WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

The Most Phished Brands of 2024 in the DNS Spotlight

Table of Contents

Executive Report

The Zscaler ThreatLabz 2024 Phishing Report named Microsoft, OneDrive, Okta, Adobe, SharePoint, Telegram, pCloud, Facebook, DHL, WhatsApp, ANZ Banking Group, Amazon, Ebay, Instagram, Google, Sparkasse Bank, FedEx, PayU, Rakuten, and Gucci as the 20 most phished brands. They are proof that popularity comes at a steep price. In their case, phishers have been exploiting their customers' trust to gain entry into as many enterprise networks as possible. Why? The 20 brands have millions of users worldwide.

The report, however, did not contain specifics about the phishing campaigns where the 20 aforementioned brands were abused. In a bid to shed more light, the WhoisXML API research team conducted an in-depth DNS investigation to find domains, subdomains, and IP addresses that could have figured in the threats or weaponized for similar attacks in the future.

Our study led to the discovery of:

- 3,120 branded domains, 12 of which turned out to be malicious
- Eight branded subdomains
- 14 IP addresses, 11 of which turned out to be associated with various threats

A Closer Look at the Branded Web Properties

To kick off our search for digital properties that could have figured or be weaponized in the future for phishing and other cyber attacks, we needed more information about the 20 most spoofed brands first, specifically the products' domain names and web pages and WHOIS record details.

Our bulk WHOIS lookup for the 20 most phished brands revealed that telegram[.]org and sparkasse[.]de had redacted WHOIS records, which meant exclusion from further investigation.

We would not be able to determine which **telegram**- and **sparkasse**-containing domains could be publicly attributed to Telegram and the Sparkasse Financial Group. We used the data in the following table for our query.

BRAND	DOMAIN NAME	WEB PAGE ADDRESS
Microsoft	microsoft[.]com	
OneDrive		microsoft[.]com/en-us/microsoft-365/onedrive/
Okta	okta[.]com	
Adobe	adobe[.]com	
SharePoint		microsoft[.]com/en-us/microsoft-365/sharepoint/
Telegram	telegram[.]org	
pCloud	pcloud[.]com	
Facebook	facebook[.]com	
DHL	dhl[.]com	
WhatsApp	whatsapp[.]com	
ANZ Banking Group	anz[.]com[.]au	
Amazon	amazon[.]com	
Ebay	ebay[.]com	
Instagram	instagram[.]com	
Google	google[.]com	
Sparkasse Financial Group	sparkasse[.]de	
FedEx	fedex[.]com	
PayU	payu[.]com	
Rakuten	rakuten[.]com	
Gucci	gucci[.]com	

Our analysis of the remaining 18 text strings (16 connected to brands with domains and two connected to brands with specific web pages) was broken down into three parts. In the first part, we looked for domains containing the 16 remaining most phished brands that had domain names. In the second part, we searched for subdomains where the string **microsoft.com**, alongside **onedrive** or **sharepoint**, appeared. The third part looked at the IP resolutions of all the malicious web properties.

Inspecting the Underbelly of the Branded Domains

The next step was to look for domain names containing text strings found in those belonging to the 16 brands left on our list, namely:

