Emails were created as a method to pass messages between users, and now they are used by individuals and organizations all around the globe, by both big and small companies across all industries. But emails also have a dark side — phishing emails that are used by threat actors to gain access to victims' systems.

Traditionally phishing emails are associated with credential harvesting attacks, but that's not the only goal of these attacks. As defined by MITRE ATT&CK framework, adversaries also send phishing emails containing malicious links or attachments to deploy malware (such as backdoors and ransomware) and further exploit the system.

These days, we know better than to open and respond to sketchy emails that make wild promises. Consequently, threat actors adapt their techniques and messages to increase the chances of successfully luring the victims. Through 2021, phishing attacks remained one of their top attack methods — 83% of organizations reported experiencing phishing attacks.

Know the basics about phishing emails? Jump down to learn about automating tasks in your phishing email investigation pipeline.

Since emails are widely used as a means of communication between the company and the outside world, security teams have to deal with large amounts of files, filtering and inspecting them to prevent phishing emails from reaching the end user's mailbox. In addition, threat actors implement different techniques to evade detection.

In this blog, we will cover the techniques used by threat actors to make phishing emails look legitimate and deliver malware to the victim's endpoint. We will show practical tools in which you can identify malicious emails and what are the next steps of the investigation you need to take following the discovery of malicious emails in your organization.

How Email Files Are Used by Threat Actors?

Threat actors use emails to get initial access to the victim, from there they can launch an attack and steal sensitive information, install backdoors, set persistence and cause further damage. Attackers mainly use attachments or links, to deploy and execute their malicious intentions.

Emails can be sent with attachments that can be of any type: documents, executables, images, video, scripts, etc. Usually, threat actors create phishing emails with a message that lures the victim into opening the attached files. Once the file is opened the first stage of the attack is executed.

Another way of delivering threats to the victim's endpoint is by using links in the message, either displayed in plain sight or hidden behind text or images. The end goal of the attackers is to trick users into opening the links, so they can steal sensitive information or deploy the first stage of the attack to the endpoint.

