Threat Actor Profile: TA544 targets geographies from Italy to Japan with a range of malware

proofpoint.com/us/threat-insight/post/threat-actor-profile-ta544-targets-geographies-italy-japan-range-malware

July 4, 2019

Blog
Threat Insight
Threat Actor Profile: TA544 targets geographies from Italy to Japan with a range of malware

July 11, 2019 Proofpoint Threat Insight Team

Overview

Proofpoint researchers began tracking an actor (referred to as TA544) in February of 2017 when reports first emerged about malicious email campaigns targeting Italian customers using the Panda Banker malware.

To date, this highly financially-motivated actor has delivered more than six unique malware payloads (in several variations of each) in high-volume campaigns (hundreds of thousands of messages per day) to victims across western Europe and Japan, where it now focuses on the distribution of the Ursnif banking Trojan and URLZone banker.

Also Read:

- Holiday Lull? No So Much
- URLZone top malware in Japan, while Emotet and LINE Phishing round out the landscape

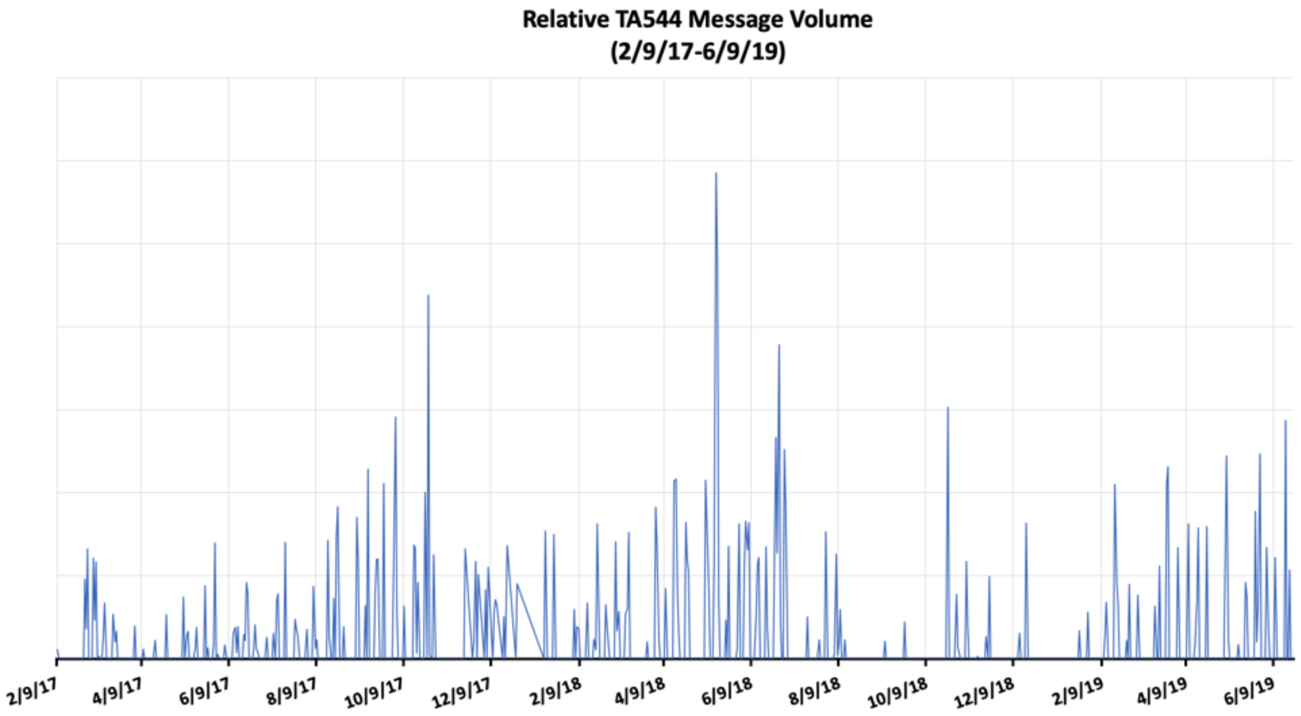


Figure 1: Relative TA544 message volume between February 2017 and June 2019

Ursnif: The preferred malware payload of TA544

Ursnif is a common banking Trojan that can:

- Steal stored data including passwords from banking websites via web injections, proxies and VNC connections
- Update itself or install modules remotely

Ursnif has many variants and names such as Dreambot, ISFB, Gozi, and Papras; it is typically distributed in high volume campaigns (hundreds of thousands or millions of messages).

