CYREN

The Thrill of the Chase

Phishing Threat Report

Table of Contents

Introduction

Launching a phishing attack today has never been easier with the proliferation of phishing kits for sale on the dark web and in underground channels on Telegram. As it becomes easier to host phishing sites with free website hosting and domain name registrars, criminals with little-to-no technical skills can learn to launch attacks by watching a simple video tutorial.

Cybercriminals are also putting more focus on mobile devices, using text messages, WhatsApp, and other messaging services to launch attacks. These threats are difficult to detect since anti-phishing solutions on mobile devices are not as robust as those on business email servers and mailboxes. It's also harder for victims to differentiate fraudulent websites from real ones, making it simple for hackers to steal valuable personal data. Once data is stolen, it is vulnerable—accessible by anyone on the internet who is searching for it. Exposed usernames, email addresses, passwords, credit card numbers, and social security numbers can easily be uncovered with online search engines.

This report details a sharp increase in the number of phishing attacks targeting customers of a large American bank. There is always a baseline number of attacks targeting customers of large retail banks and other financial services firms, and brief short-lived surges of malicious activity. However, a sustained increase over several weeks is unusual. Using commercially available threat intelligence and open sources on the internet, Cyren threat researchers detected this increase and followed a trail that began with a simple summary dashboard and ended with some shocking examples of the damage phishers inflict when they trick an unsuspecting user into divulging highly sensitive, nonpublic personal information.

Follow The Money

Attackers generally want money or passwords. These motivations become obvious when examining the breakdown of brands targeted in phishing campaigns. Financial and eCommerce institutions and popular cloud services are the most frequently spoofed brands around the world. Notice in Figure 1 below, Chase Bank, an American subsidiary of JP Morgan Chase & Co, is ranked the sixth most often spoofed brand found in phishing URLs.

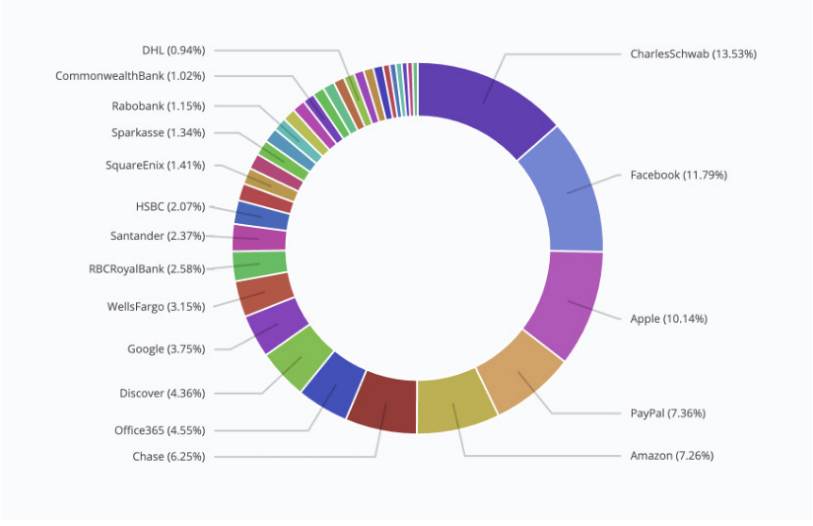

Figure 1 Phishing URLs by brand over three month period

Summarizing the data to only show brands in the financial industry, Chase climbs to third place, only a few percentage points behind PayPal.

