URLZone top malware in Japan, while Emotet and LINE Phishing round out the landscape | Proofpoint US

By June 19, 2019 Proofpoint Threat Insight Team

Published: 2019-06-19 · Archived: 2026-04-05 17:28:31 UTC

Overview

In many ways, the threat landscape in Japan resembles global trends, with the regionalization and widespread distribution of Emotet, and the steady increase in campaigns that utilize sophisticated social engineering techniques. However, while Emotet dominated malicious message volumes in many regions worldwide, URLZone, which primarily appears in Japan, remains the top email threat by volume in the region.

URLZone is currently loading the Ursnif banking Trojan configured with web injects for Japanese banks, making Ursnif a top payload in Japan as well. In the past, we have observed the long-running URLZone banker [1] loading Vawtrak and other banking Trojans and continue to monitor the distribution of both URLZone and Emotet as the latter further cements its dominance in the global landscape. It is worth noting that, while Emotet appears to be in something of a hiatus since the end of May, URLZone/Ursnif campaigns have continued, paralleling Ursnif activity in other geographies.

Campaigns

Since the beginning of 2019, numerous threat actors tracked by Proofpoint researchers conducted dozens of high-volume campaigns involving hundreds of thousands of messages that specifically geo-targeted Japan. These campaigns affected thousands of Japanese organizations, delivering banking Trojans, phishing attacks, impostor attacks, and spam at scale.

In particular, these campaigns included emails delivering the URLZone banking Trojan and engaging in LINE credential phishing. Many of these threats target Japan specifically; however, the region is also frequently included in global or multinational campaigns. These campaigns are typically sent by financially motivated cybercriminals.

Below is a brief overview of the malware payloads we frequently observe in campaigns affecting Japanese organizations.

URLZone and Ursnif

URLZone, also known as Bebloh or Shiotob, is a banking Trojan that first appeared in 2009. This is a well-established banker that we continue to observe regularly in Japanese geo-targeted campaigns a decade after its introduction. However, at this point, it appears that a single, high-volume actor remains the only distributor of URLZone.

Proofpoint researchers have observed email messages containing malicious Microsoft Excel documents with macros that, when enabled, install URLZone (Figure 1). In these campaigns, URLZone appears to be used as an initial payload, which then installs Ursnif.