How to Inspect Phishing Email Files

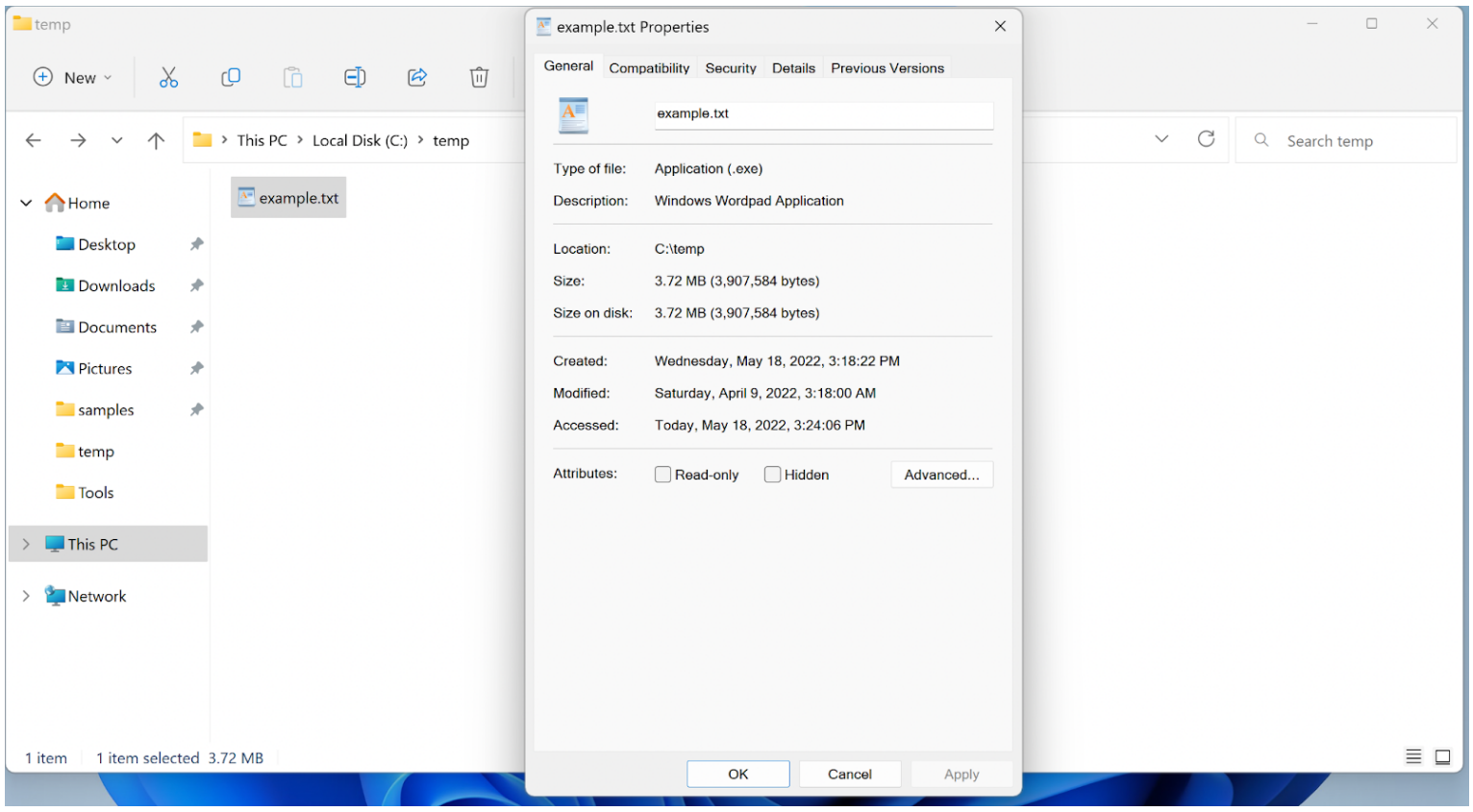
Emails consist of a header and body, inspecting them can provide helpful information for an investigation and indicate whether the emails are malicious. The message of the email can raise suspicion — for a trained eye, the attachments and the sender domain can also be a trigger to investigate the email. As SOC analysts and investigators, it is important to recognize the signs and methods of malicious emails because the threat can be delivered in several ways, and some of them are sneaky.

Inspecting Attachments

As described above, emails support a wide variety of attachments, and these files can contain malicious code (especially executables or scripts). Commonly the email provider will alert upon opening emails that contain executables. But that's not always the case for documents like pdfs and Office files which are often used and shared between organizations and individuals. These non-binary files are also commonly used by threat actors to deliver malicious payloads, and using different techniques, execute the first stage of the attack.

Threat actors use double extensions to masquerade the true file type to trick users into opening files that might seem safe (such as images or text) while it is actually an executable file. By default, Windows hides file extensions, so example.txt.exe would appear as example.txt

The second extension is the real extension of the file and defines which tool will be used to open the file. Another technique used to hide the real file extension is Right-to-Left Override (RLTO) — Windows supports languages that are written from right to left using a Unicode character that causes the text that follows it to be displayed in reverse. Threat actors use this method to blend the real file extension with the file name.



Double extension in Windows when (by default) file name extension is hidden.

Tools for inspecting attachments:

Before inspecting the attached files you will need to extract them (if the email service provider didn't do that for you), there are several free tools you can use:

- OutlookAttachView — NirSoft software to collect all of the attachments in your Outlook mailbox, you can download certain files and investigate them.
- Msg-extractor — Open-source tool to extract attachments from Outlook.
- Eml-extractor — Open-source CLI tool to extract attachments from eml messages.
- UUDWIN — Software that extracts attachments from eml and msg emails.

