THREAT REPORT

Crime Finds a Way: The Evolution and Experimentation of the Cybercrime Ecosystem

KEY FINDINGS

- Major cybercrime actors now use increasingly diverse sets of tactics, techniques, and procedures.
- Initial access brokers and other threat actors often "follow the leader" in using various techniques.
- Defenders must rapidly respond to the ever-changing threat landscape in a way previously unobserved by researchers.
- Some major cybercriminal actors have the resources available to research and develop new, complicated attack chains.

INTRODUCTION

The cybercriminal ecosystem has experienced a monumental shift in activity and threat behavior over the last year in a way not previously observed by threat researchers. Financially motivated threat actors that gain initial access via email are no longer using static, predictable attack chains, but rather dynamic, rapidly changing techniques.

This change is largely driven by Microsoft blocking macros by default and forcing everyone along the threat actor food chain from small crime commodity actors to the most experienced cybercriminals that enable major ransomware attacks to change the way they conduct business. Microsoft announced it would begin to block XL4 and VBA macros by default for Office users in October 2021 and February 2022, respectively. The changes began rolling out in 2022.

Based on Proofpoint's unique telemetry analyzing billions of messages per day, Proofpoint researchers have observed widespread threat actor experimentation in malware payload delivery, using old filetypes, unexpected attack chains, and a variety of techniques that result in malware infections, including ransomware.

This activity demonstrates the following about the overall cybercriminal threat landscape:

- Threat actors continue to test various threat behaviors to determine the most effective method of gaining initial access via email. There is no reliable, consistent technique adopted by the entire threat landscape.
- Threat actors follow the leader. One or a group of threat actors may adopt a new technique and in subsequent weeks or months, researchers will observe the same technique used by multiple threat actors.
- Some more sophisticated ecrime actors have the time and resources available to develop, iterate, and test different malware delivery techniques.

In this report, Proofpoint will examine major landscape shifts and common tactics, techniques, and procedures (TTPs) adopted by a variety of threat actors.

METHODOLOGY

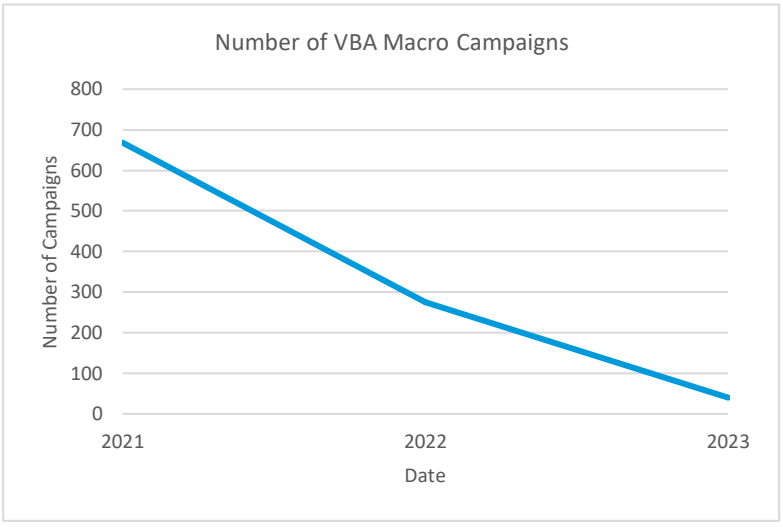
Proofpoint conducted its research of cybercriminal threats based off threat campaign data or activity that was manually analyzed and contextualized from January 2021 through March 2023. For this report, a campaign is defined as a timebound set of related threat activity analyzed by Proofpoint researchers. Even in cases where no attribution is made, threats from a given campaign result from attacks perpetrated by the same threat actor. Threats may be related by a variety of factors including distribution or hosting infrastructure, overlap in message forensics such as header components, a common payload, or other facets. Threats analyzed in this report are based on tags associated with campaign data, which are manually applied by threat researchers at the time of identification. All instances of research in this report, including case studies, refer to proprietary Proofpoint processes and data unless otherwise noted.

It should be noted that while this analysis covers thousands of campaigns and billions of threats overall, it represents only a portion of the threat landscape, and the analysis focuses on the highest priority threat actors. As a result, inherent bias is present in the choice of what activity is campaigned.

A SHIFT BEGINS

Prior to 2022, Proofpoint observed macros were heavily favored by cybercriminal threat actors as initial access payloads. VBA macros are used by threat actors to automatically run malicious content when a user has actively enabled macros in Office applications. XL4 macros are specific to the Excel application but can also be weaponized by threat actors. Typically, threat actors distributing macro-enabled documents rely on social engineering to convince a recipient the content is important, and enabling macros is necessary to view it.

In 2021, there were nearly 700 campaigns that used VBA macros, with almost the same number of XL4 macro campaigns, based on Proofpoint data. In 2022, the total number of campaigns using macros of either kind dropped nearly 66%, and so far in 2023, macros have barely made an appearance in campaign data.



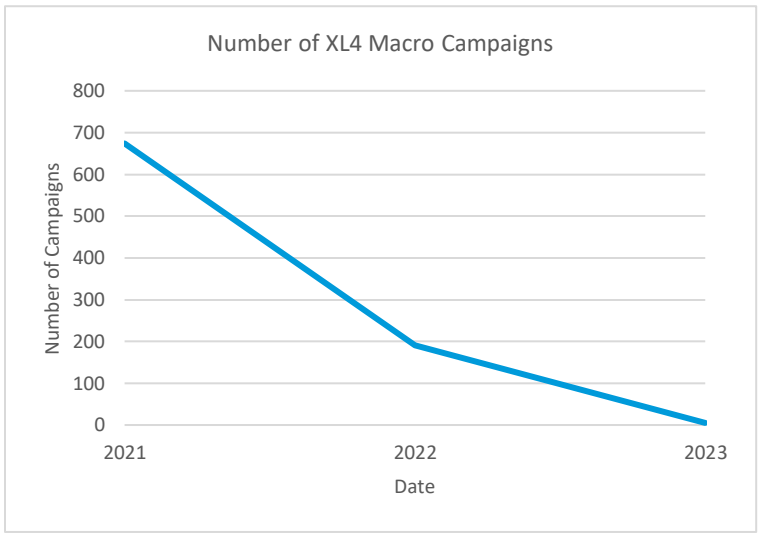


Figure: Number of campaigns leveraging macros.

Proofpoint's reporting in July 2022 highlighted the new ways threat actors were adopting to the shift away from macros, including using archive files such as ISO attachments to deliver malware. This technique was used to bypass mark-of-the-web (MOTW) attributes, which were used to block macros downloaded from the internet. In November 2022, Microsoft fixed the issue that allowed actors to use archive files to get around restrictions, and the use of ISO files by prominent ecrime threat actors declined significantly.

Shortcut (LNK) files were also initially favored as a technique from multiple ecrime threat actors beginning in mid-2022, with multiple actors classified as initial access brokers (IAB) pivoting to include LNK files in attack chains around the same time. For example, Proofpoint observed LNK attachments used by at least eight large ecrime threat actors considered IABs, with their use peaking in June and September 2022 before the actors began pivoting to new TTPs.

