

Tracking Threat Actors Using Images and Artifacts

When tracking adversaries, we commonly focus on the malware they employ in the final stages of the kill chain and infrastructure, often overlooking samples used in the initial ones.

In this post, we will explore some ideas to track adversary activity leveraging images and artifacts mostly used during delivery. We presented this approach at the FIRST CTI in Berlin and at Botconf in Nice.

Hunting early

In threat hunting and detection engineering activities, analysts typically focus heavily on the latter stages of the kill chain – from execution to actions on objectives (Figure 1). This is mainly because there is more information available about adversaries in these phases, and it's easier to search for clues using endpoint detection and response (EDR), security information and event management (SIEM), and other solutions.

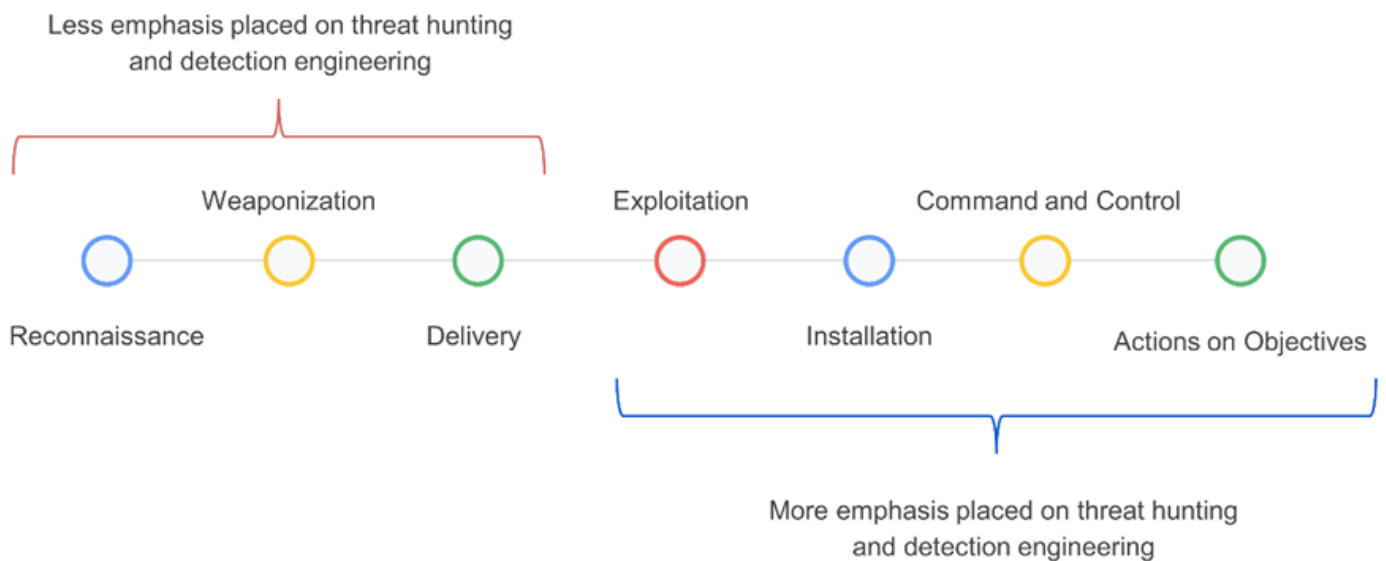


Figure 1: Stages of the kill chain categorized by their emphasis on threat hunting and detection engineering.

We have been exploring ideas to improve our hunting focused on samples built in the weaponization phase and distributed in the delivery phase, focused on the detection of suspicious Microsoft Office documents (Word, Excel, and PowerPoint), PDF files, and emails.

In threat intelligence platforms and cybersecurity in general, green and red colors are commonly used to quickly indicate results and identify whether or not something is malicious. This is because they are perceived as representing good or bad, respectively.

Multiple [studies](#) in psychology have demonstrated how colors can influence our decision-making process. VirusTotal, through the third-party engines integrated into it, shows users when something is detected

and therefore deemed "malicious," and when something is not detected and considered "benign." For example, the [sample](#) in Figure 2 belongs to a Microsoft Word document distributed by the SideWinder group during the year 2024.

The screenshot displays a malware analysis interface. At the top left, a circular gauge shows a score of 31 out of 63. A notification bar at the top states "31/63 security vendors and no sandboxes flagged this file as malicious". The file name is "55a0bbde3e32c559715cdc9c7d30d003b9e14725a6369d30edef20c1ed6dd994.docx" with a size of 355.29 KB and a last modification date of 25 minutes ago. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, CONTENT, TELEMETRY, and COMMUNITY (14). Below the tabs, there are sections for "Contacted URLs (1)" and "Contacted Domains (4)".

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

Domain	Detections	Created	Registrar
fia-gov.net	17 / 90	2023-06-12	-
mofa-gov-np.fia-gov.net	15 / 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.

Figure 2: Document used by the SideWinder APT group

The sample in question was identified at the time of writing this post by 31 antivirus engines, leaving no doubt that it is indeed a real malware sample. In the process of pivoting to identify new samples or related infrastructure, starting with Figure 2, the analyst will likely click on the URL detected by 11 out of the 91 engines, and the domains detected by 17 and 15 engines, respectively, to see if there are other samples communicating with them. The remaining two domains (related to windows.com and live.com) in this case are easily identified as legitimate domains that were likely contacted by the sandbox during its execution.

Compressed Parents (1) ⓘ			
Scanned	Detections	Type	Name
2024-01-30	52 / 65	ZIP	fdeef34eae3d21f099a347716aa0869104704ff60150cbbd98aeb5ae11870f4a

Bundled Files (13) ⓘ			
Scanned	Detections	File type	Name
2024-02-17	8 / 60	XML	word/_rels/document.xml.rels
2024-04-23	0 / 61	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
2024-03-21	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
2024-04-16	0 / 59	XML	word/styles.xml
2024-04-19	0 / 59	XML	word/theme/theme1.xml
2024-04-23	0 / 61	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	2c7adcf8bde0f7325ec069c0274435c962e0b4f2c3a76e4bdaebaa6925a8388

Figure 3: Relationships within the SideWinder APT group document

In the same sample, if you go down in the VirusTotal report (Figure 3), the analyst will likely click on the ZIP file listed as "compressed parent" to check if there are other samples within this ZIP besides the current one. They may also click on the XML file detected by 8 engines, and the LNK file detected by 4 engines. The remaining files in the bundled files section probably won't be clicked, as the green color indicates they are not malicious, and also because they have less enticing formats — mainly XML and JPEG. But what if we explore them?

XML files generated by Microsoft Office

When you create a new Microsoft Office file, it automatically generates a series of embedded XML files containing information about the document. Additionally, if you use images in the document, they are also embedded within it. Microsoft Office files are compressed files (similar to ZIP files). In VirusTotal, when a Microsoft Word file is uploaded, you can see all these embedded files in the embedded files section.

We have mainly focused on three types of embedded files within Office documents:

- **Images:** Many threat actors use images related to the organizations or entities they intend to impersonate. They do this to make documents appear legitimate and gain the trust of their victims.

- **[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.

Our hypothesis is: If malicious Microsoft Word documents are copied and pasted during the weaponization building process, with only the content being modified, the hashes of the [Content_Types].xml and styles.xml files will likely remain the same.

Office documents

To check our hypothesis, we selected a set of samples used during delivery and belonging the threat actors listed in Figure 4:

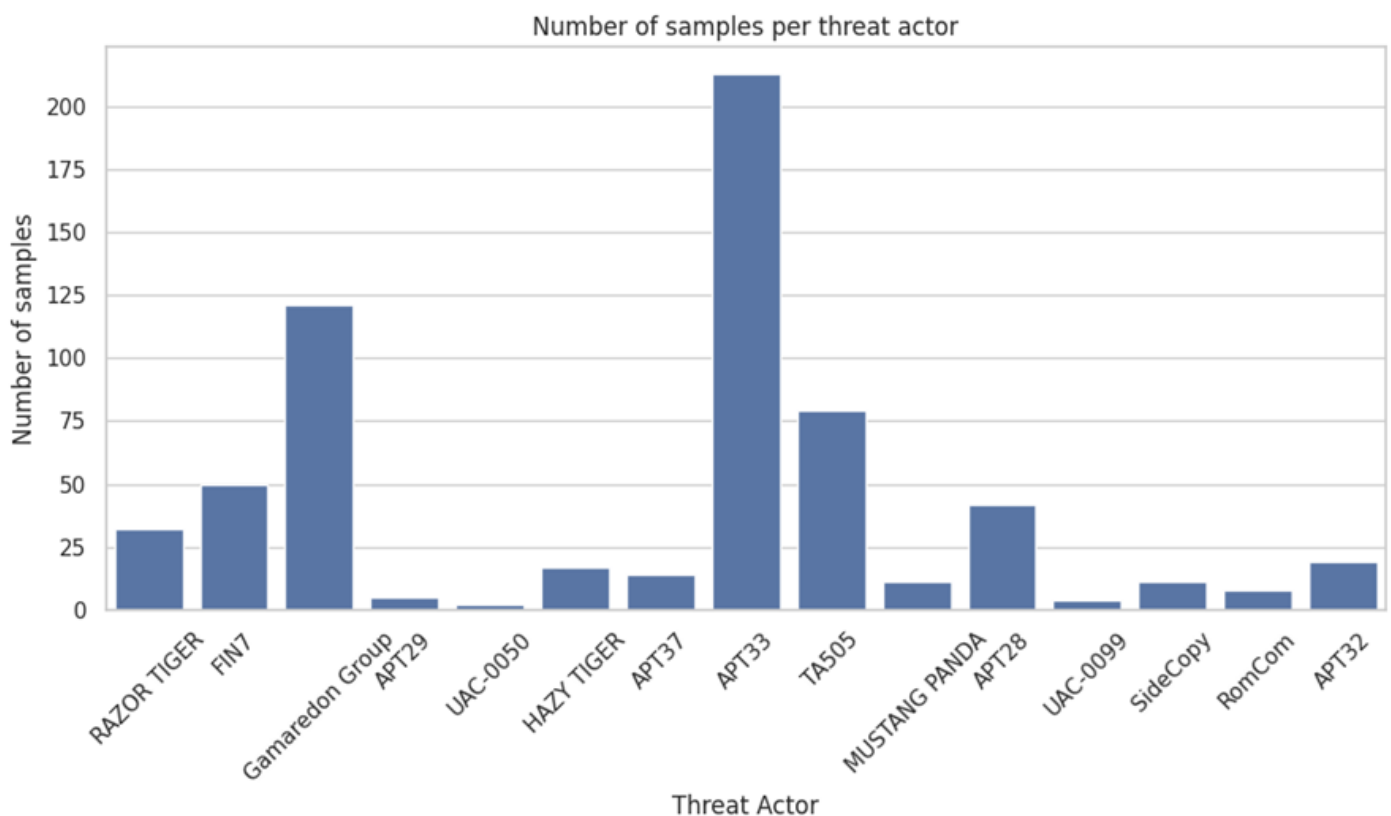


Figure 4: Number of samples per actor within the scope

Let's analyze some of the results we obtained per actor.

APT28 – Images

We started by focusing on images APT28 has reused for different delivery samples (Figure 5).

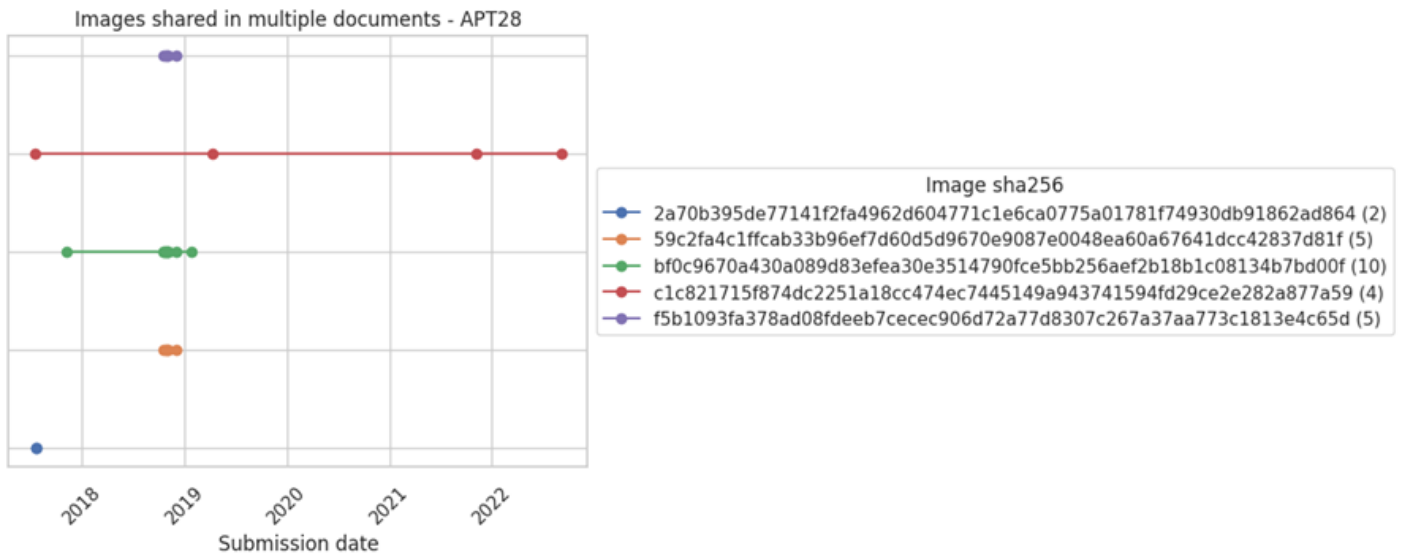


Figure 5: Images shared in multiple documents by APT28

Each line in the Figure 5 graph represents the same image, and each point represents at least two samples that used that particular image.

