ZEROFOX® | Threat Research

REPORT

Anatomy and Trends of the Evolved Phishing Ecosystem

October 2021

zerofox.com

Table of Contents

Executive Summary

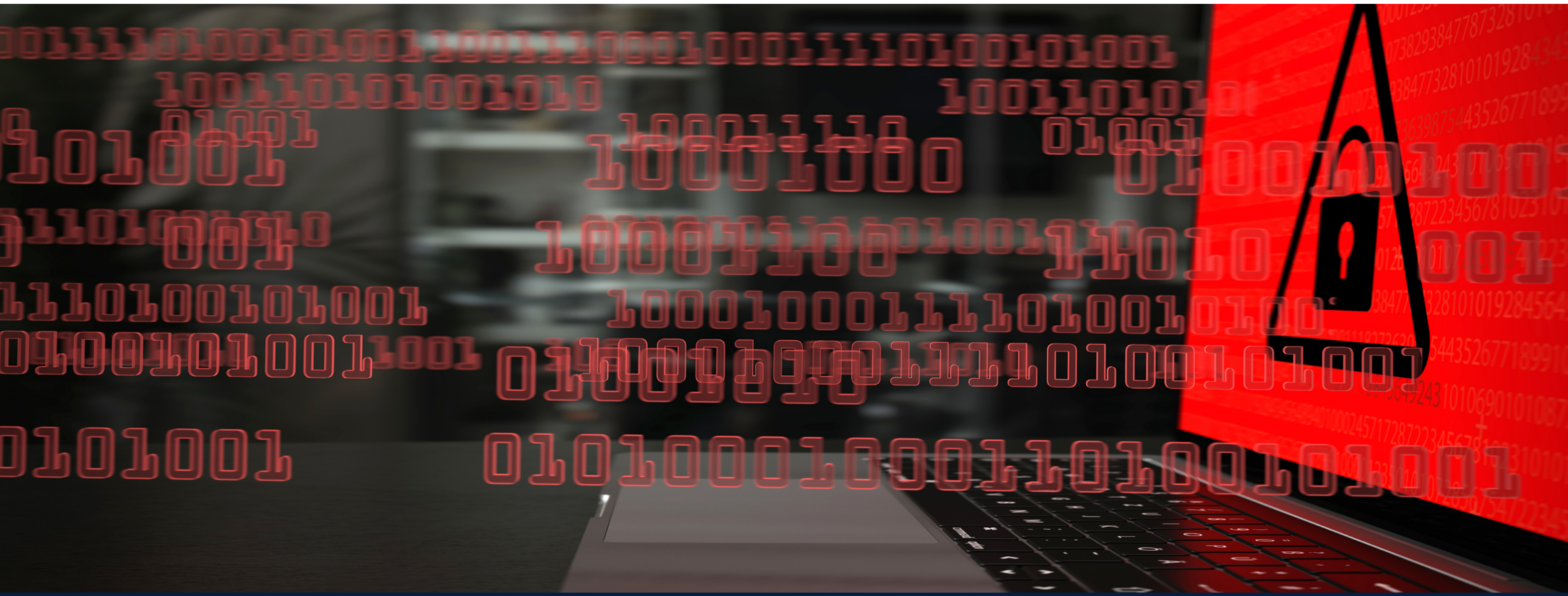
Phishing attacks aimed at consumers are commonly split into two buckets: conventional phishing and targeted spear phishing. Spear phishing is generally considered to be the more sophisticated type of attack, having specific targets; most conventional phishing is seen as a lower-level activity, targeting indiscriminately and having a low success rate.

However, behind many typical phishing campaigns is a supply chain designed to facilitate these attacks and return a profit for those perpetrating them. Across dark web marketplaces and covert channels that allow for anonymous or encrypted communication, buyers and sellers trade source code, victim data, access to services and tools disguised as legitimate services, and specialist equipment to scale phishing attacks beyond an individual threat actor's capability.

As phishing attacks persist, phishing ecosystems provide context on successful operations and ways threat actors leverage stolen data from attacks. New and emerging phishing tactics, techniques and procedures ensure phishing remains a consistent threat to enterprises. In this report detailing the anatomy and trends of the evolved phishing ecosystem, ZeroFox Threat Research provides both an overview of current threats as well as key recommendations and tools for disrupting them.

Key Takeaways

- Marketplace networks for phishing and fraud-related activities enable threat actors to obtain lucrative profits by creating, operating and selling stolen data.
- Phishing supply chains present a comprehensive ecosystem for threat actors to create and operate tools and data for profit from credential phishing attacks.
- Threat actors are using more sophisticated methods, including phishing and cyber puppeteer kits, to conduct broader-scale attacks quickly.
- The phishing ecosystem has evolved lure distribution mechanisms as well as tactics to evade detection via third-party services and APIs.
- Targeted phishing is on the rise in new innovative ways, while threat actors also look beyond the typical attack to sell victim data and build stolen data package profiles.



Identifying the Groundwork Leading to a Phishing Attack

Phishing attacks are more than just a website for account takeover, there is a wide range of attack types and the term is often overused. Attacks like spear phishing, vishing, malware and Business Email Compromise (BEC) scams are sometimes described as phishing, and each one has a different end goal.[1] Attacks leveraging spam campaigns to support fraudulent activity are carried out by stealing personally identifiable information (PII) and financial information via a web server deployed on the internet. In these cases, there are indicators that can be monitored prior to a phishing attack. Two popular methods include phishing kits and cyber puppeteer kits.

