Geofenced Amazon Japan Credential Phishing Volumes Rival Emotet

proofpoint.com/us/blog/threat-insight/geofenced-amazon-japan-credential-phishing-volumes-rival-emotet

October 16, 2020

Geofenced Amazon Japan Credential Phishing Volumes Rival Emotet

October 16, 2020 Cassandra A. and the Proofpoint Threat Research Team

Introduction

Since August 2020, Proofpoint researchers have tracked extremely high-volume Amazon Japan credential and information phishing campaigns, with suspected activity dating back to June 2020. The messages pose as Amazon Japan, suggesting that the recipient needs to review their account for "confirmation of ownership" or "updated payment information". Upon clicking a link in the message, the recipient is taken to one of several variations of Amazon-themed credential phishing landing pages that collect credentials, personally identifiable information (PII), and credit card numbers. Messages have been sent both to Japan-based organizations and those with a presence in Japan. The pages are geofenced to ensure that only Japan-based recipients are taken to the credential phishing page.

While popular brands like Amazon are often abused in credential phishing campaigns, the volume of messages sets these campaigns apart from other Amazon-branded activity. The campaigns run continuously, sending hundreds of thousands of messages each day. As of mid-October, sometimes more than a million messages are seen in a single day, rivaling Emotet message volume.

Lures and landing pages

The messages are well-crafted Japanese language lures with subjects suggesting that the recipient's information needs an update or that their account has been locked:

- Amazon.co.jp アカウント所有権の証明（名前、その他個人情報）の確認 ("Confirmation of proof of ownership of Amazon.co.jp account (name and other personal information)") (Figure 1)
- お支払い方法の情報を更新 ("Updated payment method information") (Figure 2)

- アカウントがロックされたので、ご注意下さい ("Please note that your account has been locked") (Figure 3)

Amazon <info@bnwuabd.xyz> To [username] <username@companyname.tld>

Amazon.co.jp アカウント所有権の証明（名前、その他個人情報）の確認

amazon

Amazon お客様

Amazonチームはあなたのアカウントの状態が異常であることを発見しました。バインディングされたカードが期限が切れていたり、システムのアップグレードによるアドレス情報が間違っていたりして、あなたのアカウント情報を更新できませんでした。

リアルタイムサポートをご利用ください

お客様の Amazon アカウントは 24 時間 365 日対応のサポートの対象となっておりますので、Amazon サポートチームにご連絡いただければ、アカウントの所有権の証明をお手伝いします。

お客様の Amazon アカウント

アカウント所有権の証明をご自身で行う場合は、Amazon 管理コンソールにログインし、所定の手順でお手続きください。アカウント所有権の証明についてのヘルプセンター記事も併せてご参照ください。

状態:
異常は更新待ちです

所有権の証明

数日以内アカウント所有権をご証明いただかなかった場合、Amazonアカウントは自動的に削除されますのでご注意ください。

今後ともよろしくお願い申し上げます。
Amazon チーム

Figure 1: Lure with subject, "Confirmation of proof of ownership of Amazon.co.jp account (name and other personal information)"