Most Commonly Used Attachment File Types In Malicious Emails

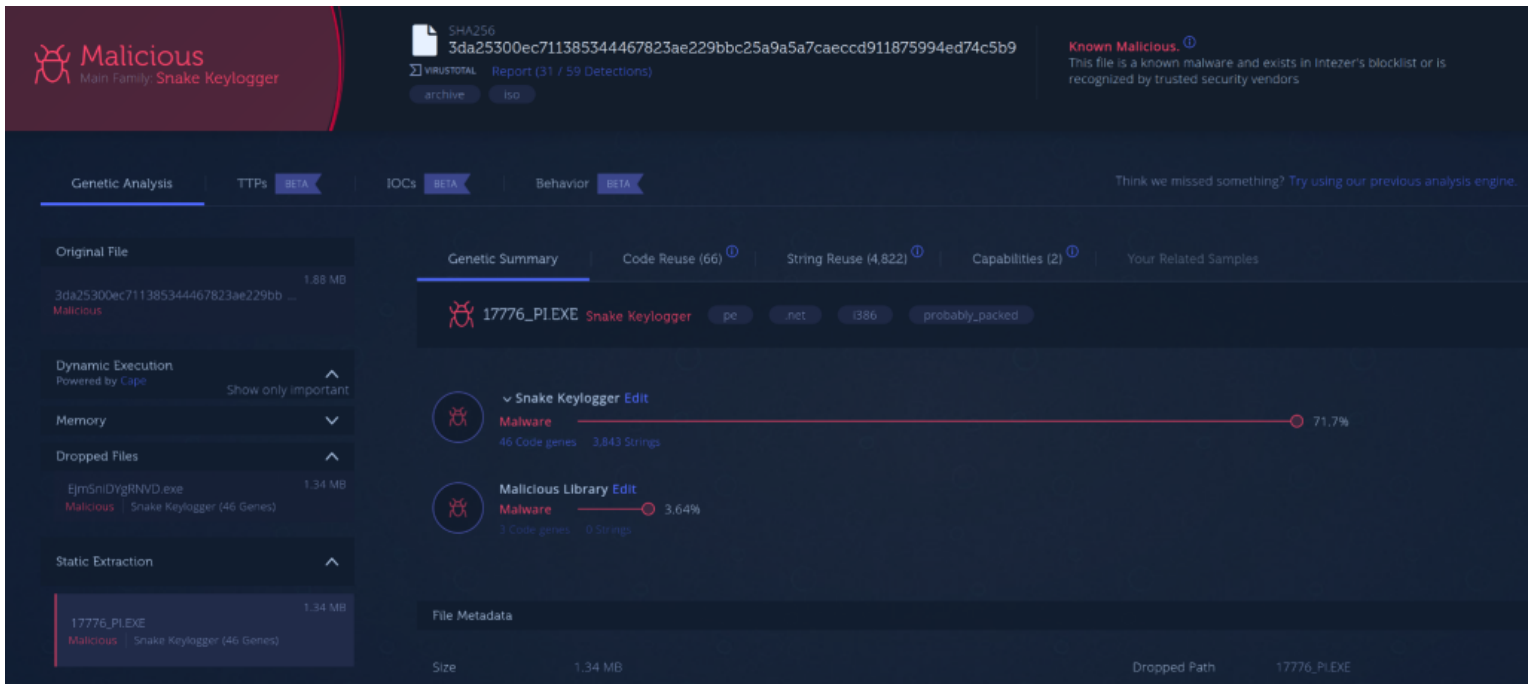
As mentioned, emails can have different types of attachments, so usually threat actors use specific file types that can be relatively easily exploited to deliver threats. Based on SonicWall's 2021 cyber threat report, the following types of attachments are commonly used by both legitimate and malicious emails, therefore emails that contain these types of attachments should be carefully inspected.