> *During Q2 2021, ZeroFox has observed several new phishing kit variants produced from popular phishing-kit-as-a-service providers targeting various brands.*

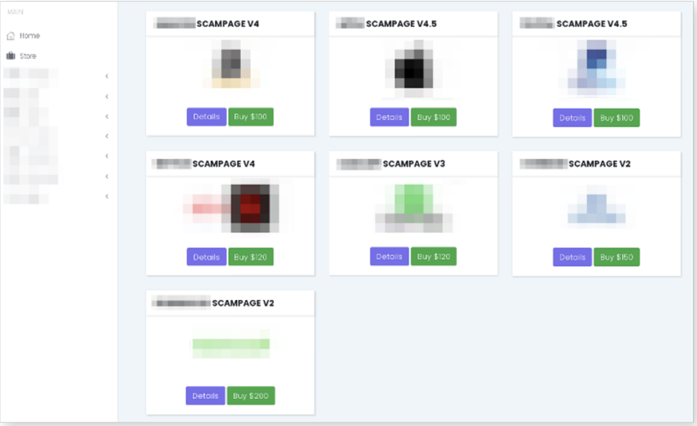
Source Code and Phishing Kits

Before beginning a phishing attack, the threat actor must obtain or create the code to render the phishing page to the victim. This commonly involves the threat actor obtaining an archive (.zip) containing pre-compiled code and resources, commonly referred to as a phishing "kit." This kit can be easily deployed to a web host to create a phishing page. These kits are bought and sold via various channels, with more sophisticated threat actors authoring kits based on demand.

Phishing kits can vary dramatically in cost based on complexity and capabilities. Simple kits containing only a few files of PHP code can cost anywhere between $10 USD and $100 USD to purchase, payable in cryptocurrency or similar means. More complex kits may cost hundreds of dollars. These commonly require backend databases, integrate third-party APIs, have built-in "anti-bot" or evasion techniques or even use a basic form of digital-rights management.

During Q2 2021, ZeroFox has observed several new phishing kit variants produced from popular phishing-kit-as-a-service providers targeting various brands.[2] Such kits are offered by private online stores, where threat actors purchase and register their active deployments. Figure 1 is a screenshot of a private store selling phishing kits that target multiple brands and platforms.

Figure 1: Private online store offering phishing kits targeting multiple brands and platforms



Source: ZeroFOX Internal Research

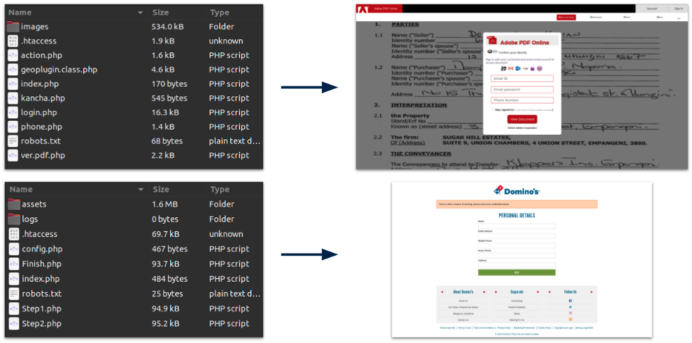
Identifying Phishing Kits and the Ecosystem They Thrive In

A phishing kit is essentially a preconstructed phishing attack nicely packaged for threat actors to leverage without sophisticated skills. It also enables them to deploy an attack quickly. Kits are generally supplied in zip files containing JavaScript, CSS and image assets along with HTML and PHP code. When copied to a web host, they create web pages that imitate the targeted brand's own login pages and processes and exfiltrate data gathered from victims.[3]

A phishing kit is sold and traded online across the dark web, deep web, social media sites and forums. These kits have varying levels of features, much like a SaaS product. They have gained traction and become popular because they offer a high return on investment for threat actors.

Figure 2 shows extracted phishing kits that look similar in construction. However, once deployed, they target separate brands with unique workflows. Regardless of how advanced or modular these phishing kits are, they are all designed to allow less sophisticated threat actors to simply copy the content to a web host and begin phishing very quickly.

Figure 2: Private online store offering phishing kits targeting multiple brands and platforms



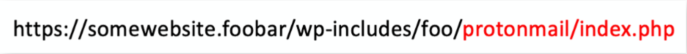
Name	Size	Type
images	534.0 kB	Folder
.htaccess	1.9 kB	unknown
action.php	1.6 kB	PHP script
geoplugin.class.php	4.6 kB	PHP script
index.php	170 bytes	PHP script
kancha.php	545 bytes	PHP script
login.php	16.3 kB	PHP script
phone.php	1.4 kB	PHP script
robots.txt	68 bytes	plain text d…
ver.pdf.php	2.2 kB	PHP script

Name	Size	Type
assets	1.6 MB	Folder
logs	0 bytes	Folder
.htaccess	69.7 kB	unknown
config.php	467 bytes	PHP script
Finish.php	93.7 kB	PHP script
index.php	484 bytes	PHP script
robots.txt	25 bytes	plain text d…
Step1.php	94.9 kB	PHP script
Step2.php	95.2 kB	PHP script

Source: ZeroFOX Internal Research

A URL similar to the one shown in Figure 3 indicates a likely phishing page with multiple directories leading to that phishing page. In some cases, it is possible to find an open directory such as the one shown in Figure 4. Here we see a ProtonMail directory link that directs to the phishing site with a zip file available as well; this is essentially the phishing kit.