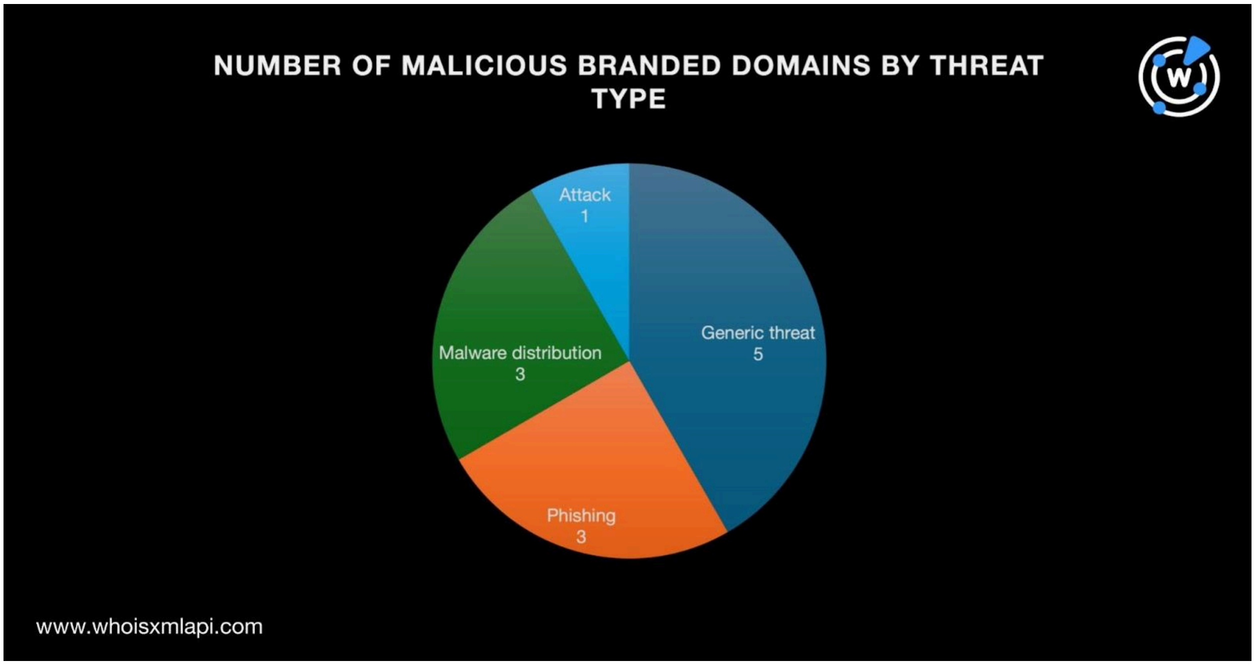
- **microsoft.**
- **okta.**
- **adobe.**
- **pcloud.**
- **facebook.**
- **dhl.**
- **whatsapp.**
- **anz.**
- **amazon.**
- **ebay.**
- **instagram.**
- **google.**
- **fedex.**
- **payu.**
- **rakuten.**
- **gucci.**

Our Domains & Subdomains Discovery searches for the 16 text strings using the **Domains only**, **Starts with**, and **Added since January 1, 2023** (based on the report's coverage) turned out 3,120 branded domains.

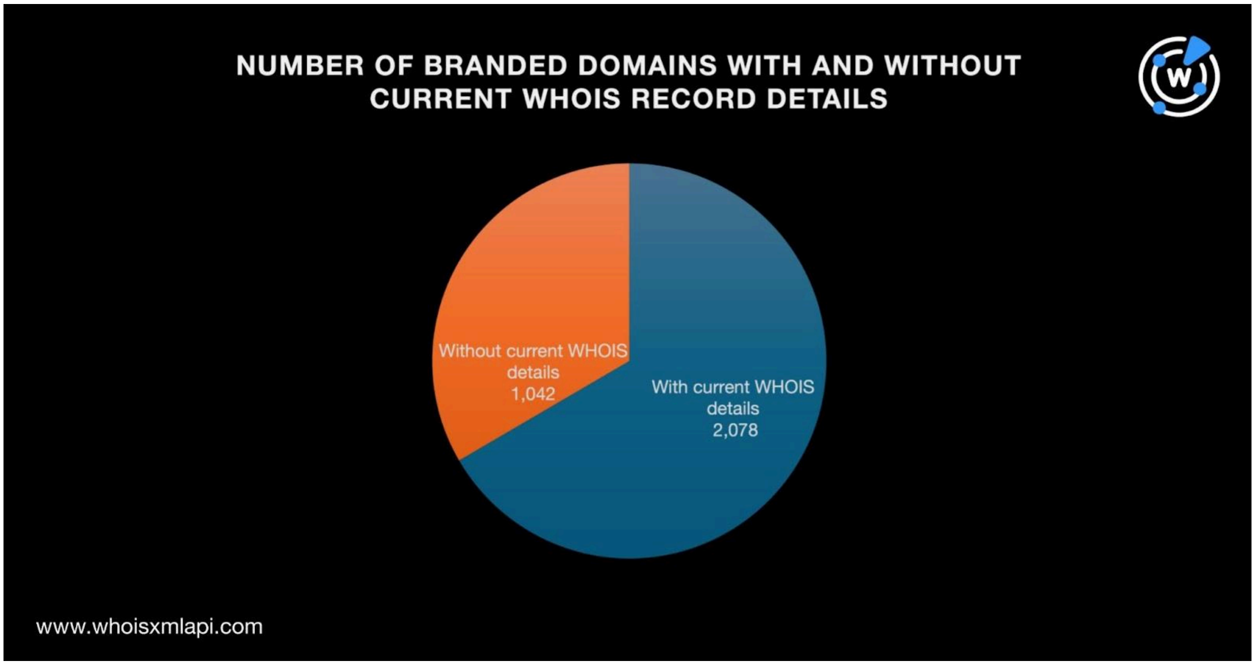
Threat Intelligence API revealed that 12 of the 3,120 branded domains were associated with various threats. Take a look at five examples below.

