# 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

f Blog <u>Threat Insight</u> 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 <u>Emotet</u> 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

# 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)"

🗄 amazon <rmlirozna@pw.com>🏠 🛛 username@companyname.tld 🏠</rmlirozna@pw.com>		
お支払い方法の情報を更新	8/30/20, 9:05 P	M
お支払い方法の情報を更新してください。Update default card for your membership	<u>p.</u>	
amazon.co.jp マイストア?   タイムセール?	ギフト券	
Amazonプライムをご利用頂きありがとうございます。お客様のAmazonプライム会	員資格は、	
2020/06/09に更新を迎えます。お調べしたところ、会費のお支払いに使用できる有効	効なクレジット	
カードがアカウントに登録されていません。クレジットカード情報の更新、新しい	クレジットカード	
の追加については以下の手順をご確認ください。		
1. アカウントサービスからAmazonプライム会員情報を管理するにアクセスし		
2. Amazonプライムに登録したAmazon.co.jpのアカウントを使用してサインイ	ンします。	
3. 左側に表示されている「現在の支払方法」の下にある「支払方法を変更する	\$」のリンクをク	
リックします。		
4. 有効期限の更新または新しいクレジットカード情報を入力してください。		
Amazonプライムを継続してご利用いただくために、会費のお支払いにご指定いたた	ゴいたカレンジット	
Amazon シットスを聴起してこれ用いたたくために、 気質のお支払いたとうたいた カードが使用できない場合は、アカウントに登録されている別のクレジットカード		
て頂きます。会費の請求が出来ない場合は、お客様のAmazonプライム会員資格は失		
て見らより。云貝の明示が出来ない場合は、の各様のAllia2017 クイム云貝貝格は大 用できなくなります。	「別し、村央をこれ」	
用できなくなります。		
Amazon.co.jpカスタマーサービス		
支払方法の情報を更新する		

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

10/3/20, 12:36 PM

amazon.co.jp

Amazonからのお知らせ

Amazonサポート | Amazonアソシエイト

弊社のモニタリングにより。普段と違う不審なログインが見つかり。誰かがお客様のいつもお使 いになった支払方法を変更しようとしていたそうです

あなたのAmazonのアカウント:

ログイン日時:2020/10/03 IPアドレス:165.145.235.233

装備:iPhone OS 13\_5\_1 like Mac OS X

場所:高崎市群馬県

Amazon会員個人情報を確認する必要・ェあります。今アカウントを確認できます。

<u>続けるにはこちらをクリック</u>

なお、24時間以内にご確認がない場合、誠に勝手ながら、アカウントをロックさせていただくこ とを警告いたします。どうぞよろしくお願いいたします。メ。 お客様のセキュリティは弊社にとって非常に重要なものでございます。ご理解の程、よろしくお願 い申し上げます。

# amazon

• 本メール内のお客様の漢字氏名が正しく表記されない場合がございます。ご了承ください。

• 弊社からのメールを希望されない会員様へも重要なお知らせとしてお送りしております。

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 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.

Amazonログイン ×	- +	- 6	0
$\leftrightarrow$ $\rightarrow$ C (i) Not secure   10	04.194.247.149/ap/signin?openid.pape.max_auth_age=0&openid.return_to=https%3A%2F%2Fwww.amazon.co.jp%2F%3Fref_%3Dnav_em_hd_re_signin&openid.identity= 🛧		8
	D グイン Eメールまたは携帯電話番号		
	利用現象 プライバシー現象 ヘルプ © 1996-2020, Armazon.com, Inc. or its affiliates		

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).

0	•	
9	٩,	http://143.92.51.22/ap/info

#### amazon

#### アカウントサービス>お支払い方法の追加・変更

AmAzon セキュリティシステム. 私たちは最近、珍しいログイン活動を発見しました. アカウントを保護するには、必要な手順を続けてください.

国/地域 Japan				
氏名				
生年月日				
年 🗸	月	~	В	~
郵便番号				
-				
節道府県				
都道府県を选択				`
住所				

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.