Ursnif 1000

Ursnif 1000, the affiliate ID that is most closely associated with TA544, is typically distributed in high-volume campaigns (hundreds of thousands of messages per day) that often target the IT, technology, and marketing/ industries in Japan.

Most Ursnif 1000 campaigns use a robust combination of geofencing techniques to verify that users are located in Japan. Messages from these campaigns drop their payloads via Microsoft Excel documents with macros, that when enabled, download URLZone (another banking Trojan), which, in turn, download Ursnif 1000.

Ursnif 4779

Ursnif 4779 is typically distributed in moderate volume campaigns (tens of thousands of messages per day) that often target technology, manufacturing, and IT verticals in Italy. Like Ursnif 1000, this variant is also associated with TA544.

Additionally, Ursnif 4779 shares much of its geofencing locale/language check techniques with Ursnif 1000. Ursnif 4779 is deployed via one of two primary methods: (1) Microsoft Excel attachments with malicious macros, that, when enabled, install Ursnif along with a complex symmetric block cipher that is referred to as a “serpent key”, or (2) steganographic images that conceal malicious PowerShell commands which install Ursnif.

Delivery

Ursnif delivery methods vary by circumstance, depending on the targeted vertical and geography. Ursnif shares code with many other banking Trojans and the source code for an earlier version was distributed on online forums for free. Often, malware authors modify or adapt Ursnif code to serve particular purposes.

Ursnif can be deployed as a primary or secondary payload. It may be delivered via password-protected Zip files; Microsoft Office document attachments with malicious macros; or compressed JScript, JavaScripts, or Visual Basic scripts. However, the most common vectors for TA544 campaigns are messages with Microsoft Office documents that contain macros, that, when enabled, install URLZone and/or Ursnif.

Trends

As of 2019, Ursnif is one of the most prevalent banking Trojans in the threat landscape. In Q4 2018, we observed Ursnif consistently reaching peak message volume.

Because of Ursnif’s variable nature, it is difficult to identify trends in delivery strategies. Payload delivery is largely dependent on the threat actor, geography, and targeted verticals. However, recent TA544 campaigns typically deploy Ursnif via Microsoft Office attachments equipped with malicious macros that install the Ursnif banking trojan. Ursnif is sometimes delivered as a standalone payload, but as in the case of TA544 with its campaigns in Japan, it is more often deployed with other malware including URLZone.

Objectives

TA544 is a financially motivated actor that uses a variety of payloads to target both European and Asian geographies. Proofpoint researchers have been able to identify commonalities between the European and Asian campaigns, despite the differences in targeting and geographic location.

One notable characteristic of TA544 is their use of steganography, which is the process of concealing code within images. TA544 has implemented this strategy in recent Japanese and Italian campaigns, embedding steganographic images of pop culture references into attached Microsoft Office Documents. When the user enables the document macro, the obfuscated code downloads and installs malware, usually URLZone and/or Ursnif as noted above.

Targeting

TA544 has historically targeted Italy (ongoing), Japan (ongoing), Germany (defunct), Poland (defunct), and Spain (defunct). In addition to malware specifically chosen for each country, each region is targeted with appropriate language translations in email bodies, subjects, filenames, and geographically relevant branding. Known targeted countries are listed in Table 1 below:

Country	Language	Malware	Volume	Verticals	Notes
Italy (Active)	Italian	Panda (Multiple Versions), Chthonic, Smoke Loader, Ursnif (Multiple Affids)	Medium Volume	Manufacturing and Retail	Proofpoint researchers began tracking of TA544 with campaigns targeting Italy in February of 2017 where it was initially discovered. Italy has been regularly targeted since.
Poland (Defunct)	Polish	Nymaim	Medium Volume	Manufacturing	Campaigns began regularly in March of 2017 and appear to have gone on hiatus in May of 2018.