MALICIOUS BRANDED DOMAIN	ASSOCIATED THREAT TYPES
amazon[.]org[.]gg	Phishing
facebook[.]com[.]br	Generic threat
fedex[.]info[.]pl	Phishing
google[.]site	Malware distribution
gucci[.]com[.]by	Attack

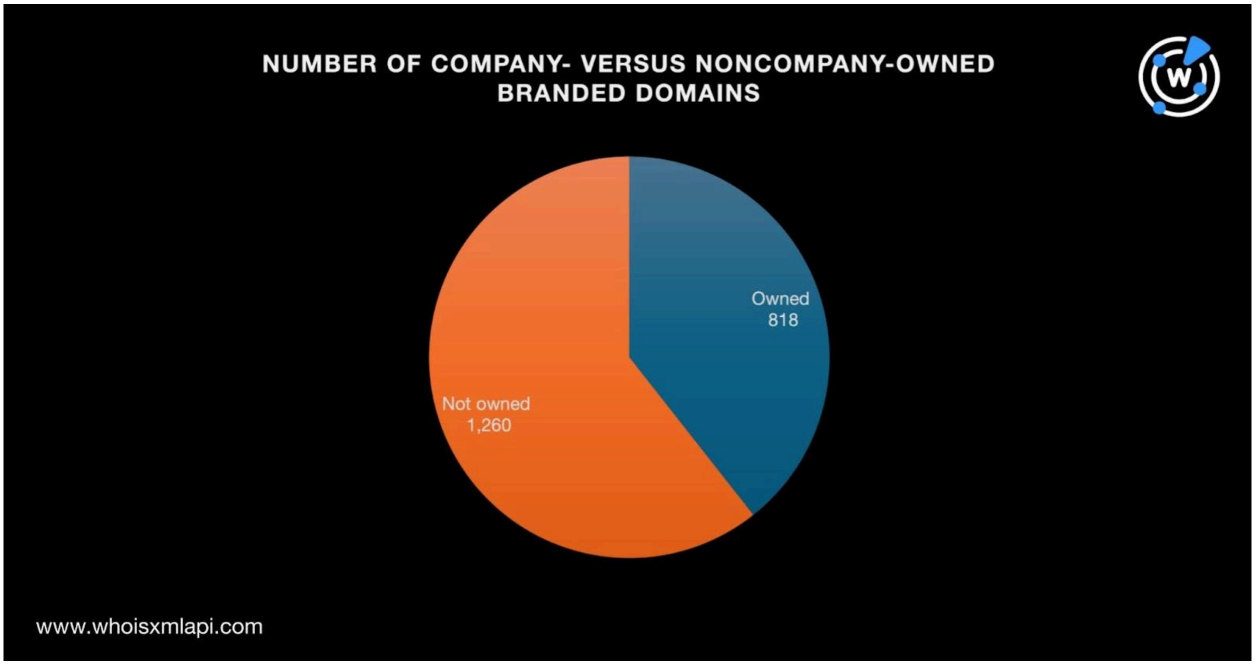
Specifically, five out of 12 malicious branded domains were associated with generic threats. Three domains each were connected to phishing and malware distribution and one with an attack.