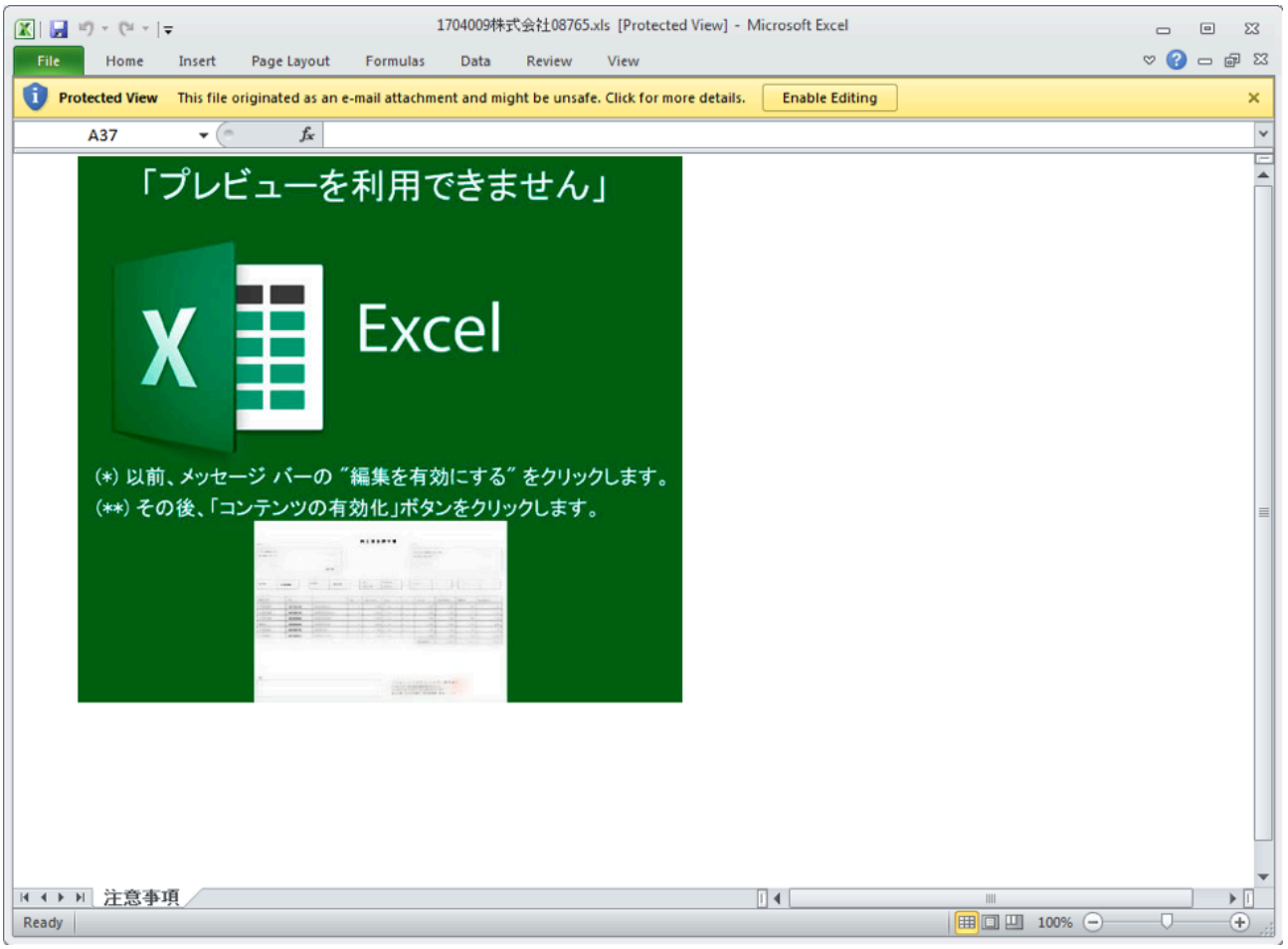

Figure 1: Example Microsoft Excel spreadsheet emailed to a Japanese recipient containing macros that, once enabled, install URLZone

Many of these campaigns reference invoices or payments. One recent campaign appeared to come from multiple random sending addresses with subjects such as :

- "FW: 請求書を送信致します。" ("We will send you an invoice")
- "Re: 請求書の送付" ("Send invoice")
- "Re: 請求書送付のお願い" ("Request for billing")
- "契約書雛形のご送付" ("Sending the contract form")
- "ご案内[お支払い期限:06月18日]" ("Information [Payment Deadline: Jun. 18]")
- "請求書の件です。" ("Invoice")
- "請求書送付" ("Invoicing")

Figure 2 shows an example email from this campaign.

