

Operation ClickBait – A Personal Lab to Analyze Email-Based Attacks

Introduction

Email is still the front line of cyber warfare—from phishing attempts to malware-laced attachments, inboxes are a constant target for attackers. To truly understand how these threats work and how they can be detected, I created **Operation ClickBait**—a personal home lab designed to **analyze email-based attacks in a safe and controlled environment**.

The goal was simple: **collect, examine, and dissect** phishing emails and malicious payloads to better understand how attackers craft convincing lures and deliver harmful content. This lab has allowed me to experiment with real-world phishing campaigns, analyze suspicious attachments, decode malicious URLs, and practice safe malware handling techniques.

By simulating the investigative process of a security analyst, **Operation ClickBait** has not only sharpened my technical skills but also helped me build a threat-aware mindset essential in modern cybersecurity.

⌚ What is Malware?

Malware, short for *malicious software*, refers to any software intentionally designed to cause damage to computers, servers, networks, or users. It includes viruses, worms, trojans, ransomware, spyware, and more. Once installed, malware can steal sensitive information, corrupt files, disrupt operations, or provide attackers with unauthorized access to a system.

In the context of email-based attacks, malware is often delivered as **attachments** (e.g., .exe, .doc, .zip) or through **links** that lead to infected websites or file downloads.

💡 What is Phishing Mail?

Phishing mail is a type of **social engineering attack** where attackers impersonate legitimate entities (like banks, services, or coworkers) to trick recipients into revealing sensitive information such as passwords, credit card numbers, or login credentials.

Phishing emails often include **urgent language**, **spoofed email addresses**, and **fake links** that lead to convincing but fraudulent websites. Some also carry **malicious attachments** to deliver malware.

In short, phishing emails aim to exploit human trust and curiosity—making them one of the most effective and dangerous forms of cyberattack today.

Requirements

Hardware

- Laptop / Computer
- 8 or 8+ GB of Ram
- 100 GB Storage

Software

- Virtual Box
- Windows 10 install in it
- Sandbox Environment
- One Malware .exe File
- Little bit of Knowledge about Technology

What I have done!

- I downloaded a malware sample to analyze it, and then attempted to send it to another email address using phishing content. This analysis will help me determine whether the email is malicious or genuine, enabling me to better protect people and companies from being hacked.