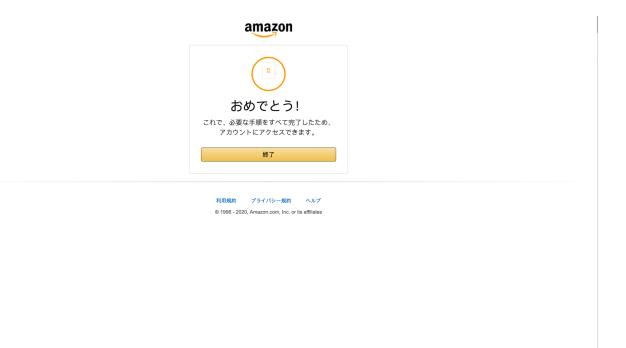
adsdarigile         Rate state s	
Cobaldbool       Anol         Jacobaldbool       - 1日ともに愛敬可能         ・1日ともに愛敬可能       - 1日ともに愛敬可能         Dobaldbool       - 1日ともに愛敬可能         Stativity       - 1日としていただけま         Stativity       - 1日としていただけま         Ot       - 1日としていただけま         Stativity       - 1日としていただけま         - コードを追加       - 1日としていたさい         - コードを追加       - 1日としていたさい         - コードを追加       - 1日としていたさい         - コードを追加       - 1日としていたちの         - 11日       - 1日としていたちの         - 11日       - 11日         - 11日       - 11日	
BROREGADE 2         ・1日ともに愛取可能            あた支払い方法         な支払い方法の追加・変更         おなかがすぶの追加・変更         おなかがずかるの追加・変更         おなかがずかったである         またはデビットカードの番号を入力してください             たちジットカード         ひいが、からの思想ののなどのかな知用いただけ             びいる               ・             ・	配達を支援するために使用することがあります。
<ul> <li>◆土日ともに愛敬可能</li> <li>              A ち支払い方法             な変し                  A支払い方法の追加・変更                  A客様の個人情報を安全に送信するために             第二者によるデータの改ざんや盗用を防い                Abbdクレジットカードあたはデビットカードの番号を入力してください                 PLジットカード             び下のクレジットカードをご利用いただけ                OK                 MTA               Mac                 MTA               Mac                 MTA               Mac                 MTA               Mac                 MTA               Mac                 Jane Kaba               Mac                 Jane Kaba               Mac                 Jassabassa               Jassabassa                 Jassabassa               Jassabassa                 Jassabassa               Jassabassa                 Jassabassabassa               Jassabassa                 Jassabassa               Jassabassa                 Jassabassa               Jassa</li></ul>	このお届け先の配送オプション
エお支払い方法の追加・変更         お客様の個人情報を安全に送信するために第三者によるデータの改ざんや盗用を防い         かのクレジットカード         シアのクレジットカードをご利用いただけま         シアのクレジットカードをご利用いただけま         シア・ケードを追加         カードを追加         カードを追加         カードを認知         クリジャカードをご利用いただけま         シア・ケードを追加         カードを追加         カードを追加         カードを追加         カードを追加         シードを追加         10       2023	周末の配送可否设定
お支払い方法の追加・変更       お客様の個人情報を安全に送信するために第三者によるデータの改ざんや盗用を防い         かのセレジットカード       市がなクレジットカードあたはデビットカードの番号を入力してください         グレジットカードをご利用いただけま       OK         ジドクヘレジットカードをご利用いただけま       OK         ジェク       ヘードを追加         カードを追加       カード番号         3958483939383838383838       9348394324         10       2023	- 土日ともに受取可能
お客様の個人情報を安全に送信するために 第三者によるデータの改さんや盗用を防い クレジットカード 以下のクレジットカードをご利用いただけま 「「「「「「「「「」」」」」 「「」」」 「」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」 「」」 「」」」 「」」 「」」 「」」」 「」」」 「」」」 「」」」 「」」 「」」」 「」」 「」」 「」」 「」」 「」」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」」 「」」 「」」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」」 「」」」 「」」 「」」 「」」 「」」 「」」」 「」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」 「	お支払い方法の追加・変更 ちかなり、ジットカードまたはデビットカードの基準を入力してください。
クレジットカード       OK         以下のクレジットカードをご利用いただけま       OK         ジンパSA       (************************************	お客様の個人情報を安全に送信するために、
以下のクレジットカードをご利用いただけま         いス       シードを追加         カードを追加       カード番号         39584839393838383838       9348394324         セキュリティコード       有効期限         3432       10       2023	
<ul> <li>ヘカードを追加</li> <li>カード情報を入力してください</li> <li>カード名義人(半角ローマ字)</li> <li>カード番号</li> <li>39584839393883883838</li> <li>9348394324</li> <li>セキュリティコード</li> <li>有効期限</li> <li>3432</li> <li>10</li> <li>2023</li> </ul>	
カード情報を入力してください カード名義人(半角ローマ字) カード番号 39584839398383838338 9348394324 セキュリティコード 有効期限 3432 10 * 2023 *	👫 VISA 🛶 📰 🄐 📷
カード名義人(半角ローマ字)     カード番号       395848393938383838383     9348394324       セキュリティコード     有効期限       3432     10	ヘカードを追加
39584839393838383838     9348394324       セキュリティコード     有効期限       3432     10 ・	カード情報を入力してください
セキュリティコード     有効期限       3432     10	カード名義人(半角ローマ字)カード番号
3432 10 • 2023 •	3958483939383838383838 9348394324
	セキュリティコード 有効期限
<u>抵行</u> 抵行	3432 10 • 2023 •
統行	
	統行

