

# Tracking Threat Actors Using Images: A Hunting & Analysis Approach

---

Joseliyo Sánchez - @Joseliyo\_Jstnk  
Security Engineer - VirusTotal



# JOSE LUIS SÁNCHEZ MARTINEZ

## AKA JOSELIYO



- Security Engineer @ VirusTotal - Google
- Former McAfee and BlackBerry security researcher



@Joseliyo\_Jstnk



/in/joseluissm/

# Agenda

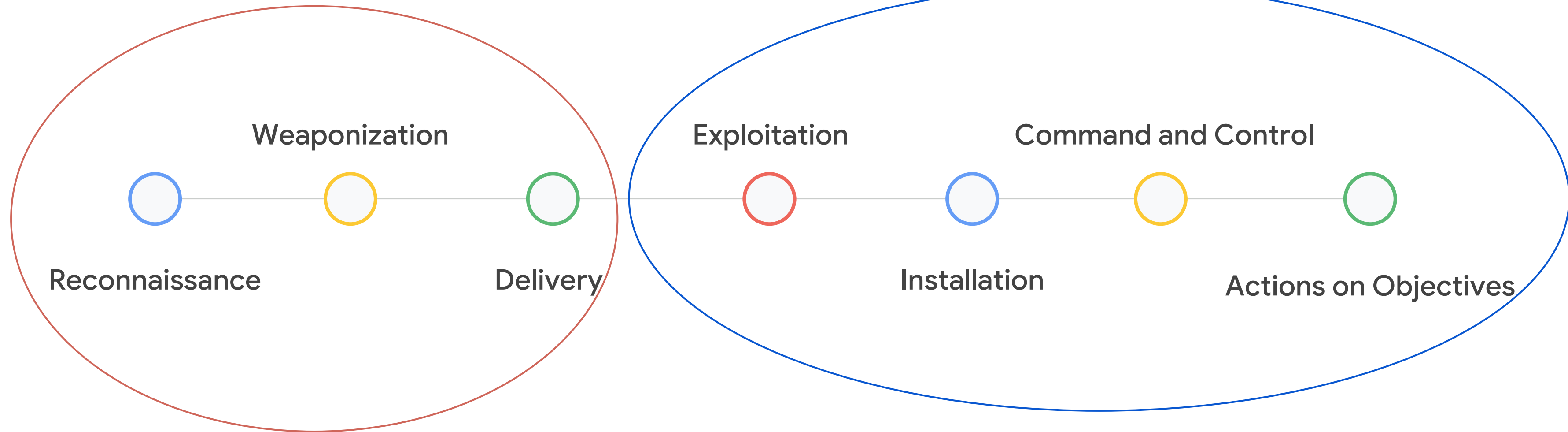
---

- Why I decided to do this research
- Research explanation
- ITW examples
- Limitations and conclusions

01

Why I decided to do this  
research

# A little bit of context



# Color theory: Emotion + Bias

---

Hundreds of color psychology studies have demonstrated that colors **can profoundly influence your decision making process.**

**Red** is most often associated with danger or focused attention.



**Malicious**



**Benign**

**Green** communicates peace, growth and health. Green means “go”.

# Color bias on VT

32 / 64

32 security vendors and no sandboxes flagged this file as malicious

55a0bbde3e32c559715cdc9c7d30d003b9e14725a6369d30edef20c1ed6dd994  
55a0bbde3e32c559715cdc9c7d30d003b9e14725a6369d30edef20c1ed6dd994.doc

docx calls-wmi exploit cve-2017-0199

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT TELEMETRY COMMUNITY 9

Contacted URLs (1)

| Scanned    | Detections | Status | URL   |
|------------|------------|--------|---|
| 2024-01-31 | 11 / 91    | -      | http://mofa-gov-np.fia-gov.net/notice/74b78aee/ |

Contacted Domains (4)

| Domain                    | Detections | Created    | Registrar                   |
|---------------------------|------------|------------|-----------------------------|
| fia-gov.net               | 19 / 90    | 2023-06-12 | -                           |
| mofa-gov-np.fia-gov.net   | 10 / 90    | 2023-06-12 | -                           |
| nexus.officeapps.live.com | 0 / 90     | 1994-12-28 | CSC CORPORATE DOMAINS, INC. |
| time.windows.com          | 0 / 90     | 1995-09-11 | MarkMonitor Inc.            |

Sample

Compressed Parents (1)

| Scanned    | Detections | Type | Name   |
|------------|------------|------|--|
| 2024-01-30 | 52 / 65    | ZIP  | fdeef34eae3d21f099a347716aa0869104704ff60150cdbc98aeb5ae11870f4a |

Bundled Files (13)

| Scanned    | Detections | File type | Name                         |
|------------|------------|-----------|------------------------------|
| 2024-02-17 | 8 / 60     | XML       | word/_rels/document.xml.rels |
| 2024-02-19 | 0 / 60     | XML       | _rels/.rels                  |
| 2024-02-12 | 0 / 60     | XML       | [Content_Types].xml          |
| 2024-02-12 | 0 / 60     | XML       | docProps/app.xml             |
| 2024-02-12 | 0 / 60     | XML       | docProps/core.xml            |
| 2024-02-12 | 0 / 60     | XML       | word/document.xml            |
| 2024-02-12 | 0 / 60     | XML       | word/fontTable.xml           |
| 2024-02-12 | 0 / 59     | JPEG      | word/media/image1.jpeg       |
| 2024-02-12 | 0 / 60     | Text      | word/media/image2.jpg        |
| 2024-02-12 | 0 / 60     | XML       | word/settings.xml            |
| 2024-02-17 | 0 / 60     | XML       | word/styles.xml              |
| 2024-02-19 | 0 / 58     | XML       | word/theme/theme1.xml        |
| 2024-02-17 | 0 / 60     | XML       | word/webSettings.xml         |

Dropped Files (3)

| Scanned    | Detections | File type        | Name   |
|------------|------------|------------------|--|
| 2024-02-12 | 0 / 60     | Text             | word/media/image2.jpg  |
| 2024-01-30 | 4 / 60     | Windows shortcut | C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\design.LNK |
| ?          | ?          | file             | 2c7adcff8bde0f7325ec069c0274435c962e0b4f2c3a76e4bdaebaa6925a8388 |

# What is there in common?



**ФАСТИВСЬКА РАЙОННА ДЕРЖАВНА АДМІНІСТРАЦІЯ КИЇВСЬКОЇ ОБЛАСТІ**  
**ФАСТИВСЬКА РАЙОННА ВІЙСЬКОВА АДМІНІСТРАЦІЯ КИЇВСЬКОЇ ОБЛАСТІ**  
 м. Соболева, 1, м. Фастів, 08500, тел.: (04565) 5-14-44, факс: 6-02-31  
 E-mail: [fastivrai@fastivska-rda.gov.ua](mailto:fastivrai@fastivska-rda.gov.ua), веб-сайт: <https://fastivska-rda.gov.ua>, Код ЄДРПОУ 04054642


від 16.05.2023 р. № 06-69/1735 На № 13225/01/2023 від 15.05.2023 р.

**Головам територіальних громад Фастівського району Київської області**  
**Київська обласна державна адміністрація**

Щодо щоденного оновлення інформації

На виконання листа Київської обласної державної адміністрації від 15.05.2023 № 13225/01/2023 щодо опрацювання листа Міністерства розвитку громад, територій та інфраструктури України, Фастівська районна державна адміністрація Київської області надала до відповідного реагування копію листа Міністерства розвитку громад, територій та інфраструктури України від 15.05.2023 № 3964/30/14-23 щодо щоденного оновлення інформації з метою здійснення моніторингу ситуації стосовно надання компенсації з використанням електронної публічної послуги «Відновлення».

Зважаючи на вищевикладене, з метою здійснення моніторингу ситуації щодо надання компенсації з використанням електронної публічної послуги «Відновлення», планування видатків державного бюджету на зазначені цілі та здійснення контролю за їх використанням, Фастівська районна державна адміністрація просить забезпечити до 18 травня 2023 року надання та щоденне оновлення (до 11 год. 00 хв.) інформації щодо створення та роботи Комісії з розгляду питань щодо надання компенсації за пошкоджені об'єкти нерухомого майна внаслідок бойових дій, терористичних актів, диверсій,



**बैदेशिक भ्रमण व्यवस्थापन निर्देशिका**

सरकारी पदाधिकारीको बैदेशिक भ्रमणलाई उपयोगी, नतिजामूलक, मितव्ययी, पारदर्शी र व्यवस्थित बनाउन वाञ्छनीय भएकाले,


नेपाल सरकारले सुरासन (व्यवस्थापन तथा सञ्चालन) ऐन, २०६४ को दफा ४५ ले दिएको अधिकार प्रयोग गरी यो निर्देशिका बनाएको छ ।

१. **संक्षिप्त नाम र प्रारम्भ** : (१) यस निर्देशिकाको नाम "बैदेशिक भ्रमण व्यवस्थापन निर्देशिका,"

(२) यो निर्देशिका तुरुन्त प्रारम्भ हुनेछ ।

२. **परिभाषा** : विषय वा प्रसङ्गले अर्को अर्थ नलागेमा यस निर्देशिकामा,

(क) "मन्त्रालय वा निकाय" भन्नाले नेपाल सरकारको मन्त्रालय, संवैधानिक निकाय वा केन्द्रीयस्तरको कार्यालय सम्झनु पर्छ र सो शब्दले प्रधानमन्त्री तथा मन्त्रिपरिषदको कार्यालयलाई समेत जनाउँछ ।



SMR-WF/4241/2/ 267

Directorate of Ships Maintenance & Repairs (WE)  
 Naval Headquarters  
 ISLAMABAD

Tele : 0092-51 20062995  
 Fax : 0092-51-9261551  
 Email : [dsmrwe@paknavy.gov.pk](mailto:dsmrwe@paknavy.gov.pk)

03 September 2021

**PAYMENT RELEASE ORDER - UPGRADE OF SR 47**

**BG RADARs ONBOARD AZMT AND DHST**


References:

A. Work Order CICP/FAC(M)/Work Order/1809 dated 30 Jun 21  
 B. M/s CSTC letter CSTCDSMRWE\_YRF\_20210730 dated 30 Jul 21  
 C. M/s CSTC RRC No 351055/327079 dated 30 Jun 94

1. Work order for upgrade of SR 47 BG onboard AZMT & DHST was issued to M/s CSTC China through existing RRC at cost of US\$ 0.858M vide reference A. M/s CSTC vide reference B has forwarded invoice for release of 20% 1<sup>st</sup> payment amounting to **US\$ 171,600 (US Dollar One Hundred Seventy One Thousand and Six Hundred only)** as per Milestone M1 (T<sub>+</sub>+ 01 M) i.e. submission of Project Plan.

2. It may be mentioned that Project Plan submitted by CSTC for upgrade of SR 47 BG Radar onboard AZMT & DHST has been supported for implementation from President Acceptance Committee.

3. Foregoing in view, it is requested that payment amounting to **US\$171,600 (US Dollar One Hundred Seventy One Thousand and Six Hundred only)** may please be



Приложение № 1  
 к подпункту «а» пункта 11  
 Инструкции по делопроизводству  
 во ФГУП «ГРЧЦ»

По списку рассылки

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ «ГЛАВНЫЙ РАДИОЧАСТОТНЫЙ ЦЕНТР» (ФГУП «ГРЧЦ») Дербиневская набережная, д. 7, стр.15, Москва, 117997  
 тел.: (495) 740 38 98, факс: (499) 230 15 31, <http://www.grtc.ru>, E-mail: [grtc@grtc.ru](mailto:grtc@grtc.ru)  
 ОКПО 36562879, ОГРН 1027739314479  
 ИНН/КПП 7706228218/772901001, ОКУД 0200000

№ \_\_\_\_\_

На № \_\_\_\_\_


Об активности хакерских группировок

Уважаемые коллеги!

В связи с повышенной активностью хакерских группировок, вредоносная деятельность которых направлена на дестабилизацию работы систем и ресурсов российских операторов связи и провайдеров хостинга, прошу провести анализ и поиск в корпоративных и технологических инфраструктурах Вашей организации индикаторы компрометации, ранее выявленные НКЦКИ в атакованных информационных системах.

**Сетевые и хостовые индикаторы компрометации**  
 IP (с&с): 93.190.202.201, 107.172.76.180, 23.132.185.120, 104.21.42.222, 172.67.167.31, 104.21.94.174, 172.67.138.211, 193.37.255.162

**CONFIDENTIAL**



No. M05/ARM/DO/2023 Dated: 29<sup>th</sup> May, 2023

**Password Updation Policy and Records.**

Assalamu Alaikum,

You are requested to change the password of your Army mail by **080000 June 2023 (Night 08/09 June 2023)** to ensure secure access and maintain the confidentiality of your email account. For setting a new password, few guidelines must be followed:

**Your new password must:**

- Contain minimum 12 characters.
- Combination of uppercase, lowercase, symbols and numbers 0-9.
- Not be the same one as last 15 passwords.

Your present password will expire after 080000 June 2023 (Night 08/09 June 2023) and after that, you will not be able to login into your Army mail using current password.