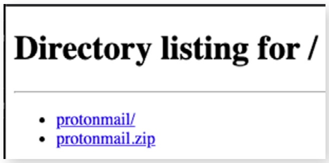
Figure 3: Sample URL indicating phishing activity



https://somewebsite.foobar/wp-includes/foo/protonmail/index.php

Source: ZeroFOX Internal Research

Figure 4: Sample directory illustrating phishing activity



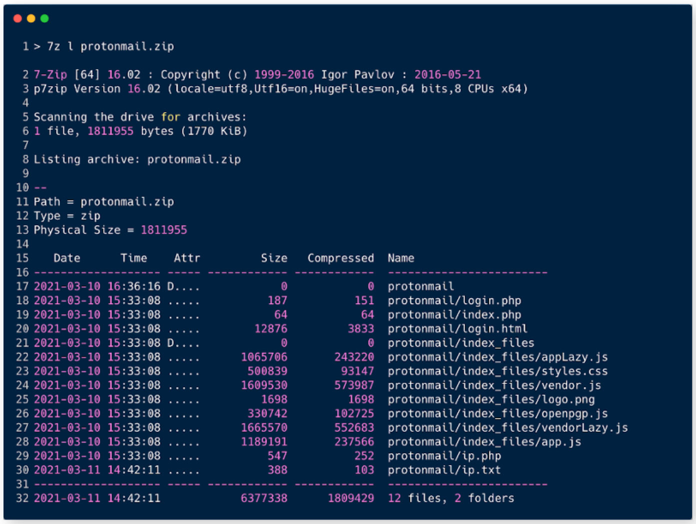
Directory listing for /

- protonmail/
- protonmail.zip

Source: ZeroFOX Internal Research

After downloading the zip file, extracting its contents will list the files within the archive. The kit may look something like the example shown in Figure 5. This is the next layer of a phishing kit: a collection of PHP files, HTML, assets like JavaScript, CSS, PNG and text files.

Figure 5: Sample phishing kit zip file



```
> 7z l protonmail.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=utf8,Utf16=on,HugeFiles=on,64 bits,8 CPUs x64)

Scanning the drive for archives:
1 file, 1811955 bytes (1770 KiB)

Listing archive: protonmail.zip

--
Path = protonmail.zip
Type = zip
Physical Size = 1811955

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2021-03-10 16:36:16 D....            0            0  protonmail
2021-03-10 15:33:08 .....          187          151  protonmail/login.php
2021-03-10 15:33:08 .....           64           64  protonmail/index.php
2021-03-10 15:33:08 .....        12876         3833  protonmail/login.html
2021-03-10 15:33:08 D....            0            0  protonmail/index_files
2021-03-10 15:33:08 .....      1065706       243220  protonmail/index_files/appLazy.js
2021-03-10 15:33:08 .....       500839        93147  protonmail/index_files/styles.css
2021-03-10 15:33:08 .....      1609530       573987  protonmail/index_files/vendor.js
2021-03-10 15:33:08 .....         1698         1698  protonmail/index_files/logo.png
2021-03-10 15:33:08 .....       330742       102725  protonmail/index_files/openpgp.js
2021-03-10 15:33:08 .....      1665570       552683  protonmail/index_files/vendorLazy.js
2021-03-10 15:33:08 .....      1189191       237566  protonmail/index_files/app.js
2021-03-10 15:33:08 .....          547          252  protonmail/ip.php
2021-03-11 14:42:11 .....          388          103  protonmail/ip.txt
------------------- ----- ------------ ------------  ------------------------
2021-03-11 14:42:11            6377338      1809429  12 files, 2 folders
```