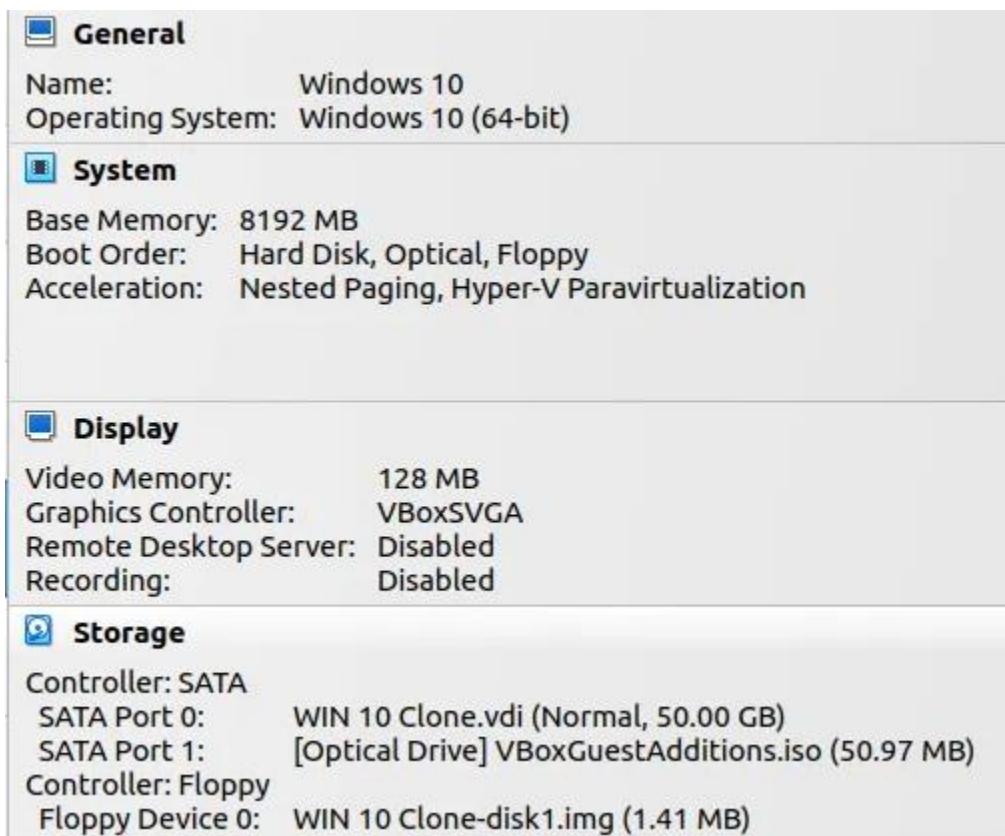
What Next

- Now I will show you a live demo of what you can do when you receive an email.
- I will demonstrate how to analyze the mail and check the mail's IP address.

- Additionally, I'll show you how to check for documentation and any attached files.
- Let's get started.

Practical Demo

- First Download the Virtual Box
- Install the Windows 10 OS in it
- Give it a Decent amount of specification
- Mine is Here



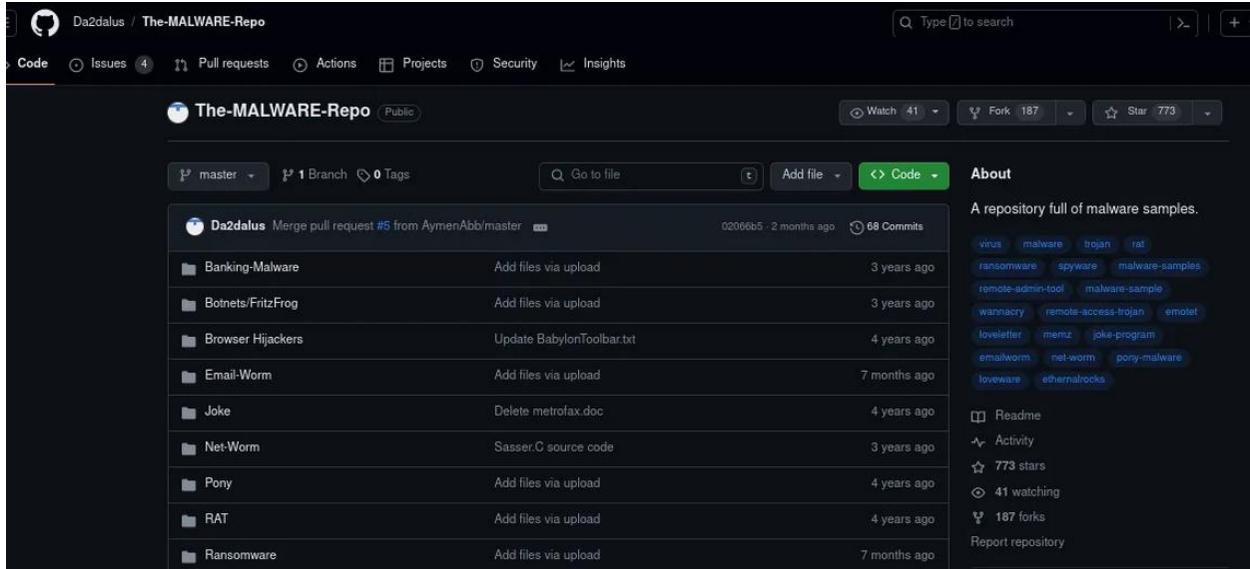
- You can give it by our need
- I Suggest you for giving 4Gb+ Ram and 50Gb Storage for better performance

Creating a Sandbox Environment

- I have made a article on how you can create a sandbox environment
- Check it out
- Make sure to take a snapshot in virtual box so if any think happen so you can restore the windows and you will save more time.