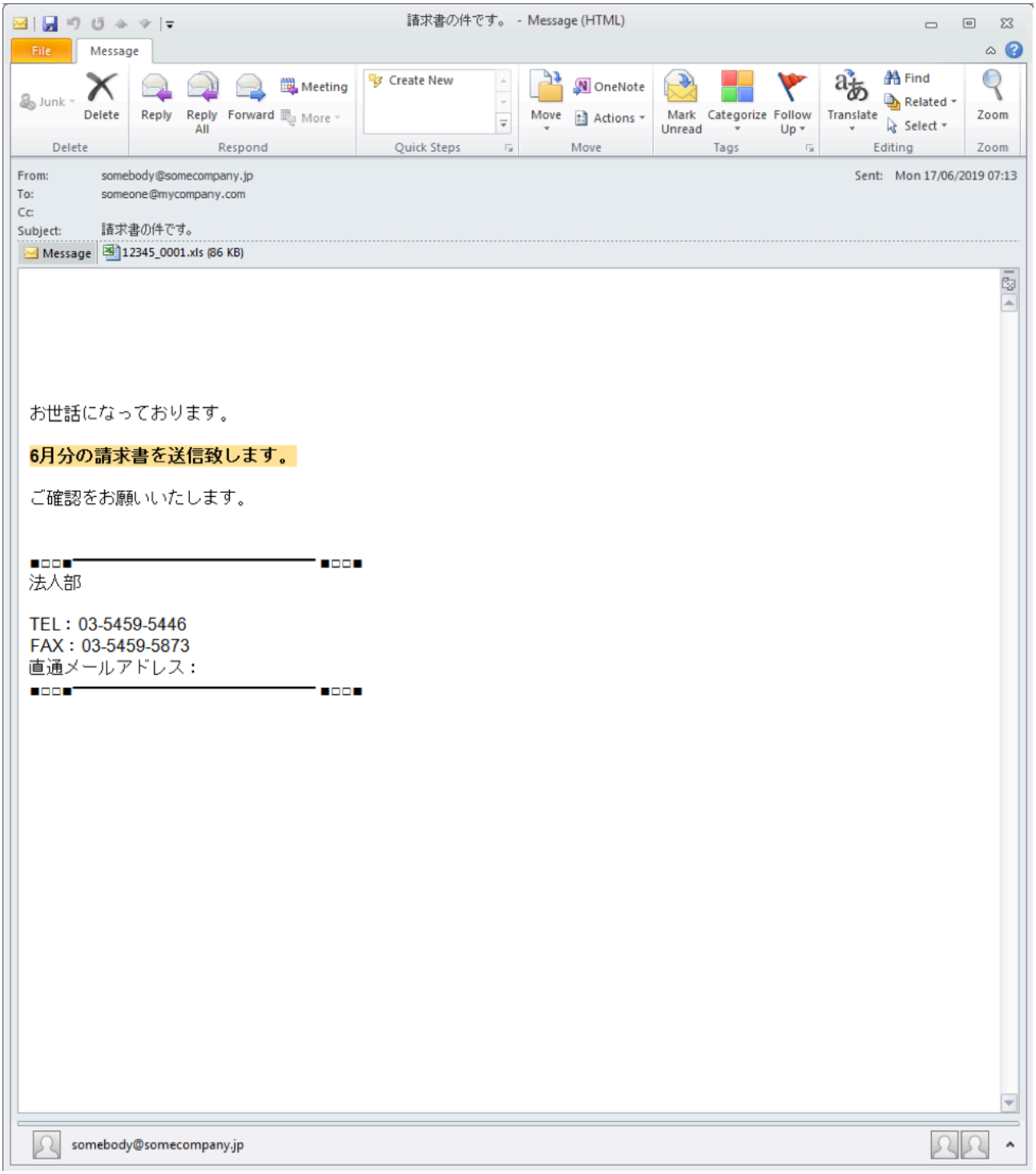

Figure 2: Sample email delivering URLZone/Ursnif on June 17, 2019

Most of these campaigns appear to originate with a single actor who operates primarily in Japan and Italy. The actor frequently employs steganography [2] - embedding malicious code in the “least significant bits” of color data in image files - as part of their geo-targeting. The macros also use multiple layers of obfuscation and various locale and language checks to ensure the victim machine is in Japan before downloading and decoding the initial payload. Examples of recent language and locale checks include:

- Excel: "Application.International(xlCountrySetting)" begins with "8" (international Dialling Code for Japan is 81)

- PowerShell error for non-existent command contains "用語 " ("The term" in Japanese)
- PowerShell cmdlet: 'Get-date' (needs to contain "年" - "Year" in Japanese)
- PowerShell cmdlet: 'Get-Culture."LCID"' needs to contain "04" (Japanese LCID is "1041")

Once URLZone determines the host environment is suitable, URLZone downloads Ursnif, which begins stealing information and operating as a more “typical” banker. [3]

Proofpoint researchers have tracked Ursnif in Japan-focused campaigns since at least March 2017. While the actor we refer to as TA544 is responsible for much of the recent Ursnif volume in Japan via initial URLZone infections, we have observed other actors distributing Ursnif variants directly. At this point, Ursnif is the most common commodity banker, both worldwide and in Japan.

Emotet

Emotet is a robust global botnet that loads third-party malware and its own modules used for spamming, credential stealing, network spreading, and email harvesting.

On April 12, 15, and 16, an actor tracked by Proofpoint threat researchers as TA542 [4] launched high-volume campaigns impacting Japan (among other countries) and targeting a wide range of industries. A large percentage of the messages in these campaigns were sent to organizations in Japan, which was noteworthy because Japan was not one of the core geographies consistently targeted by Emotet. However, the actors behind Emotet are adept at localization and have been expanding their activities into new regions regularly. Since the end of May, Emotet campaigns have largely paused; we will continue to monitor for new activity in Japan and elsewhere.