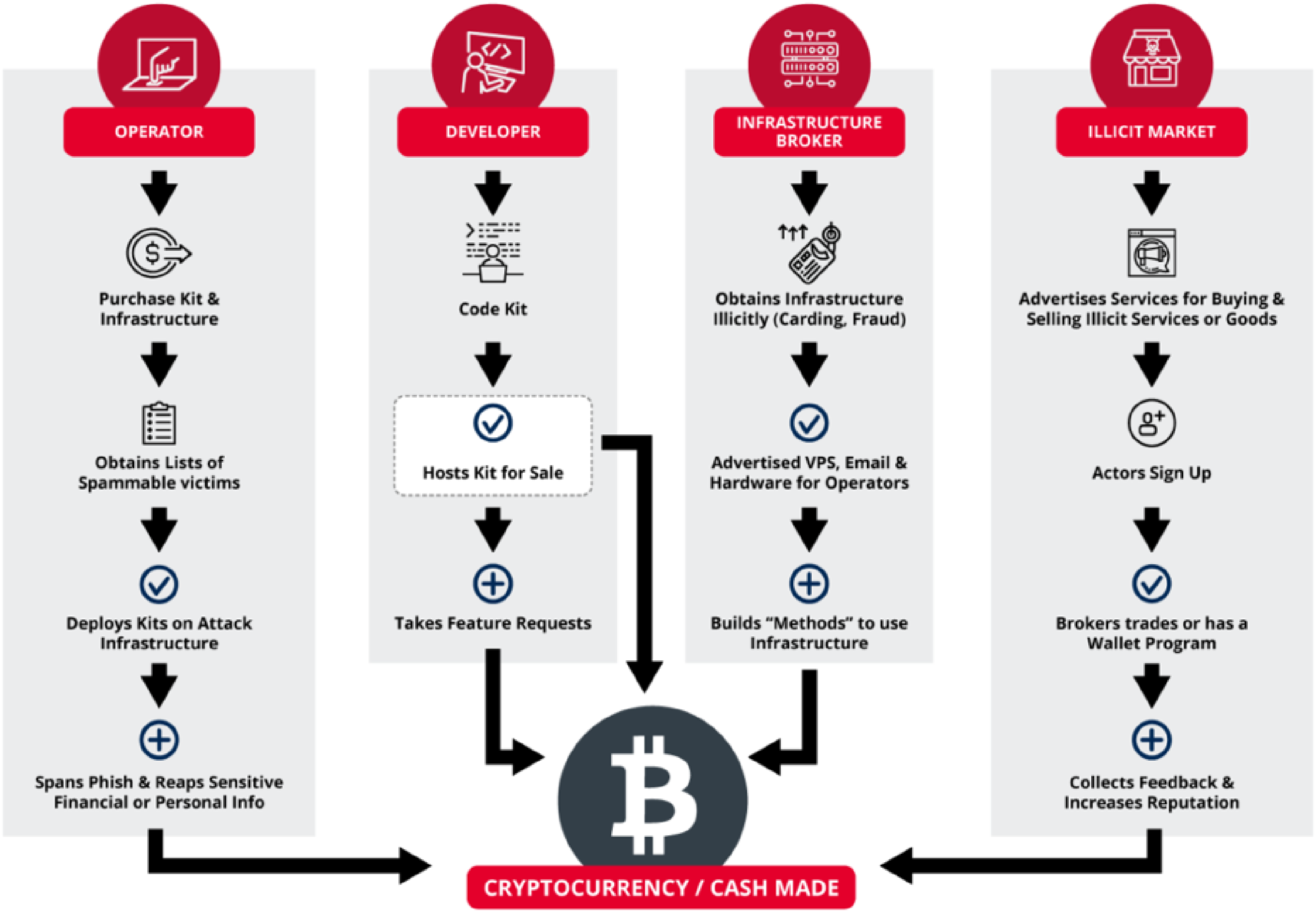
Source: ZeroFox Internal Research

These phishing kits allow actors to quickly stand up a phishing site without knowing the back-end controls or leveraging an advanced skill set. All that's left for them to do is upload to a server, deploy and then actors can begin reaping the benefits from the phishing attack.

ZeroFox threat researchers have noticed four general categories in the phishing network regardless of the threat actor or a group behind the activity. This includes the operator, developer, infrastructure broker and the illicit market. There can be any combination of persona within this ecosystem, but the basic premise is that they are all motivated by the same goal: financial gain.

The operator purchases the kit from the developer; they obtain different methods to spam using the kit and then obtain stolen data to sell. The developer builds the kit, hosts it, takes feature requests and keeps improving it, so more operators purchase it. Infrastructure brokers obtain servers, accounts and email inboxes to perform some type of spam. They will do this illicitly through tactics such as carding or fraud. Developers, operators and brokers use illicit markets as a hub to buy and sell inventory. These roles are the foundation of an "ecosystem of fraud" when it comes to phishing kits.

Figure 6: Phishing kit ecosystem and personas


OPERATOR
Purchase Kit & Infrastructure
Obtains Lists of Spammable victims
Deploys Kits on Attack Infrastructure
Spans Phish & Reaps Sensitive Financial or Personal Info
DEVELOPER
Code Kit
Hosts Kit for Sale
Takes Feature Requests
INFRASTRUCTURE BROKER
Obtains Infrastructure Illicitly (Carding, Fraud)
Advertised VPS, Email & Hardware for Operators
Builds "Methods" to use Infrastructure
ILLICIT MARKET
Advertises Services for Buying & Selling Illicit Services or Goods
Actors Sign Up
Brokers trades or has a Wallet Program
Collects Feedback & Increases Reputation
CRYPTOCURRENCY / CASH MADE

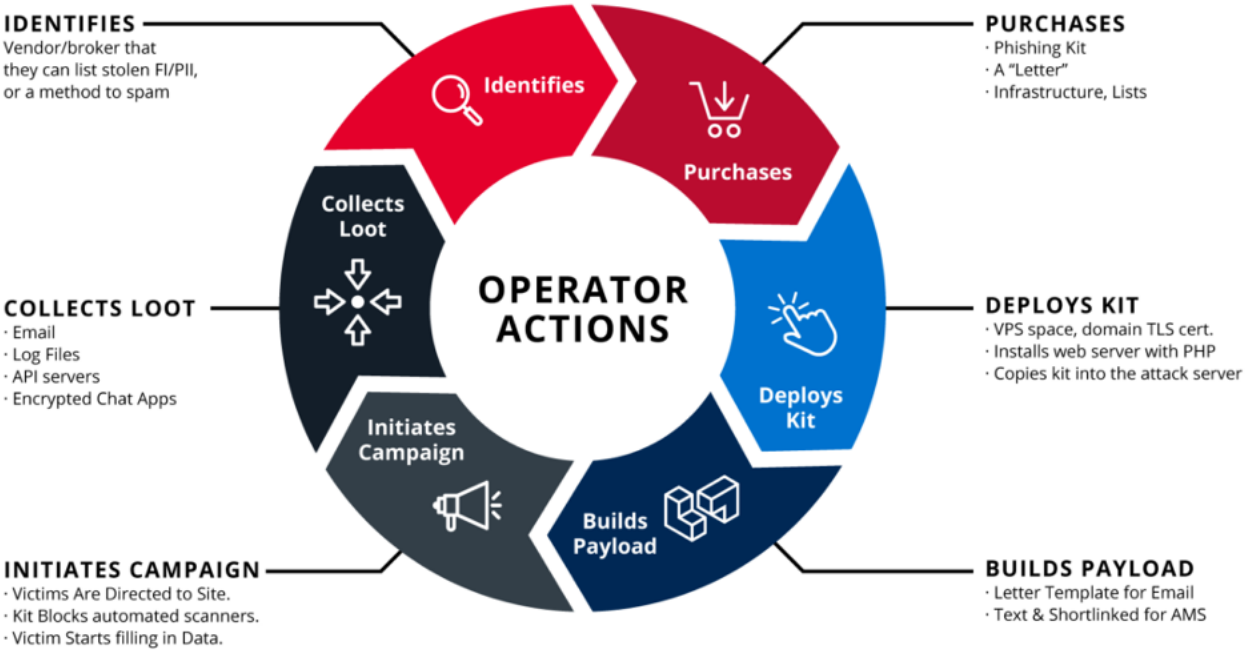
Source: ZeroFox Internal Research

Phishing Kit Campaign Phases

Operators perform spam campaigns in a flywheel-like fashion. The more they complete the flywheel shown in Figure 7, the faster and more efficient they become. First, the operator identifies a place they can go to buy or sell financial information or PII. Next, they will purchase a phishing kit along with data to help them spam, such as lists to emails or phone numbers. Sometimes they will purchase a "letter," which is a prepackaged piece of HTML designed to get past email spam filters. The operator then deploys the kit using a virtual private server (VPS), and from there, they install a web server and a LAMP stack with PHP. The purchased zip file is then copied onto the attack server. After it is copied and extracted, the operator has a payload built either through the letter template or a similar SMS spamming service to text out the phishing link.