A password change screen will appear during your next login attempt of your email account. If you face any problem or need further help, please contact at

ශ්‍රී ලංකා නාවික හමුදාව පසුගිය 2023 වසරේ සිදුකල මෙහෙයුම් මණ්ඩලයේ විශාල කොටසක් සමඟ මන්දිරවීය ජාවාරම ආතුළ නීති විරෝධී කටයුතු සිදුකල පුද්ගලයින් 343 ක් නීතිරේ රැහැනට හසුකරවීමට සමත් වෙයි

ශ්‍රී ලංකා නාවික හමුදාව පසුගිය 2023 වසරේ සිදුකල මෙහෙයුම් මණ්ඩලයේ විශාල කොටසක් සමඟ මන්දිරවීය ජාවාරම ආතුළ නීති විරෝධී කටයුතු සිදුකල පුද්ගලයින් 343 ක් නීතිරේ රැහැනට හසුකරවීමට සමත් වෙයි



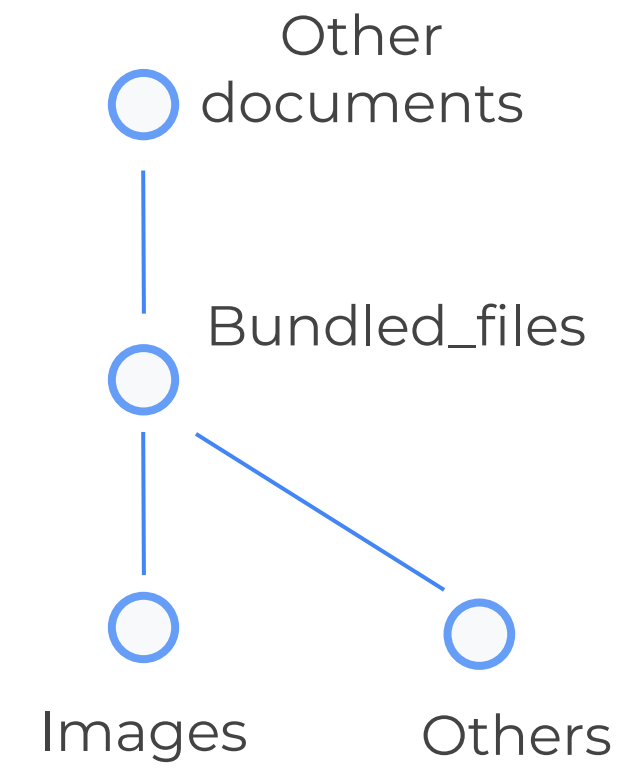
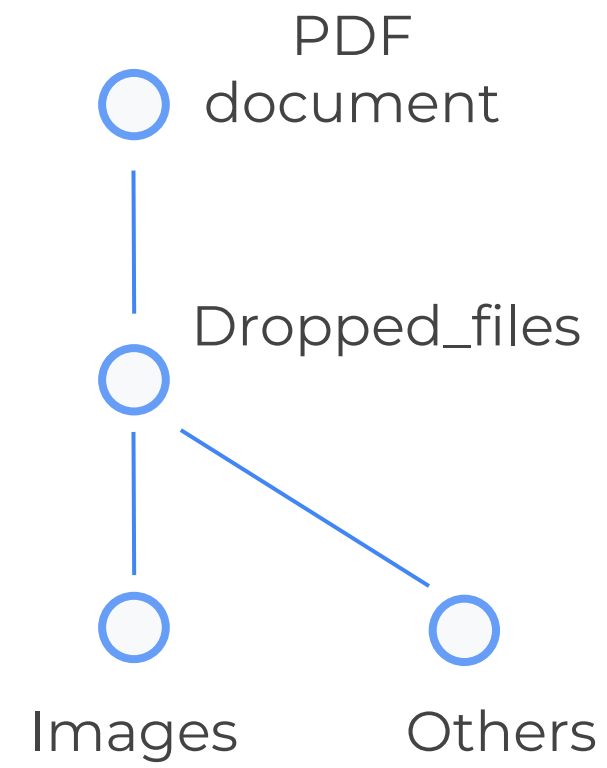
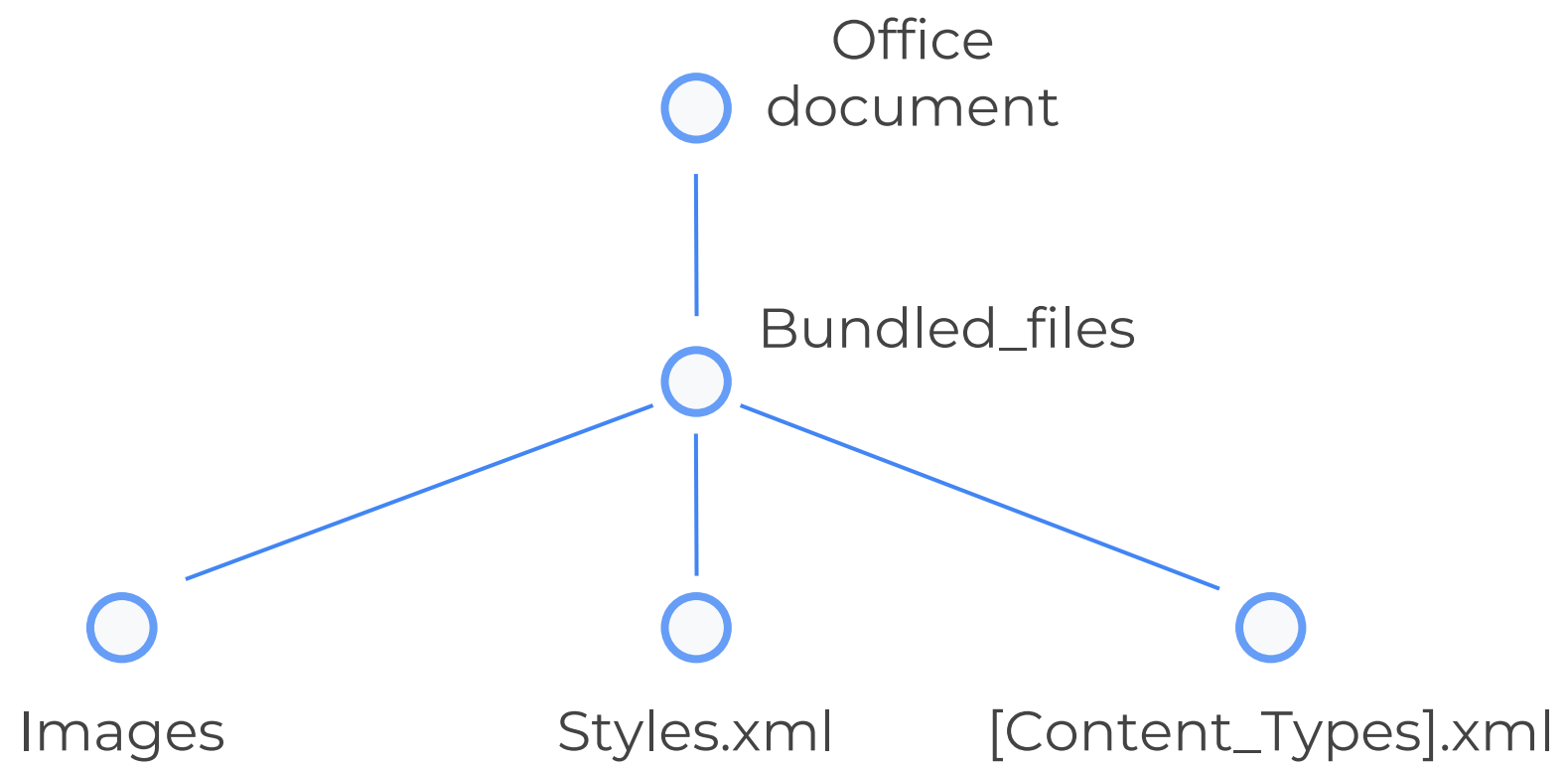



02

Research explanation

# This research focuses on...

---



# Office documents

---

**Images:** As we could see, TA are using images within their documents. Usually, related to Governments and other agencies.

**[Content\_Types].xml:** This file specifies the content types and relationships within the Office Open XML (OOXML) document. It essentially defines the types of content and how they are organized within the file structure.

**Styles.xml:** Stores stylistic definitions for your document. These styles provide consistent formatting instructions for fonts, paragraph spacing, colors, numbering, lists, and much more.

# Facts

- We have identified the use of the same [images](#) in multiple documents used by the same threat actors at different moments in time.
- We have identified the use of the same [\[Content\\_Types\].xml](#) in multiple documents used by the same threat actor and other threat actors at different points in time. Some [\[Content\\_Types\].xml](#) were more generic than others.
- We have identified the use of [styles.xml](#) in multiple documents used by the same threat actor and other threat actors at different points in time. Some [styles.xml](#) were more generic than others.

