

So Far and Yet so Close:
A story of collaboration in cybersecurity
field between Japan and Spain

日本とスペインのサイバーセキュリティ分野における国際協力

Who we are?



Canon

Masato Ikegami

- ❑ *Malware analyst at Canon IT Solutions*
- ❑ 10 years of experience in cybersecurity
- ❑ Focused on the automated analysis and classification of malware
- ❑ *Certifications: CISSP, GREM, GCTI, GCIH*



ikegami.masato@canon-its.co.jp



Ontinet

Josep Albors

- ❑ *Head of Awareness & Research at ESET Spain
(Operated by Ontinet.com)*
- ❑ 19 years of experience in cybersecurity
- ❑ Focused on malware analysis and threat intelligence
- ❑ Teacher in cybersecurity courses at several Spanish universities



josep@ontinet.com

Our collaborative research



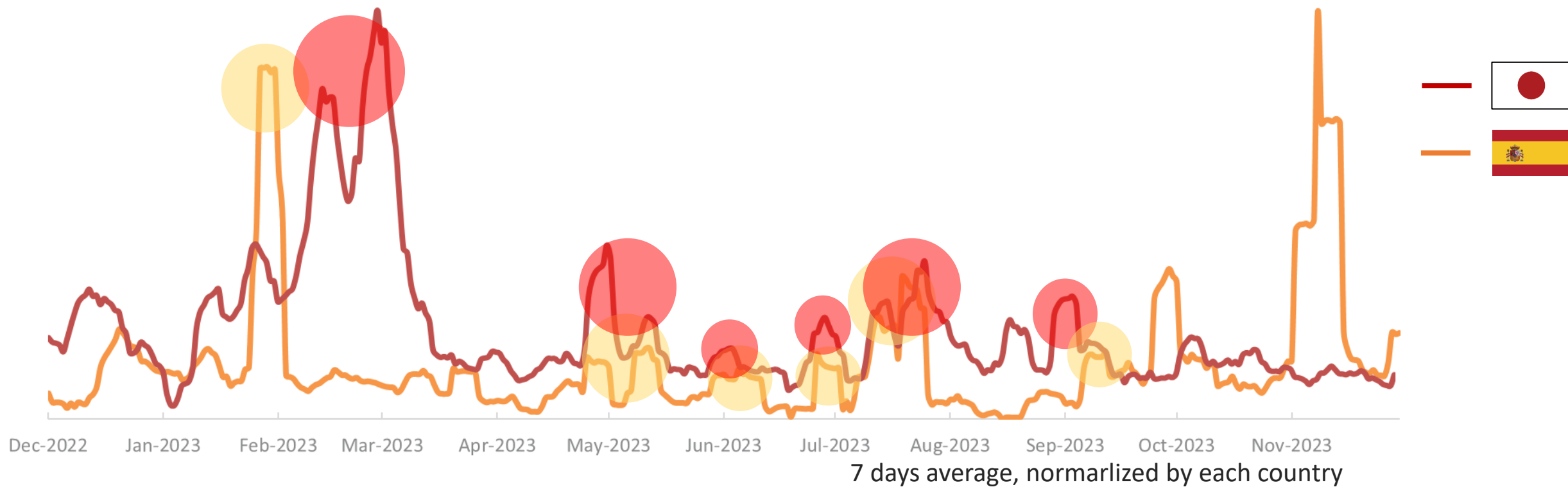
C1b3rWall / FIRSTCON (June 2024)

We gave presentations at C1b3rWall (Avila, Spain) and FIRSTCON (Fukuoka, Japan).