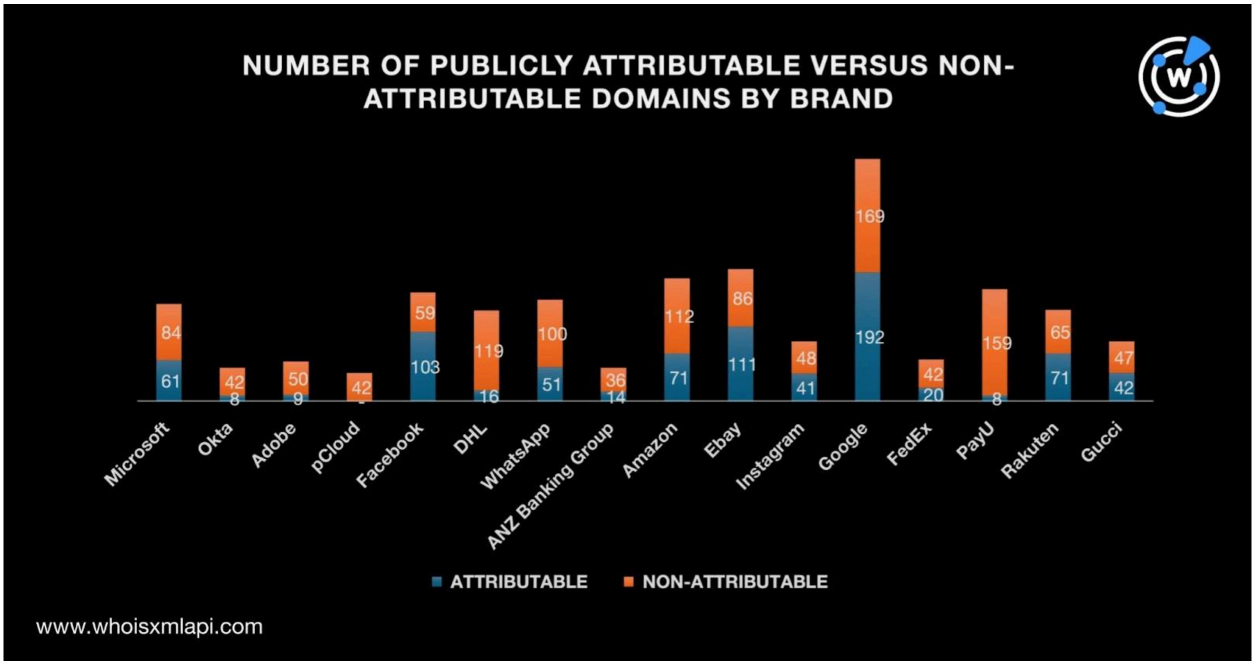
Next, we subjected the 3,120 branded domains to a bulk WHOIS lookup and found that 1,042 did not have details in their current WHOIS records. That left us 2,078 branded domains for the rest of this study.



Of the 2,078 branded domains with current WHOIS record details, 818 could be publicly attributed to the 16 brand owners while 1,260 could not.