- Microsoft Office files — Utilize the macros or embedded OLE objects to deliver threats such as Emotet or Trickbot. To properly analyze these files you need to understand the format and the techniques threat actors implement to hide malware — check out our previous blog about how to analyze malicious office files.
- PDFs — By nature these files can have links, JavaScript code, and any file type can be embedded into a PDF file. All of these features are used by threat actors to hide and deliver threats. On top of that, there are hundreds of PDF readers and many known vulnerabilities that can be exploited by specially crafted PDF files and allow threat actors to execute code on an endpoint. There are tools and methods to inspect PDF files and identify malicious files, check out this post about how to analyze PDF files.
- ZIP and RAR archive files — These are compressed file formats, a malicious executable can be compressed and attached to an email using one of the archive types. But a well-configured email gateway should be able to alert and possibly prevent the email from arriving at its final destination. But that's not always the case for password-protected archive files, which usually are not blocked, as its contents are not able to be inspected due to encryption. Another technique threat actors use to evade detection is sending one archive that contains a decoy file and another archive that contains the actual malware. This technique was used by the group behind NanoCore RAT.
- ISO and IMG disk image — These files are commonly used by attackers to evade detection from email-based Antivirus scanners. The use of ISO files allows the threat actor to bypass the Mark-of-the-Web controls, resulting in execution of the malware without warning to the user. In addition, starting from Windows 8.1, double clicking the file will automatically mount the ISO file and install the software (malware in the case of malicious files). Threat actors use this format to evade detection while fairly easily installing malware.

Inspecting attachments can be time consuming and hard and in some cases you may come to the conclusion that the file is trusted. To reduce the time you spend on analysis of files, you can automatically pipe them into Intezer that uses a proprietary code reuse database that extracts valuable information about the file: whether the file is malicious, and does it share code, behavior, IOC or strings with other samples in the database. This way you will not have to waste time on trusted files or known malicious files.

Investigating Phishing Email Campaigns — Real Life Examples

Our research team discovered a phishing campaign that used spoofed or typosquatted emails to make them look like part of a normal business-to-business (B2B) correspondence, targeting large international companies in the energy, oil & gas, and electronics industries. The attachments were primarily an IMG, ISO or CAB file. We submitted the attachments to Intezer and discovered that they belong to known information stealer malware such as Agent Tesla, Loki, Snake Keylogger, and Formbook.



Genetic analysis of the ISO sample containing Snake Keylogger.

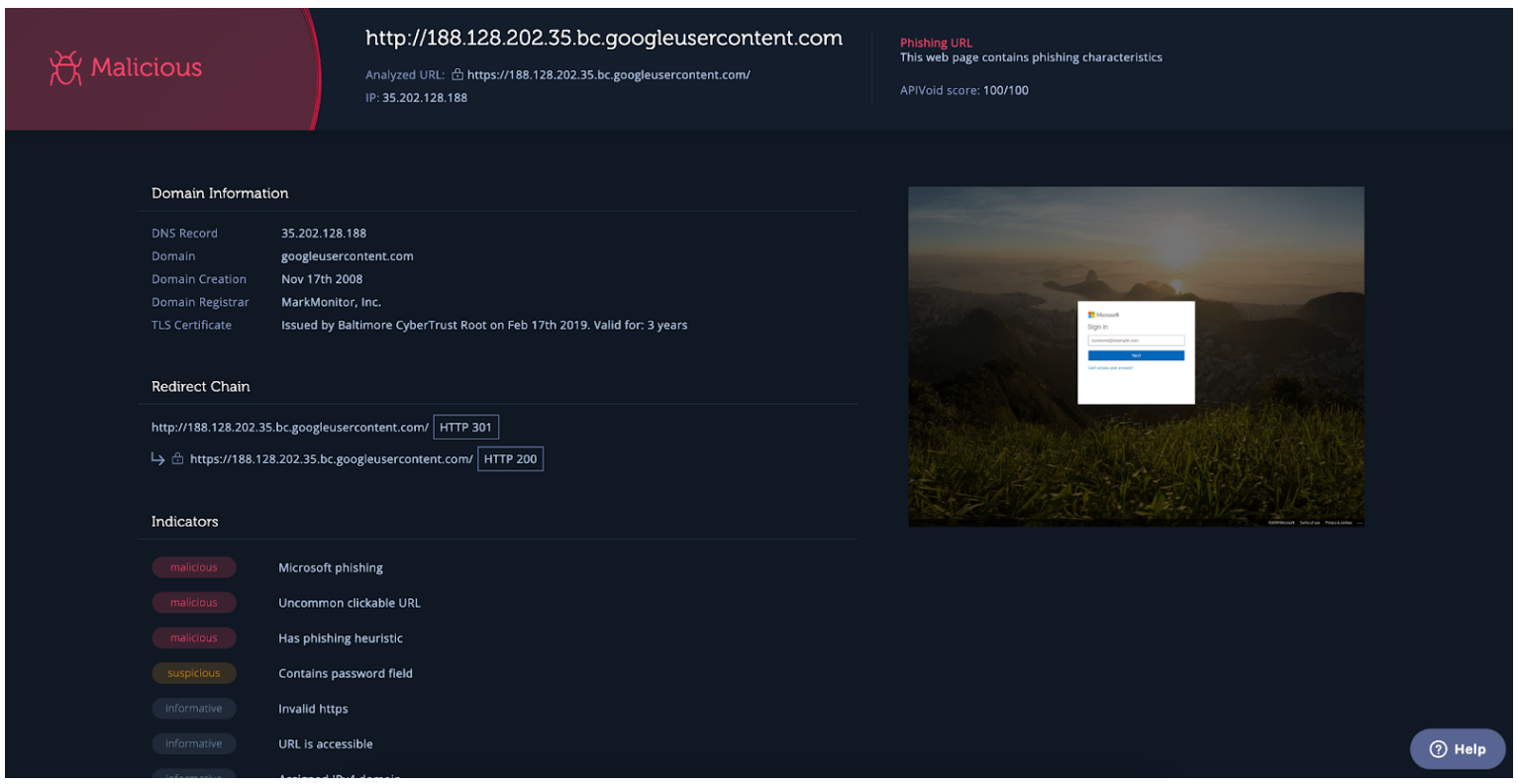
If the investigation of the file concludes that the file is malicious, it means that the email that deliverd it is also malicious and should be further investigated.