Germany (Defunct)	German	Ursnif (1001), Ursnif (1002),	Medium Volume	Technology, Manufacturing, & Hospitality	Campaigns began experimentally in February of 2017 and ended in March of 2017.
Spain (Defunct)	Castilian	ZLoader	Medium Volume	Technology, Manufacturing & Hospitality	Campaigns began experimentally in August of 2017 and ended in September of 2017.
Japan (Active)	Japanese	URLZone Ursnif	High Volume	Marketing/advertising, Technology, and IT	Campaigns began experimentally in December of 2017 using Ursnif and have been regularly targeted using URLZone and Ursnif as of June of 2019.

Table 1: Description of the countries with observed email campaigns.

Campaign History

Figure 2 illustrates a high-level overview of TA544 campaign history in the five most impacted geographies:

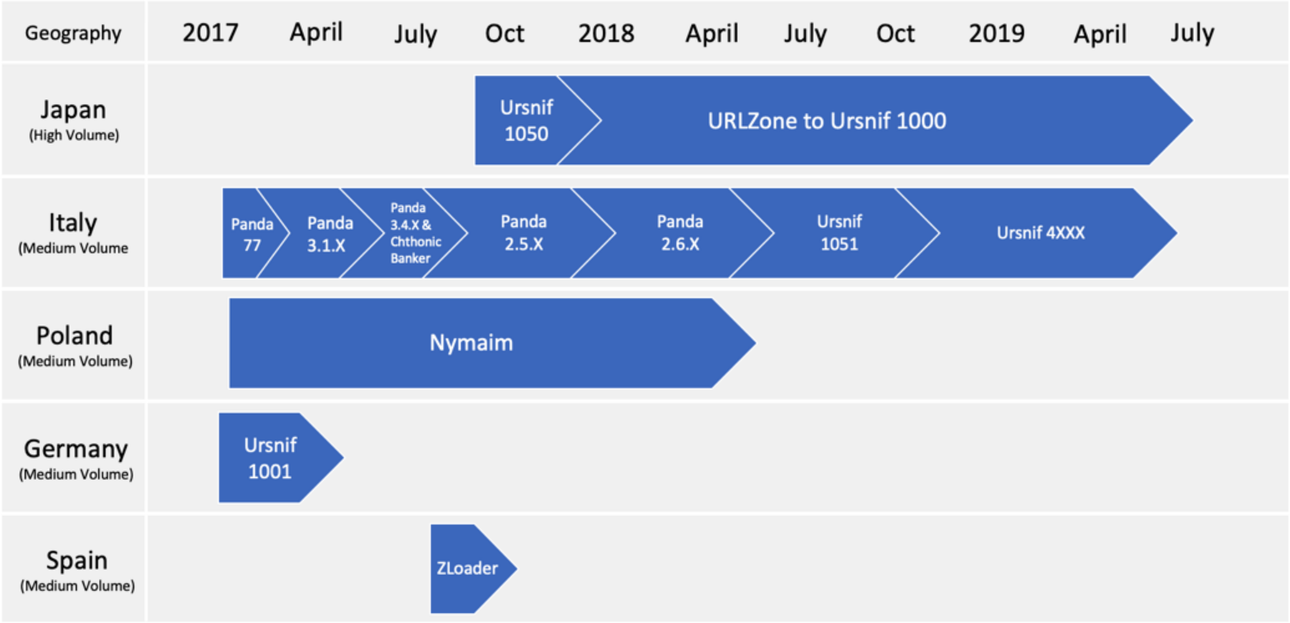


Figure 2: TA544 campaign history

Proofpoint researchers began observing TA544 in Italy at the end of 2017, primarily leveraging Panda Banker. In March of 2017, TA544 briefly experimented in Germany with Ursnif variants but ceased activity in the region after only a short one-month period. Similarly, TA544 also targeted Spanish audiences with ZLoader during the summer of 2018. During these experimental phases, TA544 conducted ongoing campaigns that targeted Polish audiences with Nymaim.