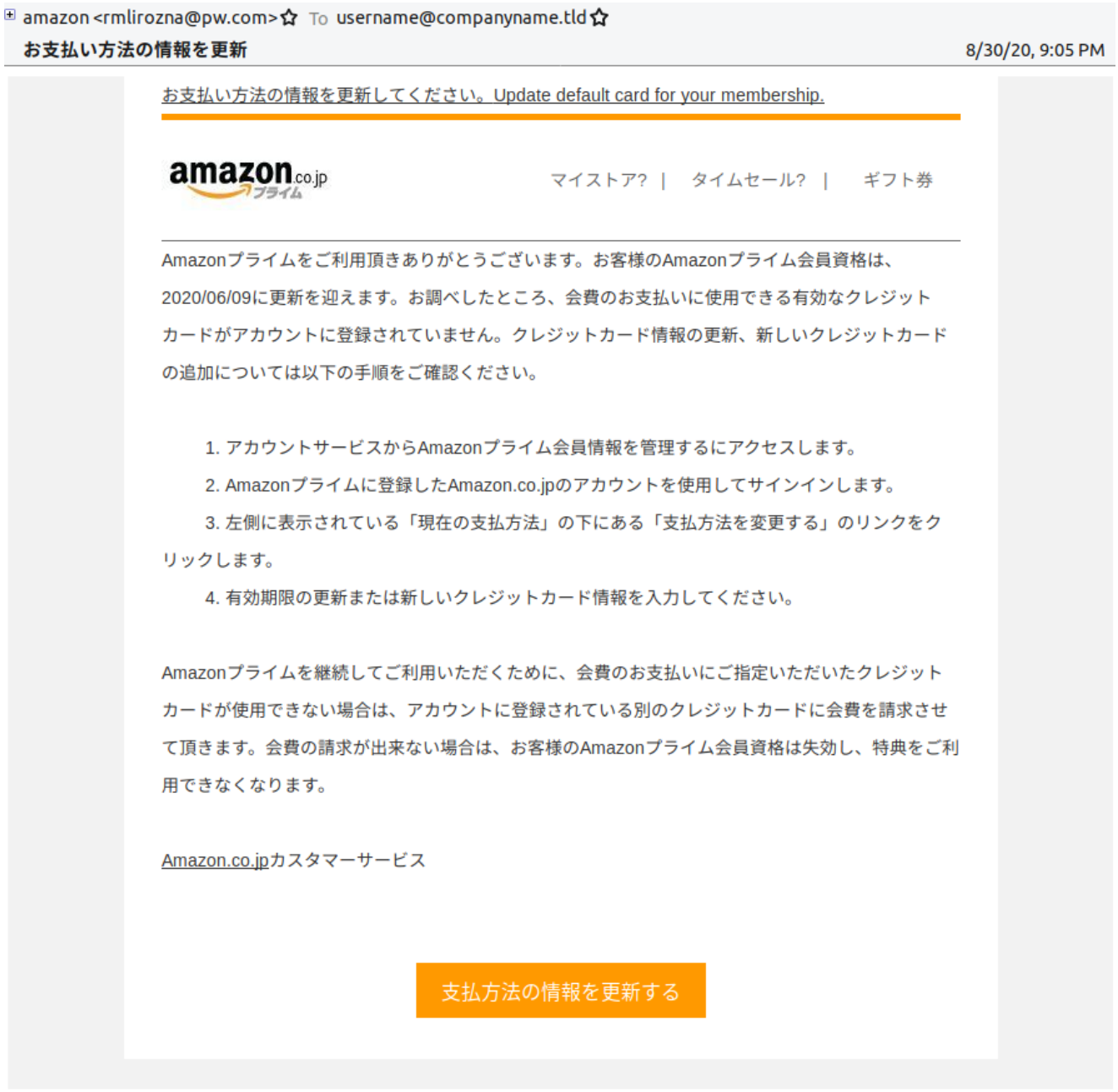

Figure 2: Lure with subject, "Updated payment method information"