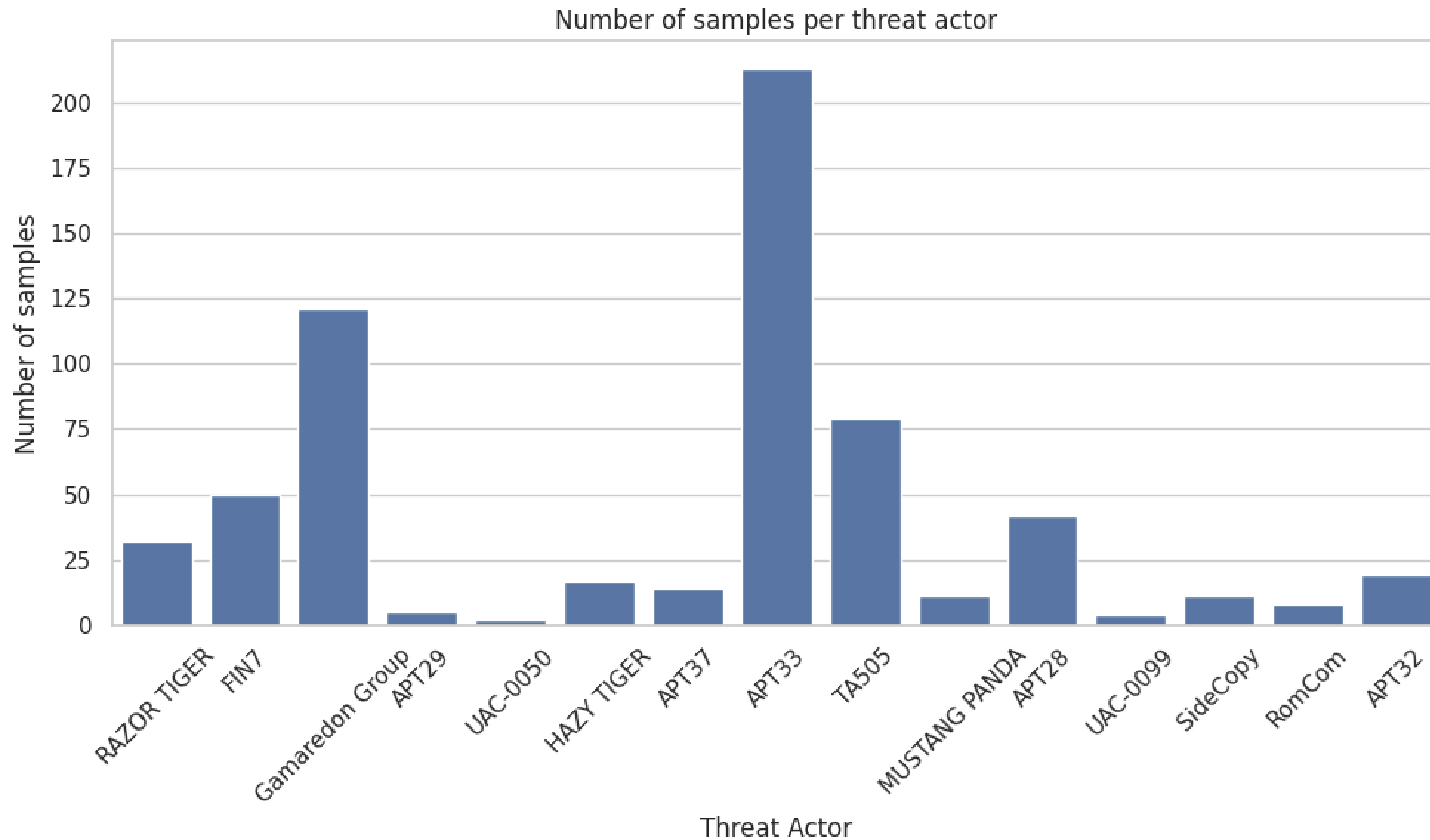
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Types xmlns="http://schemas.openxmlformats.org/package/2006/content-types">
  <Default Extension="png" ContentType="image/png" />
  <Default Extension="svg" ContentType="image/svg+xml" />
  <Default Extension="rels" ContentType="application/vnd.openxmlformats-package.relationships+xml" />
  <Default Extension="xml" ContentType="application/xml" />
  <Override PartName="/word/document.xml"
    ContentType="application/vnd.openxmlformats-officedocument.wordprocessingml.document.main+xml" />
  <Override PartName="/customXml/itemProps1.xml"
    ContentType="application/vnd.openxmlformats-officedocument.customXmlProperties+xml" />
  <Override PartName="/customXml/itemProps2.xml"
    ContentType="application/vnd.openxmlformats-officedocument.customXmlProperties+xml" />
  <Override PartName="/customXml/itemProps3.xml"
    ContentType="application/vnd.openxmlformats-officedocument.customXmlProperties+xml" />
  <Override PartName="/customXml/itemProps4.xml"
    ContentType="application/vnd.openxmlformats-officedocument.customXmlProperties+xml" />
  <Override PartName="/word/numbering.xml"
    ContentType="application/vnd.openxmlformats-officedocument.wordprocessingml.numbering+xml" />
  <Override PartName="/word/styles.xml"
    ContentType="application/vnd.openxmlformats-officedocument.wordprocessingml.styles+xml" />
  <Override PartName="/word/settings.xml"
    ContentType="application/vnd.openxmlformats-officedocument.wordprocessingml.settings+xml" />
  <Override PartName="/word/webSettings.xml"
    ContentType="application/vnd.openxmlformats-officedocument.wordprocessingml.webSettings+xml" />
</Types>
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:styles xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006"
  xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships"
  xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main"
  xmlns:w14="http://schemas.microsoft.com/office/word/2010/wordml"
  xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml"
  xmlns:w16se="http://schemas.microsoft.com/office/word/2015/wordml/symex"
  mc:Ignorable="w14 w15 w16se">
  <w:docDefaults>
    <w:rPrDefault>
      <w:rPr>
        <w:rFonts w:asciiTheme="minorHAnsi" w:eastAsiaTheme="minorHAnsi"
          w:hAnsiTheme="minorHAnsi" w:cstheme="minorBidi" />
        <w:sz w:val="22" />
        <w:szCs w:val="22" />
        <w:lang w:val="cs-CZ" w:eastAsia="en-US" w:bidirectional="ar-SA" />
      </w:rPr>
    </w:rPrDefault>
    <w:pPrDefault>
      <w:pPr>
        <w:spacing w:after="160" w:line="259" w:lineRule="auto" />
      </w:pPr>
    </w:pPrDefault>
  </w:docDefaults>
  <w:latentStyles w:defLockedState="0" w:defUIPriority="99" w:defSemiHidden="0"
    w:defUnhideWhenUsed="0" w:defQFormat="0" w:count="371">
    <w:lSDException w:name="Normal" w:uiPriority="0" w:qFormat="1" />
    <w:lSDException w:name="heading 1" w:uiPriority="9" />
    <w:lSDException w:name="heading 2" w:semiHidden="1" w:uiPriority="9" w:unhideWhenUsed="1" />
    <w:lSDException w:name="heading 3" w:semiHidden="1" w:uiPriority="9" w:unhideWhenUsed="1" />
    <w:lSDException w:name="heading 4" w:semiHidden="1" w:uiPriority="9" w:unhideWhenUsed="1"
      w:qFormat="1" />
    <w:lSDException w:name="heading 5" w:semiHidden="1" w:uiPriority="9" w:unhideWhenUsed="1"
      w:qFormat="1" />
    <w:lSDException w:name="heading 6" w:semiHidden="1" w:uiPriority="9" w:unhideWhenUsed="1"
      w:qFormat="1" />
    <w:lSDException w:name="heading 7" w:semiHidden="1" w:uiPriority="9" w:unhideWhenUsed="1"
      w:qFormat="1" />
  </w:latentStyles>
</w:styles>
```

03

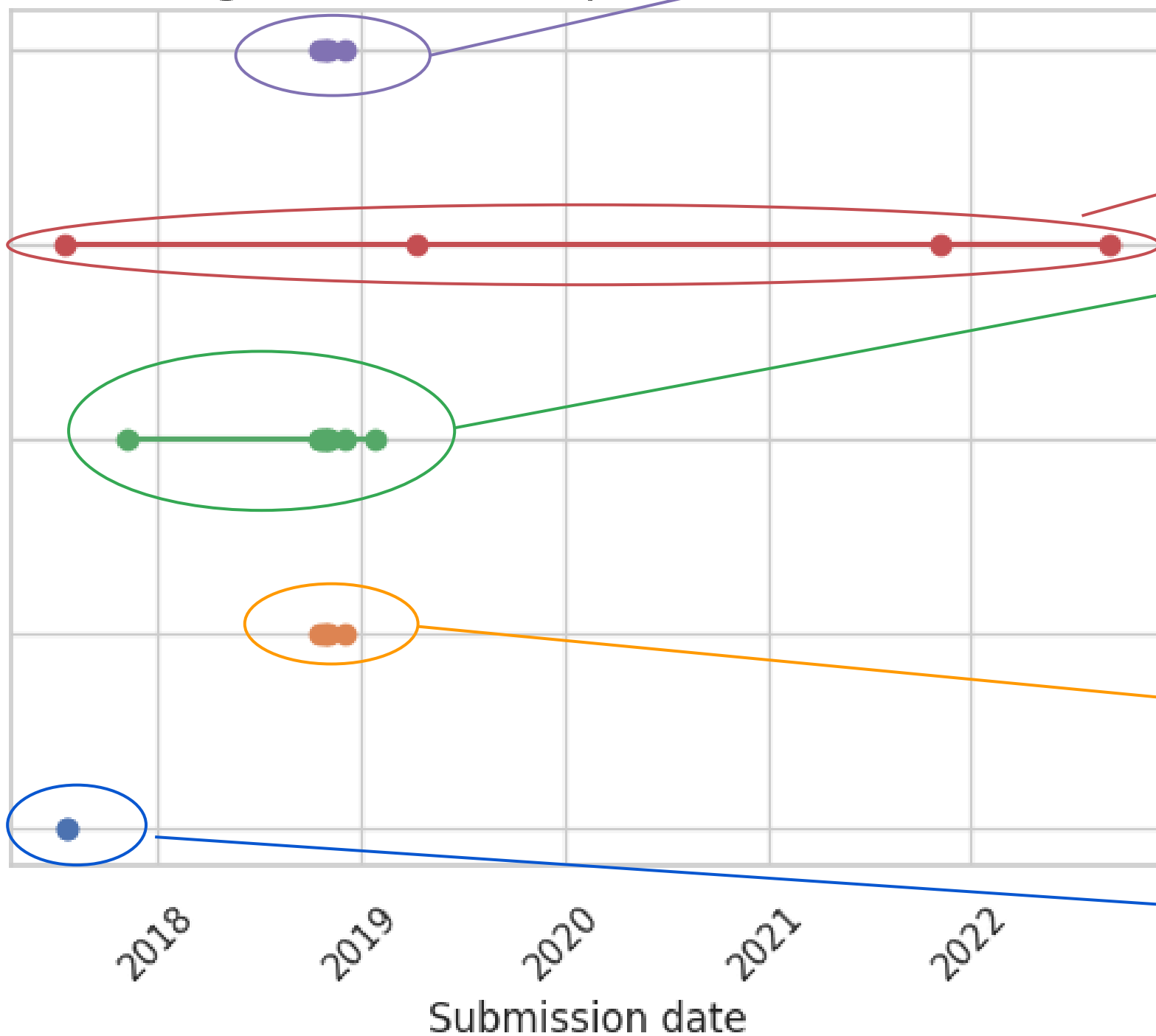
ITW examples - Office

# Scope

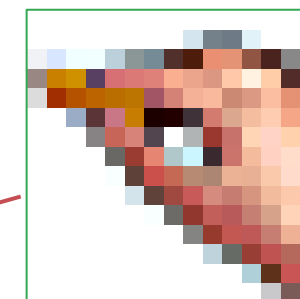


# APT28 - Images

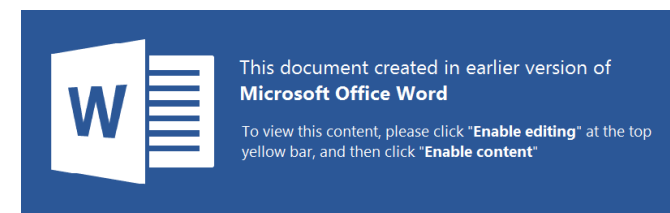
Images shared in multiple documents - APT28



Just a line (+100)



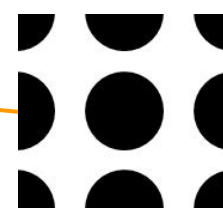
insignificant image of a hand (14)



Fake Office enable content image (13)