The **second image** of the graph shows how it was used by different Office documents at different points in time, from 2018 to 2022 (dates related to their upload to VirusTotal).

Now, the chart in Figure 6 visualizes each of these images.

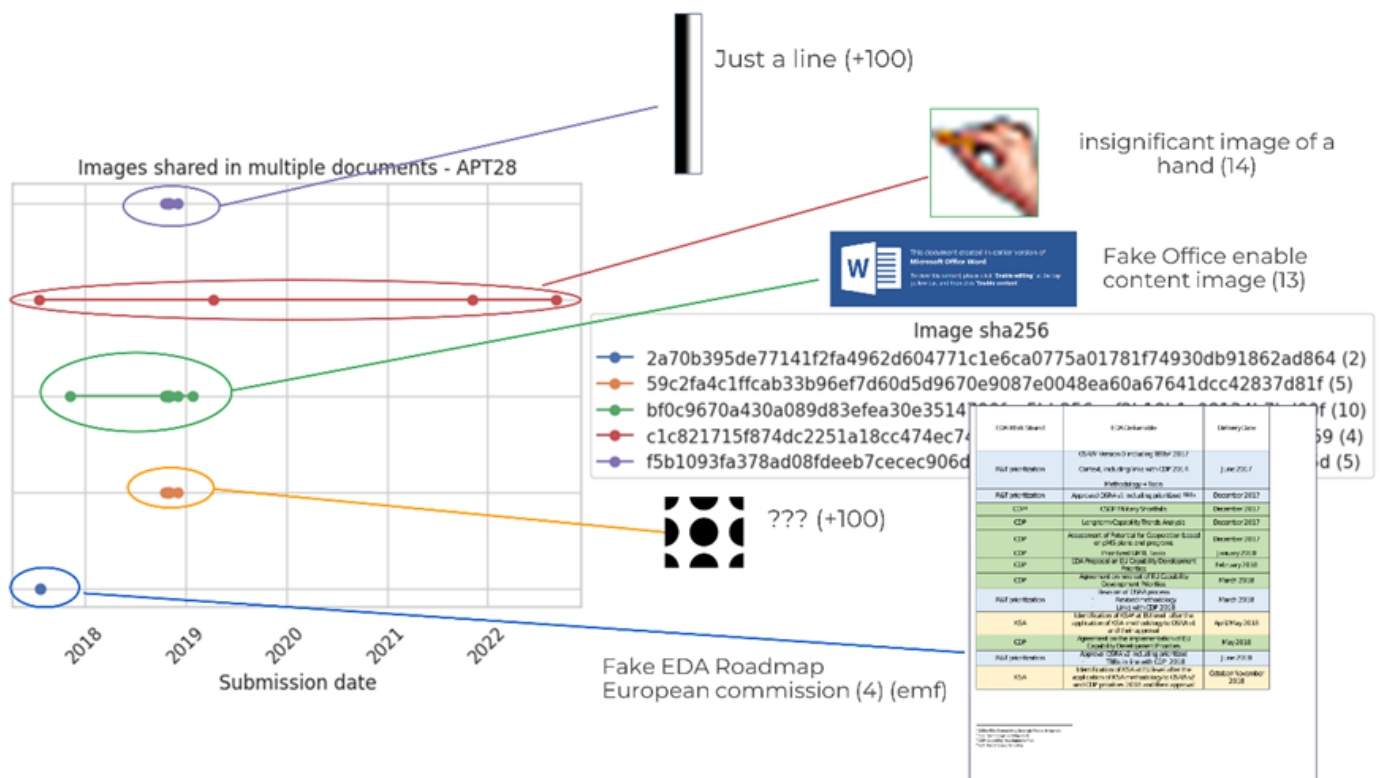
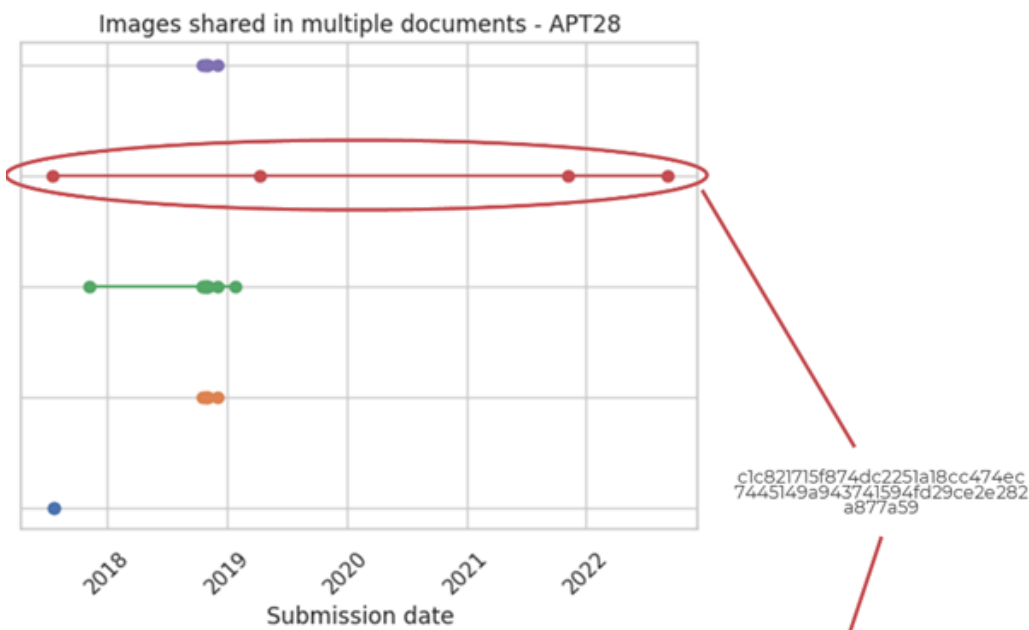


Figure 6: Content of the images shared in multiple documents by APT28

- The first image is just a simple line with no particular meaning. It's embedded in over 100 files known by VirusTotal.

- The second image is a hand and has 14 compressed parents.
- The third image consists of black circles and also has over 100 compressed parents.
- The last image is like a Word page with a table, presenting a fake EDA Roadmap of the European Commission. The image format is EMF (an old format) and it has 4 compressed parents

If we delve into the compressed parents of the [second image](#) (the one with the hand), we can see how the image is used in Office documents that are part of a campaign reported by [Mandiant](#) attributed to APT28. The image of the hand was used in fake Word documents for hotel reservations, particularly in a small section where the client was supposed to sign.



c1c821715f874dc2251a18cc474ec
7445149a943741594fd29ce2e282
a877a59

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	5e9056b5aca1839dc38ded0ded870be455e8c5303db649525502081f3bf2f54.doc.bin
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\9e77927c8f86bbe2ea82f467b74f5.docm
2021-11-14	3 / 60	Office Open XML Document	off.doc
2024-02-20	45 / 65	Office Open XML Document	b40cbf38284e6a1b9157002ad564e40fad2d85ba36437cf95c3b6326ad142520.doc
2022-07-27	36 / 61	Office Open XML Document	C:\Users\USER\AppData\Local\Temp\1a56f5dd3c01901415300a15c99f55c1.docm
2024-02-20	39 / 65	Office Open XML Document	a78b1129e42d97f62b53238ebdb636d63a6b8f6c70a43a7d011c8812b31fec53
2024-01-12	3 / 62	Office Open XML Document	C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.MSO\mso35588.tmp

MANDIANT Platform Solutions Intelligence Services Resources Company

APT28 Targets Hospitality Sector, Presents Threat to

Travelers

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

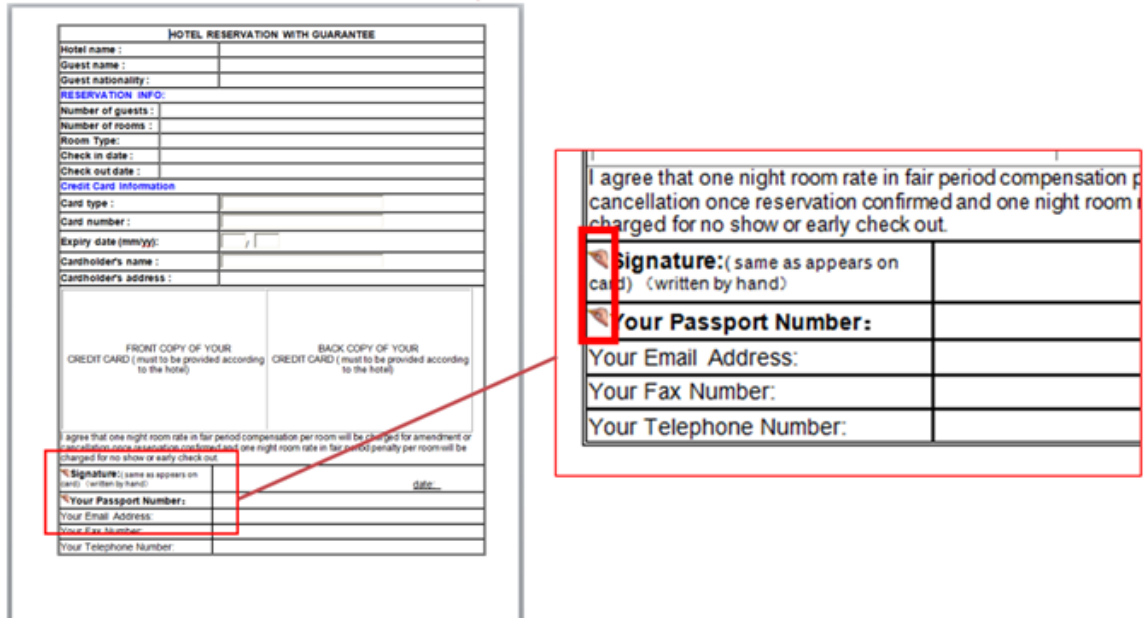


Figure 7: Pivoting through a specific image used by APT28

SideWinder – Images

SideWinder (aka RAZER TIGER) is a group focused on carrying out operations against military targets in Pakistan. This group traditionally reused images, which might help monitoring their activity.