Inspecting Links, Manually or Automatically

Most of the malicious emails use links and trick victims into visiting malicious URLs from which malware will be downloaded or victim's sensitive information will be stolen. Links can be in plain sight and appear as legitimate links to known sites such Amazon or Facebook, where in fact the domain is fake or a typosquatter. In other cases, the links are hidden behind text or images such as buttons or coupons, making it harder to notice the malicious URL.

You'll need to collect any URLs from the emails and inspect them using a URL scanner, to know if the URL was seen in previous attacks. If it is a known malicious address then the email is certainly malicious as well. But if the results are not conclusive or you wish to dig deeper, it is worth to further investigate the domain and see if it was linked to any known campaigns or threat actors.

One of the tools you can use for inspecting URLs is Intezer's URL scanner. Intezer can connect to abuse inboxes or email security systems to automatically collect and classify file attachments or URLs, allowing you to accelerate response. When you submit the extracted URL, then the scanner will produce a report that includes a screenshot of the website, the verdict of the URL (is it malicious or not), information about the domain and indicators such as if the address is blacklisted, was it used in phishing campaigns, etc.



URL scan report in Intezer.

Inspecting the Sender Address

Assuming that you have blocked a known spam address and you monitor specific keywords that indicate that an email is malicious, phishing emails still can find their way into your inbox. To identify a malicious email you need to closely inspect and understand who is the original sender of the email and whether it's a legitimate entity or an attacker.

First, examine the email in the inbox, where there are several indicators that can give away malicious emails in this stage:

1. You didn't expect to receive this email — in many cases phishing emails do not relate to previous connection or correspondence. If you haven't had any contact with the sender or their organization, flag the email as suspicious.
2. Misspelled domain or poorly written emails are a strong indication of suspicious emails and you must proceed with caution when handling these emails.
3. Take into consideration that big organizations and service providers will not send emails from free domains such as gmail[.]com or outlook[.]com. Usually these organizations have their own private domain in the format of XXX@<domain_organisation>.com

A common method used by attackers to lure victims into opening emails is by using spoofed email addresses (to make the email look like it came from a known and trusted entity) — there are sites that let you send emails from a given domain or use a certain name that will appear in the sender field. But using the information in the email's header makes it possible to detect this method.

So, if you decide to dig deeper into the email, you need to view the full email body and header. Usually you can get it by opening the additional option menu of the email service provider.