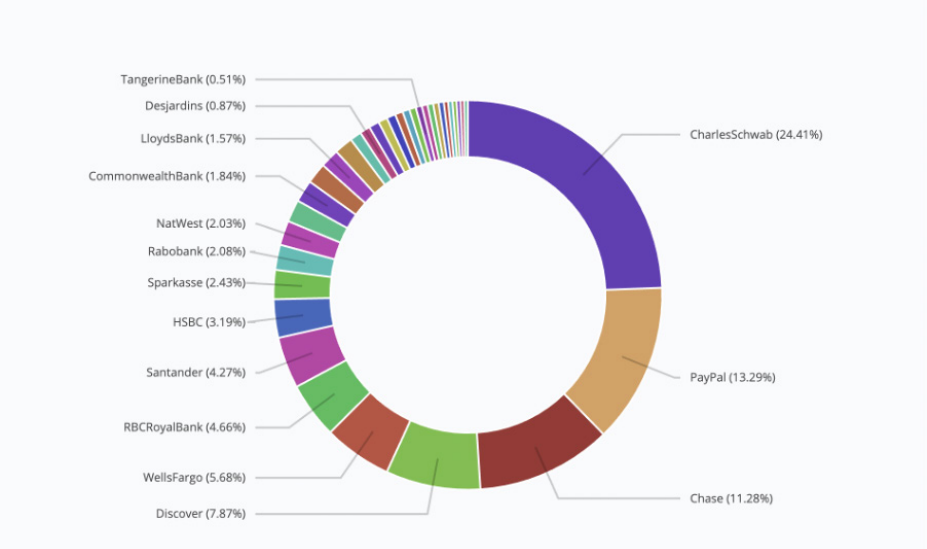

Figure 2 Financial industry brands used in phishing over three month period

Phishing Campaigns on the Rise

From the middle of May to mid-August 2021, Cyren observed a significant increase in phishing sites targeting Chase Bank account holders. This increase resulted in Chase becoming one of the most phished brands according to Cyren research data. From the end of May until this report was published, the research team saw a 300% increase in phishing URLs using the Chase brand—and behind each URL there is a phishing kit, which is the web component or the backend to the attack.

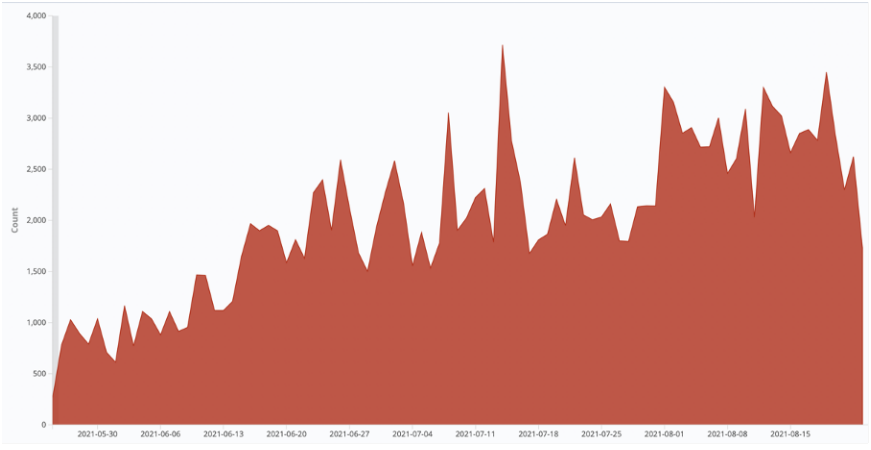

Figure 3 Daily count of phishing URLs using the Chase brand

With the increase of phishing URLs related to Chase over the three month period, there was a noticeable increase in phishing kits built to mimic the Chase banking portal.

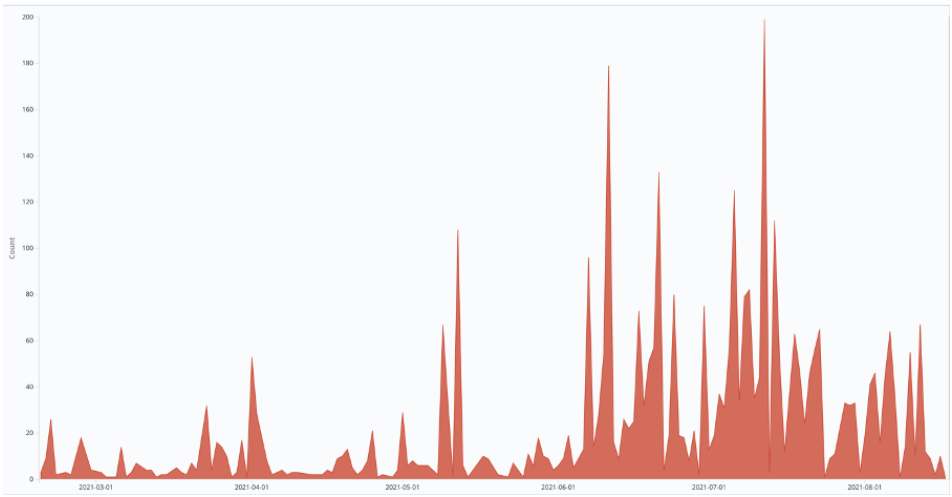

Figure 4 Number of Chase phishing kits

Of all the phishing kits collected in the last 6 months, Chase is the second most targeted brand.