Our collaborative research

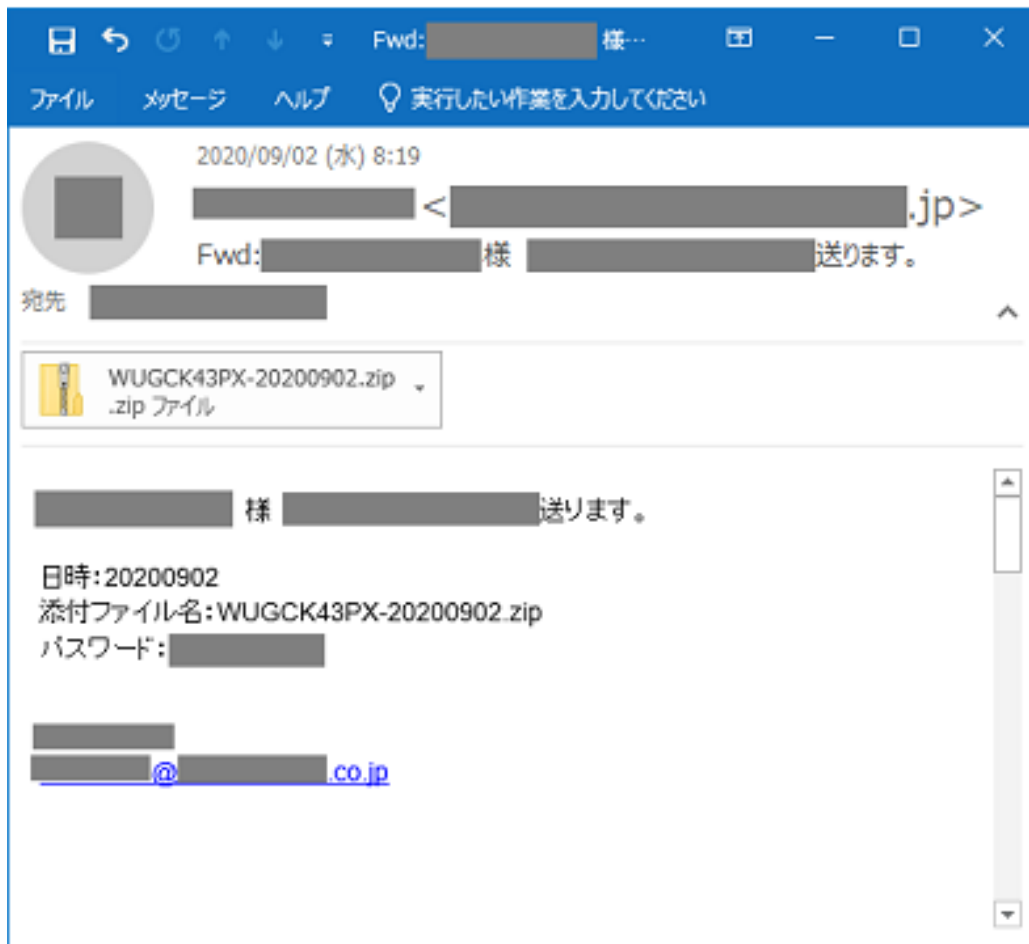
Infostealers trends

- Some detection spikes are seen simultaneously in both Japan and Spain.
- Only Spain has spikes in November.