Downloading Malware

- If you want to download a malware so you can check of the git hub repository
- **I have downloaded malware from here**



The-MALWARE-Repo

Code Issues 4 Pull requests Actions Projects Security Insights

The-MALWARE-Repo Public

Watch 41 Fork 187 Star 773

master 1 Branch 0 Tags

Go to file Add file Code

Da2dalus Merge pull request #5 from AymenAbb/master 02066b5 · 2 months ago 68 Commits

File	Action	Time Ago
Banking-Malware	Add files via upload	3 years ago
Botnets/FritzFrog	Add files via upload	3 years ago
Browser Hijackers	Update BabylonToolbar.txt	4 years ago
Email-Worm	Add files via upload	7 months ago
Joke	Delete metrofax.doc	4 years ago
Net-Worm	Sasser.C source code	3 years ago
Pony	Add files via upload	4 years ago
RAT	Add files via upload	4 years ago
Ransomware	Add files via upload	7 months ago

About

A repository full of malware samples.

virus malware trojan rat
ransomware spyware malware-samples
remote-admin-tool malware-sample
wannacry remote-access-trojan emotet
loveletter memz joke-program
emailworm net-worm pony-malware
lojeware ethernalrocks

Readme Activity 773 stars 41 watching 187 forks Report repository

<https://github.com/Da2dalus/The-MALWARE-Repo>

Send Email

- If we want to send email so we can send it from our mail box
- But the malicious mail is not send by mail it is send by some different kind of mailbox which contain some additional option for sending mail
- We can hide our email address from it and also hide sender information
- We can add Phishing link to it.

Sending Malicious Email To Next Person

- Here I have send a malicious email containing subject line
- Subject as **Hey You Have Win a Lucky Draw**
- **Given a Task to Chatgpt to write a content for Email on the topic**



You

Write a email to unknown user for topic = a small lucky draw app



ChatGPT

Subject: Introduction to Our Small Lucky Draw App

Dear [Recipient],

I hope this email finds you well. My name is [Your Name] and I am reaching out to introduce you to a small lucky draw app that we have recently developed.

Our app is designed to bring excitement and fun to any gathering or event by facilitating quick and easy lucky draws. Whether you're organizing a party, a corporate event, or a simple get-together with friends, our app can add an element of surprise and enjoyment.

Key features of our app include:



1. Simple Interface: Our app boasts a user-friendly interface that makes it easy for anyone to use,

Copied email format from chatgpt and paste it on the email sender box.

Hurry You Have Win A Lucky Draw

mohitdamke1@gmail.com

Hurry You Have Win A Lucky Draw

Subject: Introduction to Our Small Lucky Draw App

Dear Sir,

I hope this email finds you well. My name is [Your Name] and I am reaching out to introduce you to a small lucky draw app that we have recently developed.

Our app is designed to bring excitement and fun to any gathering or event by facilitating quick and

Send



Hurry You Have Win A Lucky Draw

mohitdamke1@gmail.com

Hurry You Have Win A Lucky Draw

to us. We would be happy to provide you with further information or even arrange a demo.

Thank you for considering our app, and we look forward to the possibility of helping you make your next event even more special.

Best regards,

[Lucky_Draw_Game.exe.7z \(96K\)](#)