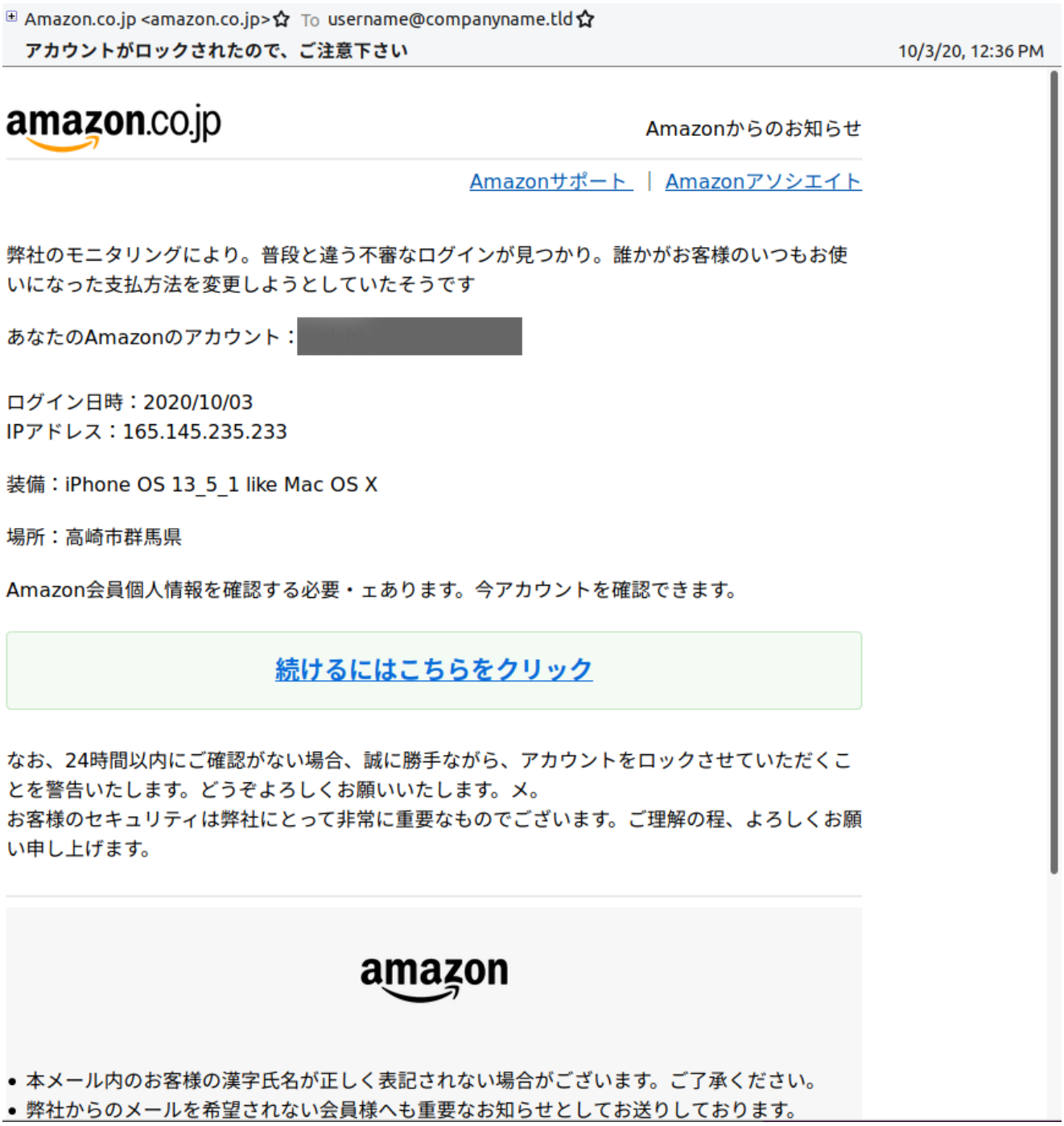

Figure 3: Lure with subject, "Please note your account has been locked"

Images in the messages, such as the Amazon logos, are hotlinked from free image hosting services, and the same image URLs have been observed across multiple campaigns.

The messages purport to be from Amazon, though they come from email addresses that initially were not disguised particularly well, such as these samples:

- rmlirozna[@]pw[.]com

- fwgajk[@]zfpx[.]cn
- info[@]bnwuabd[.]xyz
- dc[@]usodeavp[.]com

By early October 2020, we began to see a shift in effort to make the from address appear somewhat legitimate:

- amaozn[@]ama2on[.]buzz
- accout-update[@]amazon[.]co.jp
- account-update[@]amazon[.]com
- admin[@]amazon-mail[.]golf

In examining the message URLs, we see that they contain parameters for OpenID (Figure 4), the authentication protocol used by Amazon Japan. These URLs don't appear to take the user to an OpenID implementation, but the parameters in the URL string exist to provide legitimacy to the experience.