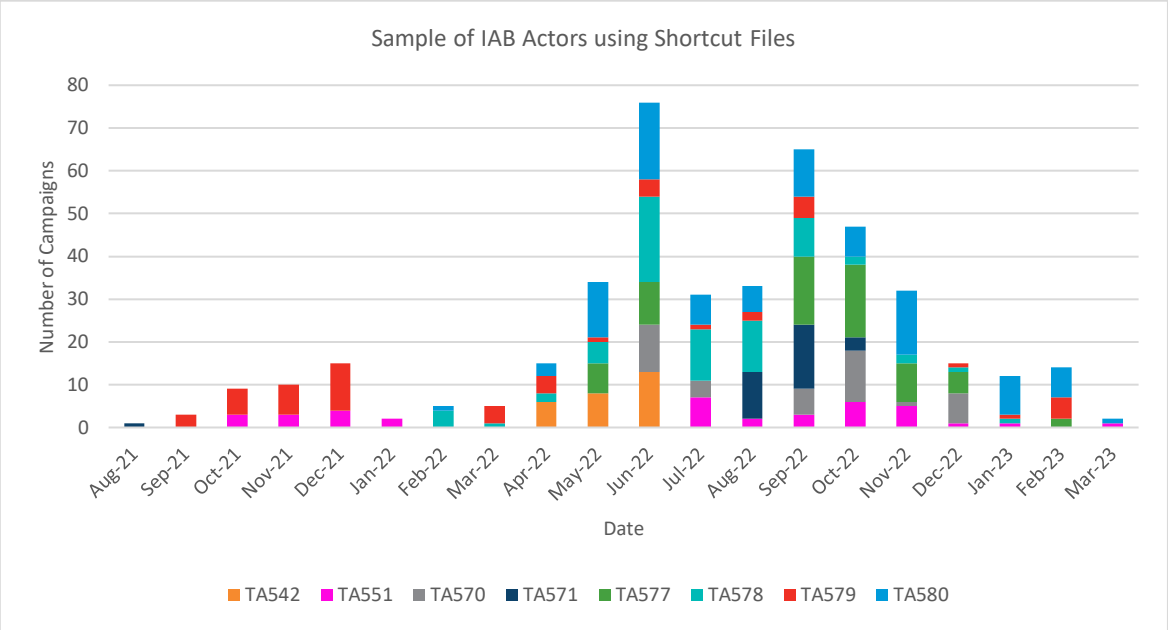


Figure: Use of shortcut (LNK) files by priority ecrime threat actors.

Initially Proofpoint researchers hypothesized that threat actors would begin using XLL files as part of the overall TTP experimentation following macros, as this technique, while not popular, had been previously observed in threat data. XLL files are a type of dynamic link library (DLL) file for Excel and are designed to increase the functionality of the Excel application. Proofpoint has observed at least six large ecrime actors experiment with XLL files in malware delivery, and multiple unattributed threat clusters, but XLL files are used significantly less than other filetypes and have not experienced a notable uptick in use across the threat landscape.

FOLLOW THE LEADER

Based on Proofpoint data, while virtually all cybercriminal threat actors are experimenting and using multiple different attack chains and TTPs in malware delivery, researchers have observed a common trend among many threat actors: when a new threat behavior or adoption of a new technique is observed by at least one actor cluster, multiple threat actors will use it in subsequent campaigns.

As detailed in the diagram above, few IAB actors were using LNK files in threat campaigns before April 2022, when four threat actors used them in attack chains delivering malware, including TA542 incorporating them to deliver Emotet. Subsequently, multiple other

threat actors began using shortcuts in campaigns before its popularity decreased earlier this year in favor of other filetypes in attack chains.

Threat actors follow the leader for several reasons, including: the likelihood of new attack chains working better than known behaviors, the ease of copying existing attack chains rather than creating new ones, the reduction in the amount of testing and development required by the threat actors, and the likelihood of some actors sharing new techniques between themselves or purchasing toolkits from the same sources.

HTML Smuggling

Since June 2022, the use of HTML smuggling has increased dramatically in Proofpoint campaign data, but after peaking in October 2022, threat actor use of the technique decreased slightly before rebounding in February 2023. The HTML smuggling technique "smuggles" an encoded script within an HTML attachment. When the HTML attachment is opened, the web browser decodes the malicious script which is used to assemble the malware payload on the victim's computer. The initial adoption of HTML smuggling as a technique was largely driven by campaigns attributed to known threat actors, including TA570 and TA577. However, since October 2022 it has been more frequently observed in campaigns associated with threats that are unattributed to a known actor.

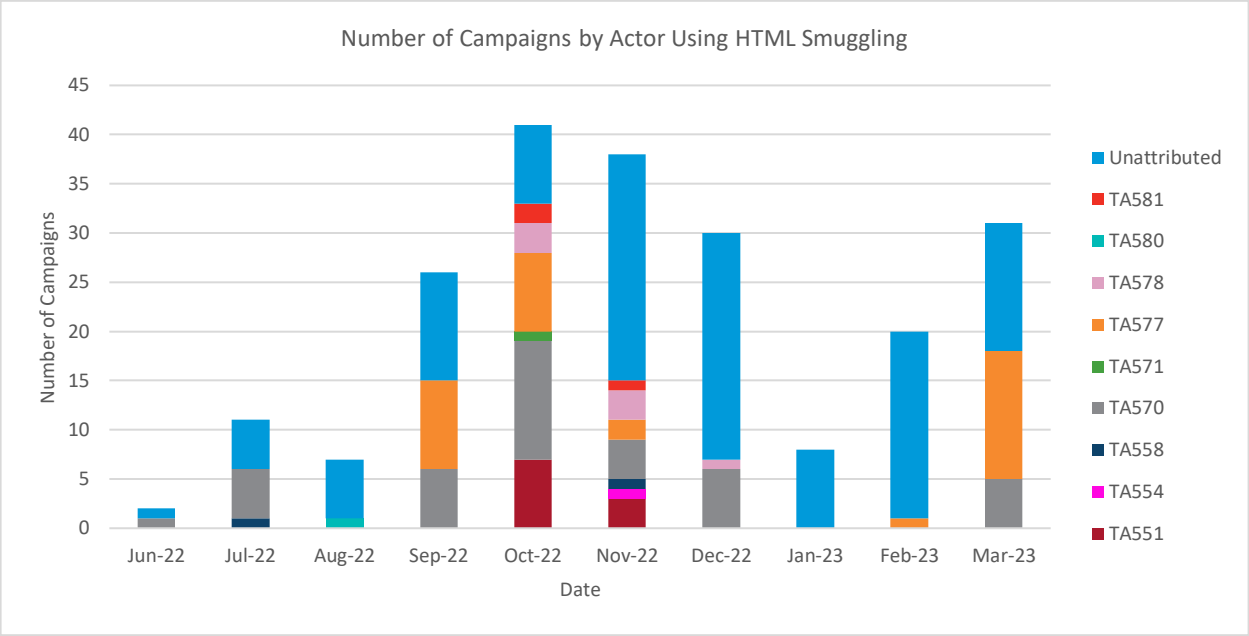


Figure: Number of cybercriminal threat campaigns using HTML smuggling from June 2022 through March 2023. (Analyst note: The HTML smuggling tag was created in Proofpoint threat data in June 2022.)