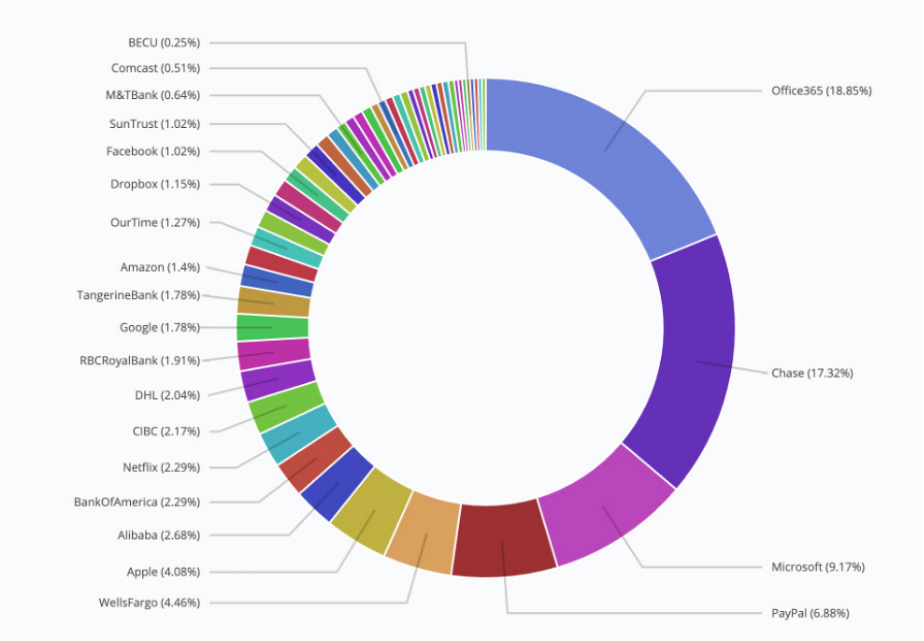

Figure 5 Concentration of phishing kits by brand

A Favorite Phishing Kit

Many of the phishing kits analyzed since May 2021 are highly sophisticated and built to harvest more than just the victims email address and password. The kits collect banking and credit card information, social security numbers, home addresses, and other very sensitive information. Some of the kits are designed to capture the one-time use codes used for two-factor authentication.

The phishing kit that is currently being heavily used is the Chase XBALTI. Although it has been available for several years, it is now primarily being used to target Chase and Amazon consumers.

Figure 6 XBALTI signature associated with a Chase phishing kit

Luring the Victims

Attackers use both emails and text messages to lure victims to their phishing sites, easily bypassing detection on mobile devices. See how the attack unfolds below.

Please note: A phishing URL sent to a text messaging is known as “smishing”.

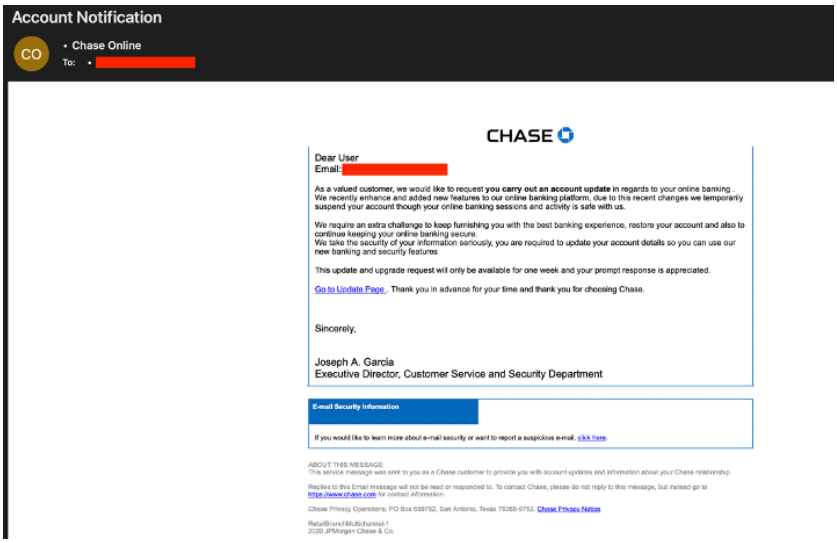

Figure 7 Example phishing email

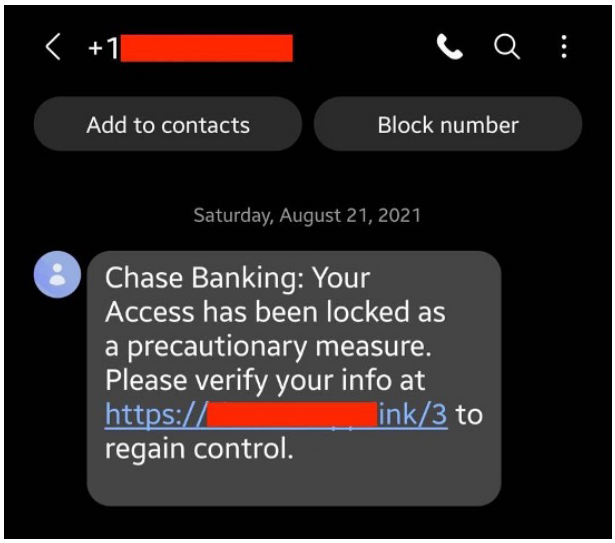

Figure 8 Example smishing text message

Setting the Hook

When the victim clicks on the link from the email or text message, they are taken to the phishing site. In this example, the phishing site is a compromised Brazilian website that looks very similar to the official site.