We identified what appear to be placeholder values in some URLs, suggesting perhaps some messages were prematurely sent, or that the corresponding values weren't available (Figure 4).

```
http://112.121.164.154/ap/signin?key=
%25%7BRECEIVER_ADDRESS%7D&openid.assoc_handle=jpflex&openid.claimed_id=
%25%7BRAND_TEXT_0%7D&openid.identity=
http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.mode=
checkid_setup&openid.pape.max_auth_age=0&openid.return_to=
https%3A%2F%2Fwww.amazon.co.jp%2F%3Fref_%3D
nav_em_hd_re_signin&ref_=nav_em_hd_clc_signin
```

Figure 4: URL with BRECEIVER_ADDRESS and BRAND_TEXT variables

We also identified use of what appears to be a placeholder email address in some URLs, "a@b.c" (Figure 5). In other URLs observed, the recipient email address populates this parameter.

```
http://45.76.229.172/ap/signin?key=
a@b.c&openid.assoc_handle=jpflex&openid.claimed_id=
http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.identity=
http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.mode=
checkid_setup&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&openid.pape.max_
auth_age=0&openid.return_to=https%3A%2F%2Fwww.amazon.co.jp%2F%3Fref_%3D
nav_em_hd_re_signin&ref_=nav_em_hd_clc_signin
```

Figure 5: URL with a@b.c and an OpenID path in place of variables

When clicked, the geofenced links in the message take the user either to a spoofed Amazon Japan login page (Figure 6), or if the user appears to be outside of Japan, to the actual Amazon Japan login page.

Figure 6: Spoofed Amazon Japan login page

Upon “logging in” with their Amazon username and password, the user is taken to a form that collects various pieces of PII, such as address, birthday, and phone number (Figure 7).

Figure 7: Information phishing landing page, requesting the user's country, name, birthday, zip/postal code, prefecture (state), street address, business name (optional), and phone number

The form also collects credit card numbers, which are loosely validated through a script hosted on the same site, and zip codes, which are validated via an API call to a third-party service (Figures 8, 9). Interestingly, the zip code we provided does not appear to be a legitimate Japanese zip code, though no errors were returned upon submitting the information.

Figure 8: Error indicating the credit card number originally provided (a random numeric string of the wrong length) is invalid