PDF Usage

Proofpoint has observed PDF files used by various threat actors over the years across the threat landscape since we first began tracking threat actors. Typically, threat actors have used PDF files that include a URL to start the attack chain. As part of the recent threat actor TTP experimentation, Proofpoint researchers began to observe PDF attachments increasingly used by multiple cybercrime threat actors including IABs. After threat actors started experimenting with container files such as ISO files and HTML

smuggling, Proofpoint began to see multiple IAB threat actors use PDF files starting in December 2022. Its use spiked in the beginning of 2023 by cybercrime threat actors and unattributed threat clusters.

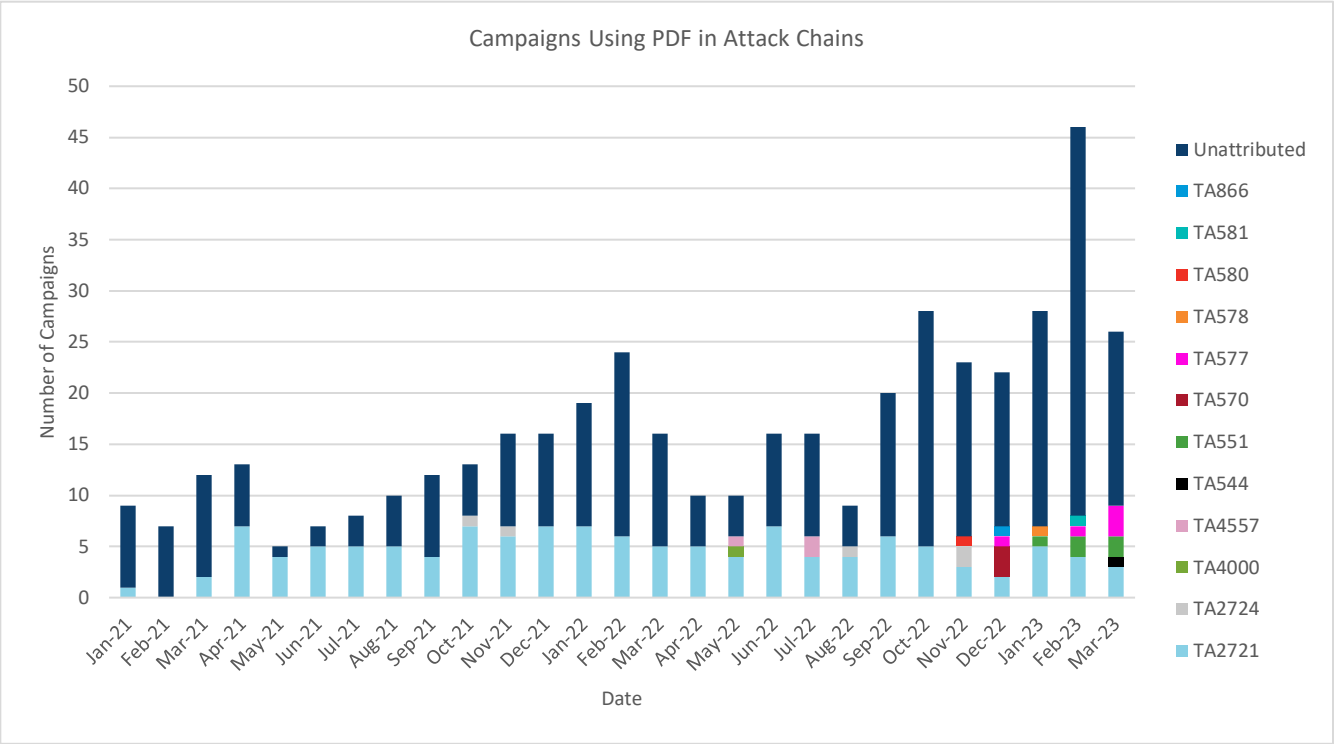
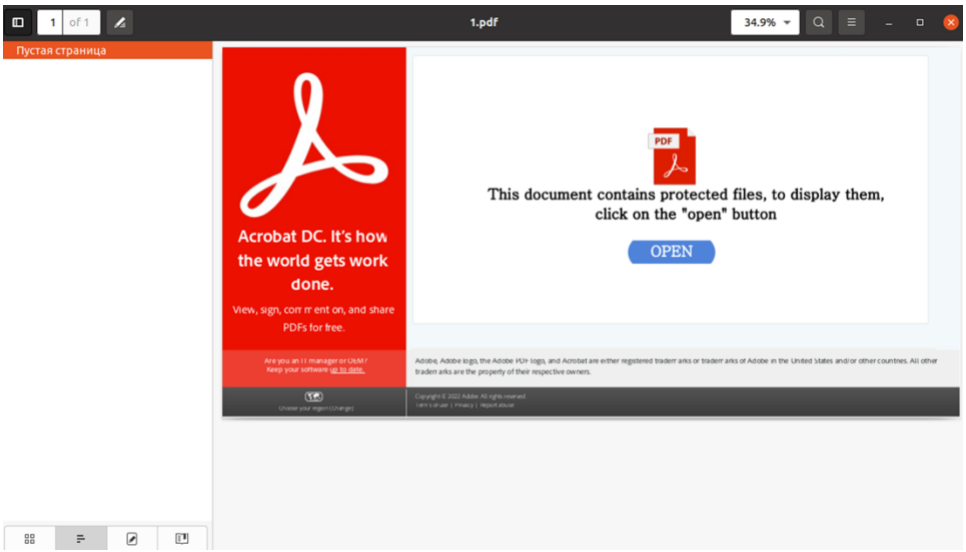


Figure: Use of PDF increases in the second half of 2022.

TA570 was one of the first large cybercrime actors to use PDF attachments with URLs leading to a zipped password protected IMG file containing shortcut file ultimately leading to Qbot.