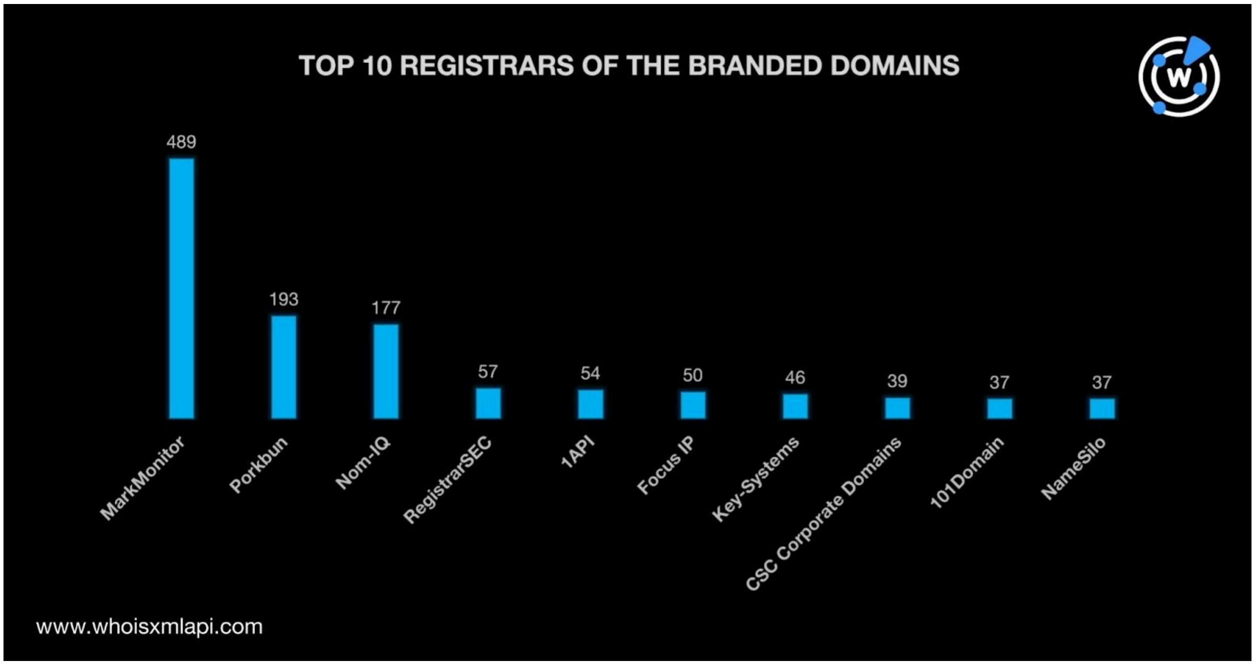


Here's a more in-depth breakdown of the 2,078 branded domains with current WHOIS record details by brand.