The campaign is initiated and deployed in a form of outreach (emails, text messages or more) where victims are directed to the phishing website. The kit excels at blocking any type of automated security scanner; meanwhile, victims begin providing data threat actors are seeking. The operator collects the data in several ways and stores the information to retrieve and list for future use.

Figure 7: Phishing kit campaign phases



IDENTIFIES
Vendor/broker that they can list stolen FI/PII, or a method to spam

PURCHASES
· Phishing Kit
· A "Letter"
· Infrastructure, Lists

COLLECTS LOOT
· Email
· Log Files
· API servers
· Encrypted Chat Apps

DEPLOYS KIT
· VPS space, domain TLS cert.
· Installs web server with PHP
· Copies kit into the attack server

INITIATES CAMPAIGN
· Victims Are Directed to Site.
· Kit Blocks automated scanners.
· Victim Starts filling in Data.

BUILDS PAYLOAD
· Letter Template for Email
· Text & Shortlinked for AMS

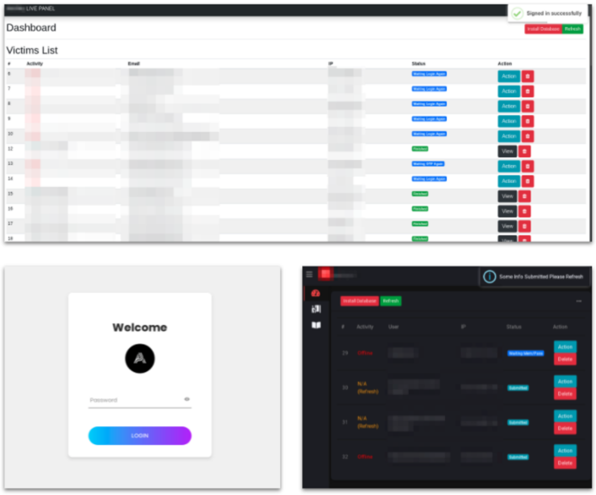
Source: ZeroFox Internal Research

Cyber Puppeteer Kits

Cyber puppeteer kits are more personalized, interactive and successful than the traditional phishing kit.[4] This makes them a substantial threat. A cyber puppeteer kit, also referenced as “live panels” among the threat actors that operate them, is a new breed of phishing kit designed almost exclusively to facilitate phishing attacks against the financial services industry. They are referred to as cyber “puppeteer” kits because the workflows are advanced, very dynamic and require live interaction between the victim and the threat actor. The threat actor is essentially “pulling strings” of the victim, guiding them through a series of pages to unwittingly authorize access to their account.

The operator controls puppeteer kits through an administrative dashboard that they log into. As shown in Figure 8, this dashboard will notify the operator of new visitors to their phishing site and allow them to manually dictate what the victim should be prompted for to enable the attacker to gain complete access. During the victim workflow, the attacker takes the provided information and directly logs into the legitimate online banking platform, echoing back any security questions to the victim for them to answer. As this is near real-time, the operators can prompt the victim for whatever information they need, as many times as they require. This allows criminals to get around additional authentication steps such as SMS-based two-factor authentication, one-time password token and device verification.

Figure 8: Sample cyber puppeteer kit and dashboard



LIVE PANEL

Signed in successfully

Dashboard

Install Database | Refresh

Victims List

#	Activity	Email	IP	Status	Action
6				Waiting Login Again	Action
7				Waiting Login Again	Action
8				Waiting Login Again	Action
9				Waiting Login Again	Action
10				Waiting Login Again	Action
12				Finished	View
13				Waiting OTP Again	Action
14				Waiting Login Again	Action
15				Finished	View
16				Finished	View
17				Finished	View
18				Finished	View

Welcome

Password

LOGIN

Some Info Submitted Please Refresh

Install Database | Refresh

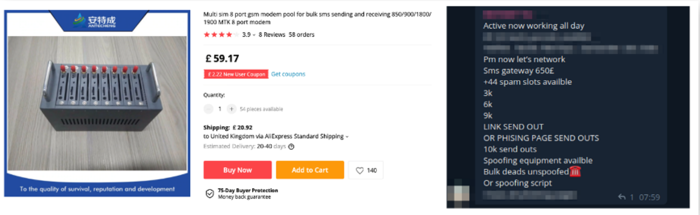
#	Activity	User	IP	Status	Action
29	Offline			Waiting Mem/Pass	Action Delete
30	N/A (Refresh)			Submitted	Action Delete
31	N/A (Refresh)			Submitted	Action Delete
32	Offline			Submitted	Action Delete

Source: ZeroFox Internal Research

Evolved Lure Distribution Mechanisms

A well-known and increasingly popular distribution method for phishing campaigns is via SMS, also referred to as smishing, where mass lures are sent to large amounts of mobile numbers. Within covert channels, threat actors or groups sell services dedicated to sending massive amounts of SMS messages. Specialist equipment and software are used to facilitate this activity, which is difficult to proactively prevent, as International Mobile Equipment Identity (IMEI) and mobile numbers can be spoofed and changed at random. Figure 9 advertises a GSM modem, a device that uses mobile phone technology to provide a data link to a remote network, and an advertisement discussing the cost of sending SMS messages for phishing activity.