By September of 2018, TA544 began to focus its attacks on Japan, using standalone Ursnif variants and/or URLZone which leads to Ursnif 1000 specifically. URLZone to Ursnif 1000 remains the primary strategy for TA544 campaigns that target Japanese audiences. During these ongoing Japanese-focused campaigns, TA544 gradually began replacing Panda payloads with Ursnif. The most recent Ursnif variants that TA544 uses to target Italian audiences are derivatives of Ursnif 4000 (4777, 4778, 4779, 4780; collectively referred to as 4XXX).

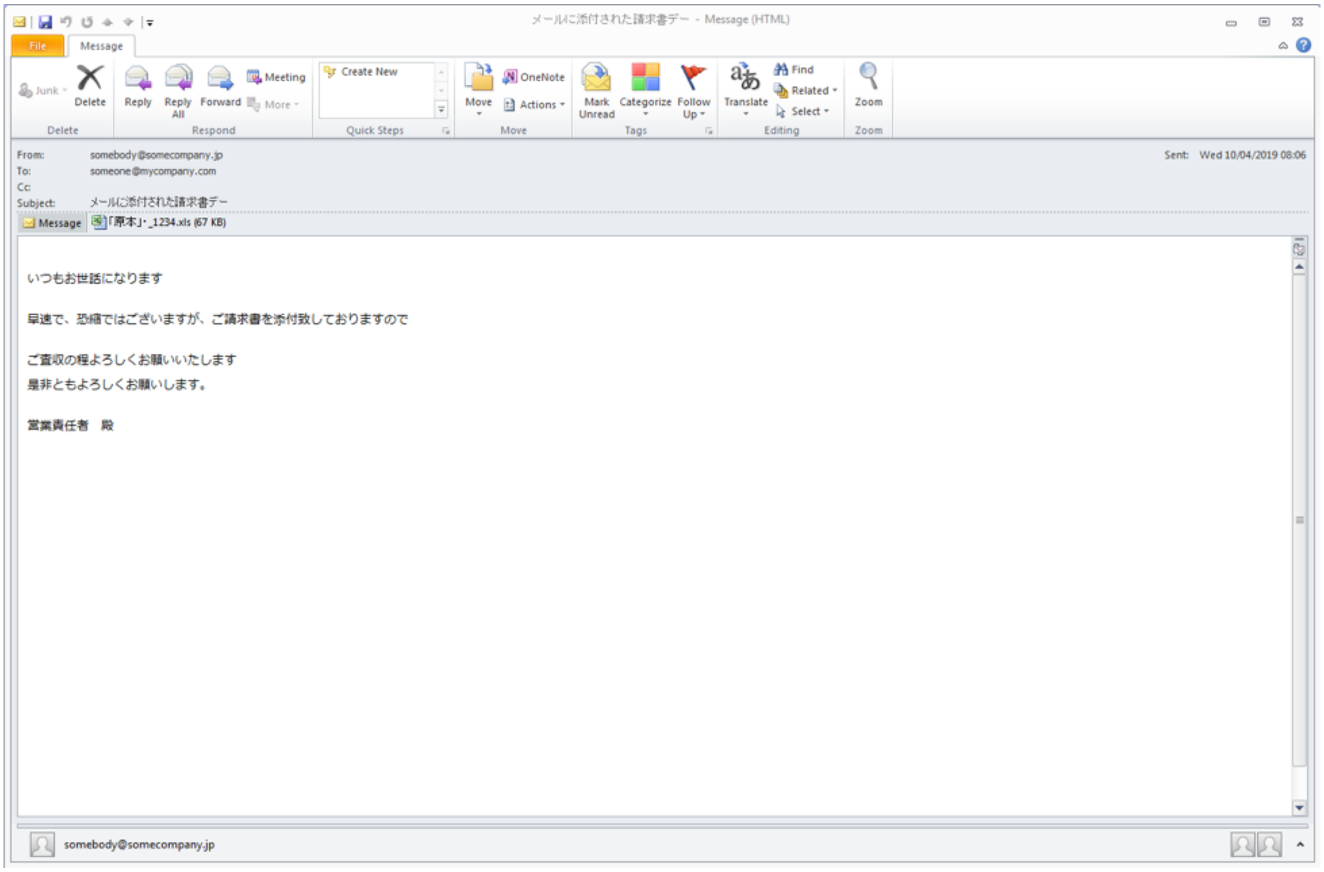
Campaigns

TA544 campaigns that target Japan often distribute messages with payment-themed subject lines such as:

- "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")

These messages often contain a short, generic message about upcoming payment deadlines, and typically contain Microsoft Excel Documents with macros, that when enabled, download and install URLZone and/or Ursnif 1000. These Excel document file names are usually a random collection of numbers:

- "12345_0001.xls" (random digits)
- "1234_56_007.XLS" (random digits)
- "0001_123_4567.XLS" (random digits)



From: somebody@somecompany.jp
To: someone@mycompany.com
Cc:
Subject: メールに添付された請求書デー
Sent: Wed 10/04/2019 08:06

Message 「原本」・_1234.xls (67 KB)

いつもお世話になります

早速で、恐縮ではございますが、ご請求書を添付致しておりますので

ご査収の程よろしくお願いいたします
是非ともよろしくお願いします。

営業責任者　殿

somebody@somecompany.jp

Figure 3: An email with Microsoft Excel attachment that contains macros, that when enabled, download and install URLZone which leads to Ursnif 1000 (Japan, April 2019)

Some of these messages may also contain attached steganographic images of notable Japanese pop culture references. These images contain scripts that can fetch and install malware (usually URLZone or Ursnif 1000) from malicious websites controlled by TA544.

Figure 4: Steganographic image that contains scripts that fetch Ursnif 1000 payloads from malicious websites controlled by TA544 (Japan, April 2019)