Image sha256

- 2a70b395de77141f2fa4962d604771c1e6ca0775a01781f74930db91862ad864 (2)
- 59c2fa4c1ffcab33b96ef7d60d5d9670e9087e0048ea60a67641dcc42837d81f (5)
- bf0c9670a430a089d83efea30e3514... (10)
- c1c821715f874dc2251a18cc474ec74... (59 (4)
- f5b1093fa378ad08fdeeb7cecec906d... (5)



??? (+100)

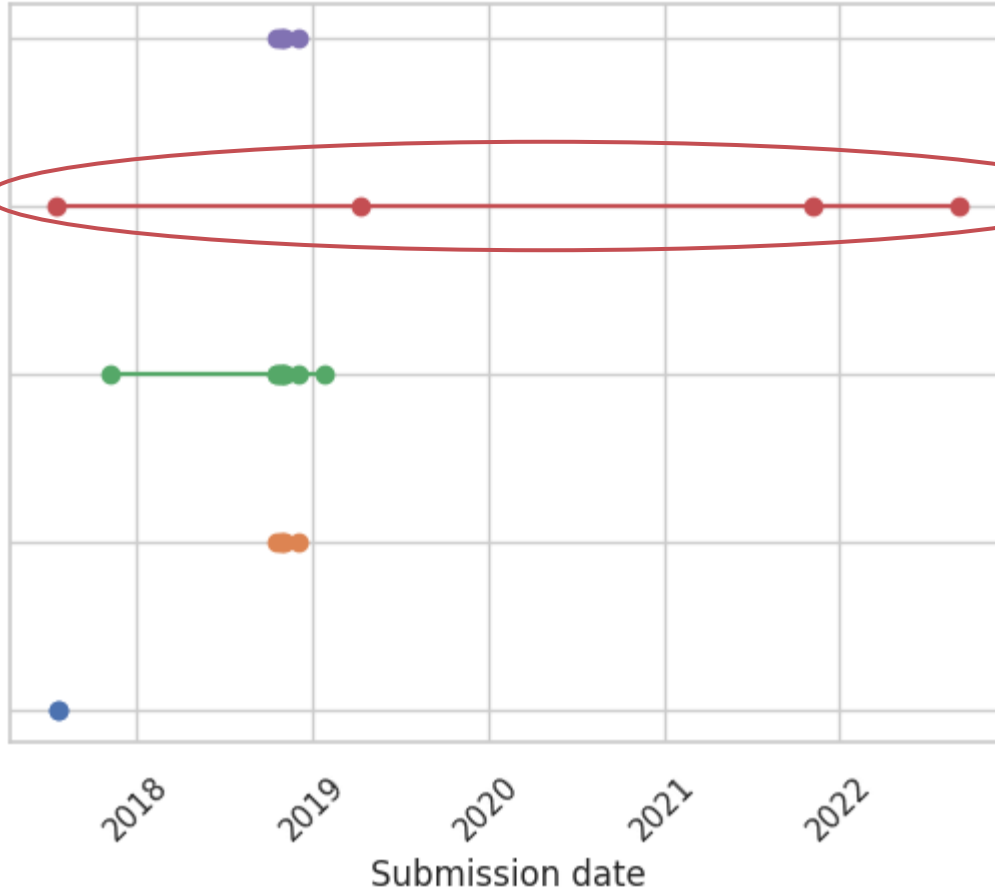
Fake EDA Roadmap European commission (4) (emf)

| EDA Work Strand    | EDA Deliverable  | Delivery Date          |
|--------------------|--|------------------------|
| R&T prioritization | OSRA <sup>1</sup> Version 0 including TBBs <sup>2</sup> 2017 Context, including links with CDP 2014 Methodology + Tools          | June 2017              |
| R&T prioritization | Approved OSRA v1 including prioritized TBBs  | December 2017          |
| CDP <sup>3</sup>   | CSDP Military Shortfalls   | December 2017          |
| CDP                | Long term Capability Trends Analysis   | December 2017          |
| CDP                | Assessment of Potential for Cooperation based on pMS plans and programs  | December 2017          |
| CDP                | Prioritized GMTL Tasks   | January 2018           |
| CDP                | EDA Proposal on EU Capability Development Priorities   | February 2018          |
| CDP                | Agreement on new set of EU Capability Development Priorities   | March 2018             |
| R&T prioritization | Revision of OSRA process<br>- Revised methodology<br>- Links with CDP 2018   | March 2018             |
| KSA                | Identification of KSA <sup>4</sup> at EU level after the application of KSA methodology to OSRA v1 and their approval            | April/ May 2018        |
| CDP                | Agreement on the implementation of EU Capability Development Priorities  | May 2018               |
| R&T prioritization | Approval OSRA v2 including prioritized TBBs in line with CDP 2018  | June 2018              |
| KSA                | Identification of KSA at EU level after the application of KSA methodology to OSRA v2 and CDP priorities 2018 and their approval | October/ November 2018 |

# APT28 - Images

c1c821715f874dc2251a18cc  
474ec7445149a943741594  
fd29ce2e282a877a59

Images shared in multiple documents - APT28



**Compressed Parents (14)**

| Scanned    | Detections | Type                     | Name   |
|------------|------------|--------------------------|--|
| 2020-11-22 | 5 / 66     | Office Open XML Document | Hotel_Reservation_Form.doc                                   |
| 2020-06-08 | 40 / 62    | Office Open XML Document | Hotel_Reservation_Form.doc                                   |
| 2020-06-09 | 40 / 62    | Office Open XML Document | 5e9056b5aca1839dc38ded0eded870be455e8c5303db6495255020       |
| 2024-02-07 | 47 / 65    | Office Open XML Document | apt  |
| 2020-10-28 | 0 / 65     | Office Open XML Document | Документ Microsoft Word.docx                                 |
| 2022-01-23 | 23 / 59    | Office Open XML Document | kl.doc   |
| 2024-02-19 | 42 / 65    | Office Open XML Document | KISD.zip   |
| 2021-11-30 | 30 / 61    | Office Open XML Document | dblink.doc   |
| 2022-09-11 | 32 / 64    | Office Open XML Document | C:\Users\<USER>\AppData\Local\Temp\9e77927c8f86bbbe22ea82f4  |
| 2021-11-14 | 3 / 60     | Office Open XML Document | off.doc  |
| 2024-02-20 | 45 / 65    | Office Open XML Document | b40cbf38284e6a1b9157002ad564e40fad2d85ba36437cf95c3b632      |
| 2022-07-27 | 36 / 61    | Office Open XML Document | C:\Users\<USER>\AppData\Local\Temp\1a56f5dd3c01901415300a15c |
| 2024-02-20 | 39 / 65    | Office Open XML Document |  |
| 2024-01-12 | 3 / 62     | Office Open XML Document |  |

**MANDIANT**  
NOW PART OF Google Cloud

Platform Solutions Intelligence Services Resources

## APT28 Targets Hospital Sector, Presents Threat to Travelers

LINDSAY SMITH, BEN READ

AUG 11, 2017 | 4 MIN READ | LAST UPDATED: AUG 10, 2023

**HOTEL RESERVATION WITH GUARANTEE**

Hotel name : \_\_\_\_\_

Guest name : \_\_\_\_\_

Guest nationality : \_\_\_\_\_