Figure 9: GSM modem used for sending SMS spam (left); message advertising costs of sending SMS messages for phishing (right)



Multi sim 8 port gsm modem pool for bulk sms sending and receiving 850/900/1800/1900 MTK 8 port modem

★★★★ 3.9 · 8 Reviews 58 orders

£ 59.17

£ 2.22 New User Coupon Get coupons

Quantity:

− 1 + 54 pieces available

Shipping: £ 20.92

to United Kingdom via AliExpress Standard Shipping

Estimated Delivery: 20-40 days

Buy Now | Add to Cart | ♡ 140

75-Day Buyer Protection
Money back guarantee

Active now working all day

Pm now let’s network
Sms gateway 650£
+44 spam slots availble
3k
6k
9k
LINK SEND OUT
OR PHISING PAGE SEND OUTS
10k send outs
Spoofing equipment availble
Bulk deads unspoofed☎
Or spoofing script

1 07:59

Source: ZeroFox Internal Research

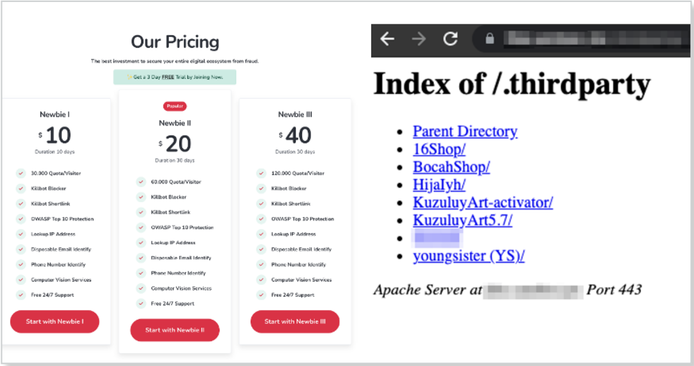
Other actors will supply lists of “leads” to buyers. These are files containing an agreed number of mobile phone numbers confirmed to be genuine and in use via Home Location Register (HLR) checks, a database containing up-to-date information for every mobile phone subscriber worldwide. An HLR lookup can verify if a mobile phone number is active, switched on and to which network that number has been assigned.

Evading Detection via Third-Party Services and APIs

The adoption of third-party services to aid in evading detection has continued to increase as more phishing kits are being analyzed to show the utilization of external API providers. Within the space, there are multiple providers of "anti-bot" services, which may appear legitimate but are designed to be explicitly used by phishing kits to improve evasive capabilities. Figure 10 displays an example of a popular anti-bot service, along with an open directory containing integrations with popular phishing kits.

These services are advertised as a tool to block unwanted visitors or "bots" from accessing the customer's website. They block or allow access based on the visitor's IP, ISP, geographical location or browser's user agent. This is also used to prevent access to other services that crawl the web to analyze content for malicious activity.

Figure 10: Pricing of a popular anti-bot service commonly integrated with phishing kits (left); an exposed directory of one of these services hosts code that allows direct integration with popular phishing kits (right)



Our Pricing

The best investment to secure your entire digital ecosystem from fraud.

✨Get a 3 Day FREE Trial by Joining Now.

Newbie I
$ 10
Duration 10 days
- ✓ 30.000 Quota/Visitor
- ✓ Killbot Blocker
- ✓ Killbot Shortlink
- ✓ OWASP Top 10 Protection
- ✓ Lookup IP Address
- ✓ Disposable Email Identify
- ✓ Phone Number Identify
- ✓ Computer Vision Services
- ✓ Free 24/7 Support

Start with Newbie I

Popular
Newbie II
$ 20
Duration 30 days
- ✓ 60.000 Quota/Visitor
- ✓ Killbot Blocker
- ✓ Killbot Shortlink
- ✓ OWASP Top 10 Protection
- ✓ Lookup IP Address
- ✓ Disposable Email Identify
- ✓ Phone Number Identify
- ✓ Computer Vision Services
- ✓ Free 24/7 Support

Start with Newbie II

Newbie III
$ 40
Duration 30 days
- ✓ 120.000 Quota/Visitor
- ✓ Killbot Blocker
- ✓ Killbot Shortlink
- ✓ OWASP Top 10 Protection
- ✓ Lookup IP Address
- ✓ Disposable Email Identify
- ✓ Phone Number Identify
- ✓ Computer Vision Services
- ✓ Free 24/7 Support

Start with Newbie III

[redacted]

Index of /.thirdparty

- Parent Directory
- 16Shop/
- BocahShop/
- Hijalyh/
- KuzuluyArt-activator/
- KuzuluyArt5.7/
- [redacted]
- youngsister (YS)/

Apache Server at [redacted] *Port 443*

Source: ZeroFox Internal Research

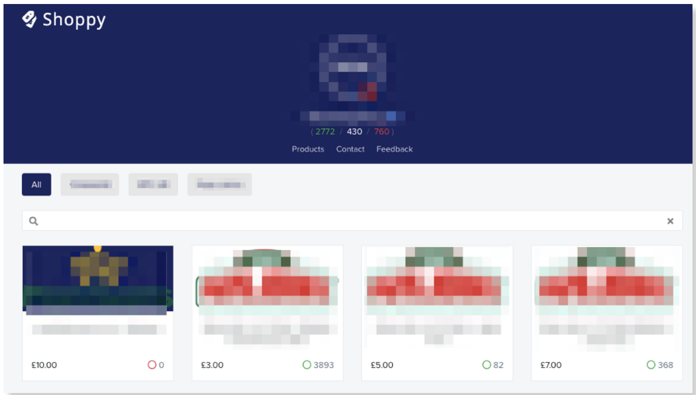
Targeted Phishing

Retail

Depending on the threat actor's appetite for risk, targeting customers of online marketplaces or stores means victims' credentials can be used to quickly cash out with high-value tech purchases or gift cards. There is also an increasing demand for compromised accounts for fast-food restaurants and grocery stores that allow purchasing of items online or via mobile apps, as shown in Figure 11.

ZeroFox has observed multiple threat actors selling access to compromised accounts for food and grocery outlets, along with "methods" instructing buyers how to use the credentials in such a way to avoid suspicion and have their orders canceled. For customers of these threat actors, a small cost of a few dollars can be converted into anywhere up to USD 100 of food with minimal risk.