Figure 3 shows a typical message with an attached malicious Microsoft Word document. These documents contained macros that, when enabled, installed an instance of Emotet.

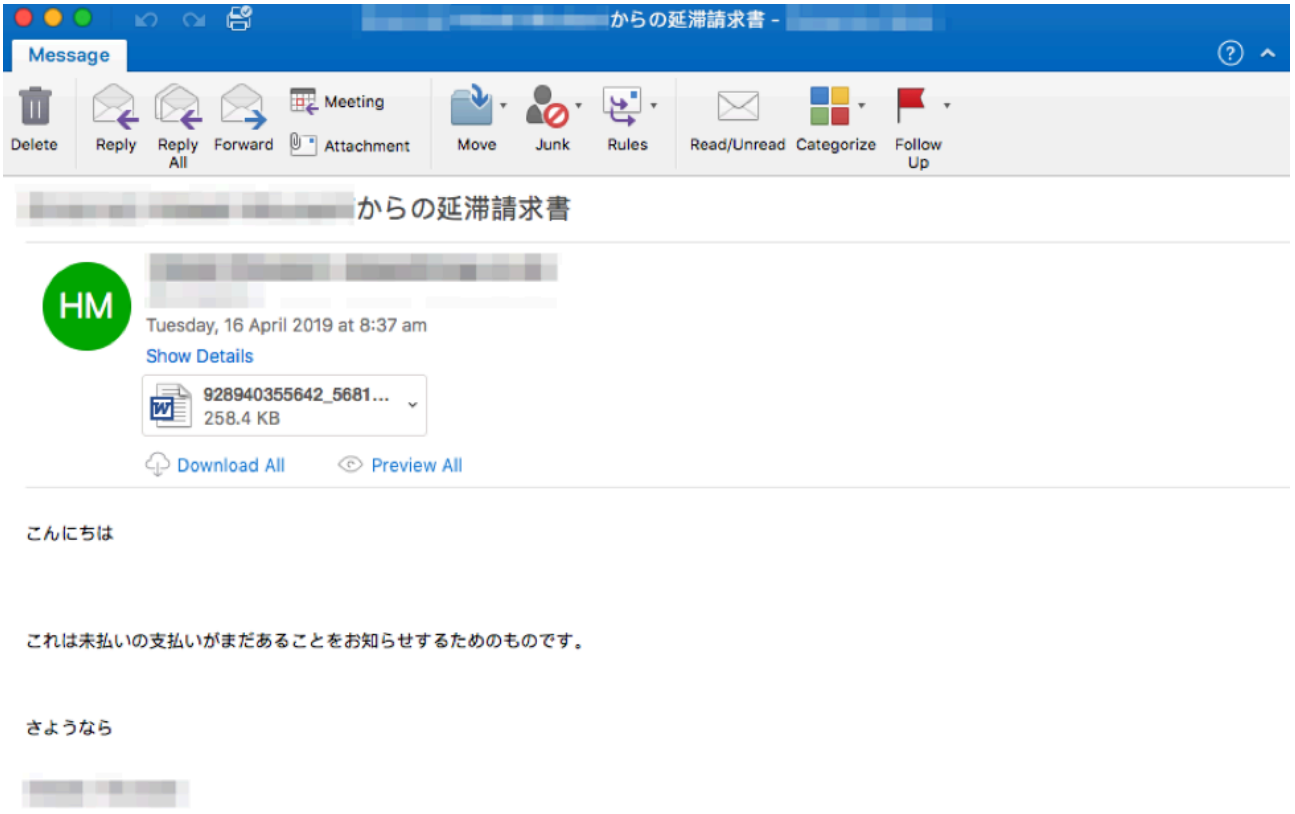

Figure 3: Example email sent to a Japanese recipient with an attached document with macros that, once enabled, install Emotet

TA505 and FlawedAmmyy

In February of 2019, Proofpoint researchers observed new Japan-focused campaigns from TA505 [5], a threat actor that recently has been focused on China, South Korea, Latin America, and the Middle East, distributing the FlawedAmmyy Remote Access Trojan (RAT) [6].