**RESERVATION INFO:**

Number of guests : \_\_\_\_\_

Number of rooms : \_\_\_\_\_

Room Type : \_\_\_\_\_

Check in date : \_\_\_\_\_

Check out date : \_\_\_\_\_

**Credit Card Information**

Card type : \_\_\_\_\_

Card number : \_\_\_\_\_

Expiry date (mm/yy) : \_\_\_\_\_ / \_\_\_\_\_

Cardholder's name : \_\_\_\_\_

Cardholder's address : \_\_\_\_\_

FRONT COPY OF YOUR CREDIT CARD (must to be provided according to the hotel)

BACK COPY OF YOUR CREDIT CARD (must to be provided according to the hotel)

I agree that one night room rate in fair period compensation per room will be charged for amendment or cancellation once reservation confirmed and one night room rate in fair period penalty per room will be charged for no show or early check out.

Signature: (same as appears on card) (written by hand) \_\_\_\_\_ date: \_\_\_\_\_

Your Passport Number: \_\_\_\_\_

Your Email Address: \_\_\_\_\_

Your Fax Number: \_\_\_\_\_

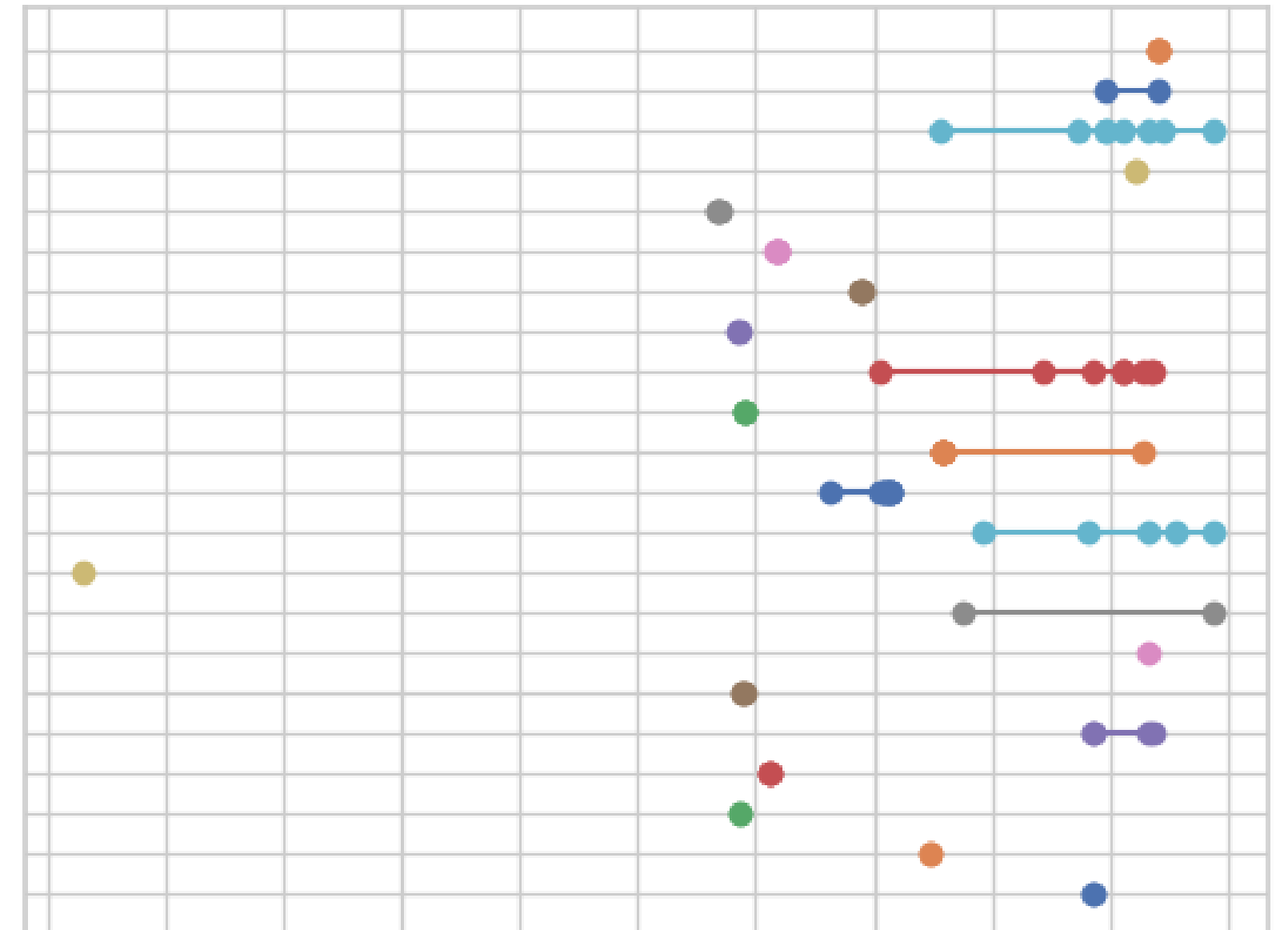
Your Telephone Number: \_\_\_\_\_



# Gamaredon - [Content\_Types].xml

[Content\_Types].xml shared in multiple documents - Gamaredon Group

ef355d5c6c8a718e971dc4c10746769af9ef5c5223da57ee8bbf385749c48cb5  
e1207710113aa8d21649e21b04d9bdc26ad4880360aef76c8f95505fe0868e8e  
dfa90f373b8fd8147ee3e4bfe1ee059e536cc1b068f7ec140c3fc0e6554f331a  
da3f604a5a73d53e2345d7e89db2ebdd8a5f41bb93ea94a04130ebc0e8662012  
c94946d6a2fbef319ee85fb485fe61d4a5caac7f9314e5f8a18bce89f92534a4  
c6de8acfdcbc515ea183ce876461b1d3c0d0d953d10962441d92c816385427b0  
a89712c843aa980af6833ecd3503a0c9d13d8c27b131e6b29d1789a5cb4733f2  
97e688635b2ed8b719b4218cdb86929d8a79fcd7cf59ef0c2521a1d845f92efe  
8bfaa27539716500b3240e688e4fdf5304fdeefe66276566959b91d9e479d92a  
7e06e02d14b36bbd047c91a6d605b72dce72e46cc68df2e51841a4e3b9a34187  
7bcad3e03afb79abd66837ac1a2bded9be508287718f608e35361e6e1ae6ab59  
775f8ca339ebe0ddcbe69474f2204b77088a9966ab5f2cadcf88fae724e9bf47  
72e1a7e789e238175e21a964870a263fd2426d6877bd868693e211a4eb23e587  
6f1ac5f0ebfb7e97d3dc4100e88eaab10016a5cac75e1251781f2ea12477af51  
6b207a20674d089c4355be395ce5c5f3fddcd2153fe00875b77324b169577cb3  
688dca40507fb96630f3df80442266a0354e7c24b7df86be3ea57069b25d12c6  
51ace631e30a76c6144eeb77ad60862e698a7e45143d15ea214905ac32a01173  
4f7fa7433484b4e655d185719613e2f98d017590146d15eedc1aa1d967636b3a  
44dc4519f570f0f045b997b61180d79257f92b5cdc076df6a67d3b2f4113c755  
388cb33f3f90471a1c04e5fd1bfb92f68e42f75de3e0ea602b59150c7be25aa0  
233afba2a1ba0a2e67fa19ad6a0a053de83051067a52a930022ed1c6bc5b0a5d  
0595fec92ebaa39887b56218746ec6b116c3aa2849f96ee1f0011729729de559

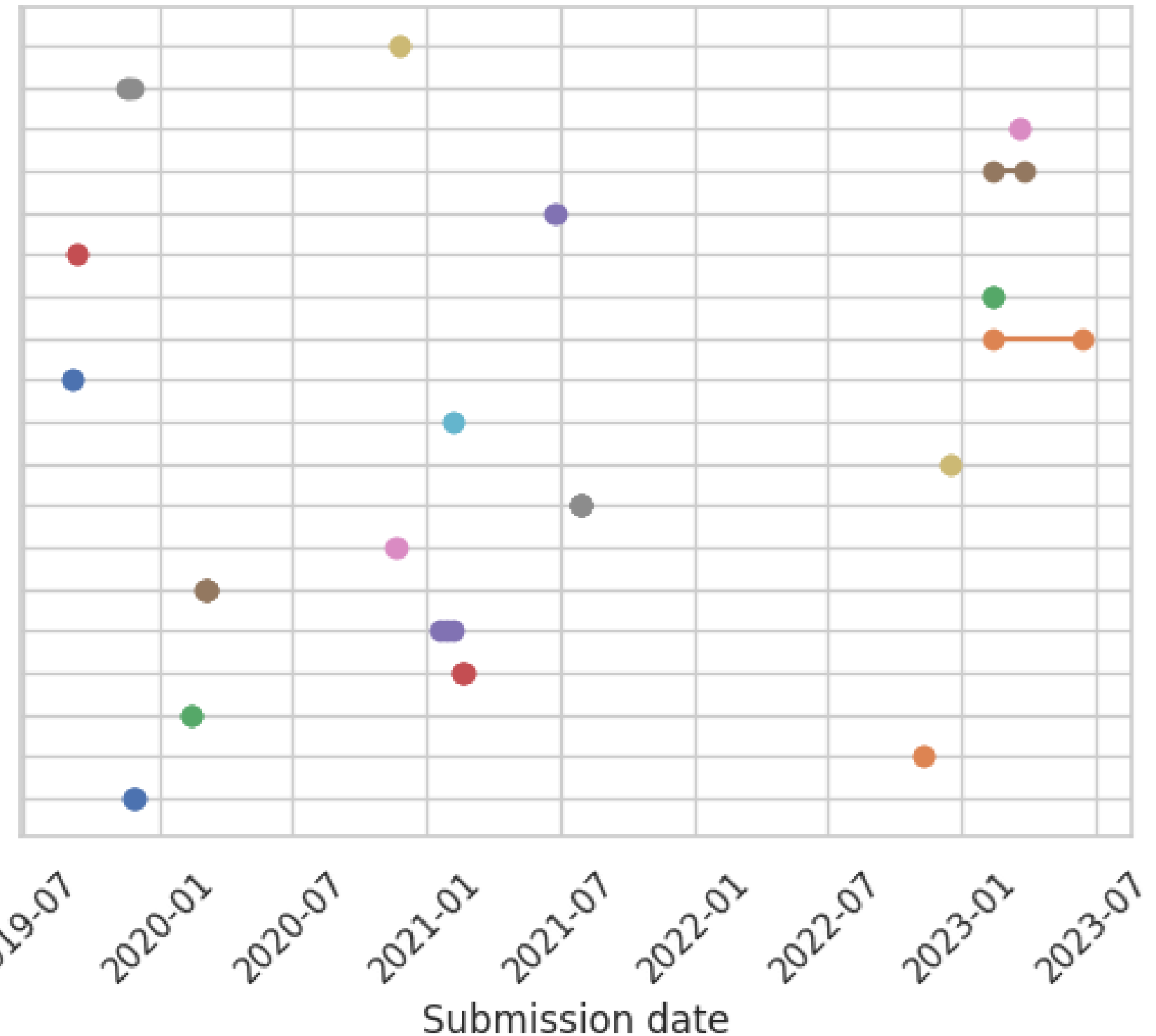


# Gamaredon - styles.xml

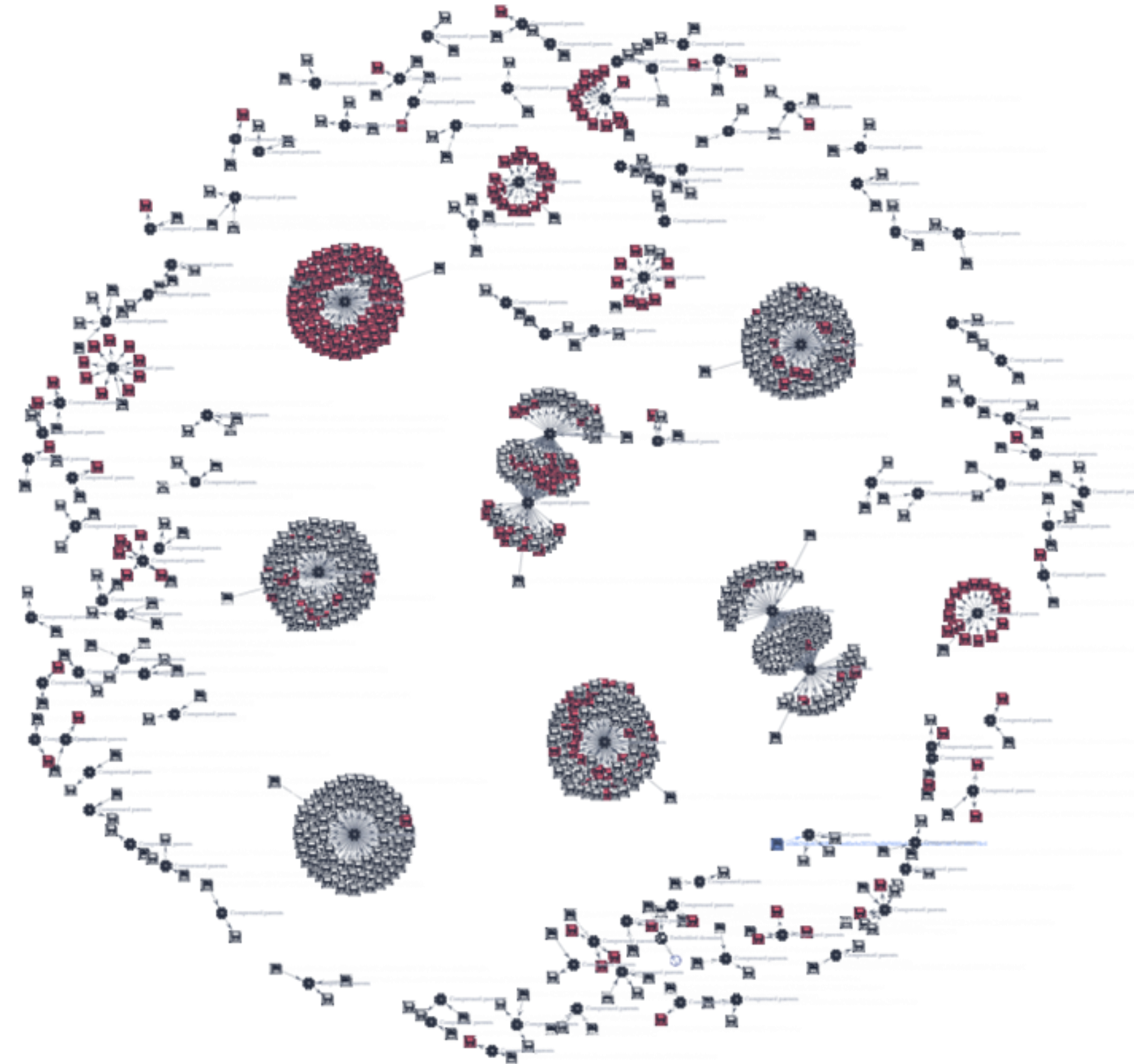
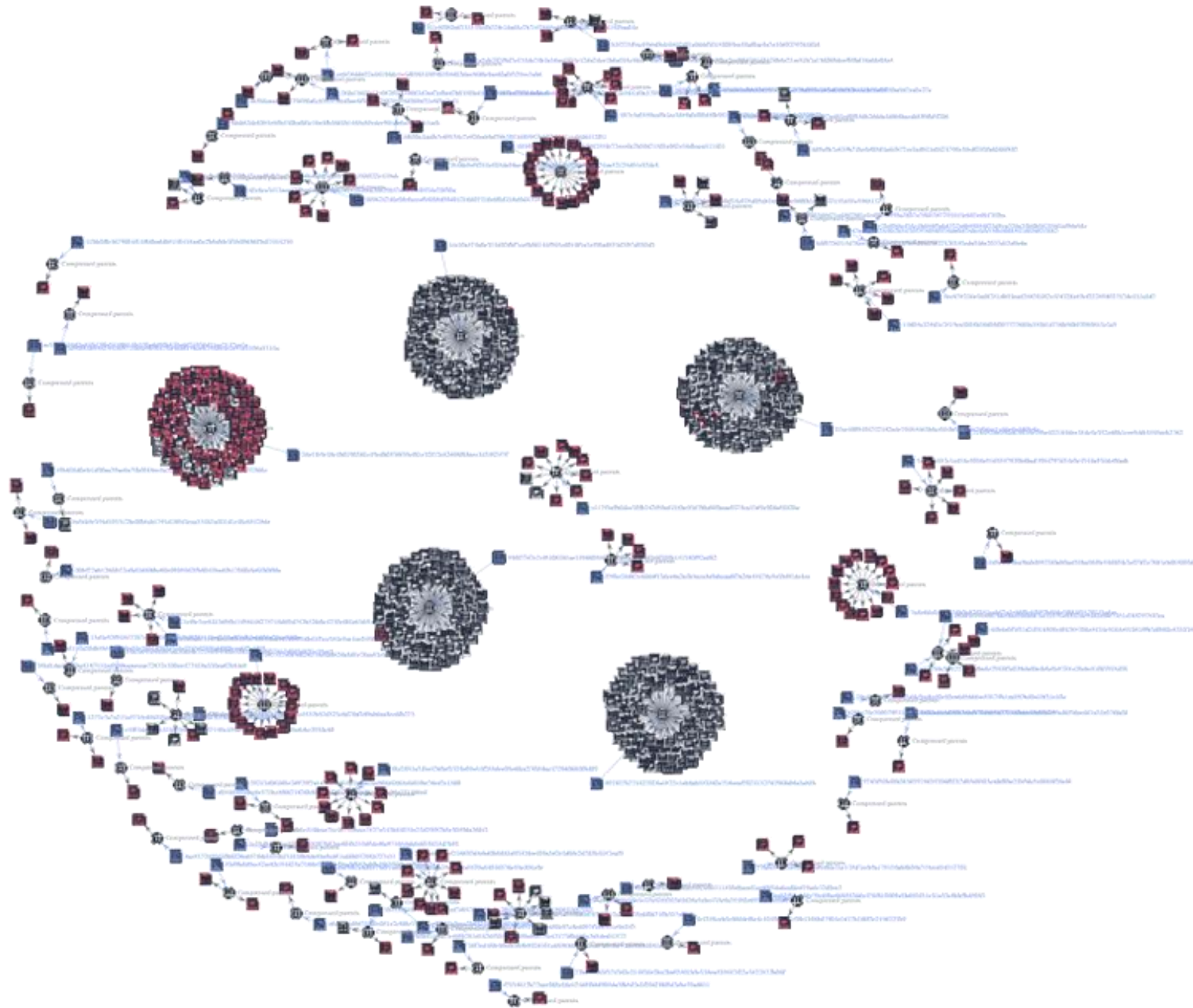
```
fdab82de6093e50b430bafd3c10a4fb46d4b1465a89cdce901ae6a56d75b1aeb  
f79be7dd67c8dddf13dce6a2a4b5aca5a9abcaa6f7a26e55478c9e3bf51dc4ec  
f5f06b4070c61248bf15c075d09ab7a6c26ec06f6b1ecf5a22143d35c5568132  
d2bc4e1a86b0300469243bfc1df1c5552b82d523c6d7faf369abdaa8ecdfb273  
c2060bde81513f4ed4cdbel1a7550d0f7879b893a28b729edf06710b327af4e1a  
baed7e3366ebfe5e37b4258303d4676c3cbc135e9a75450c693a0b8dfddf1db7  
b3f723f5ac59de6b4c0d10df1a0ddd30150099ee58af0ac0a7a10d0270764836  
897627b774427028a4527c1ab6ab553562e716eeaf702413276796fa06a3a84b  
81e40980a8333135edb22fe1dad8c7b7107665cada44dd84d2b4d1d1f49aa04e  
64b6e0f3f31d24918909cdf4285708e5434c9185e91051f9b3df580c83303500  
59df7787c7cf5408481ae149660858d3af765a0c2cd63d6309b151380f92adb2  
489824240e0fefcccf98f48699d9421660721fc6f0d24fa5b015393584db88b  
407c3a0359aa9b4ce365fafcf00d5fb9874e8a3f6da29ed92645eadc277f920c  
3ff2337e0f56626218e8a6526a8d5e78aa53eb6e88ce666b15e02c9712ece220  
3ed464652c1cd18c5036e5163557920b6bad1984797d34e0e4344a934dcfdaab  
2ed78dc9f0b4216892d5ebd0b8684d9352fee409a3d2e4d0fc2d762b4457eaf3  
2de1fc9c48c4b0190361c49cdb053fd39cf81e32f12c82d08f88aec34358257f  
28fa1364fa13a082f1a159883d2ad7cfbed2b0350bd10e2c13b8ce0b016a6ecd  
14605a329d3c7519ca4008b36d0fd007727660a330d1d736b56b92080843c3a9