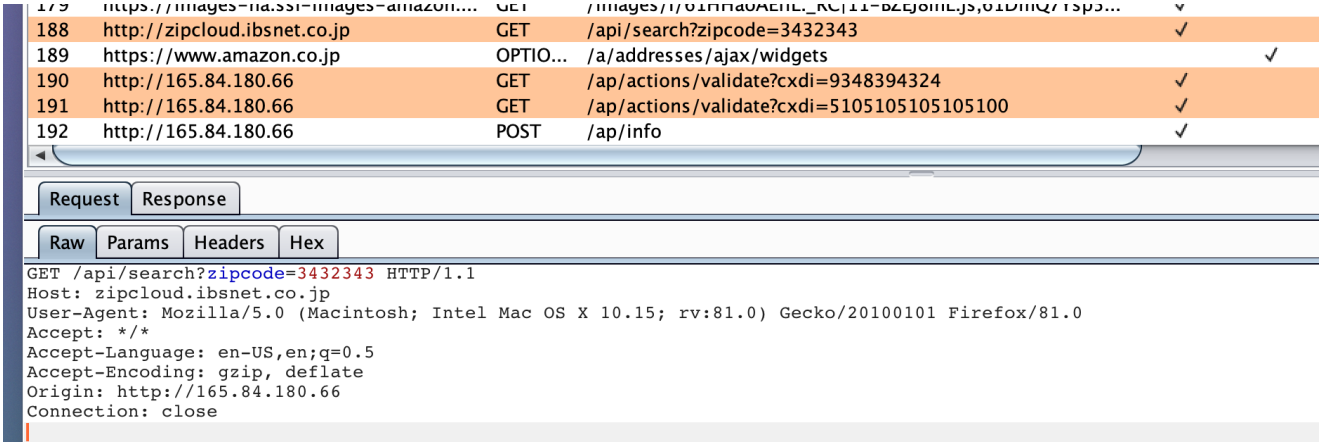

Figure 9: Intercepted traffic illustrating the call to "zipcloud.ibsnet[.]co.jp" for zip code validation, as well as calls to "/ap/actions/validate?cxdi=" for credit card number validation

After submitting valid information, users are thanked for updating their information, told they may now access their account, and redirected to the real Amazon Japan site at amazon.co[.]jp.

Figure 10: Post-submission page informing users that they may now access their account

Message volume

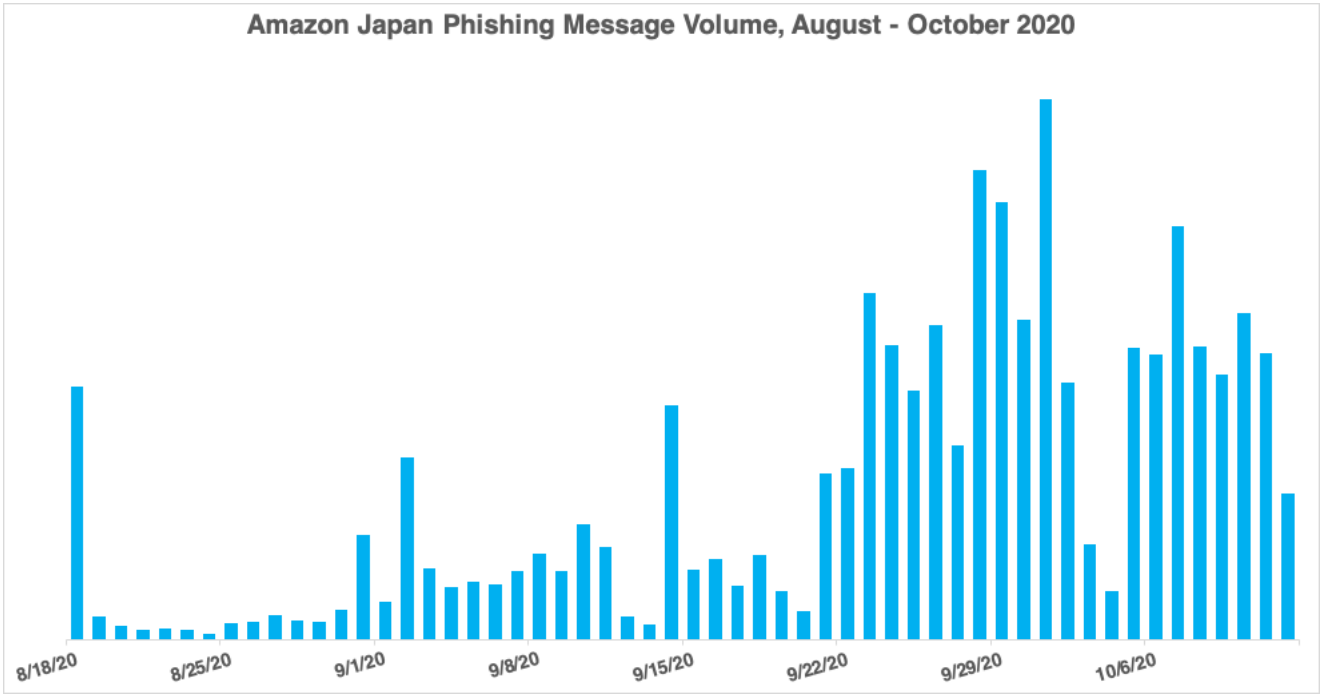

Figure 11: Message volume, August 2020 through October to date

Proofpoint has tracked these messages since mid-August, but we have identified activity as early as June 2020 that appears to be tied to the same actor. While the messages are in Japanese and the landing pages geofenced to Japanese IPs, there is no clear pattern among

recipients or industries, beyond being based in Japan or having business presence in Japan. Given the loosely linear trajectory of daily message volume observed through late August and September, volume could continue to increase over the coming months.