1. The victim is prompted for their username and password.

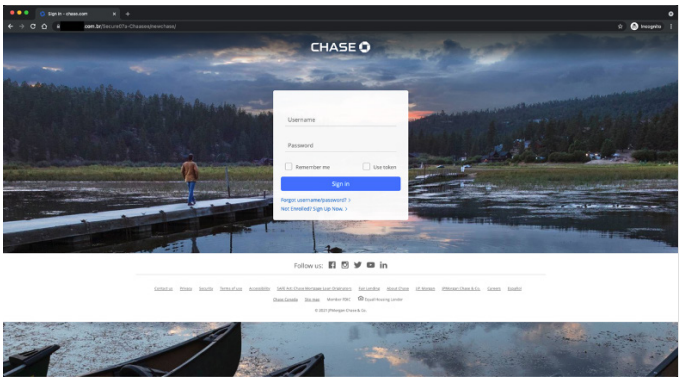

Figure 9 The landing page on a compromised website is step one

2. After entering the credentials, the victim is sent to the next page and asked to enter their email and password once again.

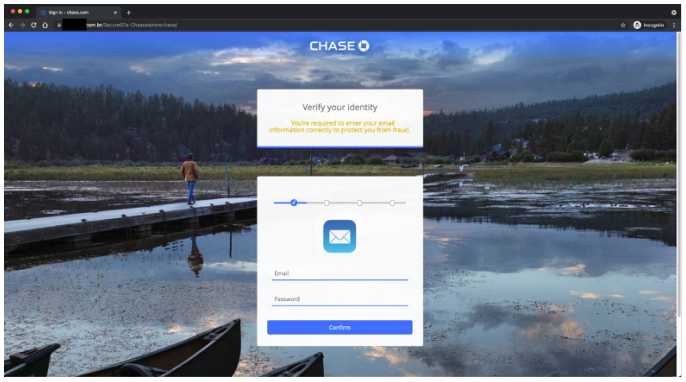

Figure 10 The second step is to get the victim's email and password

3. After the victim presses the Confirm button, they are told the credentials are incorrect and asked to enter them again. This is done by the attacker to make sure the victim didn't enter a typo.

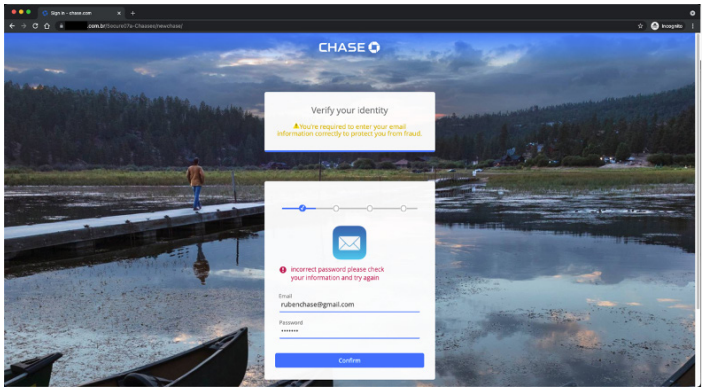

Figure 11 The third step asks the user to confirm the login info

4. Once the victim has re-submitted the credentials, they are taken to the next page to update personal information, including a social security number, mother's middle name, date of birth, and more.