FlawedAmmyy is based on the leaked source code for Version 3 of the Ammyy Admin remote desktop software, a shareware utility used for IT support purposes. As such, FlawedAmmyy contains the functionality of the leaked version, including:

- Remote Desktop control
- File system manager
- Proxy support
- Audio Chat

FlawedAmmyy is distributed via emails with document attachments. These attachments are either Microsoft Excel (.xls) or Word (.doc) attachments with macros that, if enabled, download FlawedAmmyy (Figure 4).

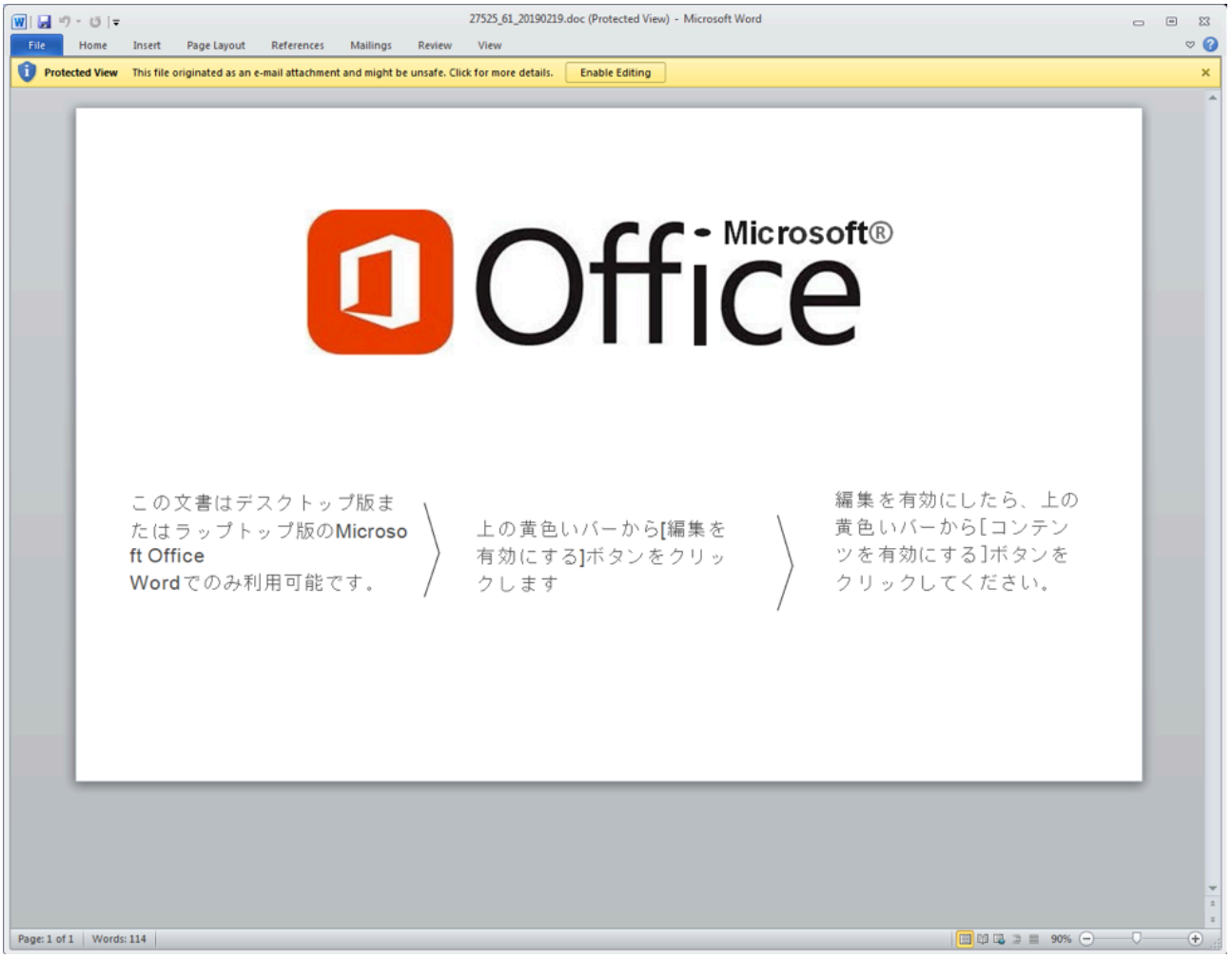

Figure 4: FlawedAmmy RAT being distributed using Microsoft Office Attachments.