Email File Header

The header contains important fields that can help in identifying malicious emails:

- From: Who sent the message, however this field can be modified as mentioned above. The anomalies we mentioned about the sender apply here as well.
- To: Recipient's name and email address. This field can help in determining the real target of an email, in case we determine that the email is malicious the recipient can determine if the attack targets specific victims.
- Received: The most reliable field that provides information about the origin of the email. An email that is being sent from one user to another passes through one or more servers until it reaches its destination, similar to post offices. Each agent adds a layer of information that contains a timestamp and information about the server from which the email was received from, that's the reason that some emails contain several Received fields. Therefore, you should inspect the header from the bottom to the top.
- Return-Path: Address to return the mail.
- DKIM signature: Checks the DKIM DNS record of the sender to confirm the authenticity of the sender using public key cryptography.
- SPF: Defines which mail servers are authorized to send emails for a certain domain based on DNS record, the goal is to prevent attackers from sending emails using your domain from any server.
    - Received-SPF field — email sent from permitted servers will show up as "Pass" but it can still be a non legitimate email if the account has been compromised. If the value of the field is either "Fail" or "Softfail", it indicates that the email may be spoofed or the domains didn't update their SPF records. Here is an example of an email that pretends to be sent by Haesung Tech, but the address is spoofed and the doesn't pass the SPF check:

```
Received-SPF: none (211.104.2.85: domain at haesungtech.com does not designate permitted sender hosts)
Authentication-Results: smf.febc.net;
  spf=none (211.104.2.85: domain at haesungtech.com does not designate permitted sender hosts) smtp.mailfrom=haesungtech@haesungtech.com
Received: from unknown (HELO server.ecomotorhk.com) (162.144.56.225)
```

Sender Policy Framework (SPF) record of a spoofed address.

Domain-based Message Authentication, Reporting and Conformance (DMARC) is another email authentication protocol that uses the information provided by either DKIM or SPF (or both). DMARC is implemented to protect the domain from unauthorized use in phishing and spoofing attacks. And DMARC enforces predefined policy to handle unwanted emails. DMARC, DKIM and SPF are used to prevent phishing and unauthorized use of domains. When you inspect emails make sure to validate the values in these fields.

Other fields in the header that you should know about:

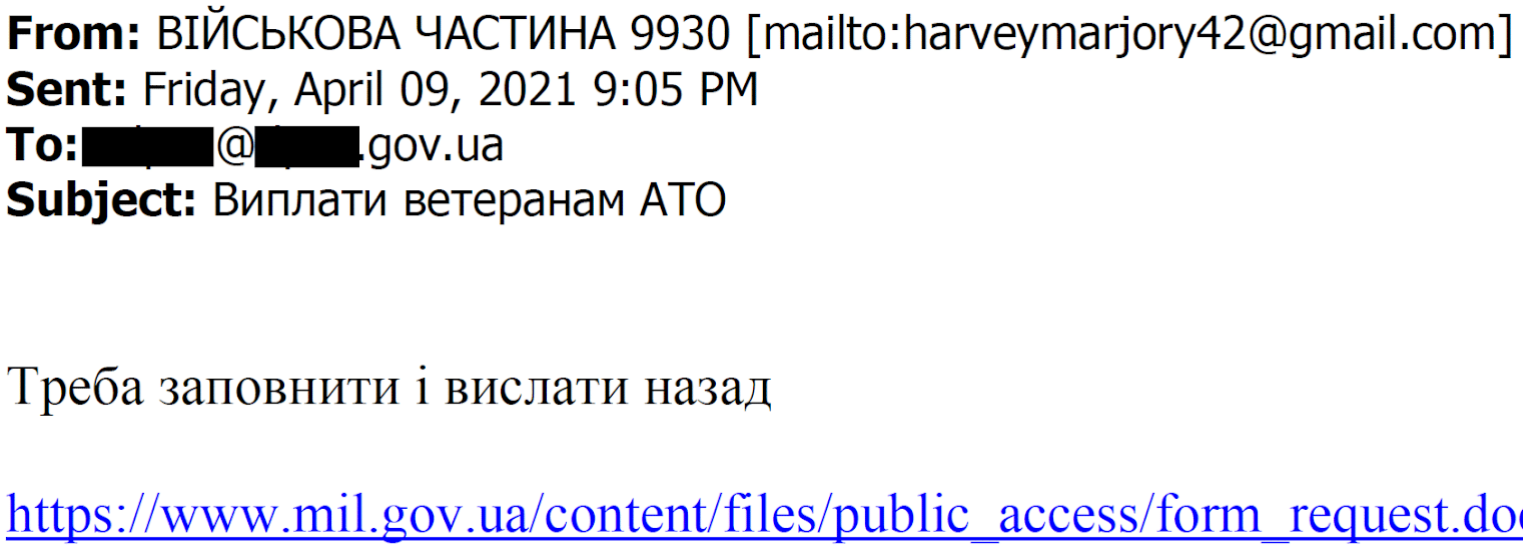
- MIME-version — Multipurpose Internet Mail Extensions (MIME) extends the standard email format, it provides support for non-ASCII character sets, audio, video and applications. Messages that use MIME must contain the version field.
- Message-ID — unique identifier used in emails.