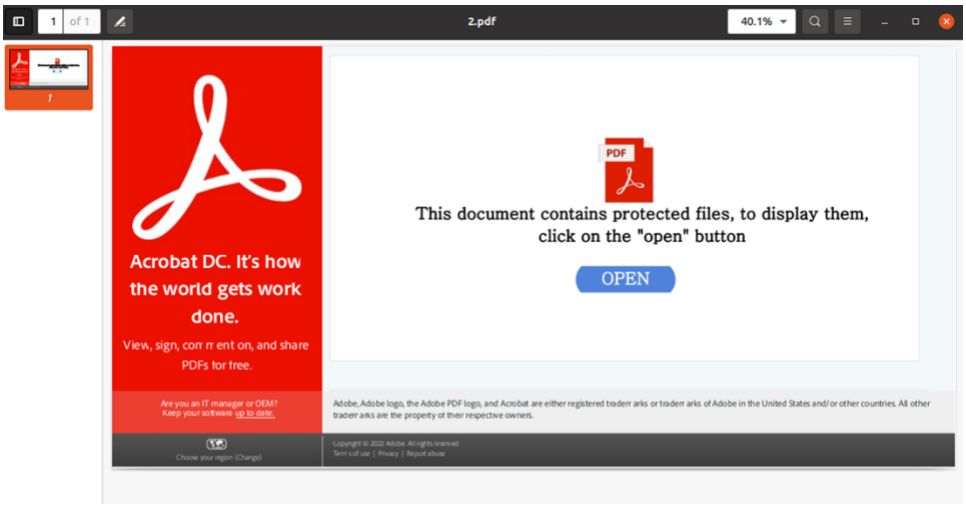
Of note, Proofpoint researchers uncovered a high-volume campaign in April 2023 where TA570 likely was experimenting with PDF encryption. In this campaign, the PDF attachments contained embedded URLs and, interestingly, open-source tools (e.g., pdf-id.py) and malware sandboxes were unable to parse the embedded URL. Proofpoint found that the PDF attachments were encrypted, which may have been an experiment from the actor to increase the difficultly for defenders to identify and block threats. Despite the parsing issue, the PDF contained an “OPEN” button with a hidden embedded URL making it easier for the victim to click the button. If clicked by the victim, the URL would redirect to a zipped WSF ultimately leading to Qbot.




```
python pdfid.py 1.pdf
PDFiD 0.2.8 1.pdf
 PDF Header: %PDF-1.7
 obj                    51
 endobj                 51
 stream                 47
 endstream              47
 xref                    0
 trailer                 0
 startxref               2
 /Page                   1
 /Encrypt                2
 /ObjStm                 5
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               1
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /URI                    0
 /Colors > 2^24          0

python pdf-parser.py -k /URI -O 1.pdf
Traceback (most recent call last):
  File "pdf-parser.py", line 638, in Decompress
    data = FlateDecode(data)
  File "pdf-parser.py", line 1015, in FlateDecode
    return zlib.decompress(C2BIP3(data))
zlib.error: Error -3 while decompressing data: incorrect header check

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "pdf-parser.py", line 1678, in <module>
    Main()
  File "pdf-parser.py", line 1497, in Main
    indexes = list(map(int, C2SIP3(object.Stream())[:offsetFirstObject].strip().split(' ')))
  File "pdf-parser.py", line 621, in Stream
    return self.Decompress(data, filters)
  File "pdf-parser.py", line 643, in Decompress
    return message + '. zlib.error %s' % e.message
AttributeError: 'error' object has no attribute 'message'
```

Figure: Malicious encrypted PDF file spoofing Adobe branding containing a parsing issue.

A few days later Proofpoint observed the same actor remove the encryption in a high-volume campaign. Listed below is an example of the PDF and embedded URL parsing.




```
python pdfid.py 2.pdf
PDFiD 0.2.8 2.pdf
 PDF Header: %PDF-1.4
 obj                    91
 endobj                 91
 stream                 38
 endstream              38
 xref                    1
 trailer                 1
 startxref               1
 /Page                   1
 /Encrypt                0
 /ObjStm                 0
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /URI                    8
 /Colors > 2^24          0

python pdf-parser.py -k /URI -O 2.pdf
  /URI (https://www.adobe.com)
  /URI ()
  /URI ()
  /URI (https://mirrornews.in/blo/64369fcc06861.zip)
```

Figure: Malicious PDF file spoofing Adobe branding without parsing issue.

OneNote Explosion

One prominent example of the follow the leader phenomenon began in December 2022, when Proofpoint researchers first observed unattributed campaigns using OneNote documents to deliver malware, specifically AsyncRAT. OneNote is a digital notebook created by Microsoft and available via the Microsoft 365 product suite. Proofpoint observed threat actors deliver malware via OneNote documents, which are .one extensions, via email attachments and URLs. By January 2023, Proofpoint threat researchers observed dozens of unattributed commodity malware campaigns using the same TTPs. Subsequently, multiple tracked threat actors adopted this technique. Within a few months, as detailed in the following diagram, there were over 120 campaigns leveraging OneNote files. Notably, all three IAB actors TA577, TA570, and TA581 started using OneNote on the same day in late January 2023. TA577 used

OneNote files more often than other IAB actors. Comparatively, TA542 started using OneNote files much later in campaigns, in March 2023.

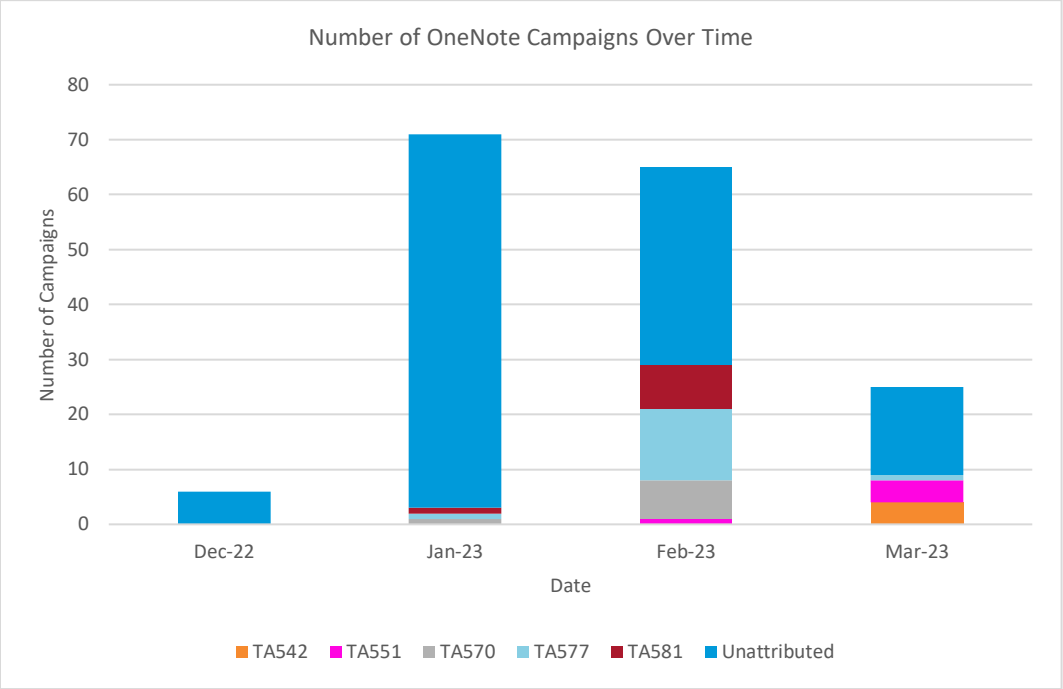


Figure: Number of OneNote campaigns observed by threat researchers between December 2022 and March 2023.

The OneNote documents contained embedded files, often hidden behind a graphic that looks like a button. Threat actors frequently included a series of embedded fields hidden behind the button to increase the likelihood of a successful user click. When the user double clicked the embedded file, they were prompted with a warning. If the user clicked continue, the file executed. The file might be different kinds of executables, shortcut (LNK) files, or script files such as HTML application (HTA) or Windows script files (WSF), visual basic scripts (VBS) files, and batch (BAT) files.