Figure 11: Online storefront selling access to accounts, points, and "methods" for popular grocery and fast-food restaurants



Shoppy

[redacted]

(2772 / 430 / 760)

Products Contact Feedback

All [redacted] [redacted] [redacted]

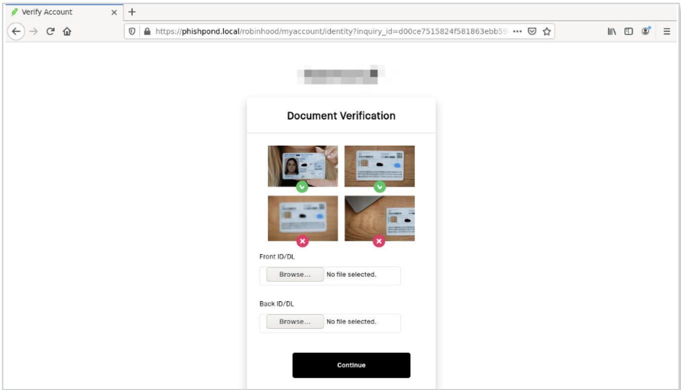
Price	Stock
£10.00	○ 0
£3.00	○ 3893
£5.00	○ 82
£7.00	○ 368

Source: ZeroFox Internal Research

Financial Services

With the increased vigilance of anti-fraud checks from both banks and online vendors, threat actors have also adapted their techniques and tools to extract more sensitive information from victims to facilitate bypassing “know your customer” (KYC) checks. Many of the latest phishing kits now include additional stages in the victim workflow to prompt the victim to provide identity documentation. Requested information can range from a single “selfie” photo to photos of passports or driver’s licenses, which can be used for fraudulent purposes in combination with other victim data.[5] Figure 12 displays an example of this technology on a phishing page fraudulently impersonating a financial services company.

Figure 12: Phishing page requesting the user to upload identity documents



Verify Account

https://phishpond.local/robinhood/myaccount/identity?inquiry_id=d00ce7515824f581863ebb5

Document Verification

Front ID/DL

Browse... No file selected.

Back ID/DL

Browse... No file selected.

Source: ZeroFox Internal Research

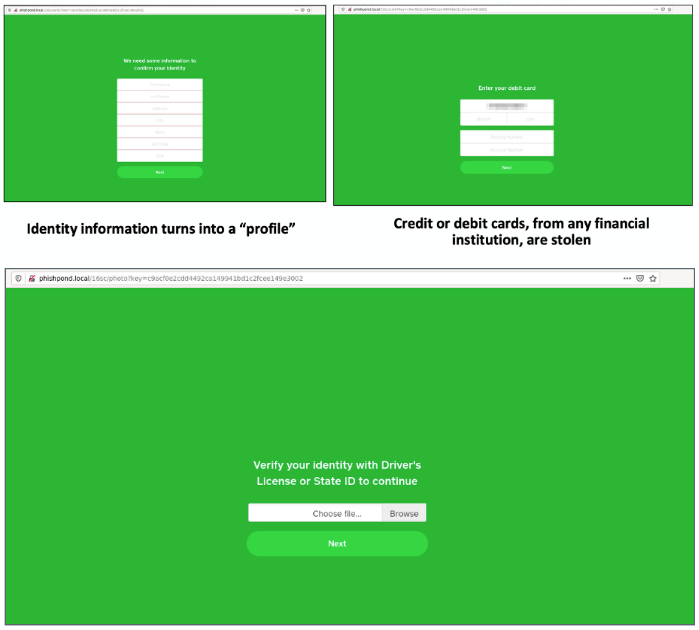
Beyond the Attack: Stolen Data Package Profiles

Phishing kit developers go to great lengths and spend hours to ensure the fraudulent site looks exactly like the brand they are targeting. Each page is uniquely built so threat actors can take the right information based on that brand. Figure 13 illustrates an example of the victim workflow in which only the email and password are populated initially. The phishing pages to follow gather more information, including everything from the victim’s name, address, Social Security number, debit card, credit card and more. This is beyond most conceptions of what phishing attacks collect and creates something much more detailed and malicious.

This complete stolen data package is referred to as a profile, or “Pro,” among threat actors. This detailed package can be sold as a whole data set; phishing attacks are no longer limited to collecting usernames and passwords. These profiles are prepackaged identity compromised toolsets. This information stored together is beneficial when attempting to compromise a victim’s financial livelihood.

This example is not representative of all phishing pages and attacks are not limited to this purview. However, this illustrates the broad spectrum within the phishing ecosystem. Phishing attacks can be more complicated than most might initially think and warrant more discussion, collaboration and research within the cybersecurity community.

Figure 13: Sample phases in a phishing attack to build stolen data package profiles



We need some information to confirm your identity

Identity information turns into a “profile”

Enter your debit card

Credit or debit cards, from any financial institution, are stolen

phishpond.local/16sc/photo?key=c9acf0e2cdd4492ca149941bd1c2fcee149e3002

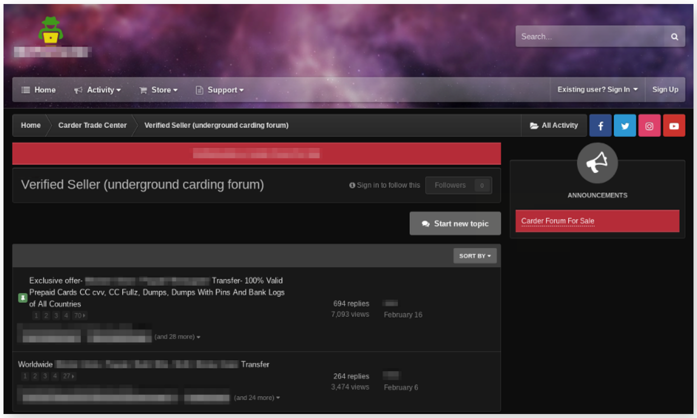
Verify your identity with Driver's License or State ID to continue

Source: ZeroFox Internal Research

Selling Victim Data

Collected data is commonly sold in the form of "fullz," meaning full credential or credit card information has been obtained from the victim. The method of selling can vary depending on the actor's capabilities but is generally done either in bulk for a set cost or on a per-account basis. Costs vary based on the value or assets of the compromised account, as shown in Figure 14. This is standard for accounts with access to monetary funds such as banks. Sellers may also agree to sell access at a reduced cost in exchange for a percentage of the purchaser's returns from "cashing out" the account.