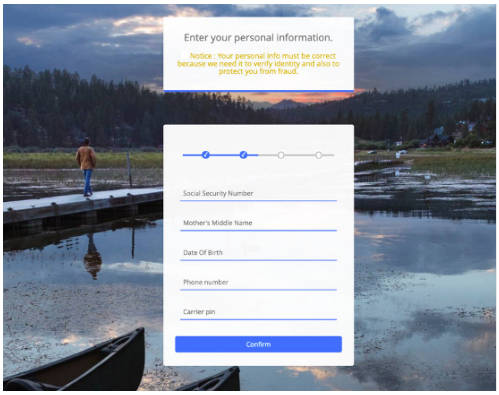

Figure 12 Step four sets up the victim for identity theft

5. After collecting the personal information, the attacker collects credit card information.

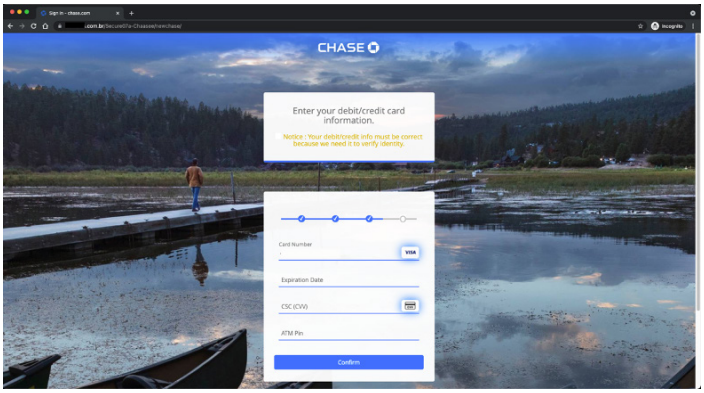

Figure 13 The fifth step is to gather payment details

6. Once that is done, the victim is asked to add information for another credit/debit card.

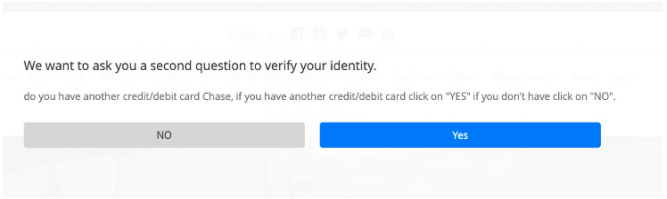

Figure 14 Then ask for more payment information

7. The last information collected is the victim's home address, which is interesting because the attacker already has the username and password, providing enough information to drain the victim's bank account. By extracting more personal details, the attacker can further monetize the victim by selling information. Complete and verified packages of identity information sell for a premium on dark web marketplaces and criminal networks.

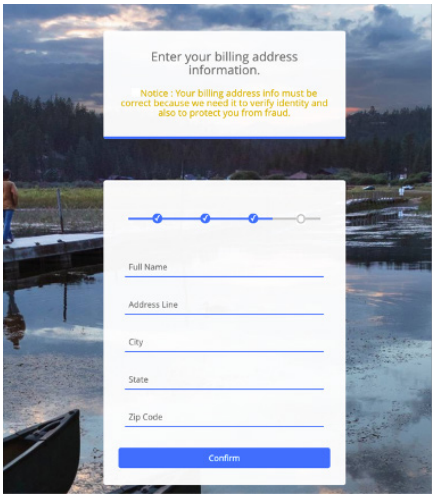

Figure 15 The final step is to get a complete profile of the victim

8. After confirming the address, the victim is taken to the final verification page.

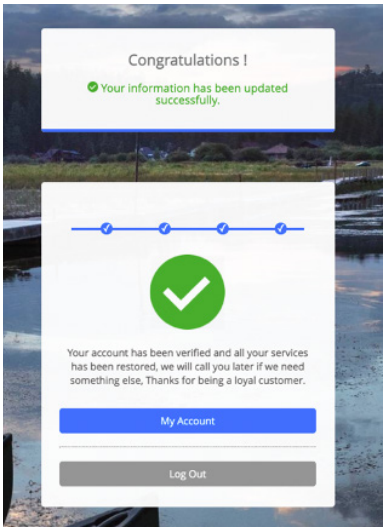

Figure 16 All done

9. When the My Account button is pressed, the victim is redirected to the official Chase website.

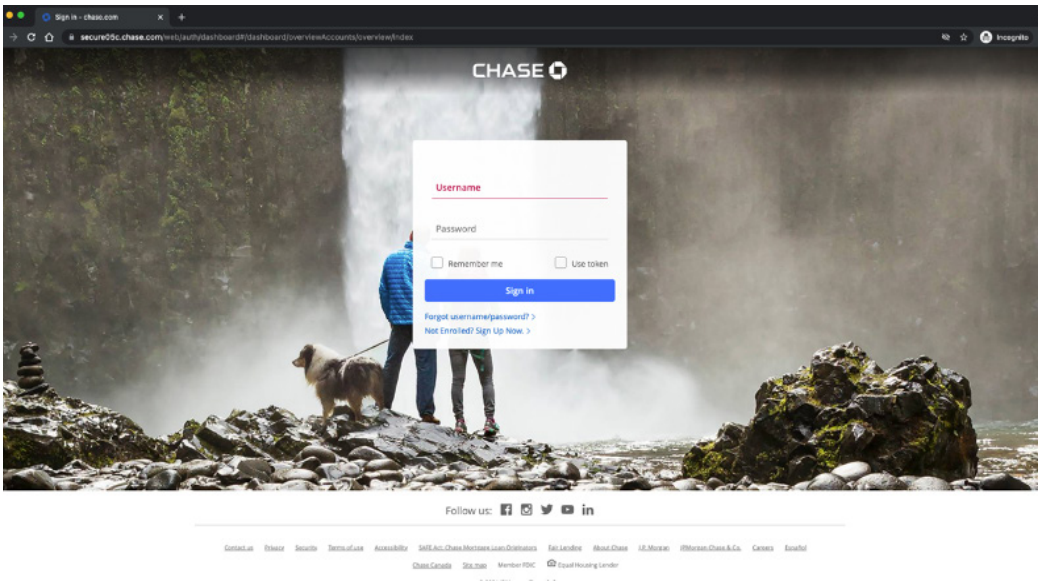

Figure 17 The victim is finally redirected to the real Chase login page

Unsecured Victim Data

After each step of the user experience, the stolen information is sent to an email address the attacker configured within the phishing kit, specifically in the file Email.php. Notice XBALTI's signature in the figure below.