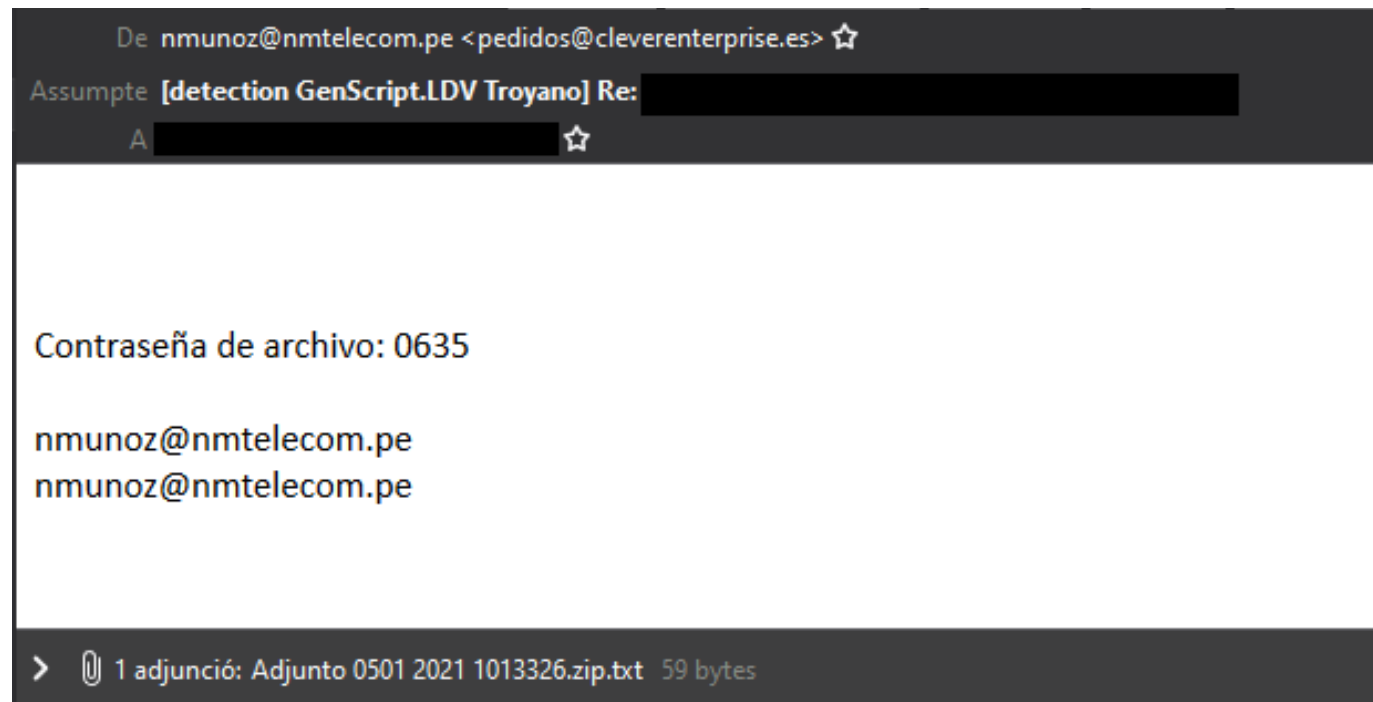


Our collaborative research

Emotet campaigns



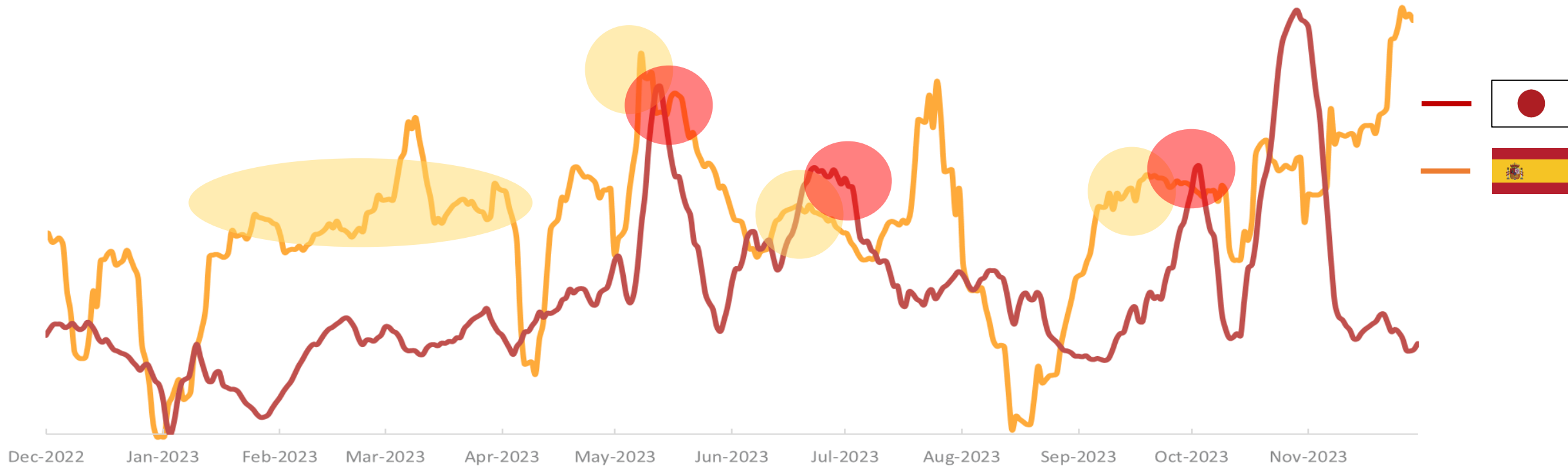
Examples of attacks using password-protected ZIP files (IPA)
<https://www.ipa.go.jp/security/emotet/situation/emotet-situation-04.html>



Our collaborative research

Scam trends

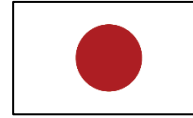
- Some detection spikes in Japan are seen a few weeks after that of Spain.
- In Spain, A spike lasts for months.