Month	Average Message Volume Per Day
August (from 8/18-8/30)	122,000
September	424,000
October (to date)	750,000

Infrastructure

Typically, the credential phishing landing page is an IP address, followed by "/ap/signin":

hxxp://103.192.179[.]54/ap/signin

Less often, a domain is used in lieu of an IP address:

oopozrjbpm[.]xyz/ap/signin

Hundreds of IP addresses have been used across multiple campaigns, as the actor tends to adopt new IP addresses for each campaign, rather than reuse IP addresses. IP addresses belong to a variety of autonomous systems, with no clear pattern among geographies or providers.

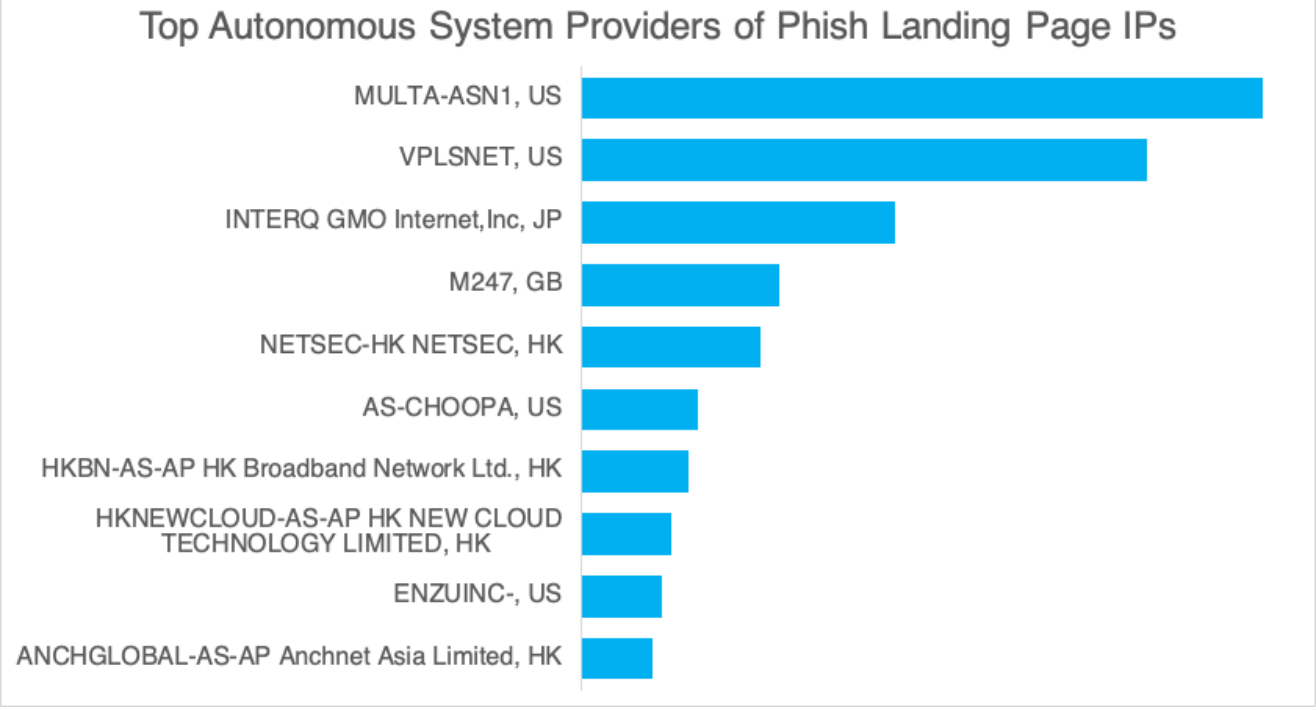

Figure 12: Top AS names for IP addresses used in lures from August 2020 through October to date

The domains used are *.xyz or *.cn TLDs, and some have been observed across multiple campaigns. The .xyz domains are registered through GoDaddy, while the *.cn domains has a sponsoring registrar of 阿里云计算有限公司（万网） (Alibaba Cloud Computing).