Figure 18 The victim data is emailed to the attacker

The stolen information is also stored in a HTML file on the compromised web server and can be viewed in a password protected dashboard.

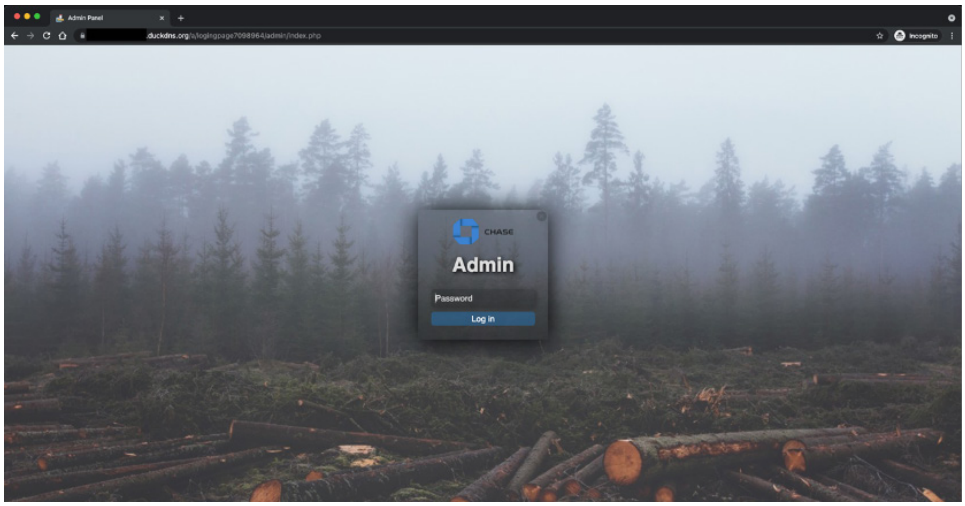

Figure 19 The Admin dashboard of an XBALTI kit

The stolen data can also be readily viewed by directly accessing files in an open web directory on the server.

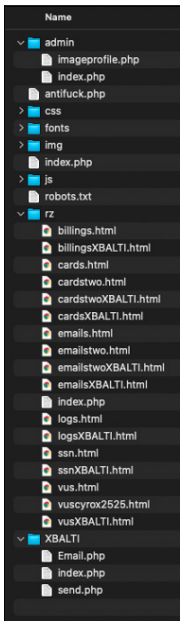

Figure 20 The folder 'rz' has the victim data

Storing unsecured victim data on the phishing server was not limited to a single installation and configuration of the phishing kit. The research team found many other instances of the XBALTI kit storing victim data in a file that was open to the internet. From the browser information associated with the victim data the team examined that mobile devices have been heavily targeted in the last few months.

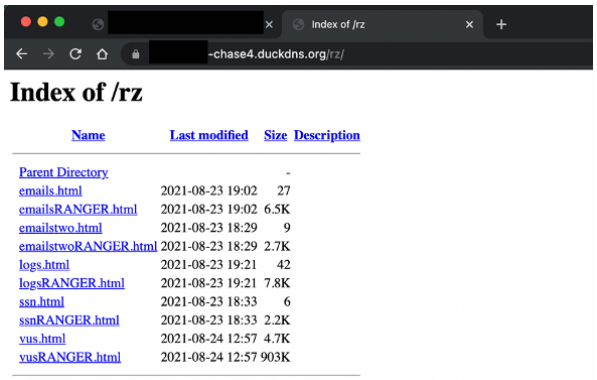

Figure 21 Another XBALTI phishing kit with unsecured victim data

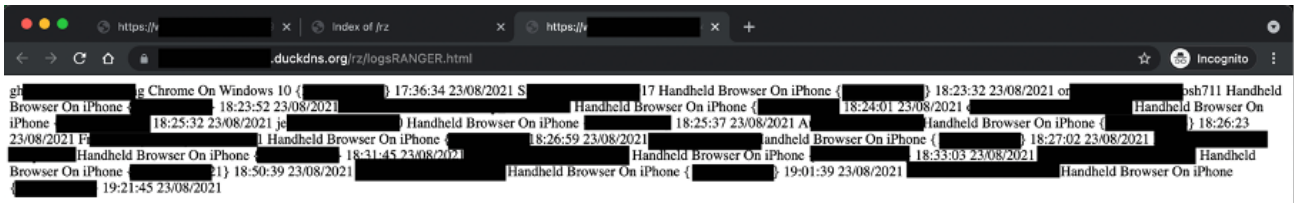

Figure 22 Usernames, passwords, and network addresses of Victims

Figure 23 Victim data from yet another unsecured kit

The XBALTI kit is just one of many Chase phishing kits that have stolen victim data stored publicly on the phishing server.