Detection of malicious OneNote documents was initially limited, and based upon observed characteristics of threat campaigns, threat actors adopted OneNote as of result of their experimentation with different attachment types to bypass threat detection. In response, Proofpoint researchers – and the security community overall – worked to develop tools and resources to improve detection and render OneNote documents considerably less effective as vehicles for malware delivery.

The OneNote threat lifecycle is a good example of the symbiotic relationship between threat actors and defenders. When new behaviors are identified, security teams must create new rules, detections, and tools to improve defenses and detections. Once a technique becomes well-known, it becomes less effective, thereby forcing threat actors to try something different. When Proofpoint first began observing OneNote used for malware delivery, the team prioritized creating detections for the various attack chains observed, and by the time it was used by IAB actors, the TTPs had become less effective due to the rules in place.

While Proofpoint still observes OneNote documents as part of malware attack chains, the technique has been used significantly less since March 2023. The drop in OneNote usage is likely due to Microsoft reportedly deploying a silent patch in January 2023 to add Mark of the Web (MOTW) attributes to OneNote files. Additionally, Microsoft announced in March 2023 that OneNote will block embedded files with dangerous extensions. Previously, users could still open these files and only a dialog warning would be displayed that opening attachments could harm their computer and data.

CHANGES FOR INITIAL ACCESS BROKERS

The entire cybercriminal ecosystem has been experimenting and developing different attack chains, and the changes may be best illustrated by examining one subset of cybercrime threat actors: initial access brokers (IABs). Ransomware and other malware operators often buy access from independent cybercriminal groups who infiltrate major targets and then sell access to the ransomware actors for a profit.

Typically, IABs are opportunistic threat actors supplying access to affiliates and other cybercrime threat actors after the fact, for example by advertising access for sale on forums. For the purposes of this report, Proofpoint considers IABs to be the groups who obtain initial access via first-stage malware payloads and may or may not work directly with ransomware threat actors.

These criminal threat actors compromise victim organizations with first-stage malware like Qbot, IcedID, or Bumblebee, and then sell their access to ransomware operators to deploy data theft and encryption operations.

Case Study: TA570

TA570, also known as the Qbot "presidents" threat actor, is one of the most prolific cybercrime threat actors and Qbot affiliates tracked by Proofpoint. It is considered to be an IAB and Proofpoint has associated TA570 campaigns with follow-on ransomware infections including Black Basta based on details in open source reporting.

Prior to June 2022, TA570 almost exclusively used both VBA macros and XL4 macros in campaigns to deliver malware payloads, typically Qbot but also less frequently IcedID. In June 2022, Proofpoint researchers observed multiple new TTPs used by TA570, notably the first use of HTML smuggling to deliver an archive file containing an LNK, as well as the first cybercriminal exploitation of the Follina vulnerability, CVE-2022-30190.

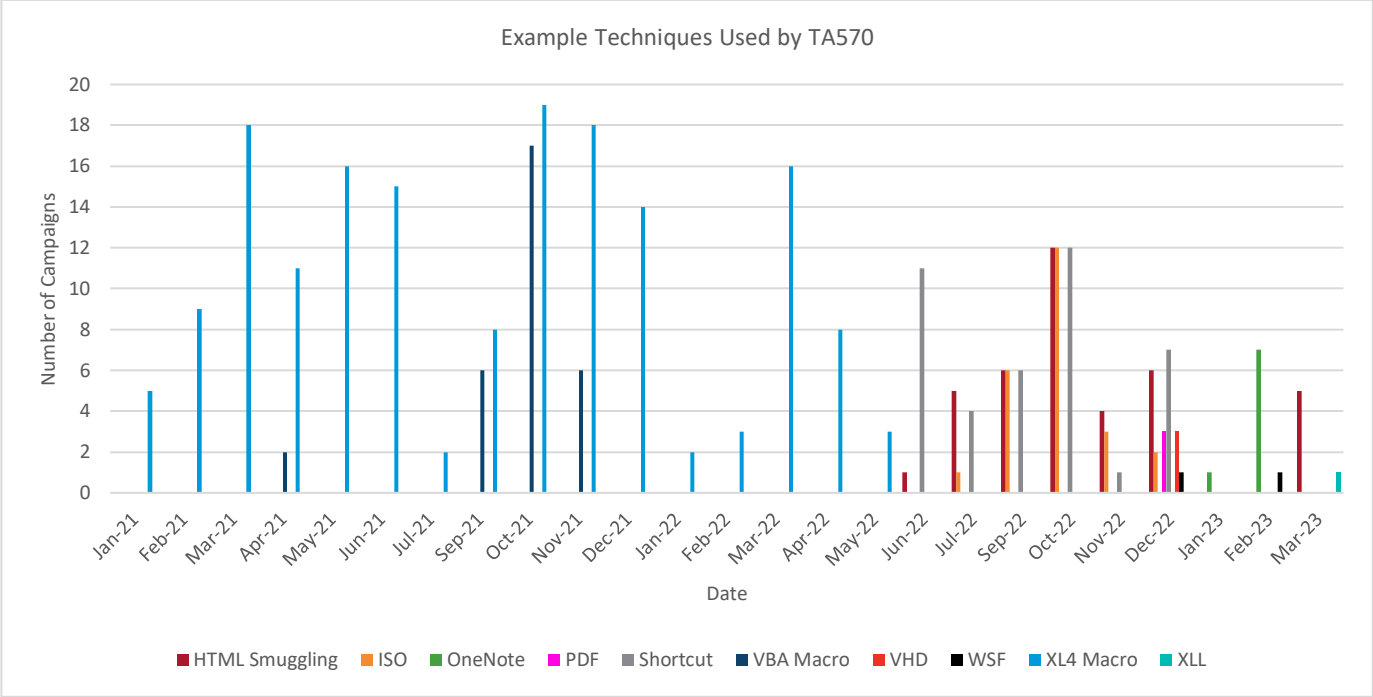


Figure: Example of multiple techniques used by TA570 in campaigns from January 2021 through March 2023.

In the following months, TA570 demonstrated multiple new and different TTPs, using as many as six different and unique attack chains in one month, and using or experimenting with numerous filetypes throughout. Observed filetypes included PDF, LNK, virtual

hard disk (VHD), ISO, OneNote, Windows Script File (WSF), and XLLs. In many campaigns, multiple different filetypes are used such as LNKs within VHDs.