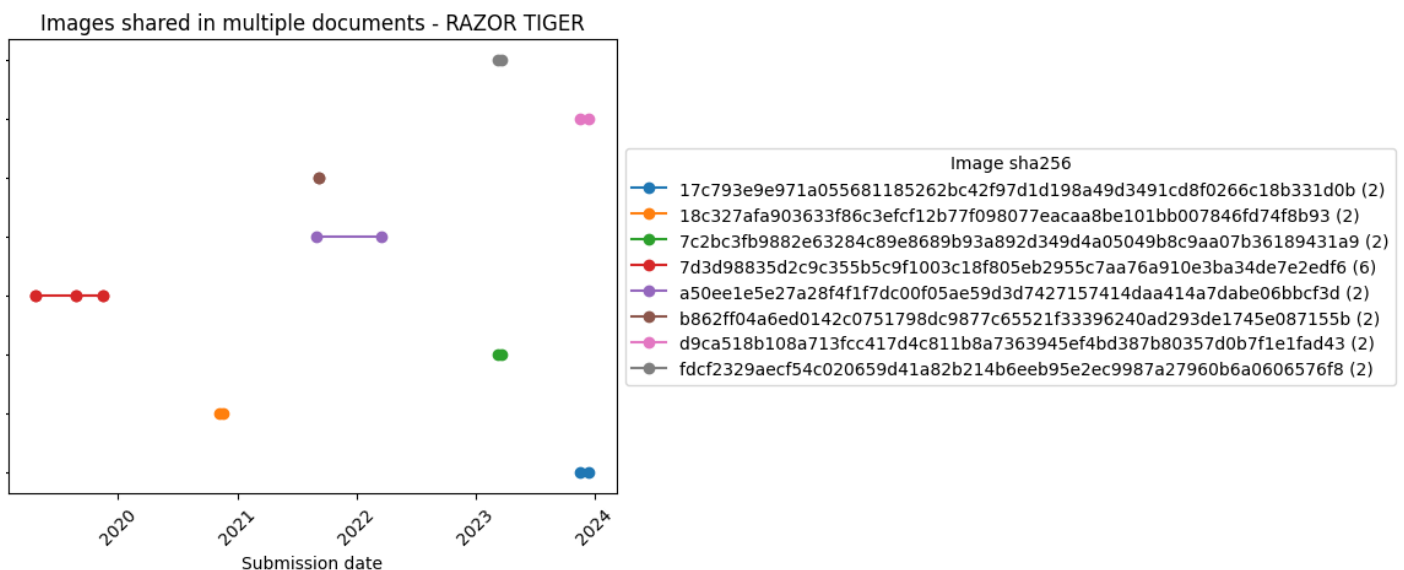


Figure 8: Images shared in multiple documents by RAZOR TIGER

In particular, the image in Figure 9 was used in a sample uploaded in September 2021 and in a second one uploaded March 2022. The image in question is the signature of Baber Bilal Haider.

ambassadors, Strategists & reps of think tanks and NHQ reps (if desired) will be invited to attend the activity.

- Venue. NIMA Conference Room at BUHO.
- Proposed Schedule. 6 & 7 Jul 21

- Security Classification of Activity. Discussion during the focused talk will remain classified. Two post event reports will be generated, one each for media/ public and other specifically for NHQ.
- Requirement from NHQ. NHQ points of view regarding desired end state of the activity is requested. In addition, to carry out meaningful discussion and to reach at logical deductions/ conclusions, it is requested that exact/ realistic on ground situation with respect to US-Pak relation (including US demands from Pakistan during and post withdrawal from Afghanistan) in contemporary scenario may be shared with NIMA. If forwarding of written information is not considered appropriate, undersigned may visit NHQ for guidance/ briefing on the subject.

2021 sample

BABER BILAL HAIDER SI(M)
Commodore (Retd.)
Director

B. Proposed Participants: Proposed participants/ discussants will be 10 - 12 for both days are as under:

- On day-1, participants/ discussants from Academia, Retired Armed Forces officials, retired ambassadors, Strategists and reps of think tanks will be invited to attend the activity.
- On day-2, participants/ discussants Retired Naval Officers, selected retired ambassadors, Strategists & reps of think tanks and NHQ reps (if desired) will be invited to attend the activity.

Venue : NIMA Conference Room at BUHO.

Proposed Schedule : 20 & 21 Mar 22

- Security Classification of Activity. Discussion during the focused talk will remain classified. Two post event reports will be generated, one each for media/ public and other specifically for NHQ.
- Requirement from NHQ. NHQ points of view regarding desired end state of the activity is requested. In addition, to carry out meaningful discussion and to reach at logical deductions/ conclusions, it is requested that exact/ realistic on ground situation with respect to topic. If forwarding of written information is not considered appropriate, undersigned may visit NHQ for guidance/ briefing on the subject.

2022 sample

BABER BILAL HAIDER SI(M)
Commodore (Retd.)
Director

Figure 9: Two different samples of RAZOR TIGER share the same image of a handwritten signature

Gamaredon – [Content_Types].xml and styles.xml

For Gamaredon we found they reused styles.xml and [Content_Types].xml in different documents, which helped reveal new samples.

Figure 10 chart displays all the [Content_Types].xml files from Gamaredon's Office documents.

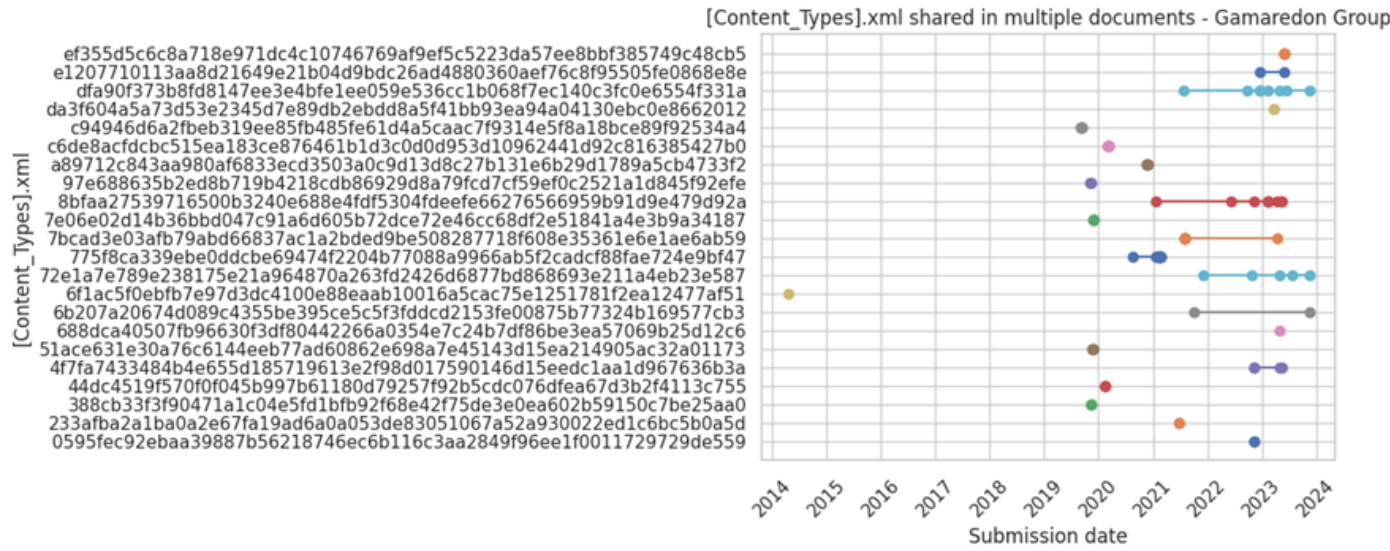


Figure 10: [Content_Types].xml shared in multiple documents by Gamaredon Group

There are a large number of samples that share the same [Content_Types].xml. It's important to highlight that these [Content_Types].xml files are not necessarily exclusively used by Gamaredon, and can be found in other legitimate files created by users worldwide. However, some of these [Content_Types].xml might be interesting to monitor.

Styles.xml files are usually less generic, which should make them a better candidate to monitor:

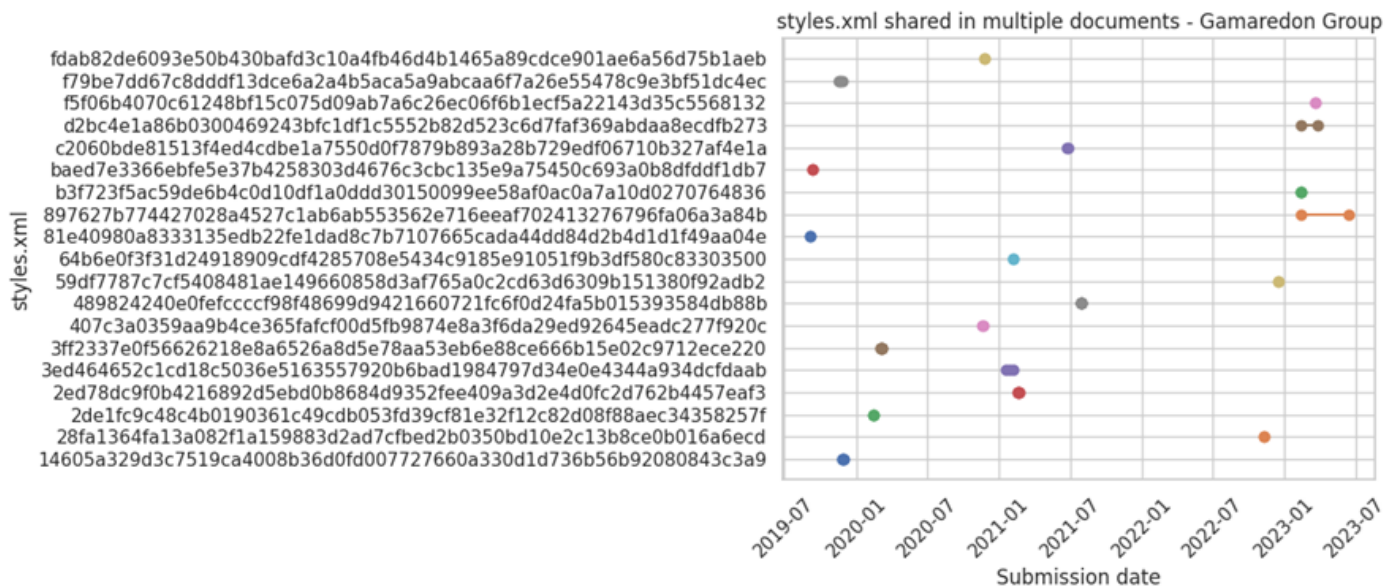


Figure 11: Styles.xml shared in multiple documents by Gamaredon Group

We see styles.xml files are less reused than [Content_Types].xml. This could be because some of the samples used by this actor for distribution are created from scratch or reusing legitimate documents.

We used identified patterns in the styles.xml files to launch a retrohunt on VirusTotal. Figure 12 visually represents the original set of style.xml files (left) and those that were added later after running the retrohunt (right).

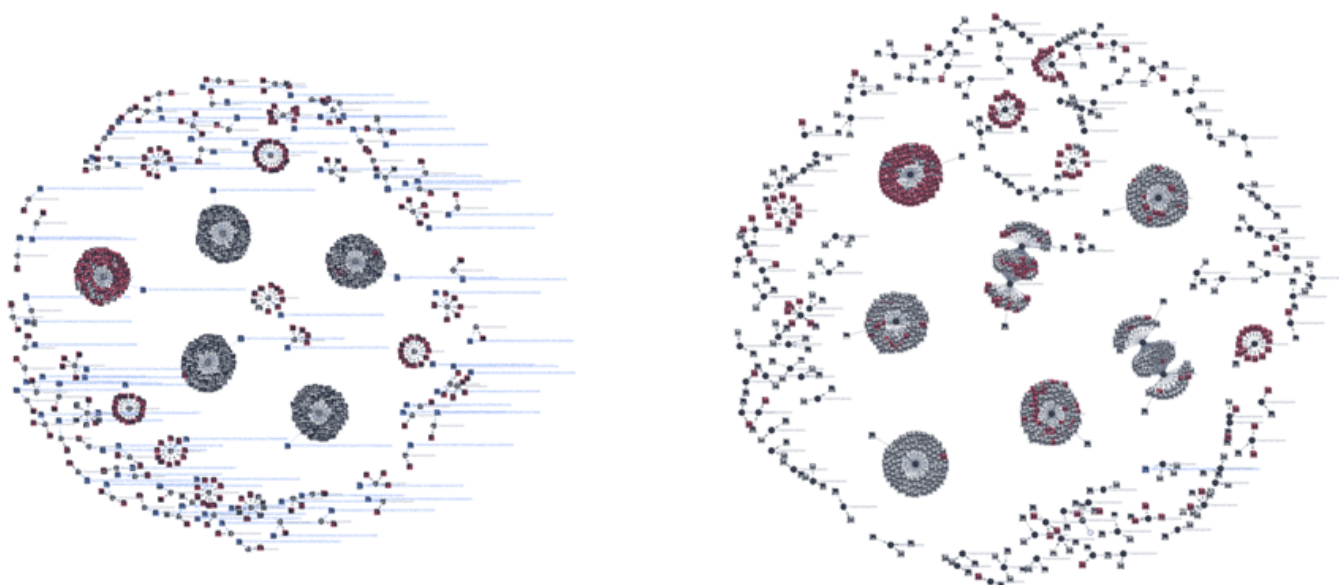


Figure 12: Initial graph of the styles.xml and its parents used by Gamaredon (left). Final graph after identifying new styles.xml and their parents using retrohunt in VirusTotal (right)

One of the new styles.xml files found in our retrohunt has 17 compressed parents, meaning it was included in 17 Office files.

