. Each logo is clickable and leads to a live phishing site targeting that specific bank. This is one of the major advantages of third-party phishing: a standard phishing site impersonating a single FI may be sent to a user completely unassociated with said FI, whereas with third-party phishing, the victim unwittingly chooses and redirects themselves to the relevant phishing website.



Step 5: Arriving at the Destination Phishing Site

After selecting their bank, the victim will be redirected one last time to the main phishing page impersonating a financial institution. For example, below is a phishing site impersonating Erste Bank in Austria, one of the banks listed in the selection screen.



The site will then prompt the victim to submit their private bank account credentials which will be collected and used in various fraudulent activities. Finally, after several hops between malicious websites, the attacker has successfully phished the victim.

Conclusions and Mitigation Recommendations

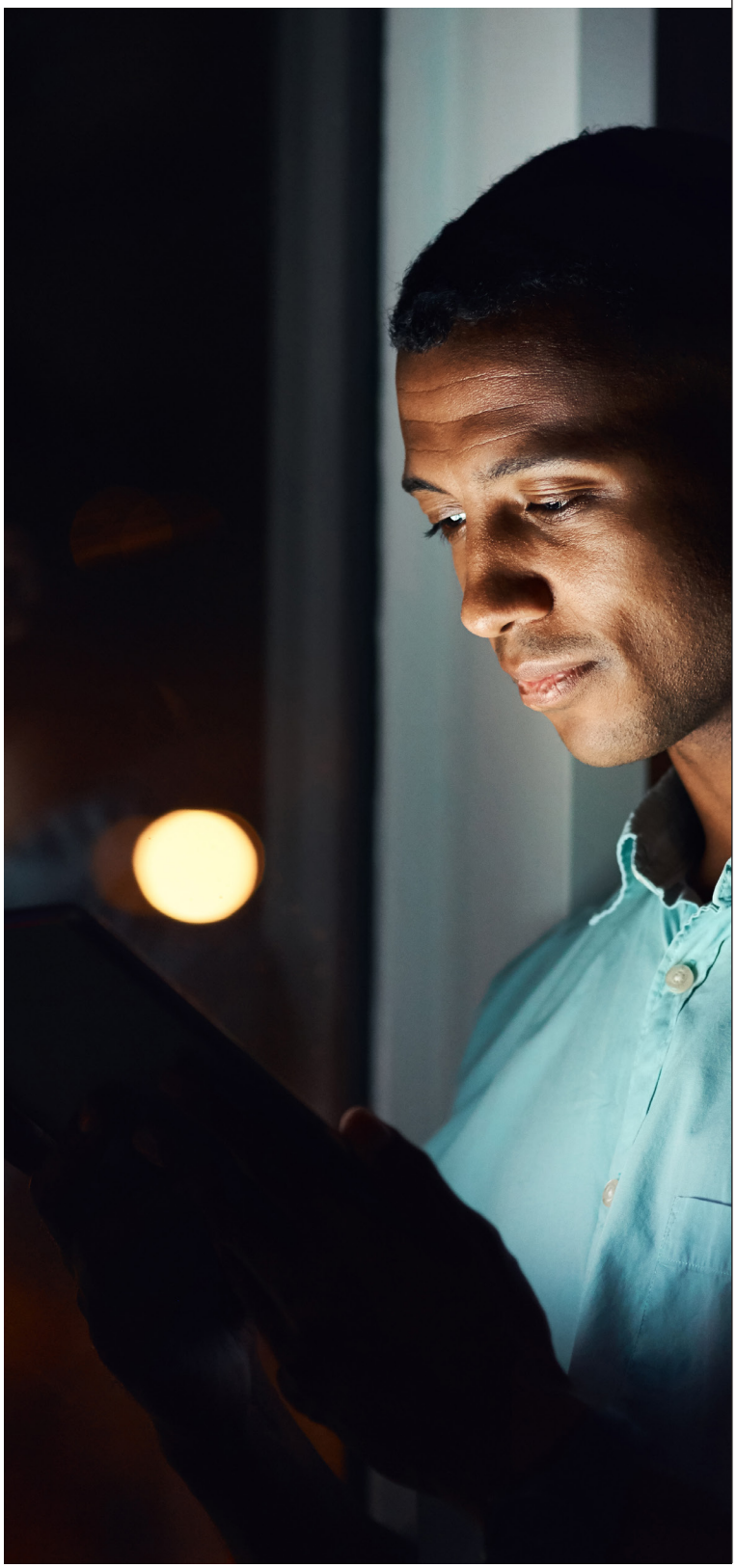
Third-party phishing adds a new wrinkle to the oldest trick in the book. Intermediary sites directing victims to various different phishing sites provides two benefits to attackers: it allows them to cast a wider net and catch more fish (so to speak), and it provides another degree between them and threat hunters who may be on their trail. We've previously published research highlighting how attackers use redirects as an evasion mechanism – third-party phishing builds on that concept, while also giving the threat actor a greater chance of ensnaring their targets.

Organizations now need to not only monitor for cyber threat activity targeting their own domains; but for third-party phishing attempts making use of an intermediary to direct traffic to a different phishing page – sometimes hosted on the same domain as the intermediary site – that may be harder to detect on its own. The increased risk associated with one website acting as a gateway to dozens of financial institutions is substantial, and security teams will need to increase their efforts to find third-party phishing sites that could be targeting them and many of their peers.

Bluevoyant regularly tracks large scale thrid-party phishing campaigns from different geographies around the world, alerts both the intermediary brands and the destination brands on these and remediates active threats on their behalf.

BlueVoyant will continue monitoring this trend as it evolves, delivering actionable threat alerts to our clients when relevant. To mitigate the risk of third-party phishing, we recommend organizations take the following steps:

1. Monitor for lookalike domains and illicit use of corporate brand assets across the web to identify potential phishing sites.
2. Educate clients and employees on third-party phishing, and encourage them to closely inspect any URL they click on for pages that require credentials or PII to be entered.
3. Remediate malicious domains using third-party phishing quickly to mitigate risk and potentially thwart large-scale attacks.
4. Work with an end-to-end Digital Risk Protection vendor, such as BlueVoyant, to proactively detect third-party phishing campaigns, receive validated alerts, and take down the threats rapidly.



BlueVoyant cyber defense.

BlueVoyant

BlueVoyant combines internal and external cyber defense capabilities into an outcomes-based cloud-native solution by continuously monitoring your network, endpoints, attack surface, and supply chain, as well as the clear, deep, and dark web for threats. The full-spectrum cyber defense solution illuminates, validates, and quickly remediates threats to protect your enterprise. BlueVoyant leverages both machine-learning-driven automation and human-led expertise to deliver industry-leading cybersecurity to more than 900 clients across the globe.

To learn more about BlueVoyant, please visit our website at www.bluevoyant.com or email us at contact@bluevoyant.com