Variations on the attack chain for this actor can be illustrated in the variability of December 2022 campaigns. For example, Proofpoint observed the following six different attack chains delivering Qbot, all beginning with thread hijacked messages:

- HTML Attachment → Password-Protected Zip → IMG → LNK → CMD → Qbot DLL
- HTML Attachment → Password-Protected Zip → IMG → LNK → Qbot DLL
- HTML Attachment → Password-Protected Zip → VHD → LNK → CMD → Qbot DLL
- HTML Attachment → Password-Protected Zip → VHD → LNK → Qbot DLL
- PDF Attachment → Actor-Controlled URL → Password-Protected Zip → ISO → WSF → Qbot DLL
- PDF Attachment → Actor-Controlled URL → Password-Protected Zip → IMG → LNK → Qbot DLL

TA570 was among the first observed by Proofpoint to repeatedly use HTML smuggling in campaigns beginning in mid-2022, as well as adopting PDFs for malware delivery in December 2022, which multiple other actors began using as well. TA570 was the second observed IAB to use OneNote documents in attack chains, which it began using in January.

Case Study: TA577

TA577, also known as the Qbot "tr" threat actor, is another prominent cybercrime threat actor and Qbot affiliate. It is considered an IAB and Proofpoint has associated TA577 campaigns with follow-on ransomware infections including Black Basta.

Like TA570, TA577 regularly used both VBA macros and XL4 macros in campaigns prior to spring 2022. In April 2022, TA577 continued to use Excel documents for malware delivery, and used a mix of the EtterSilent maldoc builder and MSI files before adopting shortcuts in May 2022. TA577 typically delivers Qbot but has also been observed delivering IcedID and Ursnif since 2021.

Since May 2022, TA577 demonstrated multiple new and different TTPs, using as many as nine different, unique attack chains in one month. Observed filetypes included PDF, LNK, VHD, ISO, OneNote, WSF, and compiled HTML help files (CHM). Many of TA577's changes align with similar attack chains used by TA570. In many campaigns, multiple filetypes are used, such as including shortcut files within ISOs.

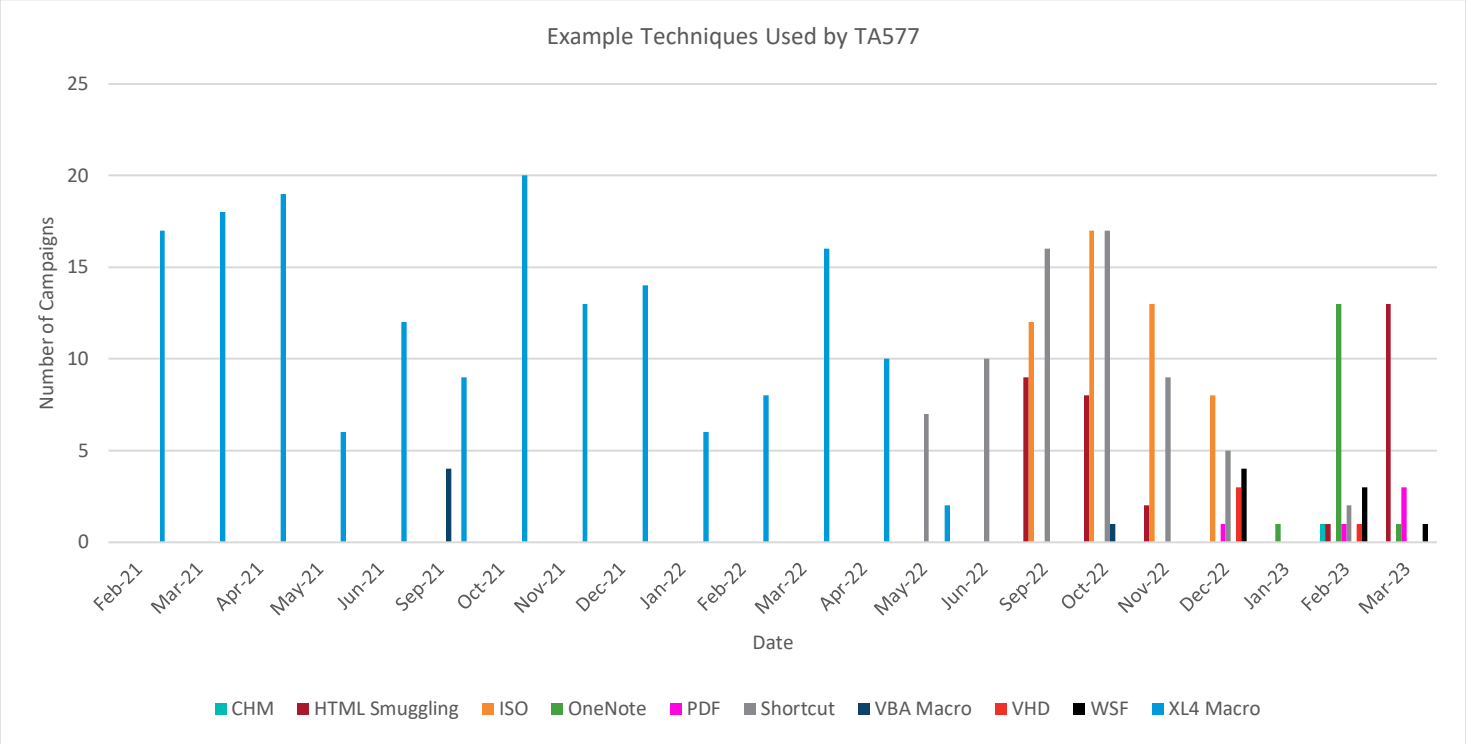


Figure: Example of multiple filetypes used by TA577.

Variations on the attack chain for this actor can be illustrated in the variability of February 2023 campaigns. For example, Proofpoint observed the following nine different attack chains, all beginning with thread hijacked messages:

- Zip Attachment⟶ OneNote File ⟶ HTA ⟶ CURL ⟶ Qbot DLL
- OneNote Attachment ⟶ HTA ⟶ CURL ⟶ Qbot DLL
- URL ⟶ Zip ⟶ OneNote File ⟶ HTA ⟶ CURL ⟶ Qbot DLL
- PDF Attachment ⟶ Actor-Controlled URL ⟶ Zip ⟶ ISO ⟶ LNK ⟶ CMD ⟶ EXE ⟶ Qbot DLL
- OneNote Attachment ⟶ WSF ⟶ Jscript ⟶ PowerShell ⟶ Qbot DLL
- PDF Attachment ⟶ OneDrive URL ⟶ JavaScript File ⟶ PowerShell ⟶ Qbot DLL
- OneNote Attachment ⟶ CMD ⟶ PowerShell ⟶ Qbot DLL
- OneNote Attachment ⟶ CHM ⟶ PowerShell ⟶ Qbot DLL
- HTML Attachment ⟶ Pop Up ⟶ HTML Smuggling ⟶ Zip ⟶ Password ⟶ IMG ⟶ LNK ⟶ CMD ⟶ REG ⟶ WSF ⟶ PowerShell ⟶ Qbot DLL

TA577 followed TA570 in adoption of HTML smuggling but was the first tracked threat actor to adopt OneNote documents in attack chains and returned from a month-long break at the end of January 2023 to deliver Qbot. TA577 is among the most active cybercriminal threat actors tracked by Proofpoint with dynamic, frequently changing attack chains.

The rate at which TA577 and TA570 both adopt and distribute new TTPs suggests both threat actor groups likely have the time, resources, and experience to rapidly iterate and test new delivery methods. Both threat actors, in addition to other initial access brokers, appear to have the pulse of the threat landscape and know when and why specific attack chains stop being effective, and will quickly create new methods to bypass detections and attempt to increase the effectiveness and likelihood of victim engagement with their payload delivery.