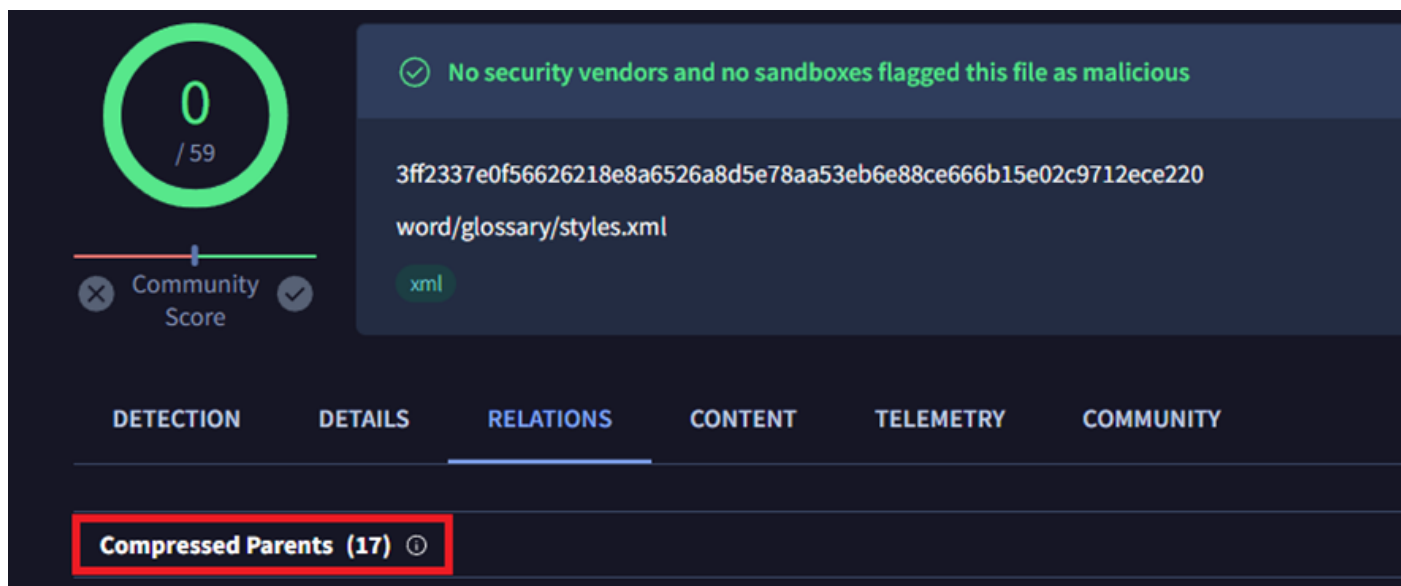


Figure 13: Number of parent documents for a specific styles.xml file used by Gamaredon

All the parents were malicious, some of them identical and the rest very similar between them. The content of many of them referred to "Foreign institutions of Ukraine - Embassy of Ukraine in Hungary," containing a table with phone numbers and information about the embassy, such as social media links and email accounts. Here's an [example](#):

„Закордонні установи України”

2 ЄД	УГОРЩИНА	HU 61311
Посольство України в Угорщині		
Представник України в Дунайській комісії		
✉ Н-1125 Budapest, Istenhegyi u. 84/b	🕒 08:00 – 17:00	🌐 www.hungary.mfa.gov.ua
	🕒 12:00 – 13:00	📘 www.facebook.com/ukran.na.gykovetseg.magyarorszag
	📧 СБ	@ emb_hu@mfa.gov.ua
	🌐 НА	📞 (00 36) 1 422 41 20
	🌐 - 1	📠 (00 36) 1 220 98 73
Надзвичайний і Повноважний	НЕПОП	(00 36) 1 422 41 20
Посол	Любов Васи́лівна	ip. 90 36 01 3000
Радник	ЛУПАК	(00 36) 1 422 41 12
	Андрій Андрійович	ip. 90 36 01 3001
Радник	БАЛОГ	(00 36) 1 422 41 10
	Іштван Арпадович	
Перший секретар	АЛЕКСАНДРОВ	(00 36) 1 422 41 27
	Сергій Олександрович	ip. 90 36 01 3002
Перший секретар	АХУНОВ	(00 36) 1 422 41 16
	Рустам Ринатович	
Перший секретар	ГАЛАЙКО	(00 36) 1 422 41 22
з консульських питань	Олег Федорович	
Перший секретар	КОНДИК	(00 36) 1 422 41 15
	Олексій Павлович	
Перший секретар	ЛУКАЧУК	(00 36) 1 422 41 13
	Іван Миколайович	
Перший секретар	ПАСІЧНИК	(00 36) 1 422 41 51
	Сергій Павлович	
Перший секретар	ПИЛИПЕНКО	(00 36) 1 422 41 29
	Олег Вадимович	

Figure 14: Document used by Gamaredon in one of its campaigns that includes multiple images which can be used to monitor new samples

The information for social media includes the logos of these platforms, such as the Facebook logo, Skype logo, an image of a telephone, etc. By pivoting, on the image of the [Facebook](#) icon, we find that it has 12 additional compressed parents, meaning it appears in 12 documents, all of them sharing the same styles.xml file.

Visualizing all together, we find a set of about 12-14 images used within the same timeframe by the actor. All of these images can be found in the “Embassy of Ukraine in Hungary” document.

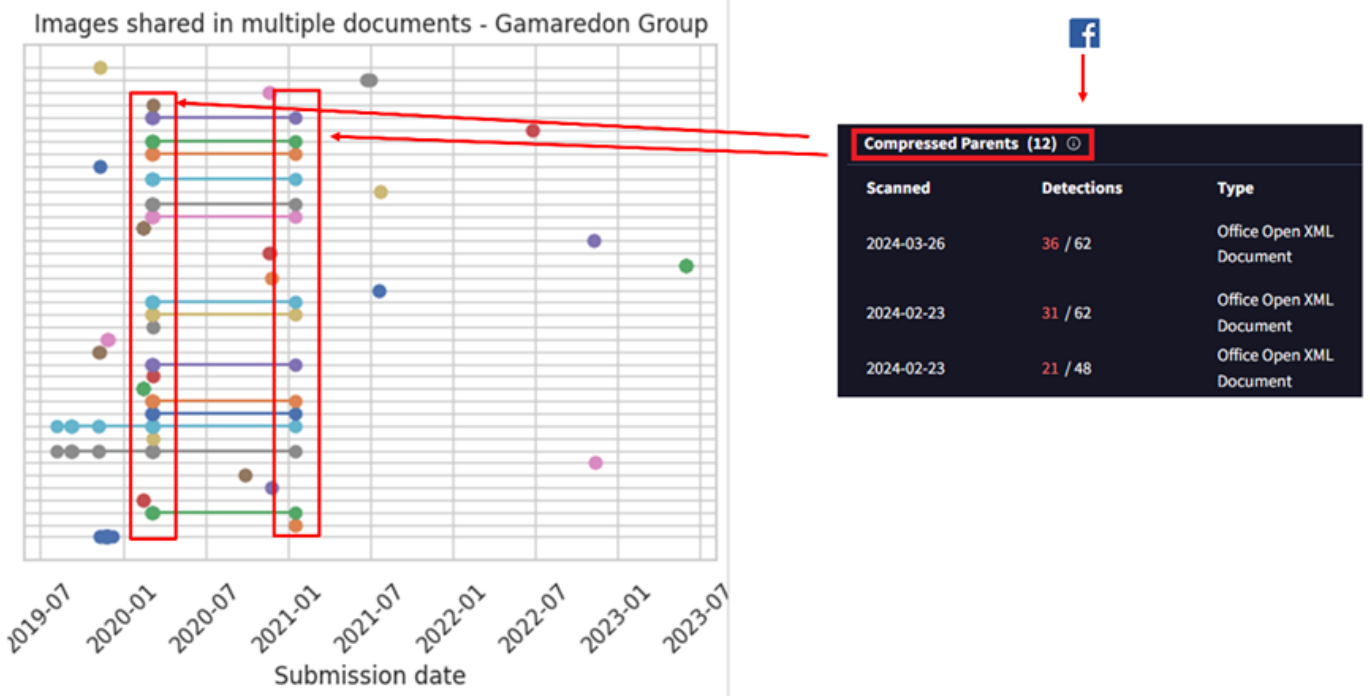


Figure 15: Pivoting through the Facebook image that included the document in Figure 14

There's a pattern evident in the previous image where different images were included in files uploaded simultaneously. This pattern is associated with multiple documents used in the same campaign of the Embassy of Ukraine in Hungary, all of them were using the same social media images explained before.

Styles.xml shared between threat actors

Another aspect we explored was if different threat actors shared similar styles.xml files in their documents. Styles.xml files are somewhat more specific and unique than [Content_Types].xml files because they can contain styles created by threat actors or by legitimate entities that originally created the document and then were modified by the actor. This makes them stand out more and can help in identifying threat actor activity.

This doesn't necessarily imply they share information to conduct separate operations, although in some cases, it could be a scenario worth considering.

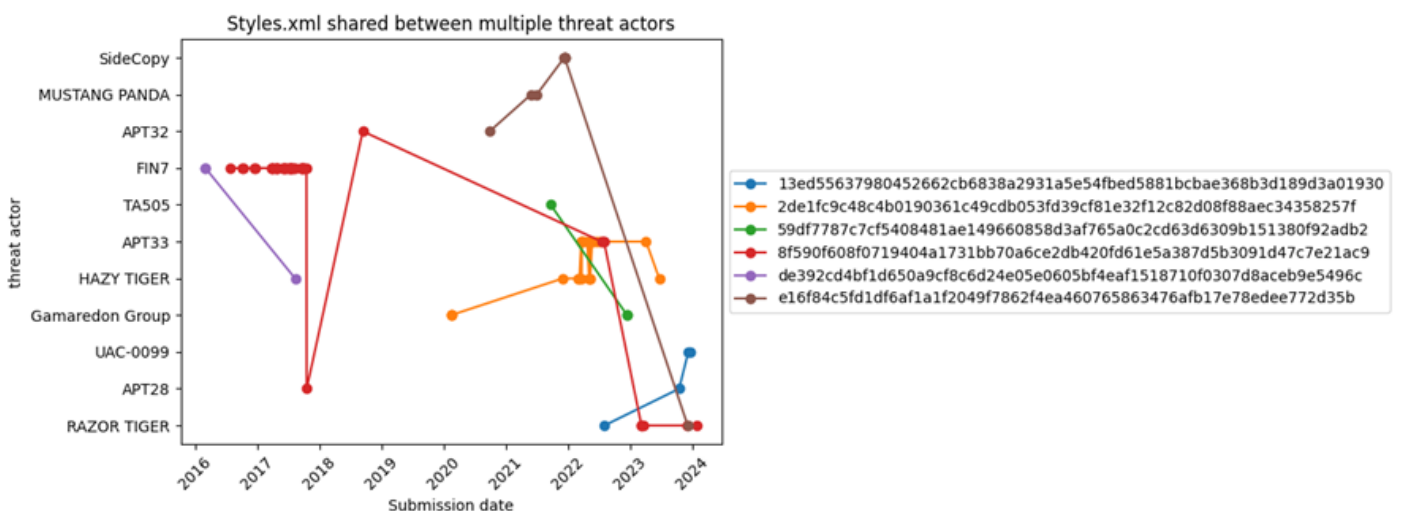


Figure 16: styles.xml shared between different threat actors

Of all styles.xml files related to actors in our initial set, only six of them were found to be shared by at least two actors. Some styles defined by the styles.xml file are very generic and could identify almost any type of file. However, there are others that could be interesting to explore further.

An interesting case is the [Styles.xml](#) file, which seems to be shared by Razor Tiger, APT28, and UAC-0099. Specifically, the samples from APT28 and UAC-0099 are attract because they were uploaded to VirusTotal within short time frames, suggesting they might belong to the same threat actor.

The file [243bab79863327915c315c188c0589202f64b3500a3fee3e2c9f3d34e8e1f154](#) attributed to APT28, the file [2c2fa6b9fbb6aa270ba0f49ebb361ebf7d36258e1bdfd825bc2faeb738c487ed](#) attributed to UAC-0099, and the file [61a5b971a6b5f9c2b5e9a860c996569da30369ac67108d4b8a71f58311a6e1f1](#) attributed to UAC-0099 all share the same [styles.xml](#) and [\[Content_Types\].xml](#).