```

styles.xml

styles.xml shared in multiple documents - Gamaredon Group

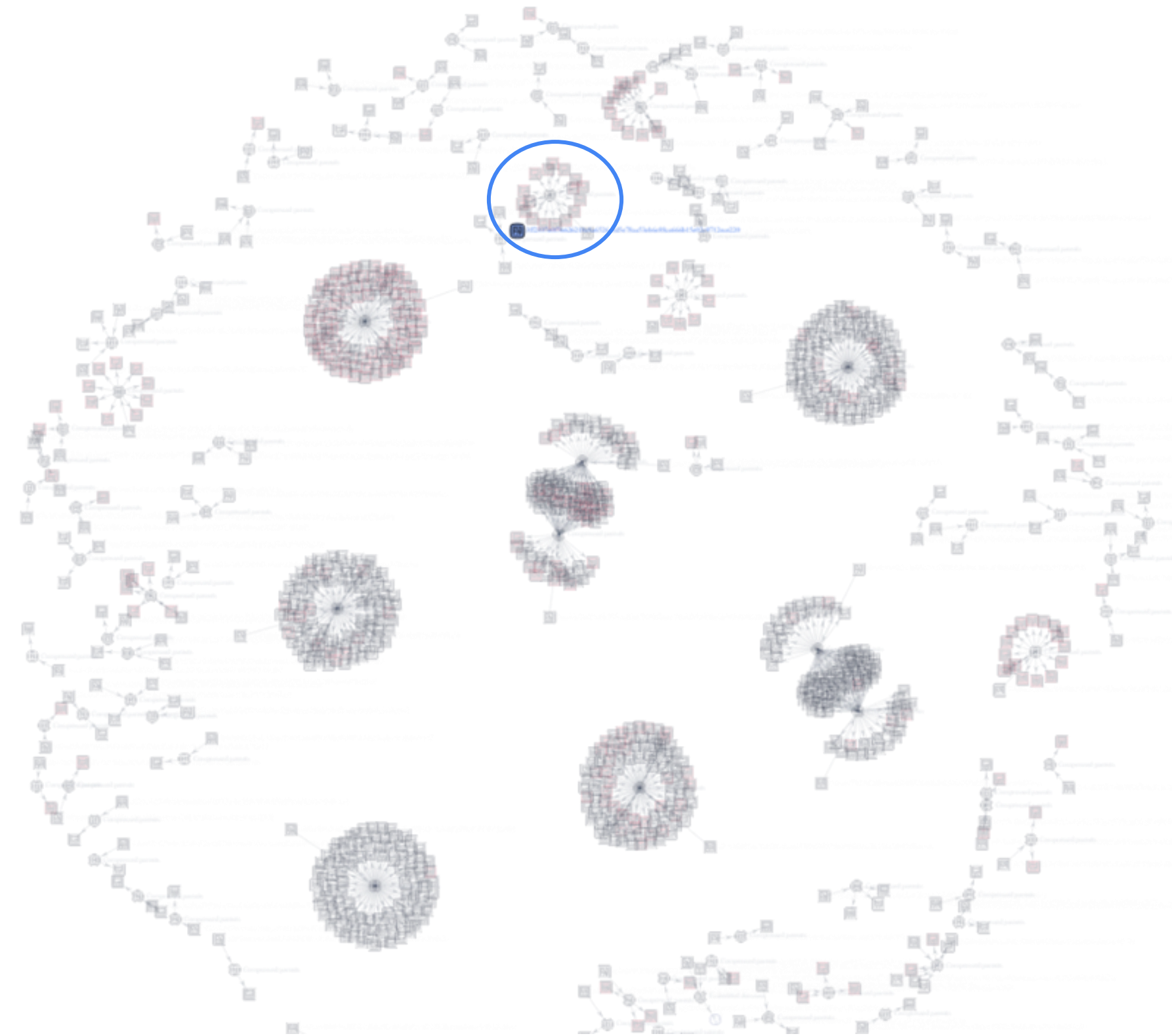
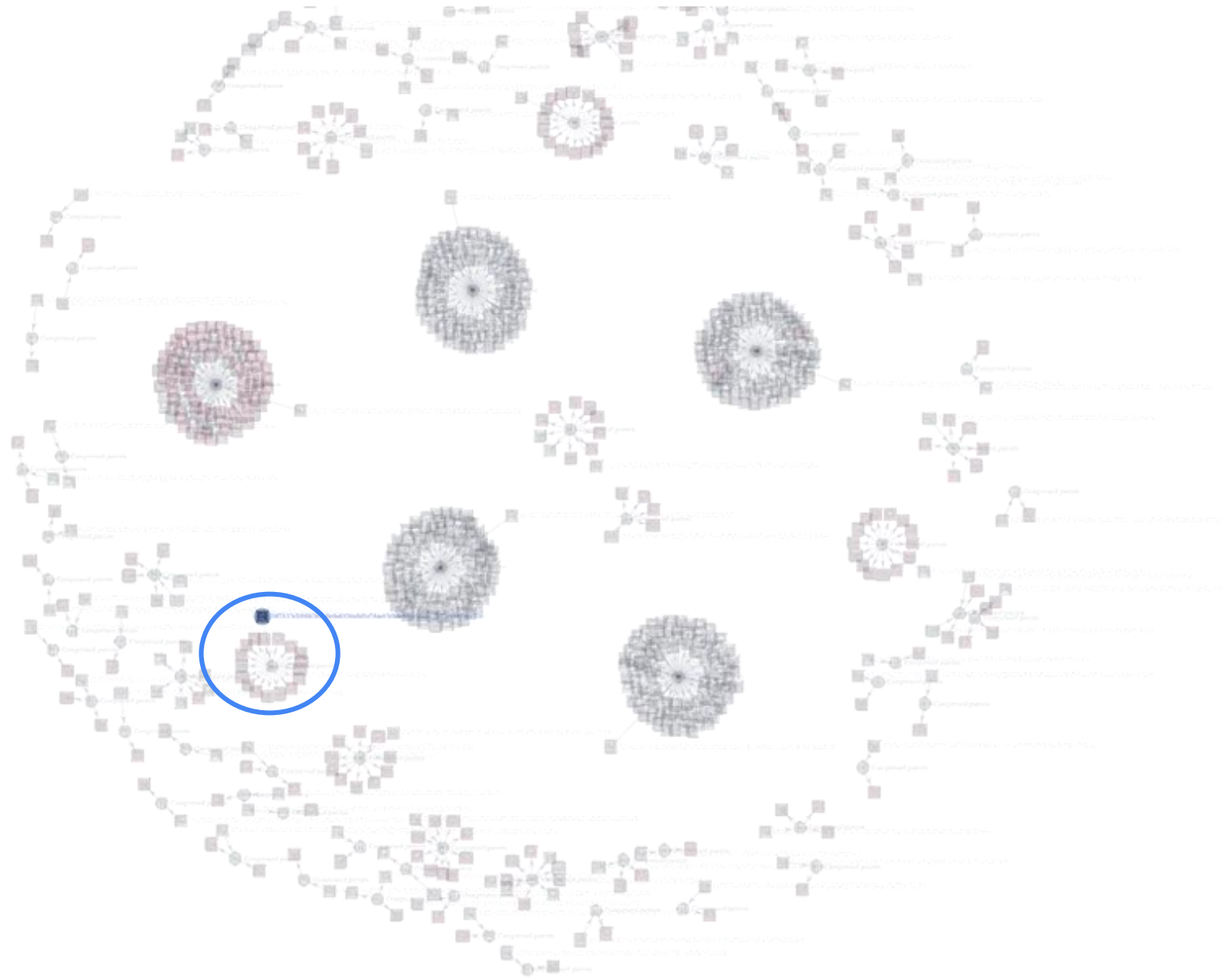


# Gamaredon - styles.xml



# Gamaredon - styles.xml

---



# Gamaredon - styles.xml

"Foreign institutions of Ukraine"  
Embassy of Ukraine in Hungary

0 / 59  
Community Score

✔ No security vendors and no sandboxes flagged this file as malicious

3ff2337e0f56626218e8a6526a8d5e78aa53eb6e88ce666b15e02c9712ece220  
word/glossary/styles.xml  
xml

Sample

## Compressed Parents (17)

| Scanned    | Detections | Type                     |
|------------|------------|--------------------------|
| 2024-02-20 | 28 / 63    | Office Open XML Document |
| 2024-02-20 | 36 / 64    | Office Open XML Document |
| 2024-02-10 | 37 / 63    | Office Open XML Document |

## „Закордонні установи України”

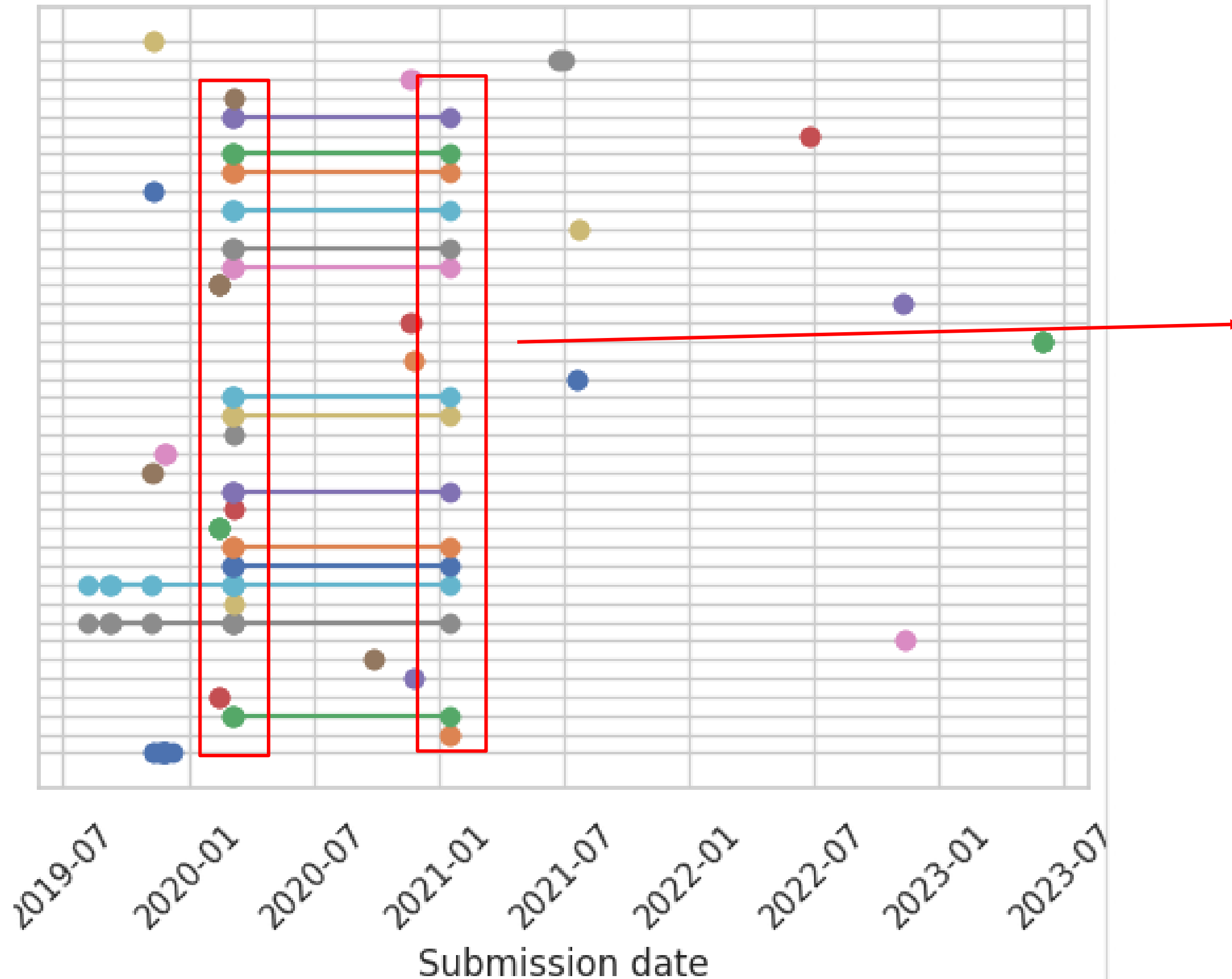
| 2 €Д                                     | УГОРЩИНА                                   | HU 61311  |
|--|--|---|
| Посольство України в Угорщині            |  |   |
| Представник України в Дунайській комісії |  |   |
| Н-1125 Budapest, Istenhegyi u. 84/b      | 08:00 – 17:00<br>12:00 – 13:00             | www.hungary.mfa.gov.ua<br>www.facebook.com/ukran.na<br>gykovetseg.magyarorszag<br>emb_hu@mfa.gov.ua<br>(00 36) 1 422 41 20<br>(00 36) 1 220 98 73 |
| Надзвичайний і Повноважний Посол         | <b>НЕПОП</b><br>Любов Василівна            | ip. 90 36 01 3000   |
| Радник                                   | <b>ЛУПАК</b><br>Андрій Андрійович          | ip. 90 36 01 3001   |
| Радник                                   | <b>БАЛОГ</b><br>Іштван Арпадович           | (00 36) 1 422 41 10   |
| Перший секретар                          | <b>АЛЕКСАНДРОВ</b><br>Сергій Олександрович | ip. 90 36 01 3002   |
| Перший секретар                          | <b>АХУНОВ</b><br>Рустам Ринатович          | (00 36) 1 422 41 16   |
| Перший секретар з консульських питань    | <b>ГАЛАЙКО</b><br>Олег Федорович           | (00 36) 1 422 41 22   |
| Перший секретар                          | <b>КОНДИК</b><br>Олексій Павлович          | (00 36) 1 422 41 15   |
| Перший секретар                          | <b>ЛУКАЧУК</b><br>Іван Миколайович         | (00 36) 1 422 41 13   |
| Перший секретар                          | <b>ПАСІЧНИК</b><br>Сергій Павлович         | (00 36) 1 422 41 51   |
| Перший секретар                          | <b>ПИЛИПЕНКО</b><br>Олег Вадимович         | (00 36) 1 422 41 29   |

Almost all of them were like this



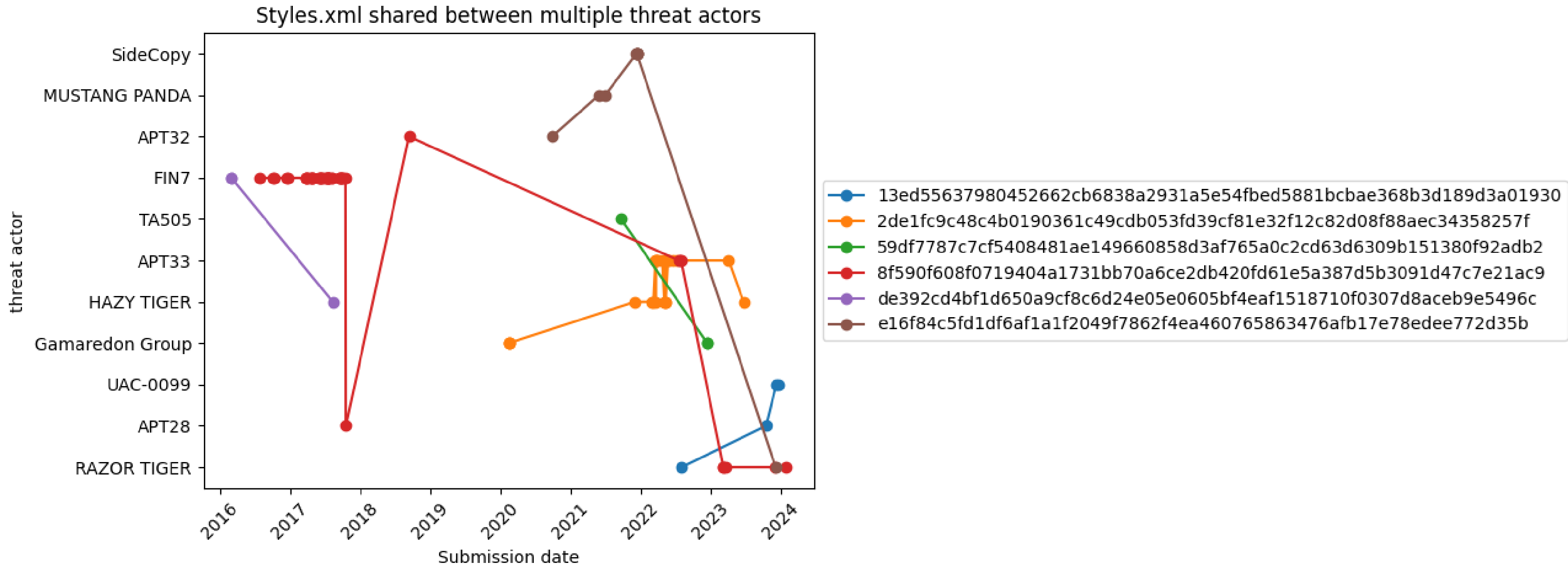
# Gamaredon – from styles to images

Images shared in multiple documents - Gamaredon Group

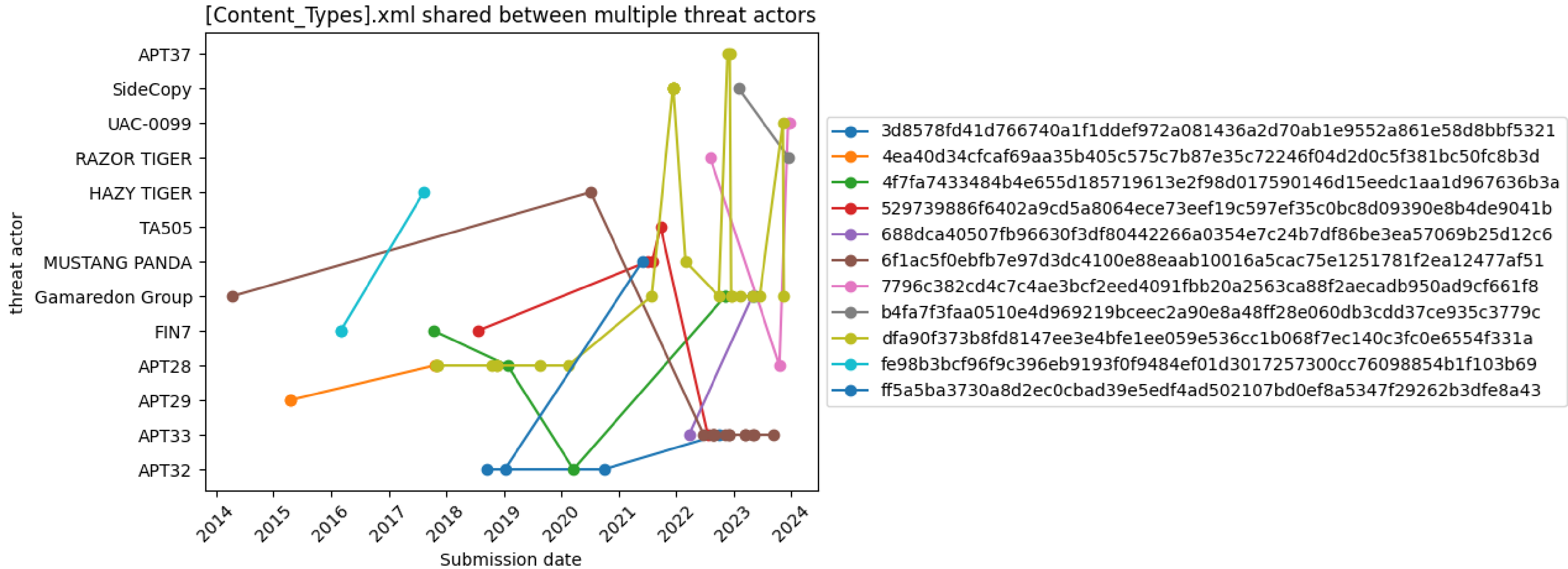


| Compressed Parents (12) ⓘ |            |                          |
|---------------------------|------------|--------------------------|
| Scanned                   | Detections | Type                     |
| 2024-03-26                | 36 / 62    | Office Open XML Document |
| 2024-02-23                | 31 / 62    | Office Open XML Document |
| 2024-02-23                | 21 / 48    | Office Open XML Document |

# Styles.xml shared between threat actors

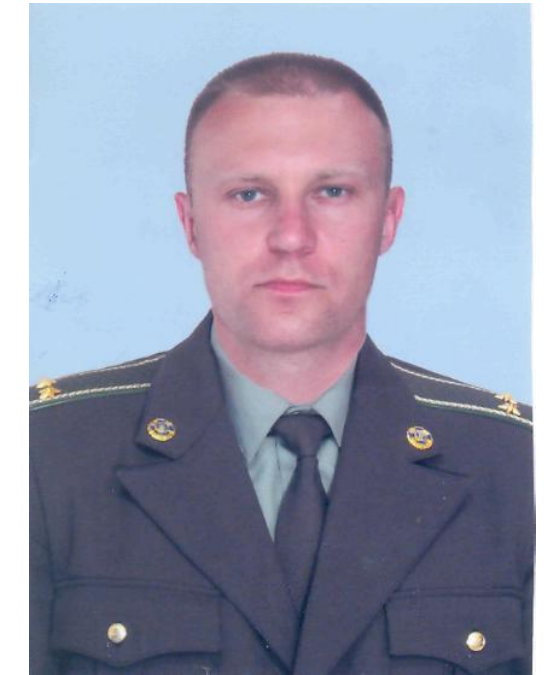


# [Content\_Types].xml shared between threat actors





# Applying AI Gemini



=====

id: eeedb710a58783bc790a4251db4d11e9efc7298ae4a81cb1fefbfff6071cb3608  
response: [Quirinale, Presidenza della Repubblica Italiana]

=====

id: 12dc492bcd1ecce31326b7e1b0a1b7c8b9236b8735e0b691df4bd765d696d7a7  
response: [Ukrainian State Border Guard Service]

=====

id: dde5c64671da502aaf82e33649385e443731f0f67de8d34a73a0c2282af3b1d3  
response: [National Health Commission of the People's Republic of China]

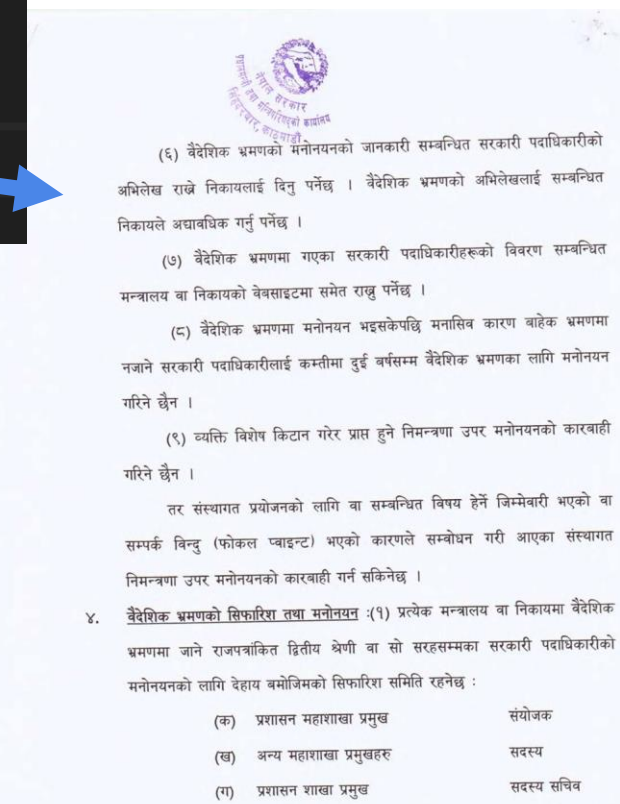
=====

id: c0d57fbbb1221e270d8b80eacc9040df9f2c0577959d67034afe52119298e8a3  
response: [नेपाल सरकार, निर्वाचन आयोग]

=====



中华人民共和国国家卫生健康委员会  
National Health Commission of the People's Republic of China



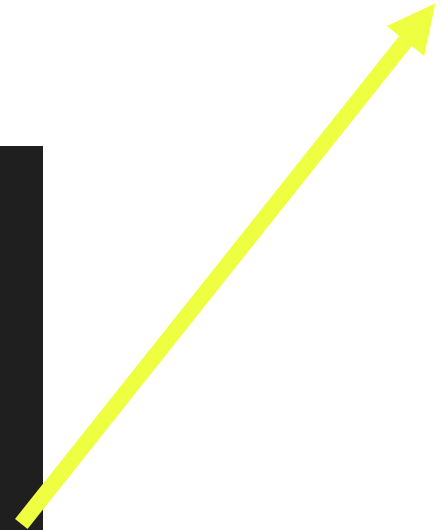
# Applying AI Gemini