Case Study: IcedID

Since 2021, Proofpoint has tracked seven threat actors using IcedID leading to around 250 campaigns, and an additional 150 unattributed campaigns. IcedID has been associated with follow-on ransomware infections including Quantum, RansomExx, and Conti.

Prior to 2022, threat actors delivering IcedID largely used macros to deliver malware, in addition to occasionally other methods such as URLs leading to zipped JavaScript payloads. But threat actors distributing IcedID, led by TA578 and unattributed threat clusters, began experimenting with new mechanisms for payload delivery starting in early 2022.

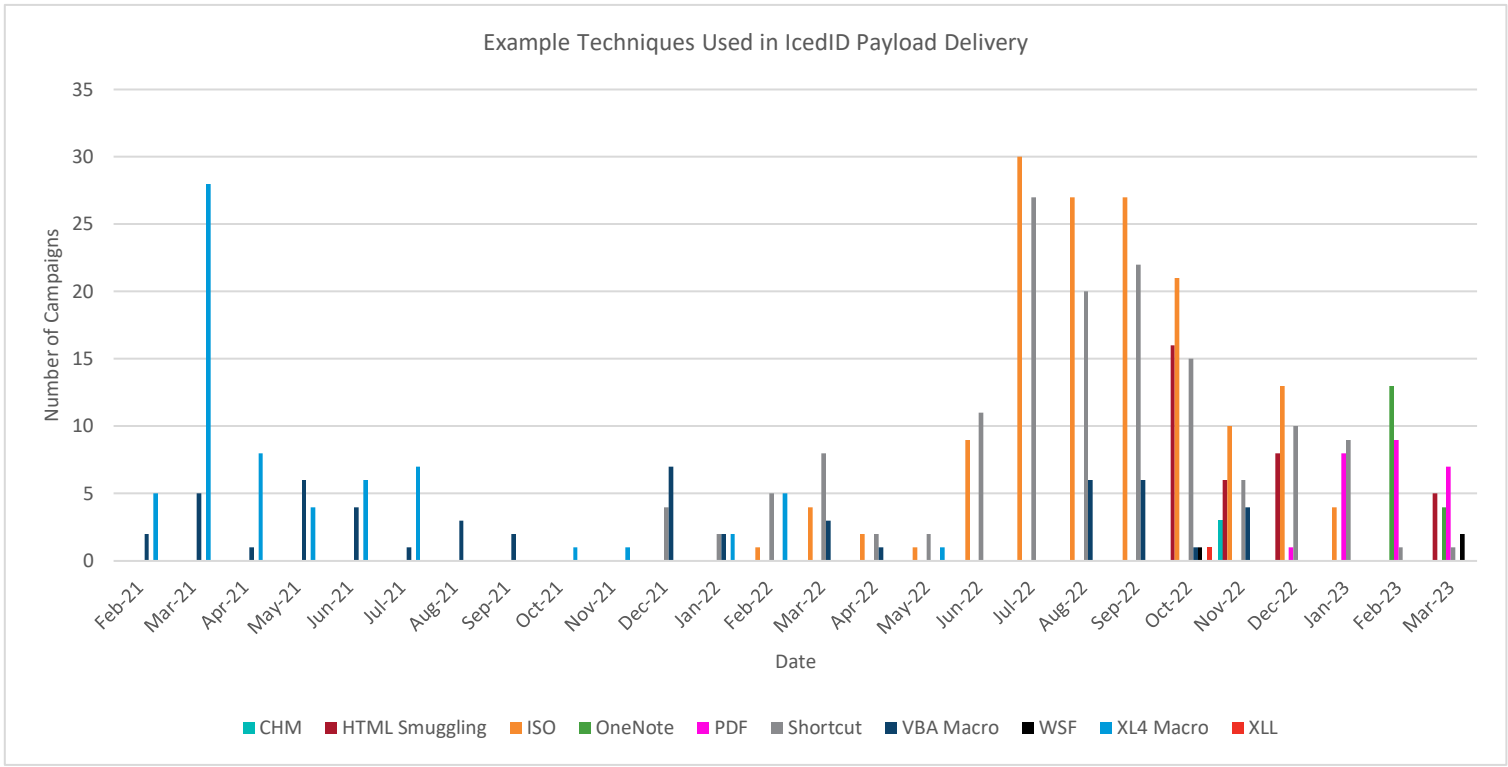


Figure: Example techniques used by threat actors delivering IcedID.

In February 2022, Proofpoint identified an unattributed IcedID campaign using thread hijacking to deliver an ISO attachment containing an LNK which led to the installation of the malware. Proofpoint subsequently observed many threat actors adopt ISO attachments and shortcuts in payload delivery throughout 2022. Beginning in October 2022, many threat actors delivering IcedID began using HTML smuggling, which aligns with the popularity of this technique across the threat landscape in the fall of that year.

Threat actors delivering IcedID also began adopting PDFs in attack chains for the first time towards the end of 2022 and beginning of 2023, aligning with the shift across the threat landscape to use PDFs as an initial step in malware delivery as described above.

By using IcedID as an example of the variability of threat actor attack chains, it is clear experimentation and adoption of dynamic TTPs is common for both tracked actors and unattributed threat clusters delivering malware that could lead to ransomware.

TARGETED CYBERCRIME

While Proofpoint has observed consistent trends in initial access brokers, targeted cybercrime threats do not all align in a similar way. Proofpoint defines targeted cybercrime as those threat actors with narrow targeting based on geography or vertical.

This is likely due to the variety of TTPs used by targeted cybercriminal threats before macros became a less effective method of malware delivery. Some targeted threats used macros as the most common initial access vector, while others ignored them entirely for other techniques that are now becoming more popular across the threat landscape.

Case Study: TA558

After using VBA macros consistently since 2019, TA558, a small crime threat actor targeting hospitality, hotel, and travel organizations, began using CHM and HTML smuggling in late 2022. TA558 has also experimented with other file types in attack chains such as RAR and ISO container files, JavaScript files, HTA attachments, WSF, and VBS files, and there was a clear trend of shifting away from macros and adopting new techniques for malware delivery. This actor has been observed delivering a wide variety of commodity malware payloads including Loda RAT, Vjw0rm, Revenge RAT, and AsyncRAT.