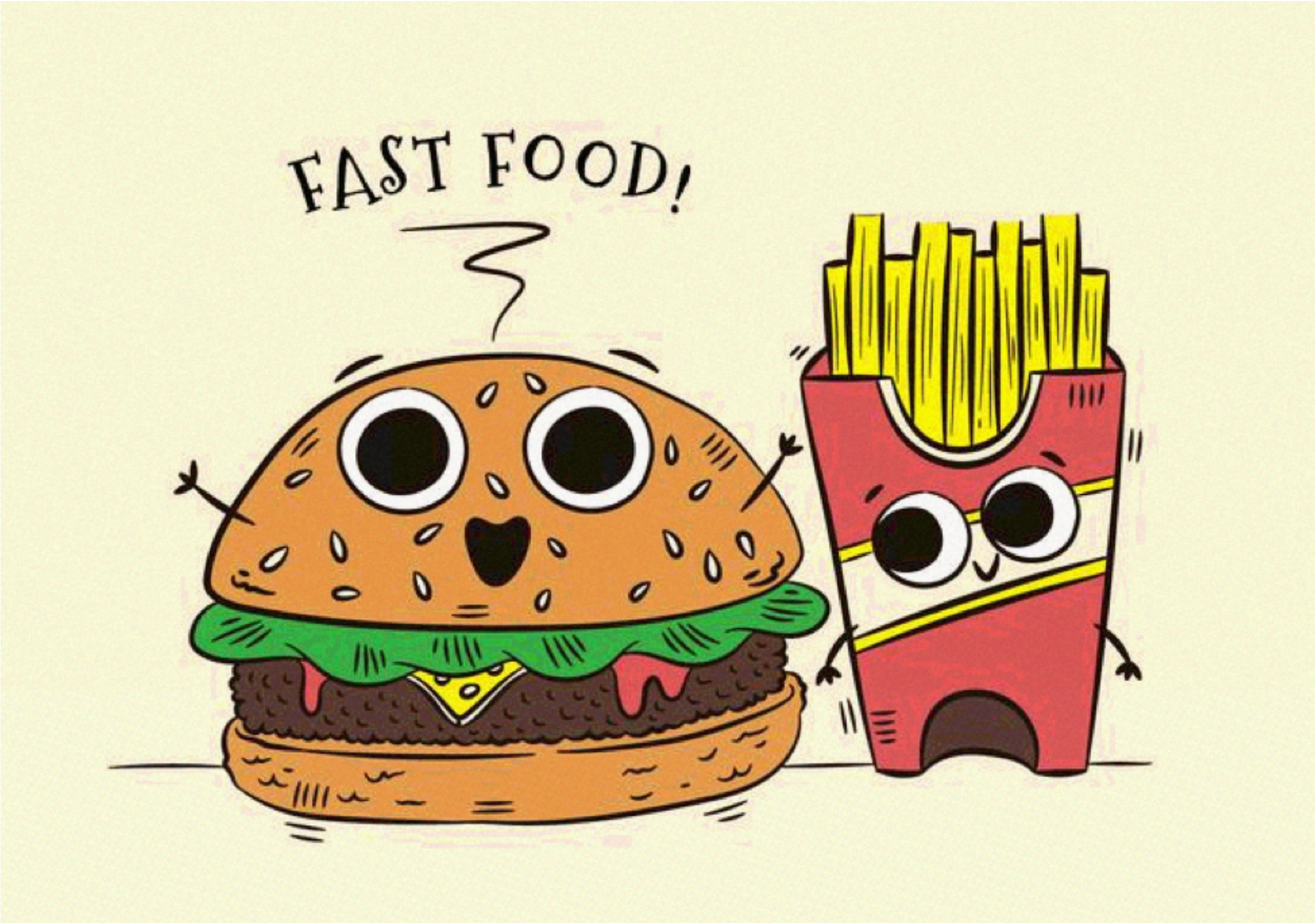


Figure 5: Steganographic image that contains scripts that fetch Ursnif 1000 payloads from malicious websites controlled by TA544 (Japan, May 2019)

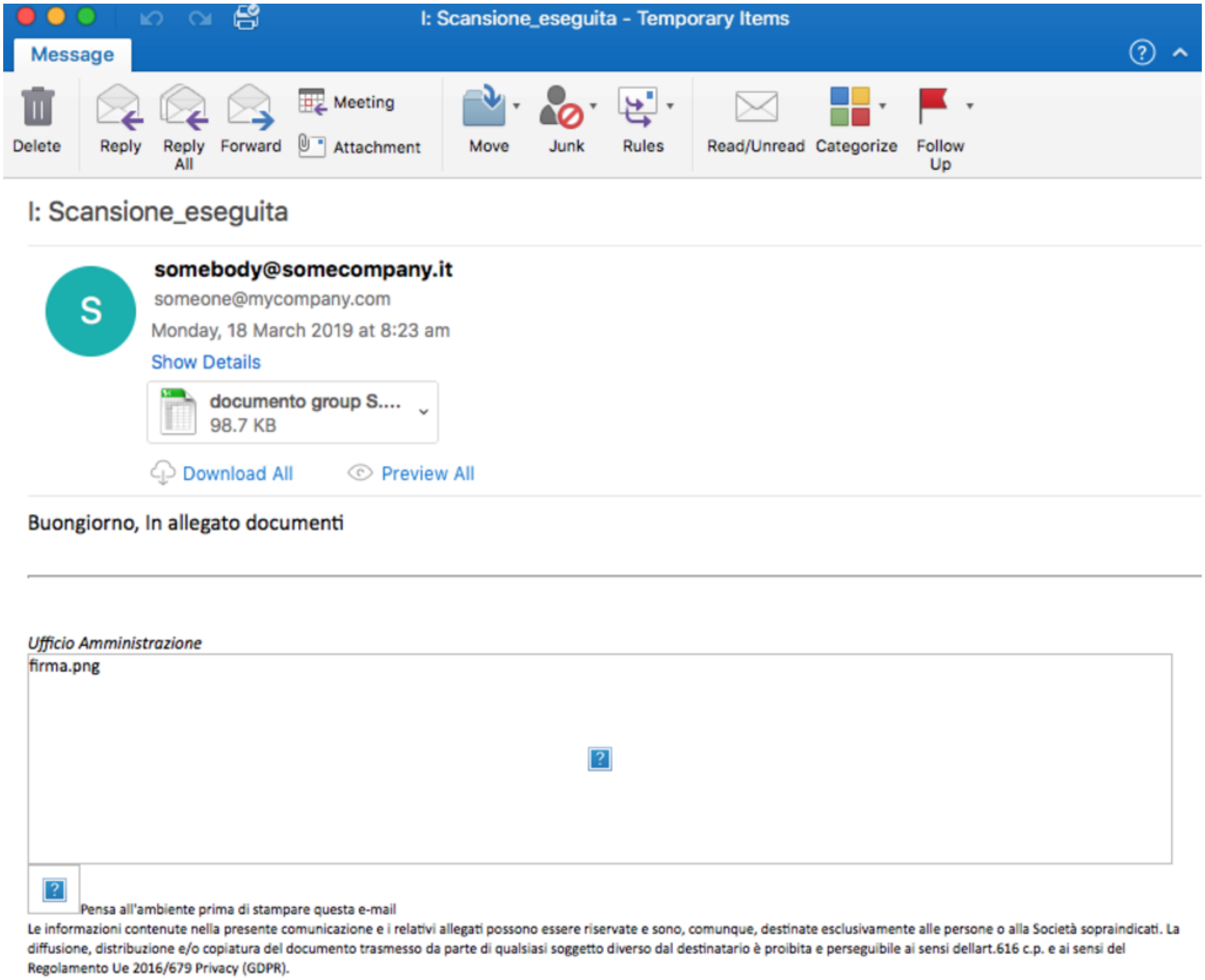
TA544 uses many of the same strategies to target Italian audiences. These campaigns utilize simple social engineering mechanisms including payment themed subject lines.