- X-header — custom email headers that can be added to the other standard headers. Email providers add specific headers for authentication, information about spam, etc. Microsoft Outlook uses X-MS-Exchange header and Google uses X-Google-DKIM. For example:
    - X-Originating-IP- the ip address of the sender
    - X-Spam-Status & X-Spam-Level- Spam record set by the mail service.

Real Life Examples

Intezer's research team discovered a phishing campaign that targeted government entities in Georgia. The attack flow starts with a phishing email containing a malicious shortened URL, as can be seen in the screenshot below. The URL redirects to a Command and control (C2) where a ZIP file or malicious document is hosted. The ZIP file contains a malicious file and in some emails also a harmless PDF file. The malicious attachment varies between RTF, DOC, PDF, JS, LNK or EXE. The main goal of the attachment is to drop the packed payloads from the C2. The packed executable loads an AutoIt payload into memory, once executed the malware steals files with predefined extensions.

The campaign demonstrates the challenge of inspecting emails, the variety of file types that are compressed into the ZIP file, can make the analysis more challenging and time consuming — you will need the skills and the tools to analyze each file type. There is a solution — automate your email pipeline. Automatically extract the attachments and submit them to platforms such as Intezer, this way instead of spending time on files that are trusted or known threats you can focus on other aspects of the suspicious email.


From: ВІЙСЬКОВА ЧАСТИНА 9930 [mailto:harveymarjory42@gmail.com]
Sent: Friday, April 09, 2021 9:05 PM
To: [redacted]@[redacted].gov.ua
Subject: Виплати ветеранам АТО