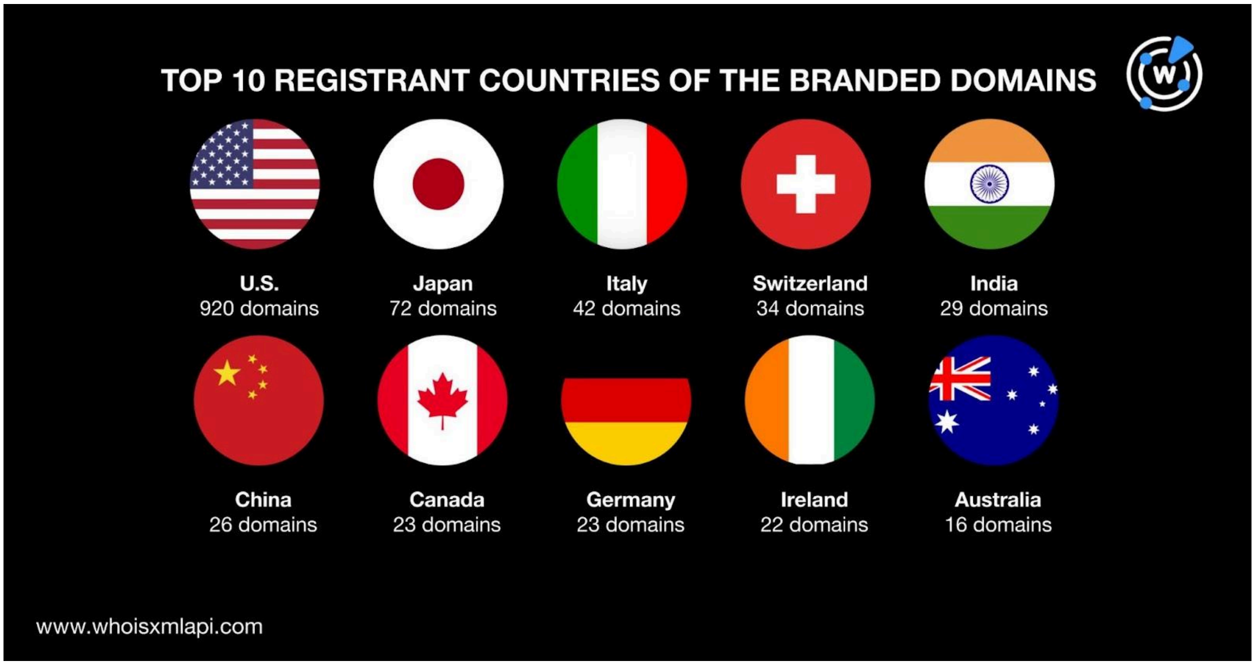


The same lookup for the 2,078 domains also revealed that:

- MarkMonitor was the top registrar, administering 489 domains. Porkbun (193 domains), Nom-IQ (177 domains), RegistrarSEC (57 domains), 1API (54 domains), Focus IP (50 domains), Key-Systems (46 domains), CSC Corporate Domains (39 domains), and 101Domain and NameSilo (37 domains each) completed the top 10.



- The domains were a mix of old and new. Various domains were several years old while the newest (google[.]org[.]ky) was added to the DNS on 14 June 2024.
- A majority of the domains, 920 to be exact, were registered in the U.S. Japan (72 domains), Italy (42 domains), Switzerland (34 domains), India (29 domains), China (26 domains), Canada and Germany (23 domains each), Ireland (22 domains), and Australia (16 domains) completed the top 10 registrant countries.