Some examples of subject lines include:

- "documenti sig."
- "Fattura per bonifico"
- "Fatturazione 123456" (random digits)
- "fatture scadute"

These messages often contain a short, generic message about upcoming payment deadlines, scanned invoices, or upcoming bill payments, and typically contain Microsoft Excel Documents with macros, that when enabled, download and install Ursnif 4XXX. These Excel document file names are usually a random collection of numbers paired with upcoming dates:

- "(9)__2019__03_8765432F.XLS" (random digit, month, random digits)
- "20190321 D O C 98765_43.xls" (today's date, random digits)
- "FtDiff0000 000000D_M_S_987654.XLS" (random digits)



I: Scansione_eseguita

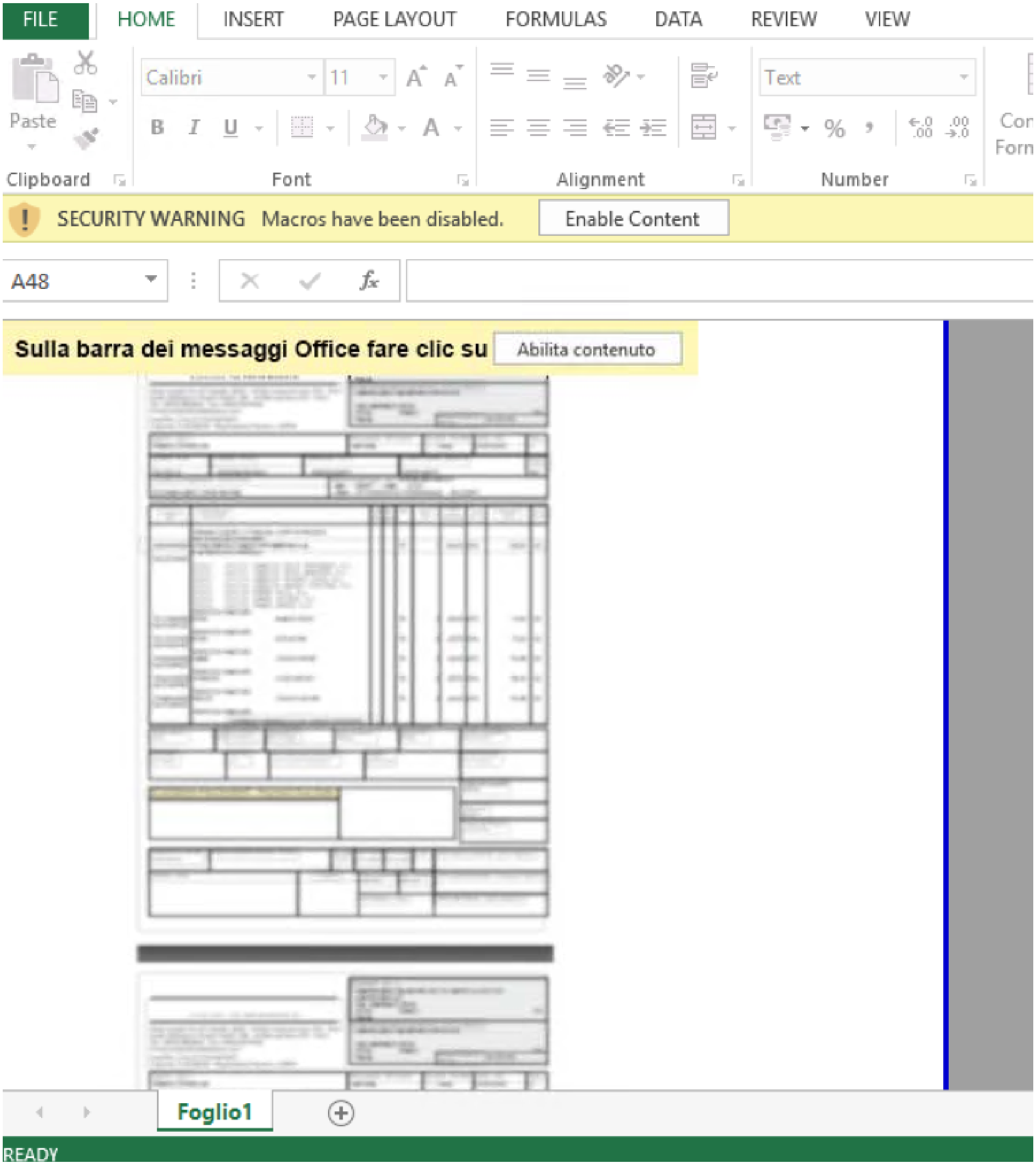
somebody@somecompany.it
someone@mycompany.com
Monday, 18 March 2019 at 8:23 am