You can see the list of hashes in the appendix of this blog

[Content_Types].xml shared between threat actors

Like in the previous case, we checked if there were Office documents among different threat actors sharing [Content_Types].xml:

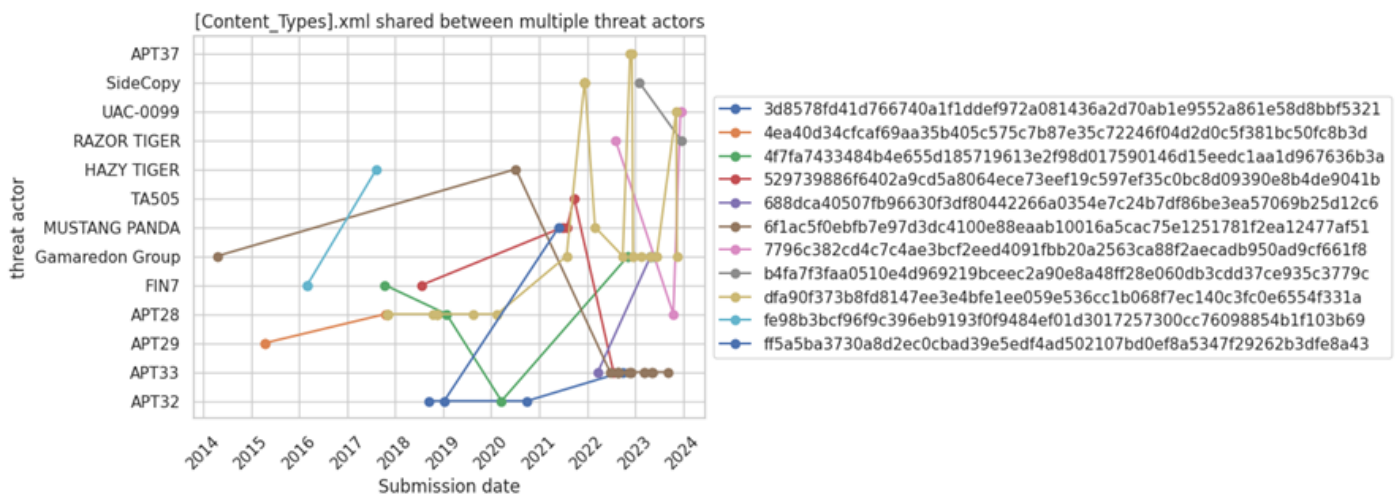


Figure 17: [Content_Types].xml shared between different threat actors

In this case, there are eleven [Content_Types].xml files that are shared by at least two different actors.

An interesting case here is the file

[dfa90f373b8fd8147ee3e4bfe1ee059e536cc1b068f7ec140c3fc0e6554f331a](#), which is shared by Gamaredon, APT37, Mustang Panda, APT28, SideCopy, and UAC-0099. Again, there could be different explanations for this.

Another interesting case that is worth analyzing in detail is [Content_Types].xml with hash [4ea40d34cfcaf69aa35b405c575c7b87e35c72246f04d2d0c5f381bc50fc8b3d](#), which is only shared by APT28 and APT29.

You can see the list of hashes in the appendix of this blog

AI to the rescue

The images reused by attackers seem to be a promising idea we decided to further explore.

We used the VirusTotal API to download and unzip a set of Office documents used for delivery, this way we obtained all the images. Then we used Gemini to automatically describe what these images were about.

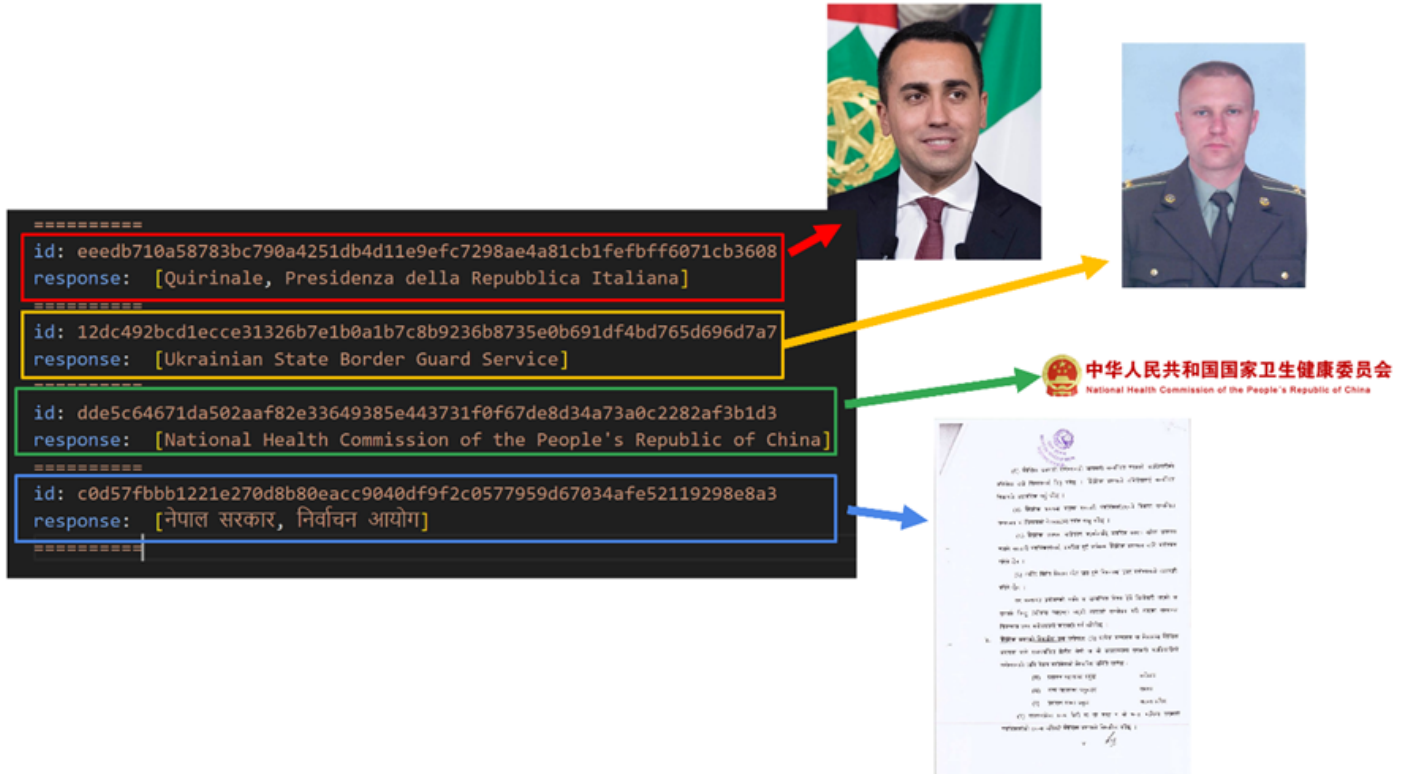


Figure 18: Results obtained with Gemini after processing some of the embedded images in the documents used by the threat actors

Figure 18 shows some examples of images that were incorporated by certain actors. There were also other results that were not helpful, mainly related to images that did not show a logo or anything specific that indicated what they were.

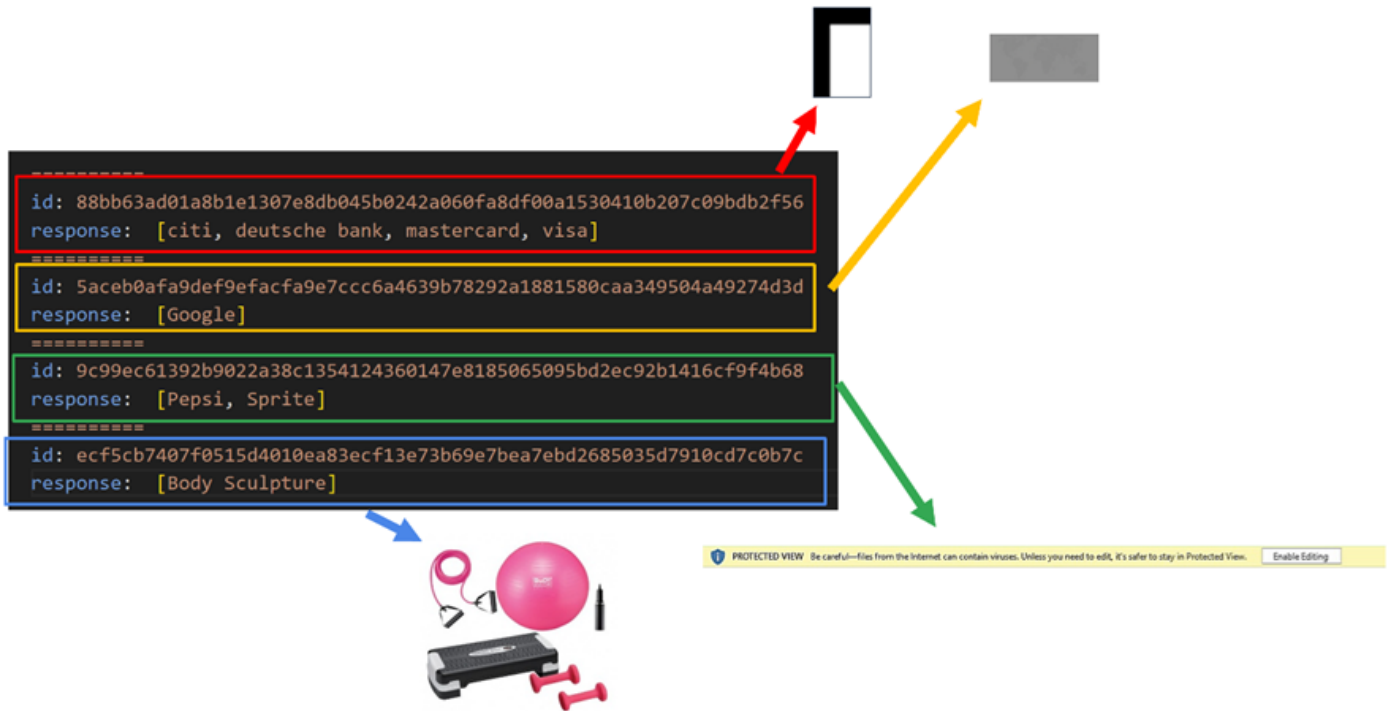


Figure 19: Results obtained with Gemini after processing some of the embedded images in the documents used by the threat actors

Using the VirusTotal API to obtain documents that you might be looking for and combining the results with Gemini to analyze possible images automatically, can potentially help analysts to monitor potential suspicious documents and create your own database of samples using specific images, for example Government images or specific images about companies. This approach is interesting not only for threat hunting but also for brand monitoring.

PDF Documents

Images dropped by Acrobat Reader

Unlike Office documents, PDF files don't contain embedded XML files or images, although some PDF files may be created from Office documents. Some of our sandboxes include [Adobe Acrobat Reader](#) to open PDF documents which generates a thumbnail of the first page in BMP format. This image is stored in the directory `C:\Users\LocalLow\Adobe\Acrobat\DC\ConnectorIcons`. Consequently, our sandboxes provide this BMP image as a dropped file from the PDF, allowing us to pivot.

To illustrate this functionality, see Figure 20 attributed to Blind Eagle, a cybercrime actor associated with Latin America.