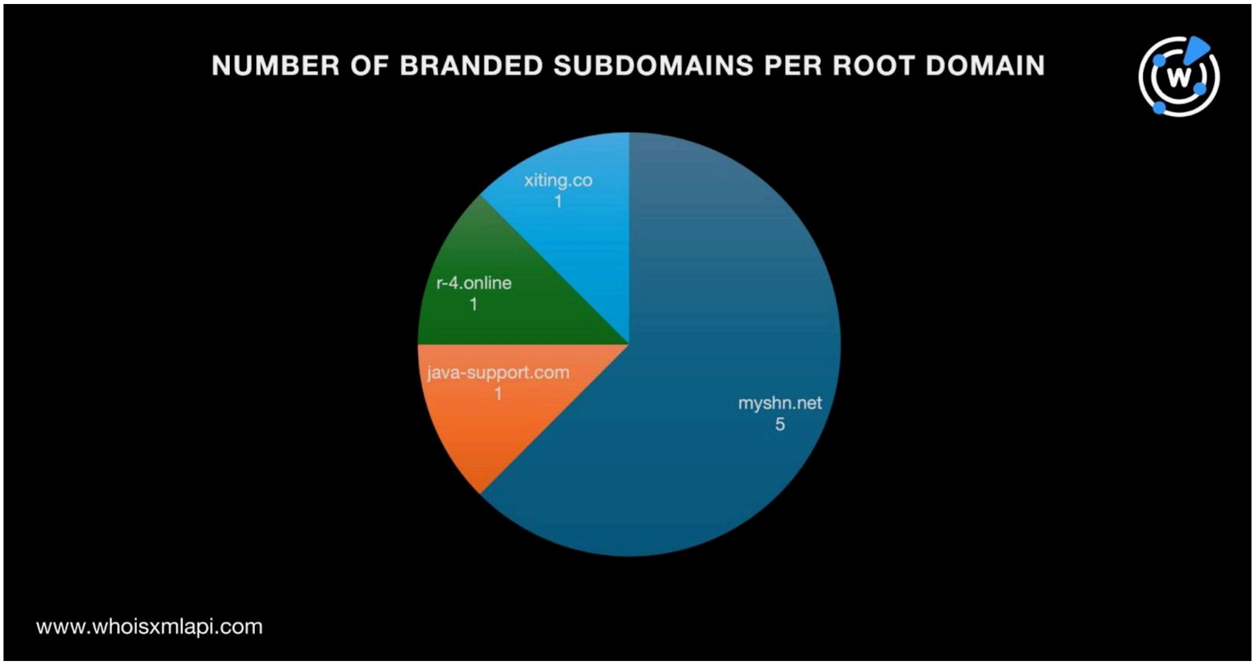


Digging Deeper into the Branded Subdomains

Since two of the most phished brands did not have dedicated domain names but instead had web pages with their owners' domain (microsoft[.]com) and specific brand names (onedrive and sharepoint), we opted to use Domains & Subdomains Discovery to look for weaponizable subdomains with these parameters instead:

- Contains the text strings **microsoft.com** and **onedrive** added since January 1, 2023
- Contains the strings **microsoft.com** and **sharepoint** added since January 1, 2023

We obtained eight branded subdomains that phishers could use in their campaigns. A more in-depth analysis allowed us to identify that five of them were under the domain myshn[.]net. Three other root domains accounted for one subdomain each.



What about the Malicious Digital Properties' DNS Resolutions?

Finally, we sought out more DNS information on the 12 malicious branded domains we uncovered earlier.

DNS lookups for the 12 domains showed that only eight of them had active IP resolutions. Altogether, they resolved to 14 unique IP addresses.

Threat Intelligence API revealed that 11 of the IP addresses were associated with various threats like the domains they hosted. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT TYPES
185[.]199[.]108[.]153	Attack Command and control (C&C) Generic Malware Phishing Spam
157[.]240[.]3[.]20	Attack
69[.]171[.]242[.]11	Malware
66[.]220[.]149[.]11	Attack

	Malware
52[.]60[.]87[.]163	Generic Malware

Our DNS deep dive into the 20 most phished brands of 2024 brought to light 3,142 connected artifacts comprising 3,120 domains, eight subdomains, and 14 IP addresses. While only a few have been weaponized for malicious campaigns, many could still be cybersquatting on the brands' popularity to prey on their millions of users worldwide.

If you wish to learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample Branded Domains

- adobe[.]ae
- adobe[.]ar
- adobe[.]art
- adobe[.]associates
- adobe[.]ba
- adobe[.]belau[.]pw
- adobe[.]bf
- adobe[.]boo
- adobe[.]box
- adobe[.]cafe
- amazon[.]abogado
- amazon[.]ac[.]mw
- amazon[.]ac[.]th
- amazon[.]ac[.]tj
- amazon[.]ac[.]za
- amazon[.]ae
- amazon[.]ah[.]cn
- amazon[.]alt[.]za
- amazon[.]altoadige[.]it
- amazon[.]amsterdam
- anz[.]ae
- anz[.]app
- anz[.]as
- anz[.]bank
- anz[.]bg
- anz[.]business
- anz[.]capital
- anz[.]cards
- anz[.]ch
- anz[.]cm
- dhl[.]arab
- dhl[.]au
- dhl[.]auction
- dhl[.]autos