While the volume of these campaigns was only in the thousands of messages, TA505 has been particularly focused on Asia and the Middle East recently; it is noteworthy when this prolific actor begins targeting a new region.

Human Centric Threats

While a variety of emails distributing malware demonstrate examples of targeting and payloads unique to Japan, internationally ubiquitous phishing attacks, business email compromise (BEC), and other forms of imposter attacks remain ongoing threats. In particular, we regularly observe:

Credential Phishing

This is the most common type of phishing observed by Proofpoint researchers. These emails target a victim's login credentials such as usernames and passwords for a range of sites and services. These campaigns are usually high-volume emails with linked or embedded spoofs of login pages for reputable entities including banks, universities, electronic signature services, and social media and file sharing platforms. Figure 5 shows an example of a phishing landing page targeting banking customers in Japan, attempting to steal a variety of personal data.

Figure 5: Credential Phishing for a Japan Post Bank customer (Source: https://www.antiphishing.jp/news/alert/jpbank_japanpost_20190304.html)

One notable type of credential phishing we have observed targets users of the LINE service. LINE is one of the most popular messaging apps in Japan, Thailand, and Taiwan, with approximately 165 million users across those countries. LINE is similar to Whatsapp, Facebook Messenger, or WeChat in China and has roughly 78 million monthly active users in Japan.

Proofpoint researchers have been observing emails messages with LINE credential phishing links targeting organizations in Japan (Figure 6). For example, these messages used subjects such as "[LINE]安全認証" which translates to "[LINE] Safety certification".

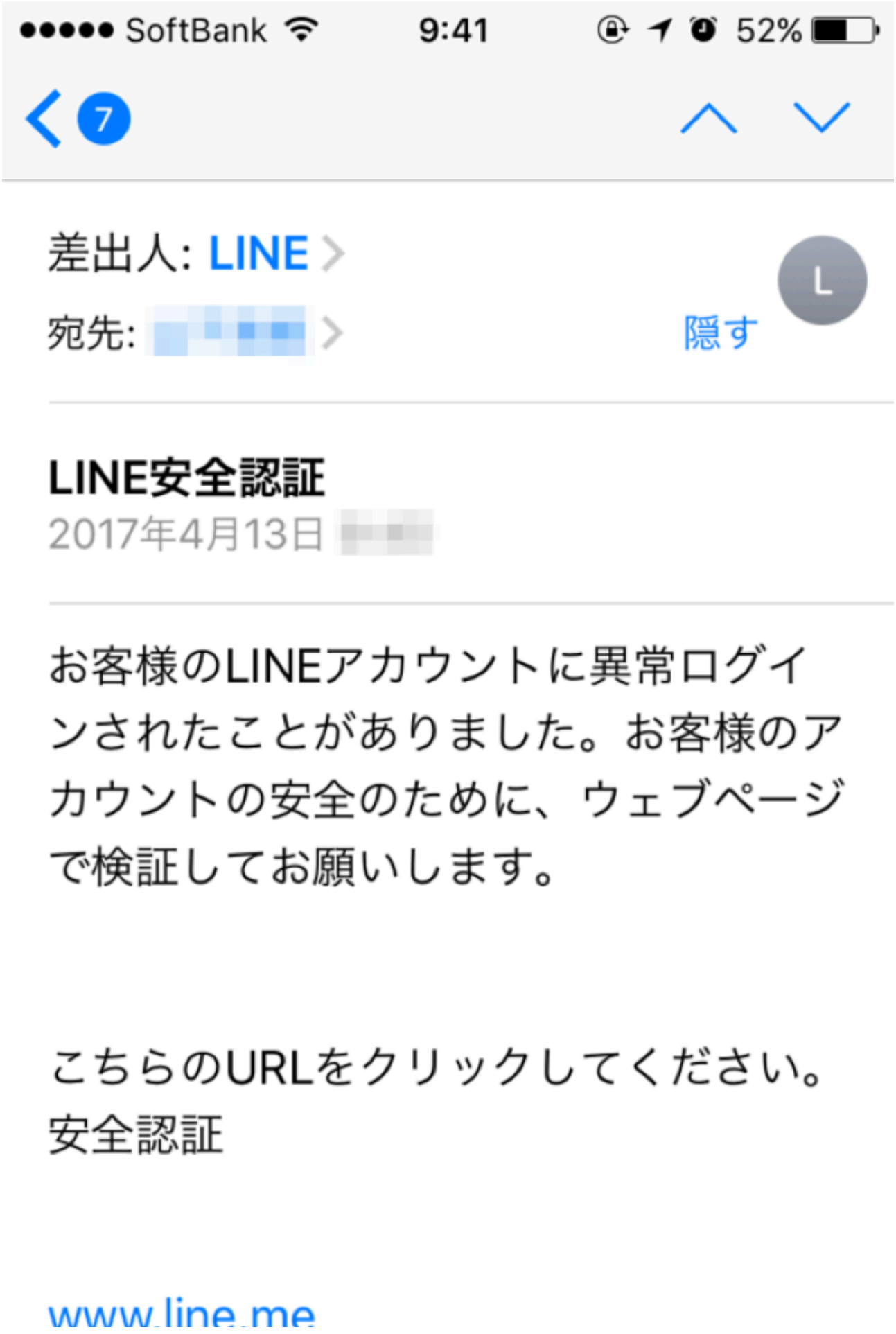
●●●●● SoftBank
9:41
52%
7
差出人: LINE
L
宛先:
隠す
LINE安全認証
2017年4月13日
お客様のLINEアカウントに異常ログインされたことがありました。お客様のアカウントの安全のために、ウェブページで検証してお願いします。
こちらのURLをクリックしてください。
安全認証
www.line.me