```
-----  
id: 88bb63ad01a8b1e1307e8db045b0242a060fa8df00a1530410b207c09bdb2f56  
response: [citi, deutsche bank, mastercard, visa]  
=====
```

```
id: 5aceb0afa9def9efacfa9e7ccc6a4639b78292a1881580caa349504a49274d3d  
response: [Google]  
=====
```

```
id: 9c99ec61392b9022a38c1354124360147e8185065095bd2ec92b1416cf9f4b68  
response: [Pepsi, Sprite]  
=====
```

```
id: ecf5cb7407f0515d4010ea83ecf13e73b69e7bea7ebd2685035d7910cd7c0b7c  
response: [Body Sculpture]  
=====
```

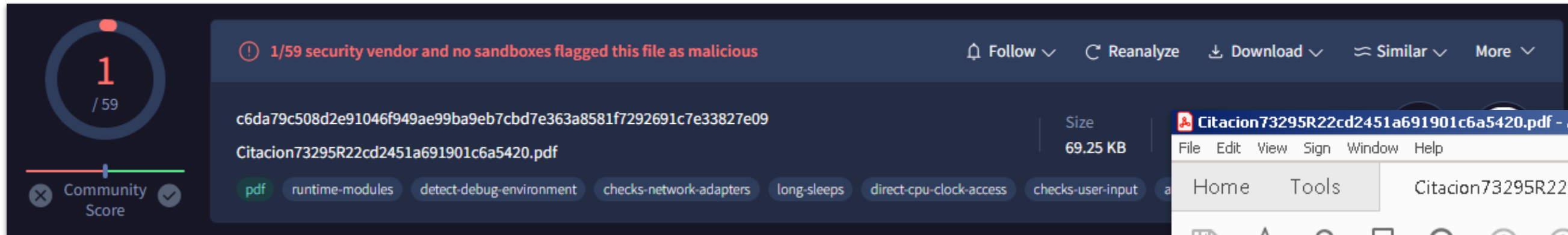


PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. [Enable Editing](#)

04

ITW examples - PDF

# Blind Eagle



1 / 59

1/59 security vendor and no sandboxes flagged this file as malicious

Follow Reanalyze Download Similar More

c6da79c508d2e91046f949ae99ba9eb7cbd7e363a8581f7292691c7e33827e09

Citacion73295R22cd2451a691901c6a5420.pdf

Size: 69.25 KB

pdf runtime-modules detect-debug-environment checks-network-adapters long-sleeps direct-cpu-clock-access checks-user-input

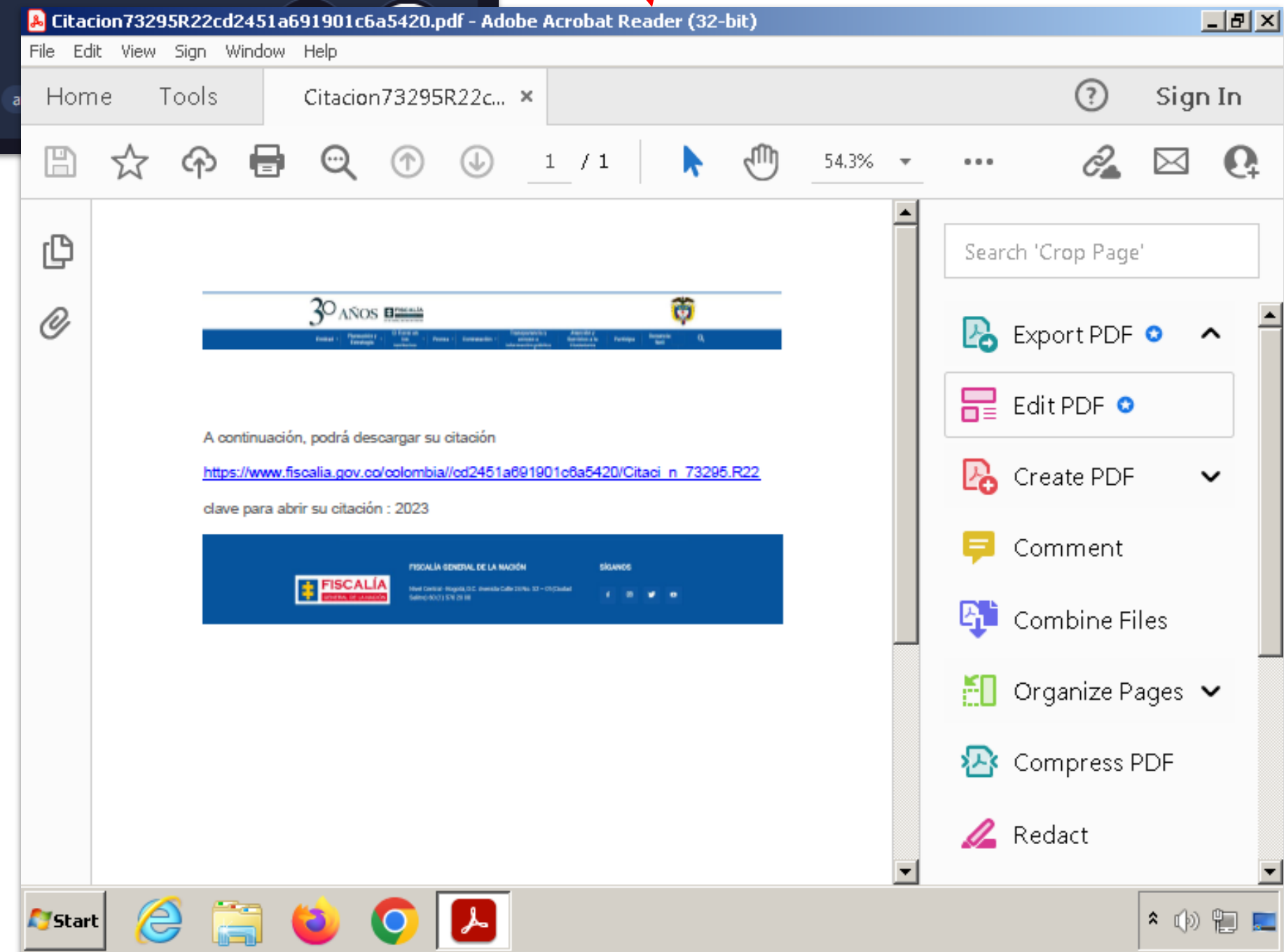
Community Score

[Sample](#)

## DFIR TIP

If you are in an incident response where PDF files were involved and opened by Adobe, remember that you have the thumbnail of the first page stored in `C:\Users\\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons` 🔍

These files are dropped during the execution of the PDF



Citacion73295R22cd2451a691901c6a5420.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools Citacion73295R22c... x Sign In

1 / 1 54.3%

Search 'Crop Page'

Export PDF

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Redact

30 AÑOS

A continuación, podrá descargar su citación

<https://www.fiscalia.gov.co/colombia/od2451a691901c6a5420/Citacion73295R22cd2451a691901c6a5420.pdf>

clave para abrir su citación : 2023

FISCALÍA GENERAL DE LA NACIÓN

# Blind Eagle

## Dropped Files (42)

| Scanned    | Detections | File type | Name   |
|------------|------------|-----------|--|
| 2023-02-23 | 0 / 58     | DOS COM   | C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index |
| 2024-03-15 | 0 / 61     | ZIP       | C:\Users\<USER>\AppData\Local\Temp\A9102w9zo_1glgy9e_20g.tmp                                     |
| 2023-03-01 | 0 / 59     | DOS COM   | C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index |
| 2023-03-01 | 0 / 59     | Text      | C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json                           |
| 2023-09-14 | 0 / 59     | JSON      | 102/Google/Chrome/User Data/SwReporter/107.294.200/manifest.json                                 |
| 2023-09-14 | 0 / 59     | Text      | 102/Google/Chrome/User Data/SwReporter/107.294.200/manifest.fingerprint                          |
| 2023-02-23 | 0 / 59     | DOS COM   | C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index |
| 2023-02-22 | 0 / 58     | BMP       | C:\Users\<USER>\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-230319231531Z-499.bmp      |
| 2023-02-23 | 0 / 59     | Text      | C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json                           |
| 2024-02-16 | 0 / 72     | Win32 EXE | c:\users\AliArbia\AppData\Local\Google\Chror   |



Community Score

No security vendors and no sandboxes flagged this file as malicious

Follow Reanalyze Download Similar More

4a4c82a81dfd6ca6c81184d1ee8002b5472caac4e63549b1fc473f52db54b02a

C:\Users\<USER>\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-230319231531Z-499.bmp

Size  
69.52 KB

Last Modification Date  
1 year ago



DETECTION DETAILS RELATIONS CONTENT TELEMTRY COMMUNITY

### Execution Parents (6)

| Scanned    | Detections | Type | Name   |
|------------|------------|------|--|
| 2023-04-20 | 14 / 60    | PDF  | Citacion73295R22cd2451a691901c6a5420.pdf     |
| 2023-03-09 | 0 / 59     | PDF  | Citacion73295R22cd2451a691901c6a5420 (1).pdf |
| 2024-03-15 | 21 / 61    | PDF  | Citacion73295R22cd2451a691901c6a5420.pdf     |
| 2023-03-09 | 1 / 59     | PDF  | Citacion73295R22cd2451a691901c6a5420.pdf     |
| 2023-10-13 | 1 / 59     | PDF  | Citacion73295R22cd2451a691901c6a5420.pdf     |
| 2023-03-26 | 1 / 54     | PDF  | Citacion73295R22cd2451a691901c6a5420.pdf     |

### Today (2)



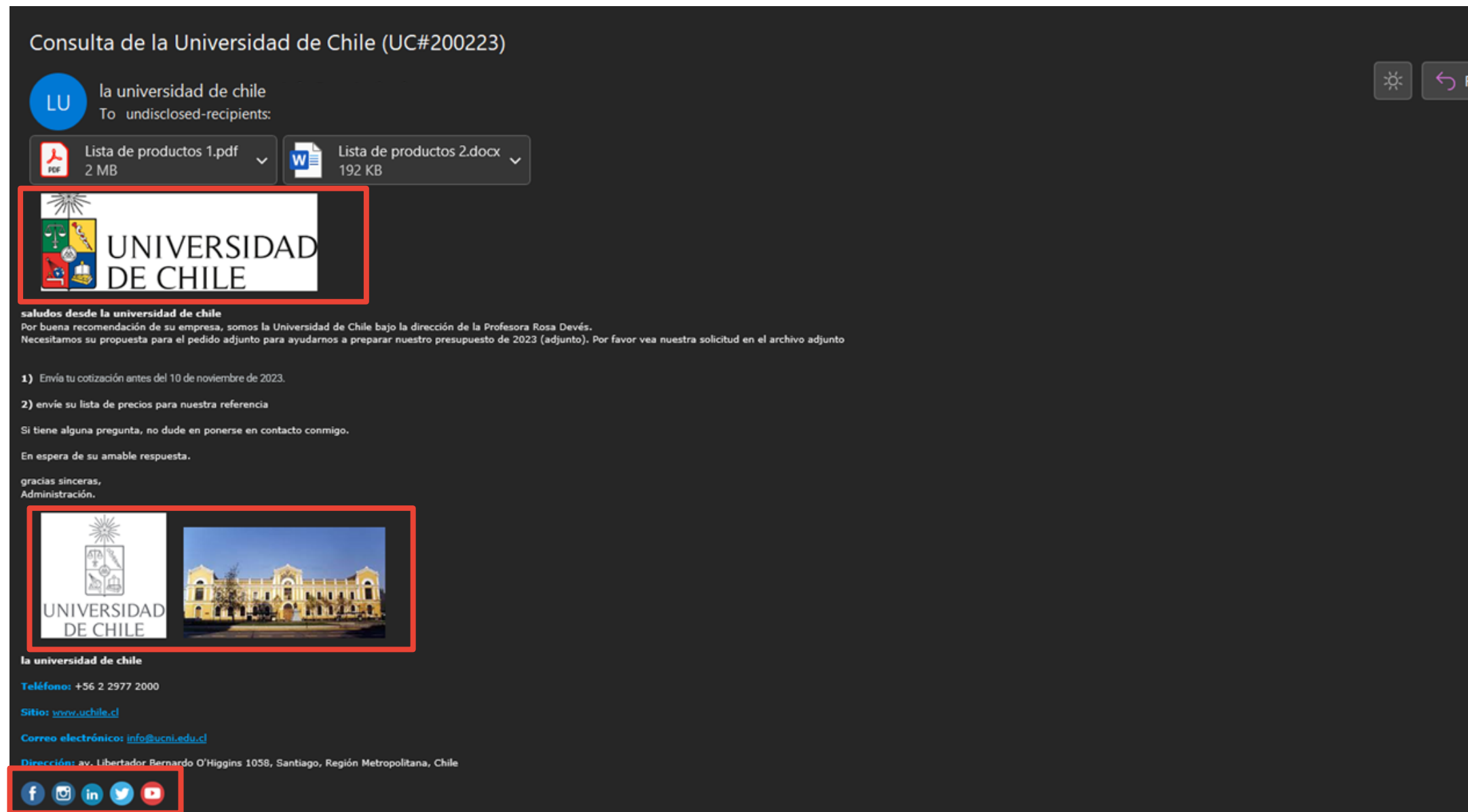
4a4c82a81dfd6ca6c81184d1ee8002b5472caac4e63549b1fc473f52db54b02a.bmp

05

ITW examples - Emails

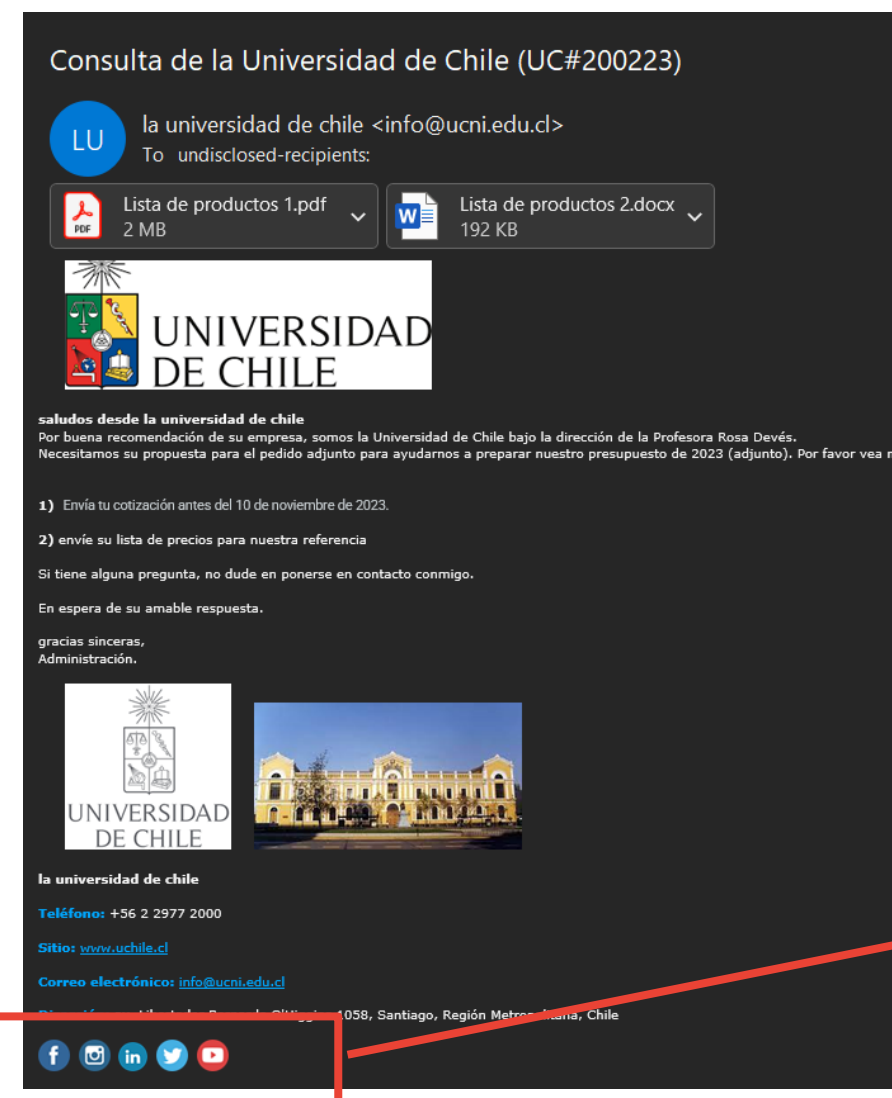
# Don't forget to follow us on social networks! > Fail

## Sample



# Don't forget to follow us on social networks! > Fail

Pivoting using the footer images from this campaign



| Scanned    | Detections | File type                | Name                           |
|------------|------------|--------------------------|--------------------------------|
| 2023-11-08 | 0 / 60     | PNG                      | linkeldin.png                  |
| 2023-02-16 | 0 / 60     | PNG                      | instagram.png                  |
| 2023-11-10 | 34 / 60    | PDF                      | Lista de productos 1.pdf       |
| 2023-02-16 | 0 / 59     | PNG                      | twitter.png                    |
| 2023-11-20 | 35 / 64    | Office Open XML Document | 54376ee15cca7c6cdecc27b701b... |
| 2023-11-08 | 0 / 60     | PNG                      | cl2.png                        |
| 2023-11-10 | 0 / 60     | PNG                      | facebook.png                   |
| 2023-02-16 | 0 / 60     | PNG                      | youtube.png                    |
| 2022-08-16 | 0 / 59     | PNG                      | cl1.png                        |
| 2023-11-08 | 0 / 60     | JPEG                     | cl22.jpg                       |