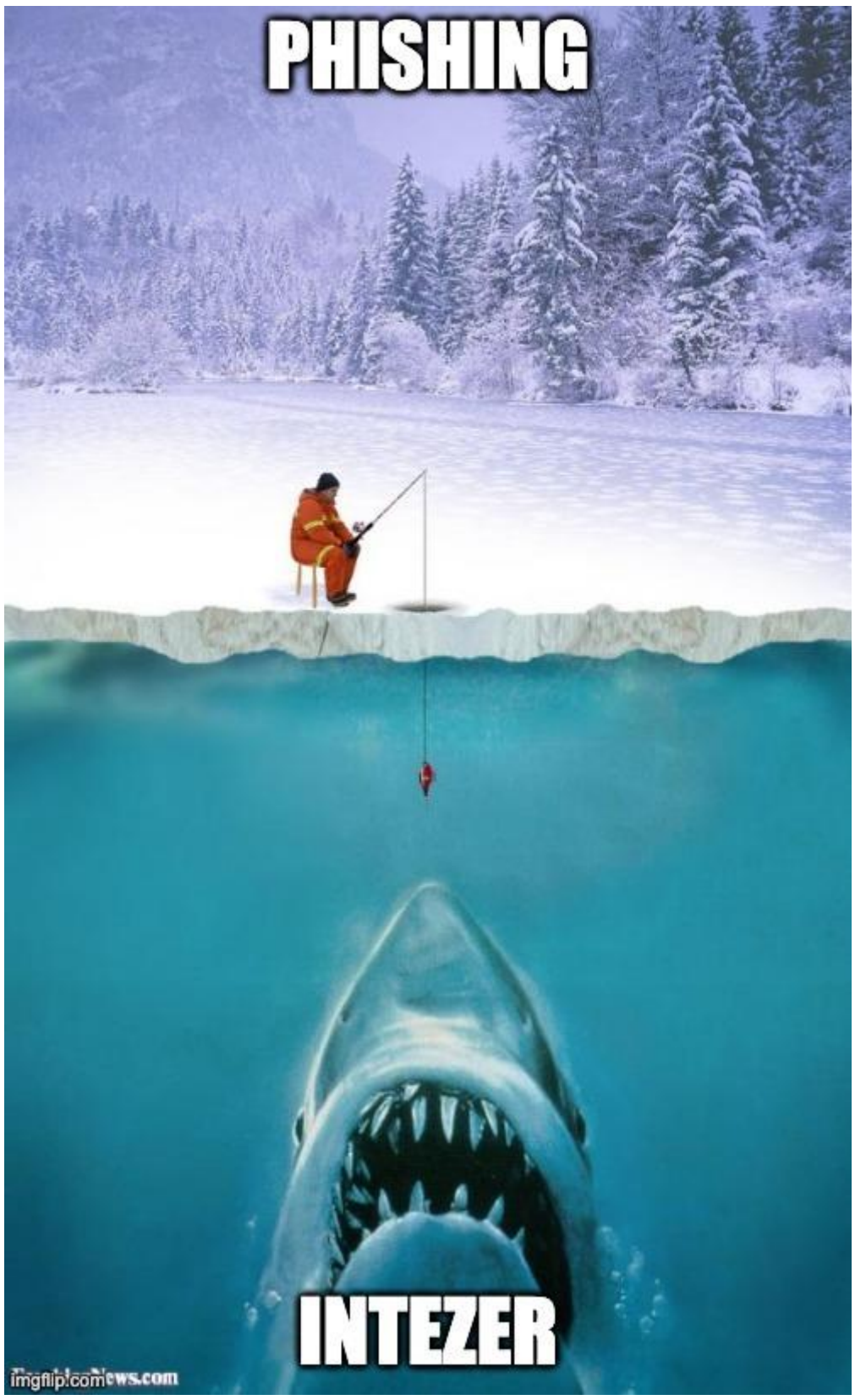
Треба заповнити і вислати назад

https://www.mil.gov.ua/content/files/public_access/form_request.doc

Phishing email targeting government entities in Georgia.

Phishing email sent to the Ukrainian government. Translation from Ukrainian — Subject: "Payments to ATO Veterans." Content: "It must be filled in and sent back."

Another campaign that was recently discovered by our research team is a new IcedID campaign that was delivered using a phishing email that uses conversation hijacking —threat actors use previously stolen email messages and use them in future attacks. This technique makes the emails look more legitimate and convincing. This campaign takes the hijacking a step further; the threat actors are now using the email address of the victim that they stole the original email from to make the phishing email even more convincing.



Conclusion

Inspecting email files can be hard because emails are frequently used, meaning there are lots of files to cover. Also because emails can contain URLs to malicious sites or different types of attachments, all of which require different sorts of skills and methods to thoroughly inspect all of the artifacts.

To make this task easier and less demanding you should consider automating your email pipeline. The goal is to put time and effort only into truly malicious files. By extracting all of the attachments and piping them into Intezer you will get a comprehensive report about each file, which will allow you to proceed to the next step. If the file is malicious, start an incident response process. Otherwise, continue to the next task in your queue until the next email.

Want to learn more about automating your email pipeline? Let's book a time to talk.


Nicole Fishbein

Nicole is a malware analyst and reverse engineer. Prior to Intezer she was an embedded researcher in the Israel Defense Forces (IDF) Intelligence Corps.

attachments Incident Response phishing emails phishing investigation pipeline