- dhl[.]baby
- dhl[.]band
- dhl[.]beauty
- dhl[.]bike
- dhl[.]bingo
- dhl[.]bio
- ebay[.]academy
- ebay[.]accountants
- ebay[.]actor
- ebay[.]adult
- ebay[.]ae
- ebay[.]ag
- ebay[.]agency
- ebay[.]airforce
- ebay[.]am
- ebay[.]ao
- facebook[.]ac[.]id
- facebook[.]accountant
- facebook[.]actor
- facebook[.]ae
- facebook[.]alsace
- facebook[.]amsterdam
- facebook[.]apartments
- facebook[.]app[.]br
- facebook[.]ar
- facebook[.]asia
- fedex[.]ai
- fedex[.]al
- fedex[.]aquila[.]it
- fedex[.]at
- fedex[.]au
- fedex[.]bond
- fedex[.]br
- fedex[.]by
- fedex[.]ci
- fedex[.]co[.]in
- google[.]abc[.]br
- google[.]abogado
- google[.]ac
- google[.]ac[.]id
- google[.]ac[.]vn
- google[.]academy
- google[.]accountant
- google[.]ad
- google[.]ads
- google[.]ae
- gucci[.]ag
- gucci[.]amsterdam
- gucci[.]aquila[.]it
- gucci[.]at
- gucci[.]auction
- gucci[.]bh
- gucci[.]bieszczady[.]pl
- gucci[.]blue
- gucci[.]boutique
- gucci[.]buzz
- instagram[.]abogado
- instagram[.]ac
- instagram[.]ai
- instagram[.]ai[.]in
- instagram[.]app[.]br
- instagram[.]ar
- instagram[.]ax
- instagram[.]bayern
- instagram[.]bbs[.]tr
- instagram[.]bg
- microsoft[.]ag
- microsoft[.]at
- microsoft[.]auction
- microsoft[.]auto
- microsoft[.]band
- microsoft[.]barcelona
- microsoft[.]bh
- microsoft[.]bialystok[.]pl
- microsoft[.]bio
- microsoft[.]biz[.]pl
- okta[.]ai
- okta[.]auspost
- okta[.]bf
- okta[.]cn

- okta[.]co[.]jp
- okta[.]co[.]nz
- okta[.]co[.]rs
- okta[.]co[.]uk
- okta[.]com[.]au
- okta[.]com[.]br
- payu[.]academy
- payu[.]agency
- payu[.]ar
- payu[.]auction
- payu[.]autos
- payu[.]ba
- payu[.]baby
- payu[.]bar
- payu[.]beauty
- payu[.]best
- pcloud[.]ac[.]cn
- pcloud[.]au
- pcloud[.]biz
- pcloud[.]blog
- pcloud[.]cf
- pcloud[.]ch
- pcloud[.]cn
- pcloud[.]co[.]th
- pcloud[.]co[.]uk
- pcloud[.]co[.]za
- rakuten[.]ae
- rakuten[.]ai
- rakuten[.]amsterdam
- rakuten[.]ar
- rakuten[.]as
- rakuten[.]barcelona
- rakuten[.]bayern
- rakuten[.]bet
- rakuten[.]biz
- rakuten[.]bj[.]cn
- whatsapp[.]ae
- whatsapp[.]agr[.]br
- whatsapp[.]ai
- whatsapp[.]ai[.]in
- whatsapp[.]ar
- whatsapp[.]at
- whatsapp[.]au
- whatsapp[.]ax
- whatsapp[.]az
- whatsapp[.]bbs[.]tr

Sample Branded Subdomains

- com[.]sharepoint[.]microsoft[.]com[.]r-4[.]online
- www[.]xiting[.]sharepoint[.]microsoft[.]com[.]xiting[.]co
- microsoft[.]com[.]office[.]o365-onedrive-rp[.]terrishn[.]myshn[.]net
- microsoft[.]com[.]office[.]m365eonedrive[.]jccbr[.]myshn[.]net

Sample IP Addresses

- 185[.]199[.]108[.]153
- 185[.]199[.]109[.]153
- 185[.]199[.]110[.]153
- 185[.]199[.]111[.]153
- 157[.]240[.]3[.]20
- 31[.]13[.]88[.]1
- 31[.]13[.]65[.]1