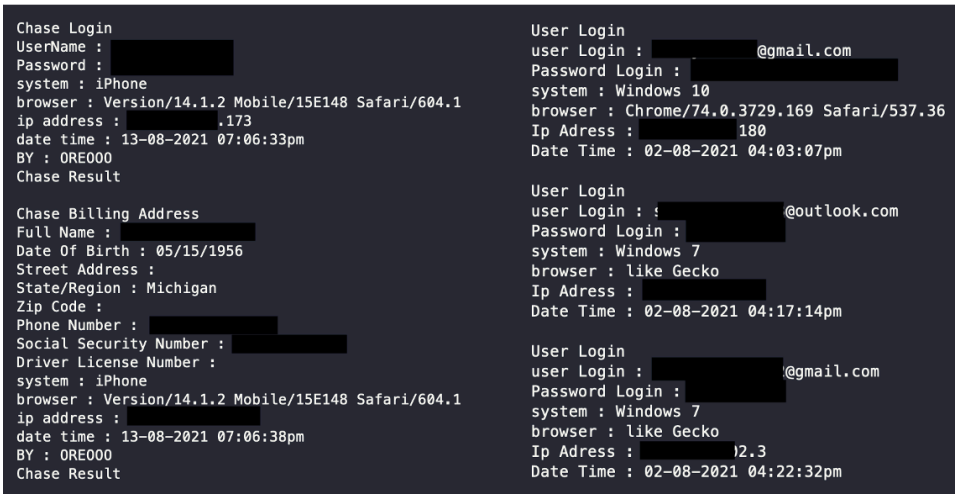

Figure 24 Usernames, passwords, and other sensitive data

Evading Detection

All of the Chase phishing kits analyzed in the last few months relied on evasion tactics to avoid detection.

One of the tactics is to be a moving target. The attackers use free dynamic domain name services like Duck DNS to point a URL to the server of their choice. This allows them to change the destination of a URL as the phishing kits get discovered and taken down.

```
https://chasebankingonline.duckdns.org
https://chasesecuresweb.duckdns.org/a/logingpage7098964/
https://mail.dispute-online-chase.duckdns.org/login/login?chase_id=&country=United%20States&iso=US
https://mail.onlinechasesecureb.duckdns.org
https://mail.secure9m-chaseverify.duckdns.org
https://mail.secure9t-chase.duckdns.org/secure/
https://onlinechasebank.duckdns.org/a/logingpage7098964/
https://secure6t-chaseverify.duckdns.org/secure/
https://secure9m-chaseverify.duckdns.org
https://secure9m-chaseverify.duckdns.org/secure
https://secure9m-chaseverify.duckdns.org/secure
https://secure9m-chaseverify.duckdns.org/secure/
https://secure9t-chase.duckdns.org/secure
https://www.chasebankingonline.duckdns.org
https://www.dispute-online-chase.duckdns.org
https://www.dispute-online-chase.duckdns.org/login/
https://www.secure9m-chaseverify.duckdns.org
https://www.secure9t-chase.duckdns.org/secure/
```

Figure 25 Chase phishing sites that used Duck DNS

Most of the kits are using user-agent blockers to prevent crawlers from accessing the site; other kits use a combination of user-agent, IP, host lookup and ISP blocking.

```
$bannedIP = array("^81.161.59.*", "^66.135.200.*", "^66.102.
    ^128.242.*.*", "^72.14.192.*", "^208.65.144.*", "^74.125
    ^194.72.238.*", "^62.116.207.*", "^212.50.193.*", "^69.6
    , "^194.90.*.*", "^212.29.192.*", "^212.29.224.*", "^212
    ^202.108.252.*", "^193.47.80.*", "^64.62.136.*", "^66.22
    , "^209.73.228.*", "^158.108.*.*", "^168.188.*.*", "^66.
```

Figure 26 IP addresses blocked from accessing the phishing site

```
session_start();
$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
$blocked_words =
    array("bot",
     "above",
     "google",
     "softlayer",
     "amazonaws",
     "cyveillance",
     "phishtank",
     "dreamhost",
     "netpilot",
     "calyxinstitute",
     "tor-exit",
     "apache-httpclient",
     "lssrocketcrawler",
     "crawler",
     "urlredirectresolver",
     "jetbrains",
```

Figure 27 Server names blocked from accessing the phishing site

```
$banned_isp = array(
    'Peak 10',
    'Quasi Networks LTD',
    'SC Rusnano',
    'GoDaddy.com, LLC',
    'Server Plan S.r.l.',
    'Linode',
    'Blazing SEO',
    'Lixux OU',
    'Inter Connects Inc',
    'Flokinet Ltd',
    'LukMAN Multimedia Sp. z o.o',
    'PIPEX-BLOCK1',
    'IPVanish',
    'LinkGrid LLC',
    'Snab-Inform Private Enterprise',
    'Cisco Systems',
```