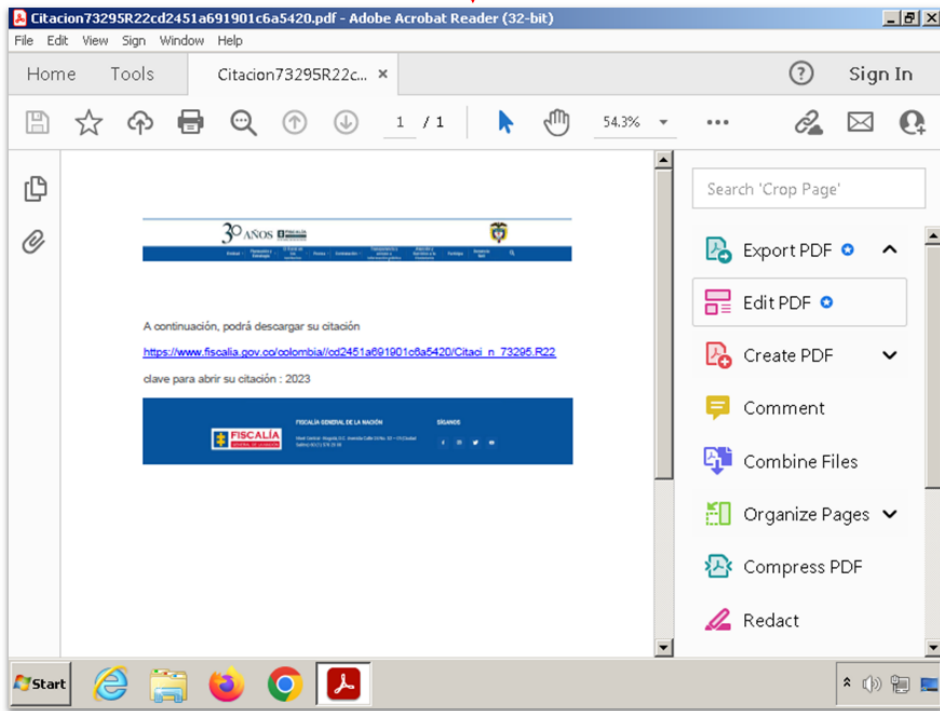
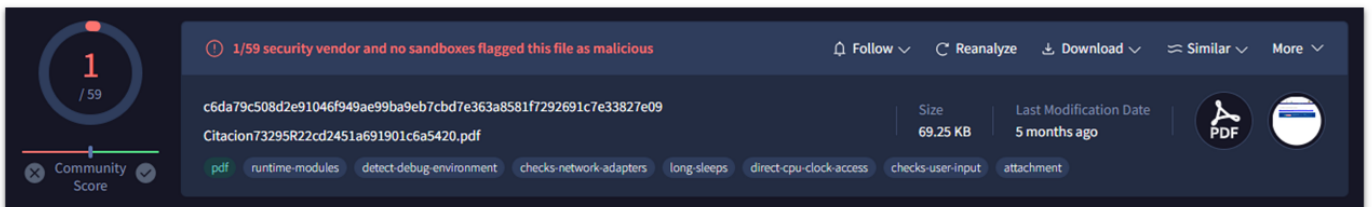


Figure 20: Content of a PDF file related to Blind Eagle threat actor

Figure 20 was provided by our sandbox. In the "relations" tab, we can see the BMP image as a dropped file:

The screenshot displays the VirusShare interface. At the top, a table lists 'Dropped Files (42)'. One entry is highlighted with a red box: a BMP file named 'C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\ConnectorIcons\icon-2303192315317-499.bmp' scanned on 2023-02-22. Below this, the file's details are shown, including a green checkmark indicating it was not flagged as malicious by security vendors. The file's SHA-256 hash is '4a4c82a81dfd6ca6c81184d1ee8002b5472caac4663549b1fc473f52db54b02a'. Below the details, the 'RELATIONS' tab is active, showing a table of 'Execution Parents (6)'. This table lists six PDF files that are parents of the BMP file, all with the same name 'Citacion73295R22cd2451a691901c6a5420.pdf' and scanned between 2023-03-09 and 2024-04-20.

Scanned	Detections	File type	Name
2023-02-23	0 / 58	DOS COM	C:\Users\user\AppData\Local\Low\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_1gfy9e_20g.tmp
2023-03-01	0 / 59	DOS COM	C:\Users\user\AppData\Local\Low\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\Local\Low\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index
2023-02-22	0 / 58	BMP	C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\ConnectorIcons\icon-2303192315317-499.bmp
2023-02-23	0 / 59	Text	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json
2024-02-16	0		

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

Figure 21: BMP file generated by the sandbox that can be used for pivoting

The BMP file itself also shows relations, in particular up to 6 PDF files in the "execution parents" section. In other words, there are other PDFs that look exactly the same as the initial one.

Typically, many actors engaged in financial crime activities utilize widely spread PDF files to deceive their victims, making this approach highly valuable. Another interesting example we found involves phishing activities targeting a Russian bank called "Tinkoff Bank."

The PDF files urge victims to accept an invitation from this bank to participate in a project.

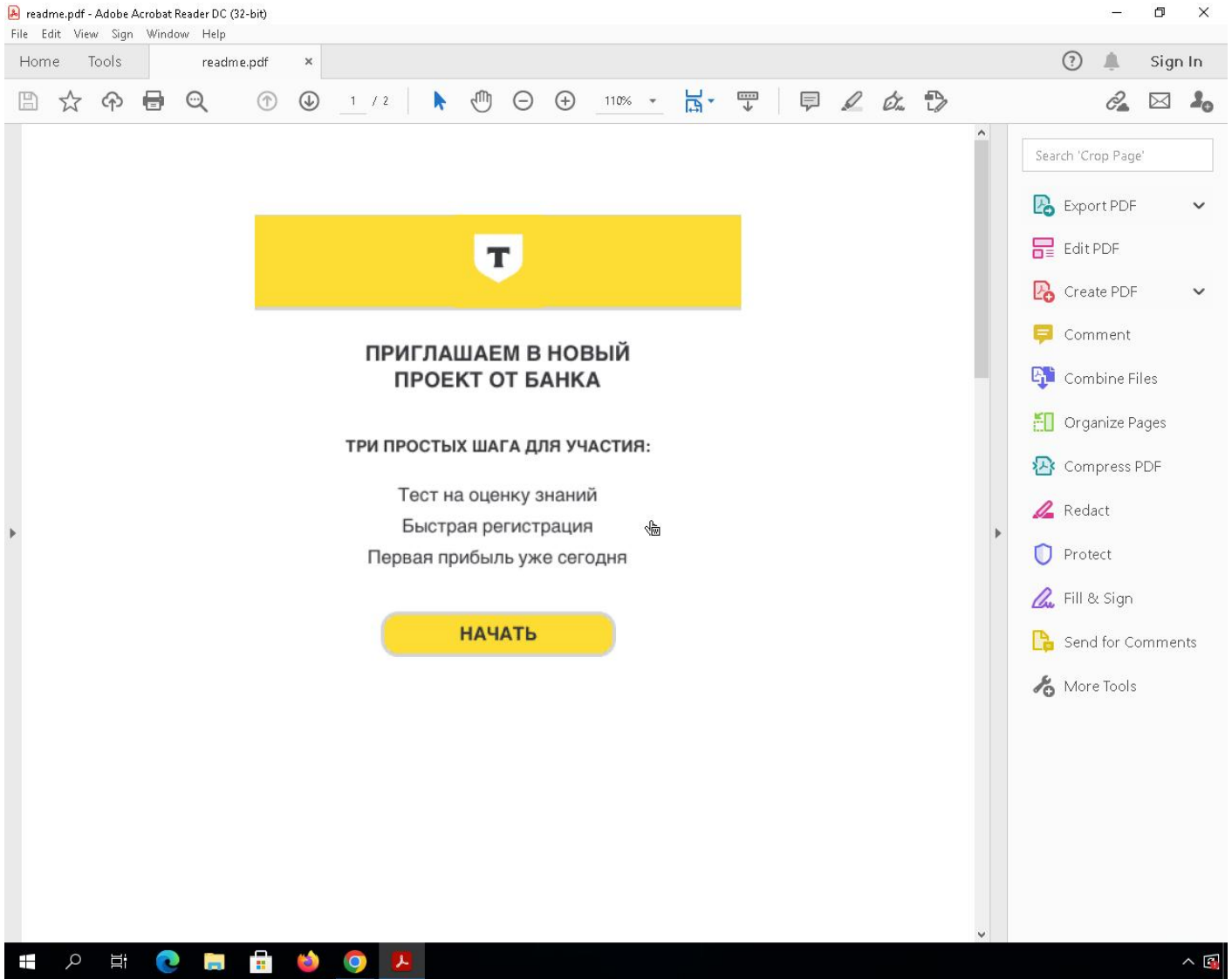


Figure 22: The content of a PDF file used by cybercrime actors

Applying the same approach we identified 20 files with identical content, most of them classified as malicious by AV engines.

Dropped Files (13)

Scanned	Detections	File type	Name
2024-04-12	0 / 59	JSON	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_Reader_RHP_Banner
2024-04-11	0 / 57	BMP	C:\Users\user\AppData\Local\Low\Adobe\Acrobat\DC\ConnectorIcons\icon-240422075003Z-230.bmp
2024-04-12	0 / 59	JSON	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files>Edit_InApp_Aug2020
2024-04-12	0 / 59	JSON	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json
2024-04-12	0 / 59	JSON	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_Reader_RHP_Retention
2024-04-12	0 / 59	JSON	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_READER_LAUNCH_CARD
?	?	file	4aba24ac35e478e91ebd4ea2e26835b4de85b91002221494534a3ccfc4c89e23
?	?	file	7856cc602c20820724c96237a6001653e934261daa68bd05b6410c51bc2d4b5e
?	?	file	b7b2619b348129c3192c7abe7c670de4c9138e73daf6aed26ea5143edc33fd7
?	?	file	c9ec54b804e3c64ccbfa507d9854207d6c391859f192365a6824a2afdeecb75

0 / 57
Community Score

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

3ec081abf2e3a9cbfc230bf171acd7e5f59d683a391fb78ba8124861acf44de.1
C:\Users\user\AppData\Local\Low\Adobe\Acrobat\DC\ConnectorIcons\icon-240422075003Z-230.bmp

Size: 63.58 KB | Last Modification Date: 1 hour ago

DETECTION | DETAILS | **RELATIONS** | CONTENT | TELEMETRY | COMMUNITY

Execution Parents (20)

Scanned	Detections	Type	Name
2024-04-15	10 / 60	PDF	117dedd7008b9e65f1f2246c1f85173ab8e9432db6b5a483c6d420f812a83e4
2024-04-11	0 / 59	PDF	Document-ZeHipdvlPktodWUHla.pdf
2024-04-18	23 / 60	PDF	Z_hJOcptvcqoFxlLSbcUHRNCbH.pdf
2024-04-11	0 / 60	PDF	244df433686613e989bfff837e765871fd77af0e28fc738874b1f68097a82438
2024-04-15	7 / 60	PDF	27a7fe9ed18a88121f64bace27b10697009c30c8a47284bcf9fc4c207215fd17
2024-04-15	10 / 60	PDF	Doc-vRWPNtltzT.pdf
2024-04-19	11 / 60	PDF	5ced342758cbe7a65682e9563d9ae0b3d97f1a1a52d65a6db2c33d34a0b41847
2024-04-22	4 / 59	PDF	6ed34cef61aae23bc2dc58ff01ffdd4111fe99ece80b06544eca0833d04c828f
2024-04-15	7 / 60	PDF	Doc-vjPmJXkZZ.pdf
2024-04-12	8 / 60	PDF	VP-XijOYEcMgWxGJchNaiqPcOuDaUtw.pdf
2024-04-15	13 / 59	PDF	__attach_version1.0_#00000000/___substg1.0_37010102
2024-04-12	0 / 60	PDF	R-ypXPPXzEGFkngVpWmlyFuOYUJPQtud.pdf
2024-04-12	5 / 60	PDF	N-nHAPsnmtARcmLNLKRkVv.pdf (NB-0913)
2024-04-16	25 / 60	PDF	F-dJlTnIsALhkBRDWjgAOW.pdf
2024-04-22	11 / 60	PDF	W-kEBhulICSBTbzh.pdf
2024-04-22	11 / 62	PDF	MI-dydNcZxgpCFenqyMODzwUJv.pdf
2024-04-15	10 / 60	PDF	S-GRliw.pdf
2024-04-22	9 / 62	PDF	Q-pMMwwwfqOxTlOajirX.pdf
2024-04-11	0 / 58	PDF	edddc65184dedba0f14fe1769b2b3501b8e4cb959d9155ecee78e7c5d71ef790
2024-04-15	9 / 60	PDF	fcf100876b9d5b382f35855c33503c4fdfe9175ebe9e173c5fc13e4d68ca7929

Figure 23: BMP file generated by the sandbox that can be used for pivoting, in this case having other 20 PDF with the same image

There are some limitations to this approach. For instance, the PDF file might be slightly modified (font size, some letter/word, color, ...) which would generate a completely different hash value for the thumbnail we use to pivot.

Images dropped by Acrobat Reader

Just like the BMP files generated by Acrobat Reader, there are other interesting files that might be dropped during sandbox detonation. These artifacts can be useful on some occasions.

The first example is a [JavaScript](#) file dropped in another PDF attributed to [Blind Eagle](#).