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

113	nups.//inayes-na.ssi-inayes-amazon	UEI	/IIIIayes/I/OINTAOAEIILNCIII-DEEJOIIIL.js,OIDIIIQ/ISP3	<b>v</b>			
188	188 http://zipcloud.ibsnet.co.jp GET /api/search?zipcode=3432343 √						
189	189 https://www.amazon.co.jp OPTIO /a/addresses/ajax/widgets √						
190	http://165.84.180.66	GET	/ap/actions/validate?cxdi=9348394324	$\checkmark$			
191	http://165.84.180.66	GET	/ap/actions/validate?cxdi=5105105105105100	~			
192	http://165.84.180.66	POST	/ap/info	$\checkmark$			
			7				
Reau	uest Response						
Raw Params Headers Hex							
Raw	Params Headers Hex						
GET /a	api/search?zipcode=3432343 HTTP/1.1						
	zipcloud.ibsnet.co.jp						
		Mac OS	X 10.15; rv:81.0) Gecko/20100101 Firefox/81.0				
Accept: */*							
Accept-Language: en-US,en;g=0.5							
Accept-Encoding: qzip, deflate							
Origin: http://165.84.180.66							
Connection: close							
Connection: close							

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

Waiting for 165.84.180.66

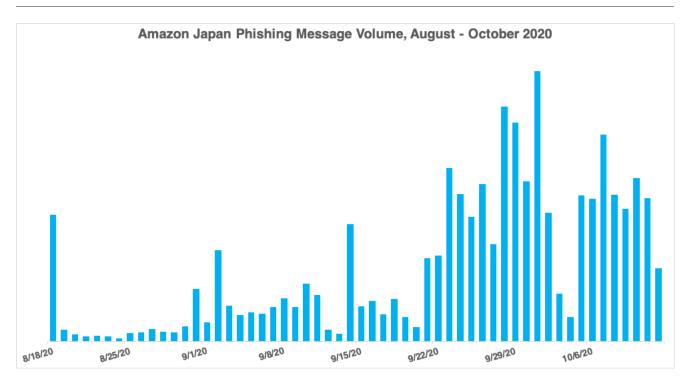


Figure 11: Message volume, August 2020 through October to date

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

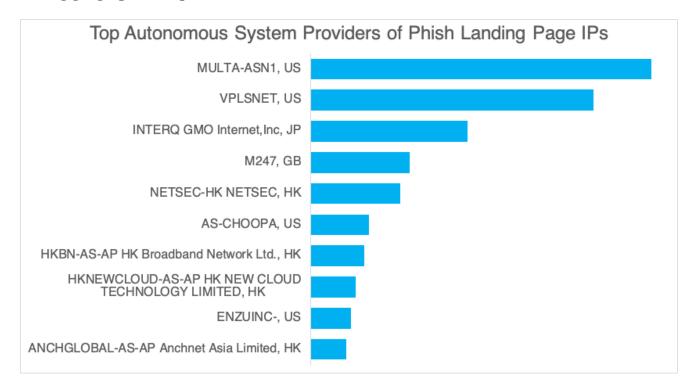
Typically, the credential phishing landing page is an IP address, followed by "/ap/signin":

```
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 <u>sponsoring registrar</u> of 阿里云计算有限公司(万网) (Alibaba Cloud Computing).

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

#### August 30-September 5 Campaign Landing Page Domains

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 oopozrjbpm[.]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 <u>domain generation algorithm</u>-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	ІОС Туре	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.

Subscribe to the Proofpoint Blog

Select