Figure 6. An example phishing lure on the LINE app in Japan. (Source: Cyamax.com)

While this particular type of human factor compromise is fairly simple in its implementation - a standard phishing-type of attack which uses the stolen branding of a recognizable legitimate commercial entity - the pervasiveness of LINE in Japan makes this type of phishing notable. Moreover, because many users repeat credentials among services, stealing credentials from LINE can net threat actors credentials for many other apps and platforms.

Impostor Threats

Impostor threats include malicious emails with the intent of attempting to impersonate a person, commercial entity, or respected brand, such as a bank or an internet service provider. This type of imposter activity could be used for financial fraud, including business email compromise (BEC), in conjunction with other social engineering mechanisms to achieve their desired result, whether delivery of malware, credential phishing, or further network compromise.

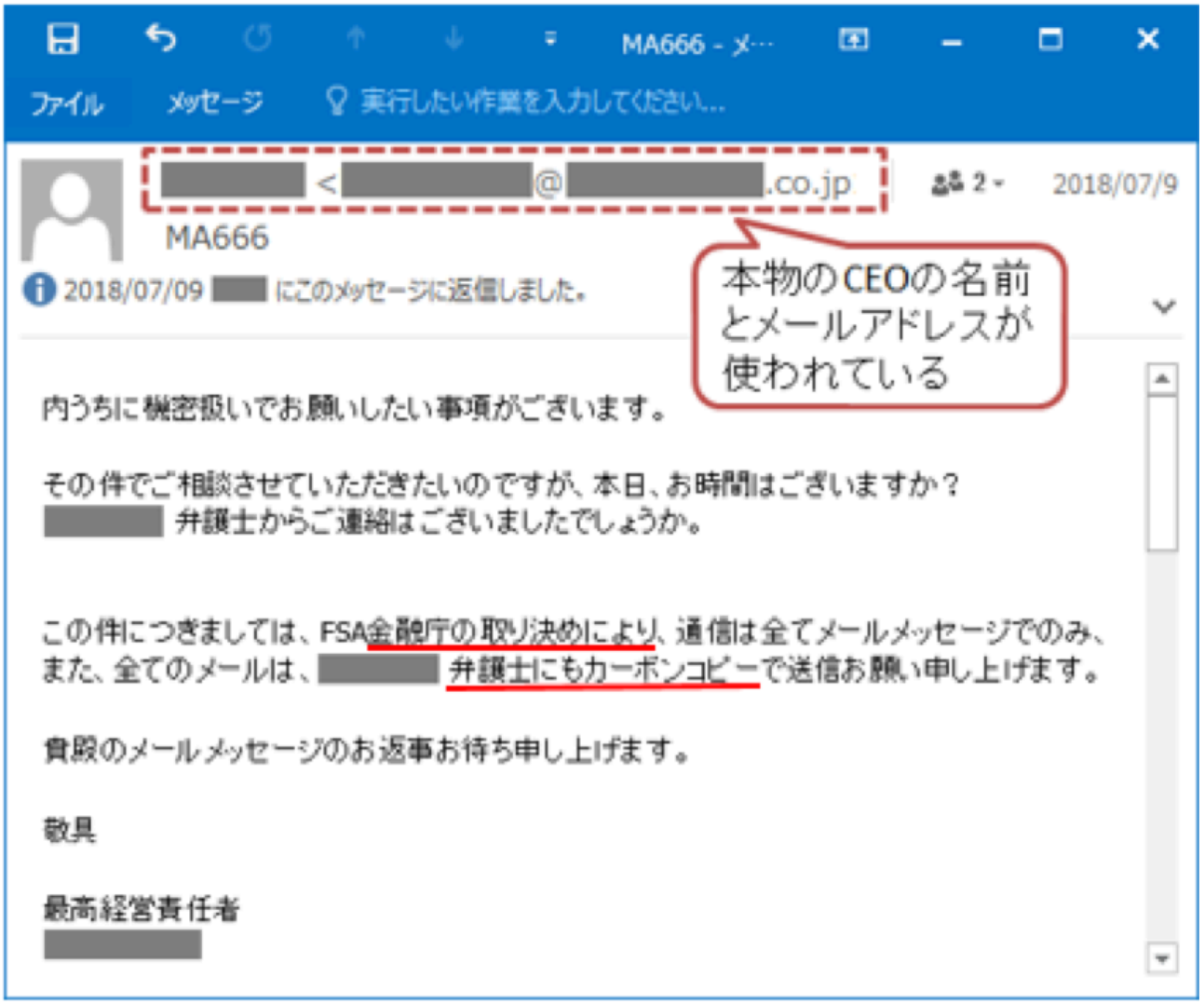

Figure 7: An example of a threat actor engaging in business email compromise (BEC) with a Japanese target. BEC is a type of known imposter activity relying on social engineering without any links or attachments leading to malware or phishing kits. (Source: https://www.ipa.go.jp/security/announce/201808-bec.html)

While BEC remains fairly rare in Japan when compared with other nations, due to the uniqueness and difficulty of interacting in the Japanese language for non-native speakers and thus presenting difficulty for constructing effective lures, this type of human factor-oriented attack is increasing in popularity worldwide.

Conclusion

In 2019, threats specific to Japanese organizations and business interests, whether abusing Japanese brands or geo-targeted malware and credential phishing campaigns, mean that defenders at companies within Japan must be cognizant of highly targeted attacks as well as broad-based international attacks.

Ursnif and the Emotet botnet are the most prevalent malware threats affecting Japan, creating palpable risks for organizations and individuals by utilizing compelling lures and sophisticated social engineering mechanisms.

While Japan-targeted threats are not new, URLZone in particular, with its unique application by a single prolific actor in the region, sets Japan apart from other geographies. The Japanese language also creates unique

challenges for non-native speakers in crafting effective social engineering approaches, but high volumes of Ursnif and Emotet suggest that financially motivated actors may have “cracked the code,” creating emerging risks for defenders, organizations, and consumers in the region. As always, a combination of layered defenses and end user education is critical to protecting data, intellectual property, and critical infrastructure in the face of increasing attacks targeting the region.

References

[1] https://www.proofpoint.com/us/threat-insight/post/Vawtrak-UrlZone-Banking-Trojans-Target-Japan

[2] https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/

[3] https://www.cybereason.com/blog/new-ursnif-variant-targets-japan-packed-with-new-features

[4] https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service

[5] https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter

[6] https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat

---