Figure 28 Internet Service Providers blocked from accessing the phishing site

```
#  MICROSOFT IP RANGES

65.52.0.0-65.55.255.255

#  G-DATA SOFTWARE IP RANGES

195.205.70.0-195.205.70.255
212.23.128.176-212.23.128.179
212.23.140.96-212.23.140.127
212.23.136.48-212.23.136.63

#  SOPHOS IP RANGES

194.203.134.128-194.203.134.255
213.86.172.128-213.86.172.159
212.161.106.240-212.161.106.247
85.35.56.80-85.35.56.87
88.44.165.208-88.44.165.223
81.93.18.144-81.93.18.151
213.139.142.80-213.139.142.95
81.223.13.240-81.223.13.255
85.126.49.88-85.126.49.95
85.222.200.248-85.222.200.255
193.189.184.158-193.189.184.158
145.253.124.128-145.253.124.159
195.171.192.0-195.171.192.127
195.171.192.128-195.171.192.255
212.243.136.40-212.243.136.47
178.15.194.112-178.15.194.127
195.65.248.136-195.65.248.143

#  GOOGLE CHROME IP RANGES

66.249.64.0-66.249.95.255
74.125.0.0-74.125.255.255
66.102.0.0-66.102.15.255

#  ADNET TELECOM IP RANGES

31.215.209.0-31.215.209.127

#  MCAFEE IP RANGES

83.236.159.0-83.236.159.7
62.189.112.128-62.189.112.255
194.123.34.184-194.123.34.191
193.128.126.16-193.128.126.23
62.189.129.0-62.189.129.63
194.78.128.132-194.78.128.135
80.148.18.8-80.148.18.15
31.161.25.96-31.161.25.103
31.161.27.96-31.161.27.103
31.161.90.40-31.161.90.47
31.149.153.160-31.149.153.167
12.39.242.112-12.39.242.119
12.22.195.192-12.22.195.199
174.90.35.192-174.90.35.207
208.42.249.0-208.42.249.15
12.198.240.128-12.198.240.255
192.187.128.0-192.187.128.255
216.49.80.0-216.49.95.255
161.69.0.0-161.69.255.255
165.193.42.64-165.193.42.127
216.35.7.96-216.35.7.127
165.193.42.128-165.193.42.191
208.69.152.0-208.69.159.255
205.139.39.0-205.139.39.63
64.41.151.0-64.41.151.255
64.41.168.232-64.41.168.239
12.181.44.192-12.181.44.199
12.184.29.176-12.184.29.191
64.41.199.48-64.41.199.55
8.21.160.0-8.21.163.255
8.18.24.0-8.18.27.255
```

Figure 29 Blocked IP addresses that belong to security companies

Conclusion

We constantly hear about phishing but seeing victim data brings the concept to life. Criminals have built an entire supply chain around phishing. Phishing kits are built once, sold many times, and deployed onto thousands of active web servers each day. The victim data is immediately used to commit fraud or a follow-on attack. Once the attackers are done with the victim data, they package it and sell bundles of exposed passwords and other personal data on the dark web.

American banks are required to have safeguards in place to prevent phishing and other forms of fraud, and Chase is no exception (see link below). Large cloud providers including Google, Microsoft, and Amazon have robust operations to remove phishing kits from their data centers, but there are many other hosting companies that don't have the resources or motivation to do the same. Also, attackers are nimble – constantly evolving and sharing techniques to avoid detection. When one phishing kit is removed, another will pop up in its place. As email detection improves, the attackers switch to mobile. It's a never-ending cycle that gets increasingly complex and organized.

Phishing wouldn't be a popular attack type if it didn't work. Some users can spot a phishing email in a few seconds, but many unsuspecting people routinely fall victim to phishing attacks. Whether it's the financial analyst that wires tens of thousands of dollars to fraudsters, the executive that exposes login credentials, or just the bank customer juggling remote work life, everyone is vulnerable to attack.

Here are a few things employees and consumers can do to improve their defenses:

- Avoid clicking links or dialing the phone number in emails or text messages. Contact the company using the information on their website or using the official mobile app. Chase customers can report relevant phishing emails to Chase Bank.
    - https://www.chase.com/digital/resources/privacy-security/security/report-fraud
- Ask for help from someone that knows how to spot phishing. Many organizations have implemented a process for employees to report suspicious messages, hopefully using a specialized anti-phishing and remediation solution. Some mobile providers have a service for submitting suspected smishing messages. There are several free lookup services on the internet:
    - https://www.cyren.com/security-center/url-category-check-gate
    - https://www.virustotal.com/gui/home/url
    - https://phishtank.org/
- At least for now, slow down. Many phishing attacks can be avoided by inspecting the message for spelling errors and other inconsistencies. Examine the copyright date in the email footer, make sure the URL in the browser location window is correct, and trust your instincts. If something seems fishy, it probably is phishy.