8 / 60

8/60 security vendors and 1 sandbox flagged this file as malicious

010571377f15371f4981e5a34928023a9aa656c5c676a4a9272cee38a905618

Estado de cuenta.pdf

Size: 71.30 KB | Last Modification Date: 1 month ago

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

Dropped Files (61)

Scanned	Detections	File type	Name
2022-07-20	0 / 58	Web Open Font Format	Chrome Cache Entry: 873
2023-10-11	0 / 60	GZIP	NPR90W/NetRadioSmall.exe.WebView2/EBWebView/Default/Cache/Cache_Data/f_00019f
2022-02-21	0 / 58	Text	Chrome Cache Entry: 303
2016-08-04	0 / 55	Text	Chrome Cache Entry: 737
2023-04-19	0 / 59	GZIP	Chrome Cache Entry: 1084
2023-10-11	0 / 60	GZIP	NPR90W/NetRadioSmall.exe.WebView2/EBWebView/Default/Cache/Cache_Data/f_0001a5
2023-04-13	0 / 59	GZIP	Chrome Cache Entry: 1381
2022-07-18	0 / 58	GZIP	C:\Users\user\AppData\Local\Programs\DigiParts EPC\Epc_app.exe.WebView2\EBWebView\Default\Cache\Cache_Data\0_000006 (copy)
2023-08-30	0 / 59	GZIP	Chrome Cache Entry: 932
2023-08-09	0 / 59	Web Open Font Format	monnee/dist/fonts/work-sans-v5-latin-regular.woff2
2022-02-21	0 / 58	Text	Chrome Cache Entry: 283
2023-10-11	0 / 54	GZIP	NPR90W/NetRadioSmall.exe.WebView2/EBWebView/Default/Cache/Cache_Data/f_0001a2
2019-06-12	0 / 56	C++	Chrome Cache Entry: 566
2024-03-31	0 / 61	ZIP	C:\Users\<USER>\AppData\Local\Temp\A9wxr6pr_1a4mank_2bc.tmp

Execution Parents (47)

Scanned	Detections	Type	Name
2024-02-25	8 / 60	PDF	Estado de cuenta.pdf
2023-12-18	22 / 61	PDF	05184813ce52dd1d86d808e444e87f1e1ac6e0bf34460208b52852b963b86607.pdf
2022-03-19	0 / 58	PDF	FORMATO ACREDITACION DE APORTES - HOYOS.pdf
2023-10-09	0 / 63	Office Open XML Document	/wp-content/uploads/2023/10/96-Con-DIAN-1245-2023-Tiquetes-de-transporte-aereo-a-San-Andres-excluidos-de-IVA.docx
2024-02-20	0 / 61	PDF	120249300100270781_00001.pdf
2024-03-21	0 / 61	PDF	4-Ensayo-Depositos-Judiciales.pdf
2024-01-16	0 / 59	PDF	37. FONDO DE EMPLEADOS ENERGI/FONDO.pdf
2023-11-03	0 / 61	PDF	Compilacion-Doctrina-Oficial-Ley-2277-2022-01112023.pdf
2022-05-05	0 / 60	PDF	Instructivo pago PSE.pdf
2024-02-25	10 / 61	PDF	Estado de cuenta.pdf
2024-03-05	0 / 60	PDF	120245900100358871_00002.pdf
2023-09-18	0 / 60	PDF	120233100001563851_00001.pdf
2022-04-20	0 / 59	PDF	DIAN__MUISCA_ Catálogo de solicitudes.pdf
2023-07-17	0 / 60	PDF	OFICIO BROEKHOF COLOMBIA SAS.pdf
2023-04-26	0 / 60	PDF	DIAN ESTADO DE CUENTA NOTIFICACION DE ESTADO DE CUENTA.pdf
2022-04-11	0 / 62	Office Open XML Document	GSGU08.docx
2022-07-22	0 / 60	PDF	RADIAN RedCapital Colombia - Proceso rápido.pdf
2024-02-25	7 / 61	PDF	Estado de cuenta.pdf
2024-02-28	0 / 59	PDF	OFICIO_2296.pdf
2024-03-07	0 / 60	PDF	72b07b424932650691395604ca78c4e484abd9f531a08271c9b17645c46d176d
2022-02-16	5 / 61	PDF	dian.pdf
2024-02-25	10 / 61	PDF	Estado de cuenta.pdf
2022-07-11	16 / 60	PDF	f4dc4c3684186766b76d43a9e7bfa10427177195f5d84c75a81d9b5b0887fe8a.dian.pdf
2022-03-10	7 / 58	PDF	dian.pdf
2024-02-25	8 / 61	PDF	Estado de cuenta.pdf
2022-03-03	8 / 60	PDF	88202b193f837225d12713a2fd28a39cb320e27fdb9055651f1277313b58b28f.dian.pdf
2024-02-25	5 / 58	PDF	Estado de cuenta.pdf
2023-10-03	0 / 61	PDF	Oficio_Incumplimiento_ART_139_Fanalca.pdf
2022-07-18	0 / 60	PDF	10902_11508.pdf
2023-08-01	0 / 60	PDF	DIAN_COEX_20230713_002_00000L000687813647.pdf

Figure 24: BMP file generated by the sandbox that can be used for pivoting, another example of Blind Eagle threat actor

The dropped JavaScript file's name during the PDF execution was "Chrome Cache Entry: 566" indicating that this file was likely generated by opening an URL through Chrome, possibly triggered by a sandbox click on a link within the PDF. Examining the file's contents, we observe some strings and variables in Spanish.

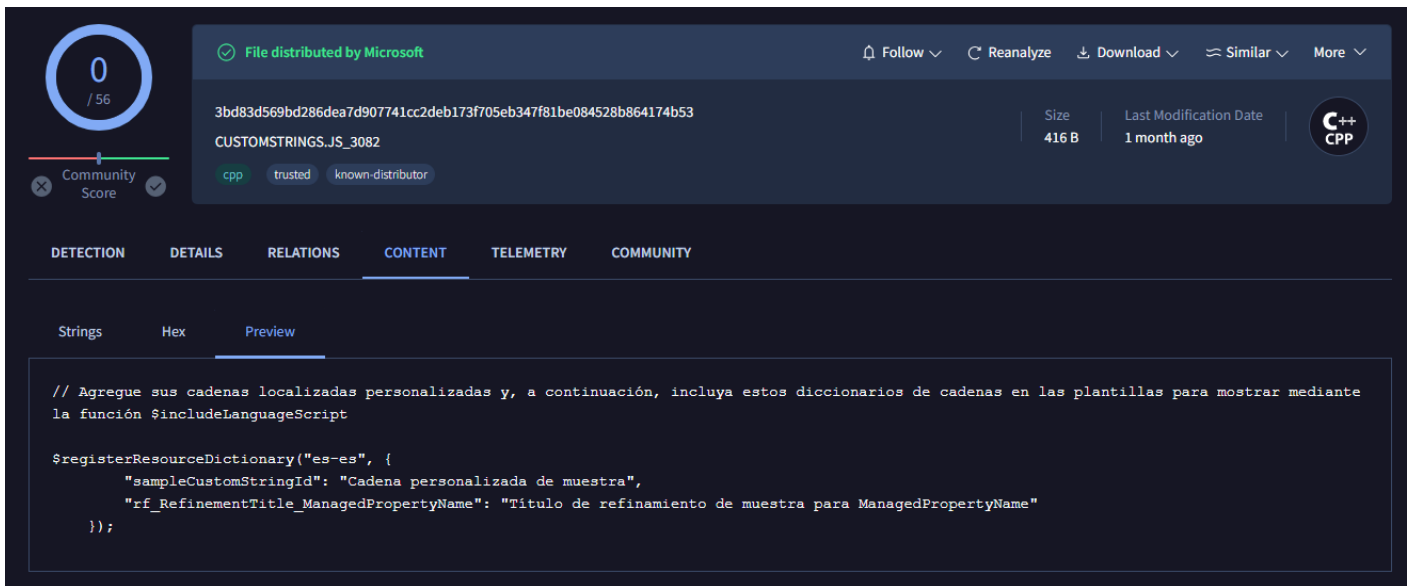


Figure 25: Artifact generated by the sandbox via Google Chrome when connecting to a domain

The strings “registerResourceDictionary”, “sampleCustomStringId”, “rf_RefinementTitle_ManagedPropertyName” are related to Microsoft SharePoint as we were able to confirm. These files were probably generated after visiting sites that have Microsoft Sharepoint functionalities. We found that all the PDFs containing this artifact dropped by Google Chrome came from a website belonging to the Government of Colombia.

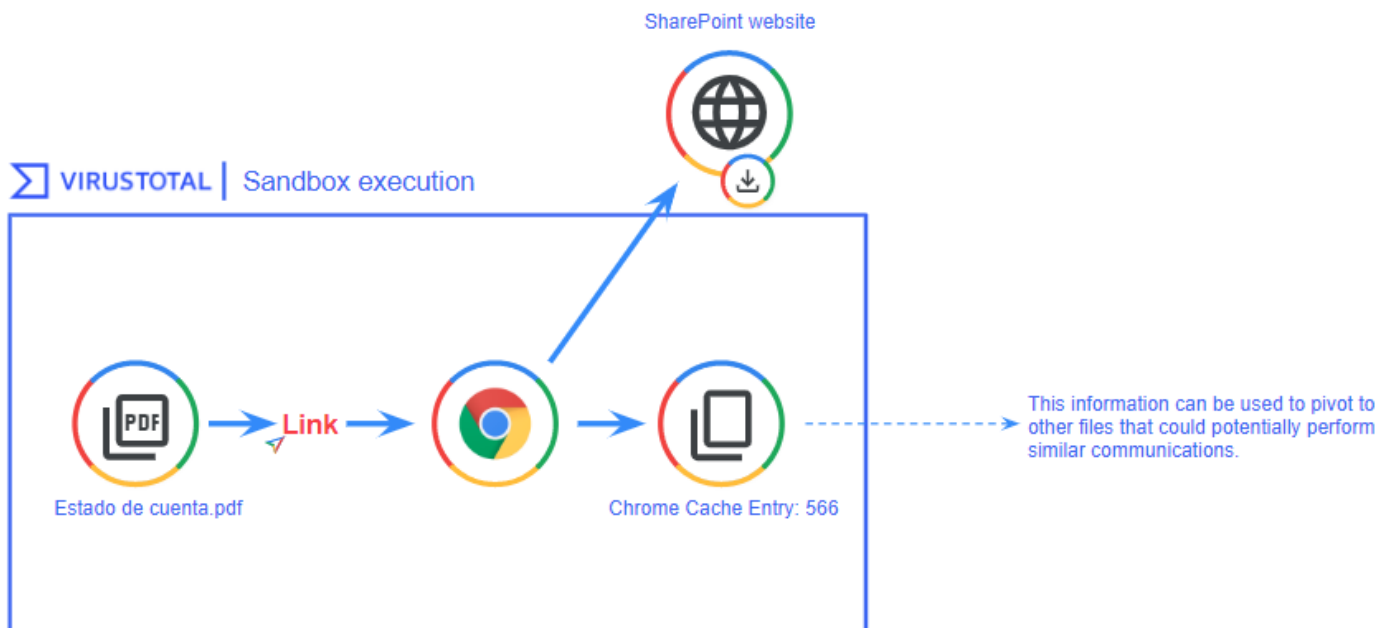


Figure 26: Flow of artifact generation related to Google Chrome that can be used for pivoting in VirusTotal

Email files

Many threat actors incorporate images in their emails, such as company logos, to deceive victims. We used this to identify several mailing campaigns where the same footer was used.

Campaign impersonating universities

On November 13, 2023, we [details](#) about a new campaign impersonating universities, primarily located in Latin America. By leveraging the presence of social network logos in the footer, we were able to find more universities in different continents targeted by the same attacker.

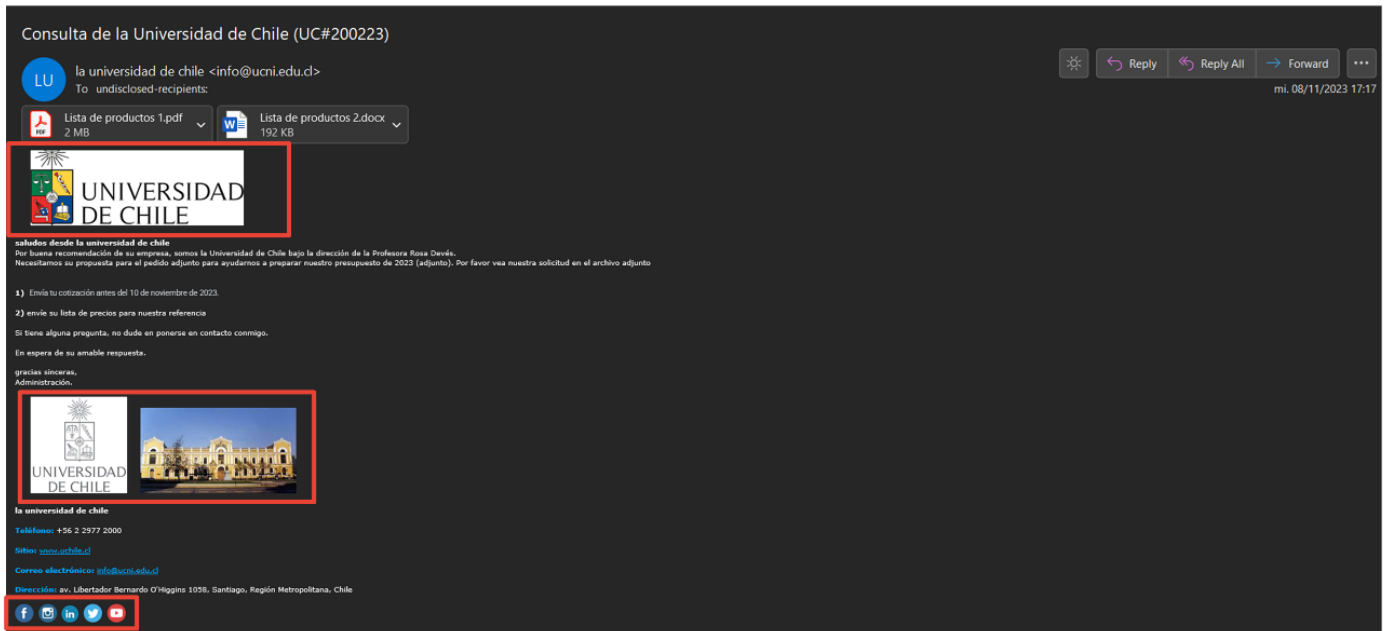


Figure 27: Email impersonating a university that contains multiple images

Pivoting through the images related to the University of Chile doesn't yield good results, as it's too specific. However, if we pivot through the images of the social media footer, represented as email attachments, we can observe multiple files using the same logo.