Buongiorno, In allegato documenti

Ufficio Amministrazione
firma.png

Pensa all'ambiente prima di stampare questa e-mail
Le informazioni contenute nella presente comunicazione e i relativi allegati possono essere riservate e sono, comunque, destinate esclusivamente alle persone o alla Società sopraindicati. La diffusione, distribuzione e/o copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita e perseguibile ai sensi dellart.616 c.p. e ai sensi del Regolamento Ue 2016/679 Privacy (GDPR).

Figure 6: An email with Microsoft Excel attachment that contains macros, that when enabled, download and install Ursnif 4XXX (Italy, May 2019)



SECURITY WARNING Macros have been disabled.

Sulla barra dei messaggi Office fare clic su Abilita contenuto

Figure 7: Microsoft Excel attachment that contains macros, that when enabled, download and install Ursnif 4XXX (Italy, June 2019)

Some of these messages may also contain attached or linked steganographic images of notable Italian pop culture references. These images contain scripts that can fetch and install an Ursnif payload from malicious websites controlled by TA544.

Figure 8: Steganographic image that contains scripts that fetch Ursnif 4XXX payloads from malicious websites controlled by TA544 (Italy, June 2019)

Conclusion

Since early 2017, TA544 has emerged as one of the most prolific and geographically focused threat actors in the threat landscape, distributing tens of millions of malicious messages across eight countries within the last two years. To date, TA544 has delivered more than six unique malware payloads (in several variations of each) in high-volume campaigns (hundreds of thousands of messages per day) to victims across western Europe and Japan.

Originally specializing in the Panda banking malware in Italy, it has since branched out to Poland, Germany, Spain, and Japan, using a variety of other malware including Chthonic, Smoke Loader, Nymaim, ZLoader, and finally URLZone in combination with Ursnif, both banking Trojans. TA544 currently targets marketing/advertising, technology, and IT verticals in Japan, and manufacturing and retail verticals in Italy.

Given their recent behavior, we can expect TA544 to remain a prominent threat in Japanese and Italian geographies. There is no indication of TA544 abandoning their primary payload delivery mechanism (malicious Microsoft Office VBA macros), although we have seen an increase in the use of steganographic images.

Subscribe to the Proofpoint Blog