August 30-September 5 Campaign Landing Page Domains

Domain	Creation Date	Registrant Details
00pozrjbpm[.]xyz	2020-04-24	Registrant State/Province: Xiang Gang Registrant Country: CN
1mmmms2jy8[.]xyz	2020-06-14	Registrant State/Province: Xiang Gang Registrant Country: CN
4lz1qen0ls[.]xyz	2020-06-14	Registrant State/Province: Xiang Gang Registrant Country: CN
5b0rnizmhn[.]xyz	2020-04-24	Registrant State/Province: Xiang Gang Registrant Country: CN

While much of the registrant data for these domains was redacted at the time we checked, we did notice commonalities across ‘Creation Date’ and several of the registrant detail fields.

September 6-12 Campaign Landing Page Domains

Domain	Creation Date	Registrant Details
00pozrjbpm[.]xyz	2020-04-24	Registrant State/Province: Xiang Gang Registrant Country: CN
jiyingkou[.]cn	2019-09-20	Registrant: 王帅国 Registrant Contact Email: rxbnn3[@]163[.]com
enjinchang[.]cn	2019-09-19	Registrant: 王帅国 Registrant Contact Email: rxbnn3[@]163[.]com

juhaicheng[.]cn	2019-09-20	Registrant: 王帅国 Registrant Contact Email: rxbnn3[@]163[.]com
getongliao[.]cn	2019-09-20	Registrant: 王帅国 Registrant Contact Email: rxbnn3[@]163[.]com

Apart from 00pozrjbpm[.]xyz, reused from the August 30-September 5 campaign, the domains for the September 6-12 campaign share common traits. Like the previous set of domains, the creation dates and registrant information suggest that they may be related in some way. Moreover, "rxbnn3[@]163[.]com" is a prolific domain registrant, as this address appears as a registrant contact across 251 domains as of this publication. In addition to the domains associated with rxbnn3[@]163[.]com shown above, the email is also linked to a number of domain generation algorithm-like domains:

- swwkppe[.]cn
- lmkafwgi[.]cn
- pdscmkq[.]cn
- awsmgrc[.]cn

Conclusion

The Amazon brand is commonly spoofed by threat actors seeking credentials, but the volume and persistence of these campaigns set them apart from other Amazon-themed activity. The consistent reuse of message assets, landing pages, and steadily increasing message volume suggest that this activity could be driven by a botnet. Moreover, there is no apparent weekend lull in message volume, as we sometimes observe with less automated operations. If this is indeed powered by a botnet, it's unlikely that message volume will decrease soon. Threat actors often make incremental changes to their operations, and elements like different branding or collection of slightly different information could be easy pivot points for this actor over the coming months.

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
hxxp://182.16.26[.]194/ap/signin	URL	Amazon Japan credential phish landing page

hxxp://23.133.5[.]144/ap/signin	URL	Amazon Japan credential phish landing page
hxxp://43.249.30[.]212/ap/signin	URL	Amazon Japan credential phish landing page
00pozrjbpm[.]xyz/ap/signin	URL	Amazon Japan credential phish landing page
jiyingkou[.]cn/ap/signin	URL	Amazon Japan credential phish landing page
enjinchang[.]cn/ap/signin	URL	Amazon Japan credential phish landing page

Update 30 June 2021: Proofpoint is still tracking this activity however it is no longer using geofencing techniques.