7 days average, normalized by each country

Our collaborative research

Tech support scam in Japan



The screenshot shows a Microsoft Support page in Japanese. A blue Windows Security alert is overlaid on the page. The alert text reads: "MS WINDOWS DEFENDER - 警告アラート システム", "** セキュリティ上の理由と安全のため、アクセスがブロックされました **", "お使いのシステムは、スパイウェアの問題に感染していると警告しています。以下のデータが得られました 違反しました。", and lists "メールパスワード", "銀行のパスワード", "フェイスブックログイン", and "写真 & ファイル". Below the list, it states: "Windows セキュリティ機能により、オンラインでパスワードを侵害する可能性がある望ましくないアドウェアがこのデバイス上で見つかりました 身元情報、財務情報、ファイル、個人の写真または文書。"

The alert dialog box is titled "セキュリティサービス" and shows "App: Ads.fiancetrack(2).dll" and "Threat Detected: Trojan Spyware". It contains icons for a shield, a shield with a checkmark, and a person with a shield. The text inside the dialog says: "セキュリティ上の理由と安全のため、アクセスはブロックされています。" and "Windows セキュリティのフリーダイヤル: 050-". At the bottom of the dialog are "Microsoft", "Cancel", and "Scan" buttons.

At the bottom right of the page, there is a blue bar with the text "(無料通話) 050-".

Contact support in the browser instead.

Our collaborative research

Tech support scam in Spain



The screenshot shows a Windows desktop with a scam website in the background. The website text includes: "Su ordenador con la...", "LLAMADA GRATUITA : 900 649 691", and "Informe automáticamente a Microsoft detalles de posibles incidentes de seguridad Política de privacidad". A Windows system alert window is open, titled "Alerta del sistema de Windows (!!!)", with the message: "¡¡¡ Información importante !!! Su Ordenador de Microsoft ha sido bloqueado. Error: 0x800920e0. LLAME INMEDIATAMENTE A MICROSOFT: 900 649 691 (LLAMADA GRATUITA). Tiene un virus y su unidad de disco duro se eliminará si cierra esta página. Per favor llame con urgencia al soporte técnico de Microsoft al número gratuito 900 649 691 para detener el proceso de borrado de datos. LLAMADA GRATUITA : 900 649 691." Below the alert, there are "Cancelar" and "Cerrar" buttons. In the bottom right, there is a green button labeled "LLAMADA GRATUITA : 900 649 691" and a green "Cerrar" button. At the bottom, a "User Name:" and "Password:" login form is visible with "Cancel" and "OK" buttons.

The screenshot shows a Windows Security alert window titled "Windows_Defender_Centro de seguridad". The window contains the following text: "Póngase en contacto con nosotros inmediatamente para que nuestros ingenieros puedan guiarle por teléfono durante el proceso de eliminación. Su ordenador está deshabilitado. Llamar al Soporte de Windows: 900 433 208". Below this, it says "Adresse IP: [redacted] 5/16/2024, 10:49:06 AM", "Location: Murcia, Spain", and "ISP: DIGI SPAIN TELECOM S.L.". The main message reads: "El acceso a este PC ha sido bloqueado por razones de seguridad. Llamar al Soporte de Windows: 900 433 208". At the bottom, there are "Anular" and "OK" buttons. The "Seguridad Windows" logo is circled in red.

Collaboration between countries

JPCERT and INCIBE have signed a collaboration agreement to address challenges in cybersecurity last February.



Collaboration between companies



Company C



Company O

Lessons learned

- Campaigns observed in one country are often observed later in another country.
- Having said that, the situation differs in some points from one country to another, but we can learn from the points in common to enhance our cybersecurity.
- Cross-country cooperation is important.

Thank you for listening.

ご清聴ありがとうございました。

¡Muchas gracias!



✉ ikegami.masato@canon-its.co.jp



✉ josep@ontinet.com

X x.com/josepalbors