Scanned	Detections	File type	Name
2023-11-08	0 / 60	PNG	linkedin.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	ci2.png
2023-11-10	0 / 60	PNG	facebook.png
2023-02-16	0 / 60	PNG	youtube.png
2022-08-16	0 / 59	PNG	ci1.png
2023-11-08	0 / 60	PNG	ci22.jpg

Scanned	Detections	Type	Name
2023-03-14	27 / 60	Email	3yOXfE1-67450-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	3yPyYx-D-67450-0920E2263924CF2555660053ba7.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 (Koc 2022 okul projesi).msg
2022-11-22	25 / 62	Email	f352c14-6499-4694-C313-93dadacbbc24f/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	7dbee02ad41a4cc350590955efef34bc033220d0bf9927c2d10f2651216d4d0d
2023-12-03	28 / 61	Outlook	Consulta de la Universidad de Chile (UC#200223).msg

Figure 28: Using the images from the email footer to pivot and identify new emails

Just by analyzing one of the social media logos, we saw 33 email parents, all of them related to the same campaign.

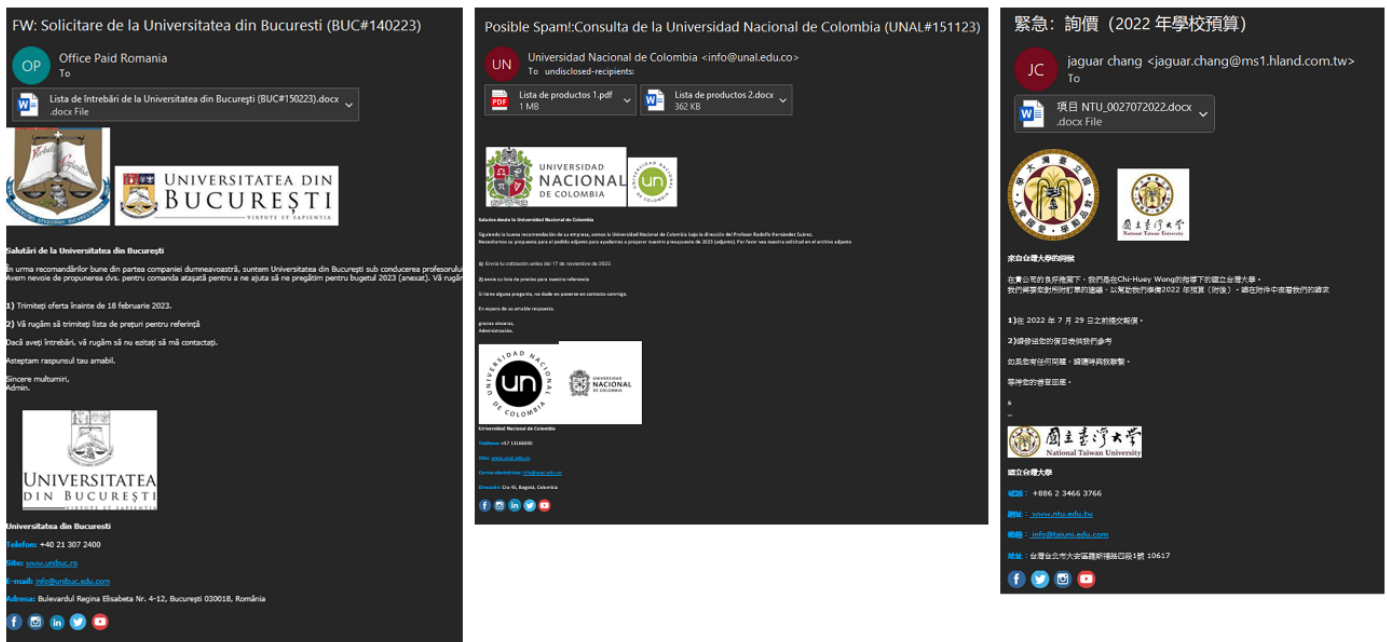


Figure 29: Other emails identified through image pivoting techniques

Campaigns impersonating companies

Another usual case is adding a company logo in the email signatures to enhance credibility. Delivery companies, banks, and suppliers are some of the most observed images during our research.

For example, this [email](#) utilizes the corporate image of China Anhui Technology Import and Export Co Ltd in the footer.



Figure 30: Email impersonating a Chinese organization using the company logo in the footer

Pivoting through the image we found 20 emails using the same logo.

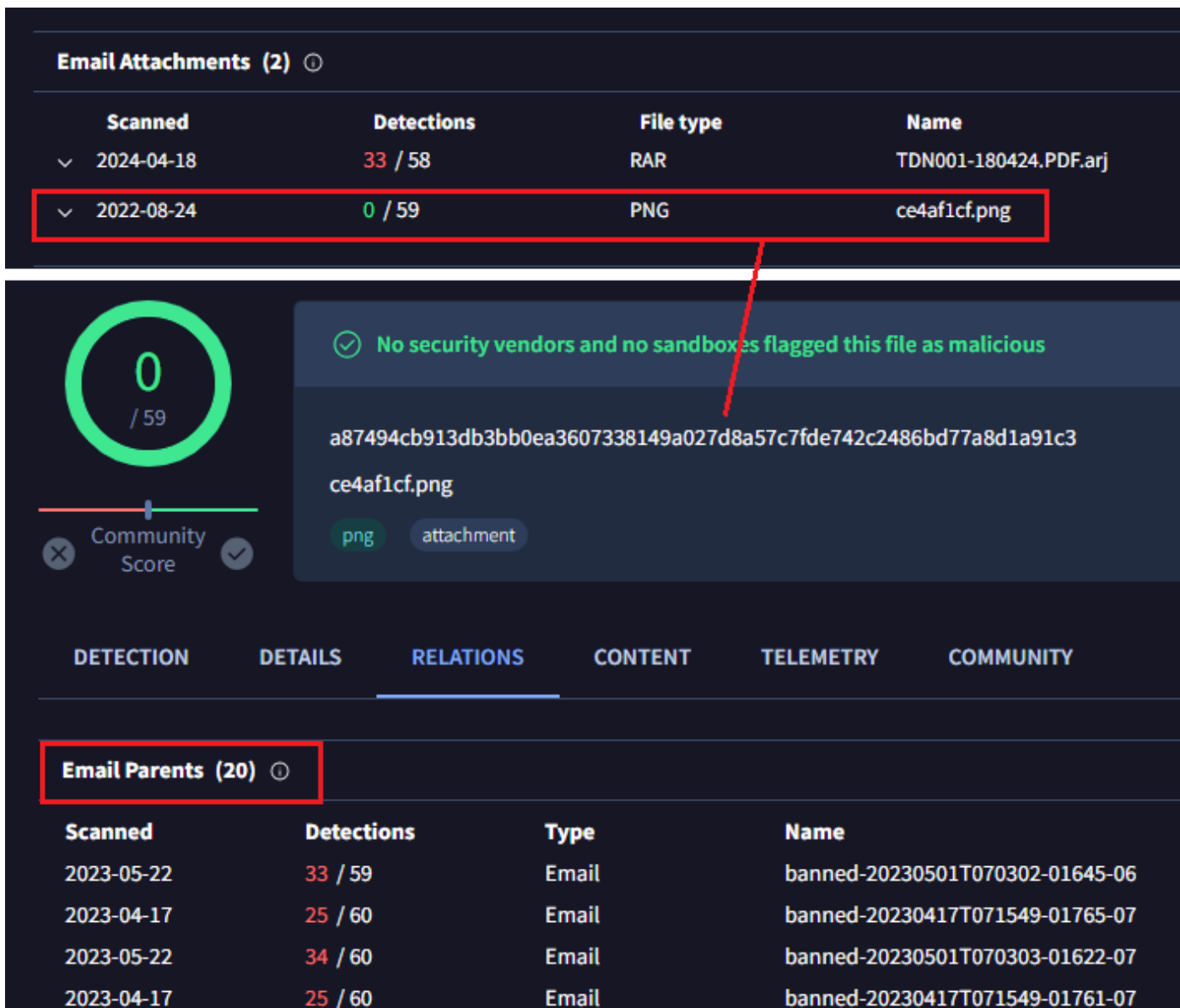


Figure 31: Other emails identified through image pivoting techniques

Wrapping up

We can potentially trace malicious actors by examining artifacts linked to the initial spreading documents, and in the case of images, AI can help us automate potential victim identification and other hunting aspects.

In order to make this even easier, we are planning to incorporate a new `bundled_files` field into the IOCs JSON structure, which basically will help to create livehunt rules. In the meantime you 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 hunting activities.

We hope you found this research interesting and useful, and as always [we are happy to hear your feedback](#).

Stay tuned for the next blog post on PDFs and emails approach!

APPENDIX

[Content_types].xml shared between threat actors

[Content_Type].xml sha256	Shared by
3d8578fd41d766740a1f1ddef972a081436a2d70ab1e9552a861e58d8bbf5321	APT33, APT32
4ea40d34cfcaf69aa35b405c575c7b87e35c72246f04d2d0c5f381bc50fc8b3d	APT29, APT28
4f7fa7433484b4e655d185719613e2f98d017590146d15eedc1aa1d967636b3a	FIN7, Gamaredon, APT28, APT32
529739886f6402a9cd5a8064ece73eef19c597ef35c0bc8d09390e8b4de9041b	FIN7, APT33, TA505, Mustang Panda
688dca40507fb96630f3df80442266a0354e7c24b7df86be3ea57069b25d12c6	Gamaredon, APT33
6f1ac5f0ebfb7e97d3dc4100e88eaab10016a5cac75e1251781f2ea12477af51	Gamaredon, Hazy Tiger, APT33,
7796c382cd4c7c4ae3bcf2eed4091fbb20a2563ca88f2aecadb950ad9cf661f8	Razor Tiger, APT28, UAC-0099
b4fa7f3faa0510e4d969219bceec2a90e8a48ff28e060db3cdd37ce935c3779c	Razor Tiger, SideCopy Gamaredon, APT37, Mustang
dfa90f373b8fd8147ee3e4bfe1ee059e536cc1b068f7ec140c3fc0e6554f331a	Panda, APT28, UAC-0099, SideCopy
fe98b3bcf96f9c396eb9193f0f9484ef01d3017257300cc76098854b1f103b69	FIN7, Hazy Tiger
ff5a5ba3730a8d2ec0cbad39e5edf4ad502107bd0ef8a5347f29262b3dfe8a43	Mustang Panda, APT32

styles.xml shared between threat actors

Styles.xml sha256	Shared by
13ed55637980452662cb6838a2931a5e54fbed5881bcbae368b3d189d3a01930	APT28,

2de1fc9c48c4b0190361c49cdb053fd39cf81e32f12c82d08f88aec34358257f	UAC-0099, Razor Tiger Hazy Tiger, Gamaredon, APT33
59df7787c7cf5408481ae149660858d3af765a0c2cd63d6309b151380f92adb2	TA505, Gamaredon APT28, FIN7, Razor Tiger, APT32, APT33
8f590f608f0719404a1731bb70a6ce2db420fd61e5a387d5b3091d47c7e21ac9	Hazy Tiger, FIN7 APT32, SideCopy, Mustang Panda, Razor Tiger
de392cd4bf1d650a9cf8c6d24e05e0605bf4eaf1518710f0307d8aceb9e5496c	
e16f84c5fd1df6af1a1f2049f7862f4ea460765863476afb17e78edee772d35b	