Images attached in the email

Other 33 emails with the same footer images affecting in other countries and universities

| Scanned    | Detections | Type    | Name   |
|------------|------------|---------|--|
| 2023-03-14 | 27 / 60    | Email   | 3yOXfEI-67450-E219181982653EE36201b4696.txt                                  |
| 2022-07-29 | 24 / 61    | Outlook | FW 緊急: 詢價 (2022 年學校預算) .msg  |
| 2022-08-03 | 15 / 61    | Outlook | Acil Teklif Talebi (2022 okul projesi).msg                                   |
| 2022-07-27 | 11 / 60    | Outlook | SpamTrap 緊急: 詢價 (2022 年學校預算) SpamTrap .msg                                   |
| 2023-11-16 | 31 / 61    | Email   | Consulta de la Universidad Nacional de Colombia (UNAL#151123).eml            |
| 2022-07-27 | 10 / 61    | Outlook | 緊急: 詢價 (2022 年學校預算) .msg   |
| 2022-11-22 | 23 / 62    | Email   | 29d6a6f71d3c8b35cb96fa8a32c4fa01aa5b84e553edbc850501d9164795a19b             |
| 2022-07-28 | 10 / 61    | Email   | Temp[119].eml  |
| 2022-11-22 | 22 / 62    | Outlook | 37993bdaf1b183b4ca12d780fecc195392948dac0830ea8990953656ae2e32d2             |
| 2023-11-15 | 31 / 61    | Email   | 3yPyxD-67450-0920E2263924CF255560053baf7.txt                                 |
| 2022-07-28 | 17 / 61    | Email   | Fw 緊急: 詢價 (2022 年學校預算) .eml  |
| 2022-11-10 | 24 / 59    | Outlook | FW_Acil_Teklif Talebi (Koç 2022 okul projesi).msg                            |
| 2022-11-22 | 25 / 62    | Email   | fc355b1d-6499-4694-6318-08dacbcb24f/934cf05b-b2ee-d9b3-917d-a3fe13db330b.eml |
| 2023-03-12 | 0 / 59     | Email   | 1843529230925574232.eml  |
| 2023-11-09 | 33 / 61    | Email   | Consulta de la Universidad Central del Ecuador (UCE#081123).eml              |
| 2023-11-26 | 29 / 60    | Outlook | 7dbe02ad41a4cc350590955efe3f4bc033220d0bf9927c2d10f2651216d40d0              |
| 2023-12-03 | 28 / 61    | Outlook | Consulta de la Universidad de Chile (UC#200223).msg                          |



# Don't forget to follow us on social networks! > Fail

FW: Solicitare de la Universitatea din Bucuresti (BUC#140223)

OP Office Paid Romania

Lista de întrebări de la Universitatea din București (BUC#150223).docx .docx File



**Salutări de la Universitatea din București**


În urma recomandărilor bune din partea companiei dumneavoastră, suntem Universitatea din București sub conducerea profesorului Avem nevoie de propunerea dvs. pentru comanda atașată pentru a ne ajuta să ne pregătim pentru bugetul 2023 (anexat). Vă rugăm

- 1) Trimiteți oferta înainte de 18 februarie 2023.
- 2) Vă rugăm să trimiteți lista de prețuri pentru referință

Dacă aveți întrebări, vă rugăm să nu ezitați să mă contactați.

Așteptam răspunsul tau amabil.

Sincere mulțumiri,  
Admin.




**Universitatea din Bucuresti**

Telefon: +40 21 307 2400

Site: [www.unibuc.ro](http://www.unibuc.ro)

E-mail: [info@unibuc.edu.com](mailto:info@unibuc.edu.com)

Adresa: Bulevardul Regina Elisabeta Nr. 4-12, București 030018, România



Posible Spam!:Consulta de la Universidad Nacional de Colombia (UNAL#151123)

UN Universidad Nacional de Colombia  
To undisclosed-recipients:

Lista de productos 1.pdf 1 MB

Lista de productos 2.docx 362 KB



Saludos desde la Universidad Nacional de Colombia

Seguindo la buena recomendación de su empresa, somos la Universidad Nacional de Colombia bajo la dirección del Profesor Rodolfo Hernández Suárez. Necesitamos su propuesta para el pedido adjunto para ayudarnos a preparar nuestro presupuesto de 2023 (adjunto). Por favor vea nuestra solicitud en el archivo adjunto

- 1) Envía tu cotización antes del 17 de noviembre de 2023.
- 2) envíe su lista de precios para nuestra referencia

Si tiene alguna pregunta, no dude en ponerse en contacto conmigo.

En espera de su amable respuesta.

gracias sinceras,  
Administración.



Universidad Nacional de Colombia

Teléfono: +57 13166000

Site: [www.unal.edu.co](http://www.unal.edu.co)

Correo electrónico: [info@unal.edu.co](mailto:info@unal.edu.co)


Dirección: Cra 45, Bogotá, Colombia



緊急：詢價（2022 年學校預算）

JC jaguar chang <jaguar.chang@ms1.hland.com.tw>  
To

項目 NTU\_0027072022.docx .docx File



來自台灣大學的問候

在貴公司的良好推薦下，我們是在Chi-Huey Wong的指導下的國立台灣大學。我們需要您對所附訂單的建議，以幫助我們準備2022年預算（附後）。請在附件中查看我們的詢求


- 1)在 2022 年 7 月 29 日之前提交報價。
- 2)請發送您的價目表供我們參考

如果您有任何問題，請隨時與我聯繫。

等待您的善查回應。

s

—



國立台灣大學  
National Taiwan University


國立台灣大學

電話：+886 2 3466 3766

網址：[www.ntu.edu.tw](http://www.ntu.edu.tw)

郵箱：[info@taiuni.edu.com](mailto:info@taiuni.edu.com)

地址：台灣台北市大安區羅斯福路四段1號 10617



05

Conclusions and limitations

# Conclusions - Limitations

---

We can potentially trace malicious individuals by examining evidence linked to the initial documents they use to launch their intrusions.

- Today we do not incorporate **bundled\_files** into the JSON structure that can be used to create a livehunt rule, **but it is planned to be added**. Instead we can use **vt\_behaviour\_files\_dropped.sha256** for those scenarios where the files are dropped.
- In certain situations, the **styles.xml** and **[Content\_Types].xml** files within office documents can provide valuable clues for identifying and tracking the same threat actor.
- The method presented here offers an alternative to traditional hunting or pivoting techniques, serving as a valuable addition to a team's activities.
- We are happy to hear your feedback and suggestions | <https://www.virustotal.com/gui/contact-us> and [joselsm@virustotal.com](mailto:joselsm@virustotal.com)

---

# Thank you

Joseliyo Sánchez  
@Joseliyo\_Jstnk  
joselsm@virustotal.com

virustotal.com



**@Joseliyo\_Jstnk**



**/in/joseluissm/**