Figure 14: Forum dedicated to selling and sharing of victim data and credit card information sourced from phishing attacks



Verified Seller (underground carding forum)

Exclusive offer- [redacted] Transfer- 100% Valid Prepaid Cards CC cvv, CC Fullz, Dumps, Dumps With Pins And Bank Logs of All Countries
1 2 3 4 70
[redacted] (and 28 more)
694 replies
7,093 views
[redacted]
February 16

Worldwide [redacted] Transfer
1 2 3 4 27
[redacted] (and 24 more)
264 replies
3,474 views
[redacted]
February 6

Source: ZeroFox Internal Research

Phishing Research, Disruption and Defense

As mentioned earlier, phishing attacks and kits are designed for ease of use and deployment. It is common for these kits to call assets directly from the targeted brand's website or content delivery network (CDN). This leaves a trail in assets you control like referrer logs.[6] An effective detection method is to look for these assets being called from URLs structured in specific ways. Reviewing the referrer logs for any calls to leverage an organization's legitimate logo from URLs ending in that specific path will lead researchers directly to active deployments.

ZeroFox's internal tools allow us to collect hundreds of unique phishing kits a day to determine exactly what phishing kit is behind an active phishing page. This insight enables our team to enrich the automated analysis of these domains and pull extra information such as victim data, weaknesses within the code and information on the threat actor themselves. However, solutions such as web beacons can also be leveraged. These can be proactively embedded within designated sites and assets. When a phishing kit pulls from these resources, immediate action can be taken to begin the threat disruption process.

Additionally, Phishpond is a resource the ZeroFox Threat Research team developed to help analyze phishing kits.[7] This tool aims to help defenders and researchers analyze the tactics, techniques and procedures (TTPs) employed by phishing operators and developers. The tool is readily available and can be leveraged to find exfiltration endpoints quickly, identify weaknesses in phishing kits and uncover additional intelligence, fingerprint known kits or find new ones.

This insight enables our team to enrich the automated analysis of these domains and pull extra information such as victim data, weaknesses within the code and information on the threat actor themselves.

Recommendations

As phishing campaigns become more sophisticated and widespread, organizations should continue to take steps to minimize the risk of becoming a victim of a cyber-attack.

- Enable two-factor authentication for all organizational accounts to help mitigate phishing and credential stuffing attacks.
- Enforce administrative or application control restrictions to prevent the unauthorized installation of software or media.
- Ensure antivirus and intrusion detection software is up to date with all patches and rule sets.
- Utilize account permissions best practices, such as role-based access control, least privilege and restricting root/admin permissions.
- Segment critical network resources using zero-trust configurations.
- Maintain regularly scheduled backup routines, including off-site storage and integrity checks.
- Limit file egress by size and type.
- Disable macros whenever possible.
- Avoid opening unsolicited attachments and never click suspicious links.
- Enforce best practices on passwords, such as complexity, forced expiration and prohibiting password reuse.
- Do not share passwords and do not reuse the same password on different websites and applications.
- Log and monitor all administrative actions as much as possible. Alert on any suspicious activity.
- Consider disabling, or at least logging, all network activity outside of regular business hours for most users where possible.

Conclusion

Today's global threat landscape is filled with high-profile cyber activity and continues to demonstrate the evolving nature of cybersecurity and cyber threats. Adversaries will continue to evolve their tactics in new, effective ways. As threat actors get creative with technology and attack vectors, phishing supply chain ecosystems can help business leaders and security teams understand the inner workings of digital fraud threat actors and the importance of securing applications to prevent phishing attacks. Security researchers will continue to disclose new vulnerabilities that directly affect enterprise organizations and their cohorts. However, it is of utmost importance for security teams to follow routine recommendations and strategize regarding additional ways to defend against new security vulnerabilities. Taking the minimum amount of recommended security precautions is not enough in today's threat landscape. Moving forward defenders must be even more well-equipped to handle the changing landscape.

ZEROFOX®

To learn more about how to protect your public attack surface with ZeroFox, visit zerofox.com.

References

[1] https://www.zerofox.com/blog/phishing-attack-101/

[2] https://www.zerofox.com/blog/16shop-cash-app-phishing-kit/

[3] https://www.zerofox.com/blog/what-is-a-phishing-kit-analysis-and-tools/

[4] https://www.zerofox.com/webinars/dismantling-puppeteer-kits/

[5] https://www.zerofox.com/blog/cares-act-fraud/

[6] https://globalspex.com/the-importance-of-referrer-logs/

[7] http://github.com/zerofox-oss/phishpond

ABOUT ZEROFOX

ZeroFox provides enterprises protection, intelligence and disruption to dismantle external threats to brands, people, assets and data across the public attack surface. The ZeroFox Platform includes advanced AI-driven analysis to detect complex digital threats on the web, deep and dark web, social media, mobile app stores, marketplaces, email, collaboration tools, and more. OnWatch™ alert management and managed threat intelligence services staffed with 150+ expert threat analysts become an extension of your team and deliver actionable threat intelligence to help you keep up with security demands. Integrated adversary disruption and takedown services leverages strong industry platform partnerships and intelligent automation to quickly disrupt threats before they go public.