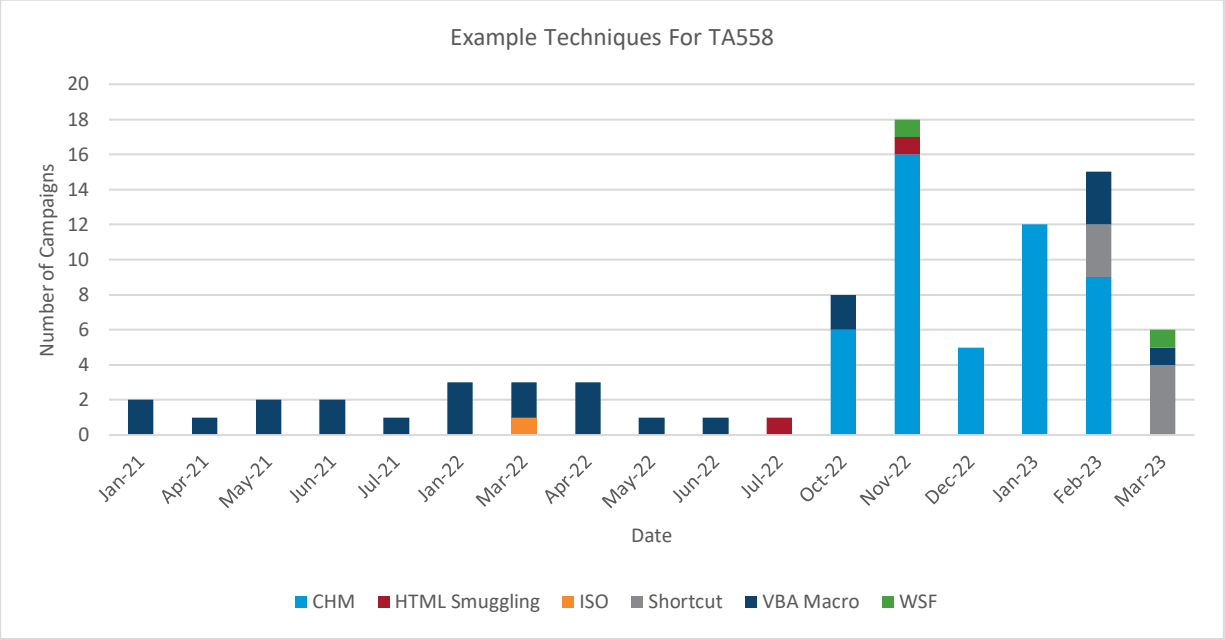


Figure: Example campaigns for TA558 using a variety of techniques.

Despite TA558 decreasingly using macros, they have continued to use reservation-themed lures with business-relevant themes such as hotel room bookings. TA558 also has remained consistent with their targeting which is mainly Portuguese and Spanish speakers, typically located in the Latin America region, with additional targeting observed in Western Europe and North America.

Case Study: TA2541

TA2541 is a cybercriminal actor that uses themes related to aviation, transportation, and travel and targets organizations that align with those interests. Proofpoint has tracked this actor since 2017. The group initially sent macro-laden Microsoft Word attachments that downloaded remote access trojan (RAT) payloads but quickly pivoted to malware delivery via URLs, typically using cloud services such as Google Drive and Discord, leading to various scripts and compressed executables. Over the last several years TA2541 has largely been consistent with their attack chains by leveraging URLs to various scripts and avoiding the use of Office macros.

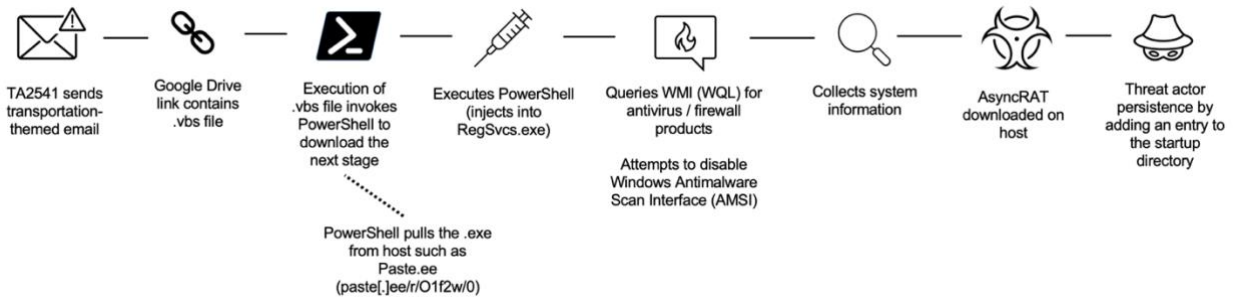


Figure: TA2541 attack chain.

TA2541 has distributed over 10 different types of malware, all using the same infection chain. TA2541 has also been consistent with using the themes fight, aircraft, fuel, yacht, charter, etc. in their VBS file names. While other threat clusters have used similar attack chains such as URLs to VBS files, TA2541 has been one of the most consistent with their email lures, VBS file names, and infection chain.

Case Study: TA2721

TA2721 is among the most consistently active targeted cybercriminal threat actors, and predominately targets Spanish-speaking users at organizations globally. The group targets multiple industries from finance to entertainment. The group uses Spanish-language lures to distribute a known – but infrequently used – RAT called Bandook.

TA2721 leverages the same type of budget or payment-themed lures throughout its campaigns to prompt a user to download a PDF. The attached PDF contains an embedded URL and password that, when clicked, leads to the download of a password protected compressed executable that contains Bandook.

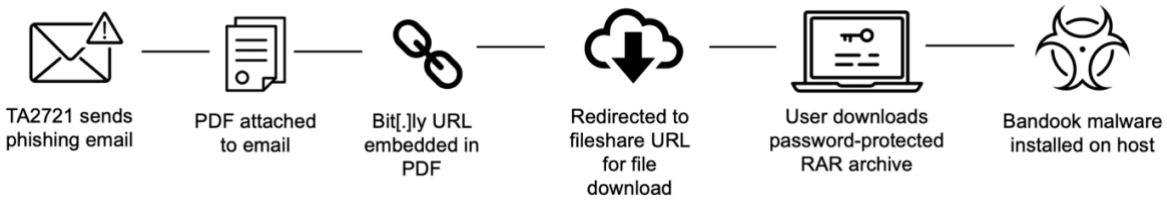


Figure: TA2721 attack chain.

The actor has used the same TTPs since Proofpoint first began tracking it in 2021. While TA2721 has remained consistent overtime, more threat actors including IABs, as described above, began using the PDF to embedded URL technique for malware delivery with increasing frequency over the last year. As other threat actors continue to experiment with TTPs, TA2721 remains consistent, with only occasional changes to the lure theme, PDF template, and password.

Conclusion

The experimentation with and regular pivoting to new payload delivery techniques by tracked threat actors, especially IABs, is vastly different from attack chains observed prior to 2022 and heralds a new normal of threat activity. No longer are the most experienced cybercriminal actors relying on one or a few techniques, but rather are frequently developing and iterating new TTPs. The rapid rate of change for many threat actors suggests they have the time, capability, and understanding of the threat landscape to rapidly develop and execute new techniques.

These changes also impact defenders. The fast pace of TTP adoption forces threat hunters, detection engineers, and malware analysts to quickly identify trends in actor behavior and create new defenses to protect against exploitation.

Proofpoint anticipates threat actors will continue to experiment with new methods of payload delivery, and while many cybercriminals use the same TTPs for weeks or months at a time, it is unlikely there will be a single attack chain or series of techniques that remain consistent or have the same staying power as macro-enabled attachments once had.

LEARN MORE

For more information, visit **proofpoint.com**.