x

Send

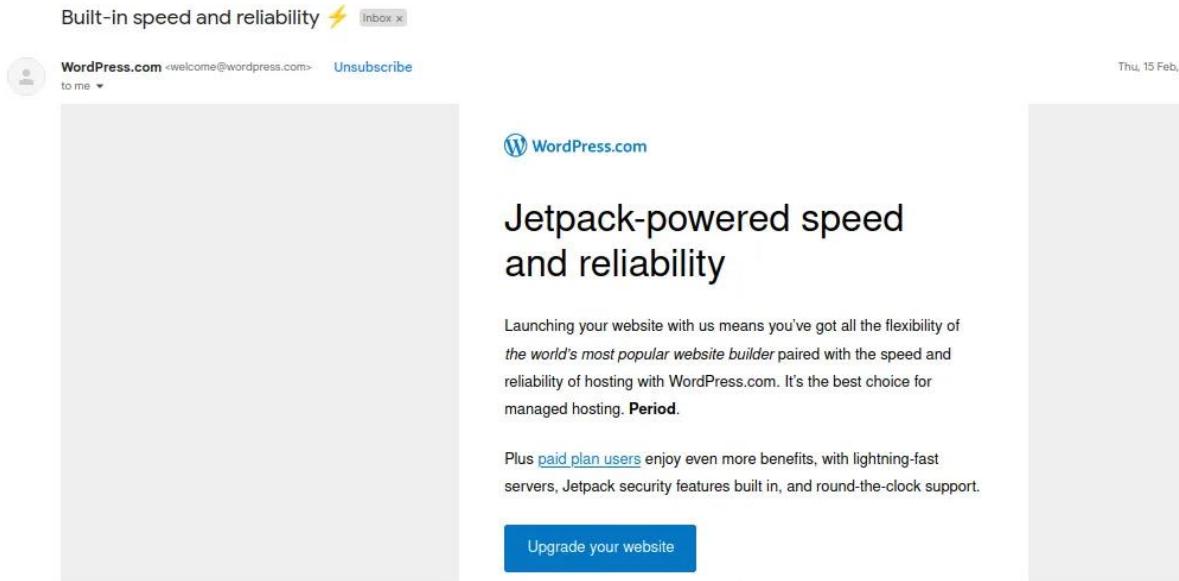


Attached Malware File to it by changing its name to **Lucky_Draw_Game**

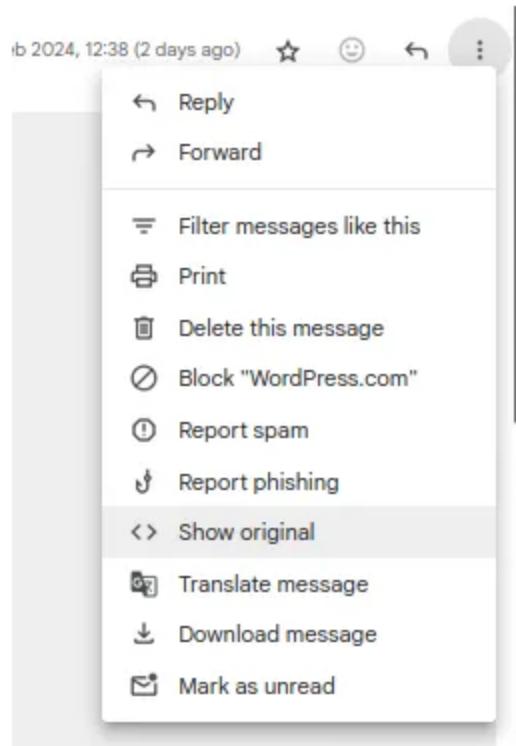
- So user will think that it is a game app but it is a malware
- **NOTE : The Mail is not been sent properly scanner has scan malware file and it disable to download the file and so we cannot download the file but we can test it manually**

• Email Analysis

- We can check for the email by just checking for its header
- Lets take an example for WordPress email



- First step is to check for the content read it carefully and notice it there are some mistakes
- Note that it contain some attachment with it if yes so **don't open it**.
- Check for the Header by clicking on 3 dots



Click on Show Original

Original message

Message ID	<ccpBfSHx1YxplugLVOlCG2iMlmSvf73McA0PMfpeDrk@wordpress.com>
Created on:	15 February 2024 at 12:38 (Delivered after 0 seconds)
From:	"WordPress.com" <welcome@wordpress.com>
To:	mohitdamke1@gmail.com
Subject:	Built-in speed and reliability ⚡
SPF:	PASS with IP 192.0.80.222 Learn more
DKIM:	'PASS' with domain wordpress.com Learn more
DMARC:	'PASS' Learn more

[Download original](#)

[Copy to clipboard](#)

• Here is a bunch of information about email

Delivered-To: mohitdamkel@gmail.com
 Received: by 2002:ab3:7458:0:b0:252:4b1d:40a8 with SMTP id g24csp421891lti;
 Wed, 14 Feb 2024 23:08:03 -0800 (PST)
 X-Google-Smtp-Source: AGHT+IGfS/nup0Uot3ak7XBB+885xDLRvTo1zJ0yBx8DuL57t0Wd3pyAR5ZTS0nCp13H3Efa3zs6
 X-Received: by 2002:a05:6808:1184:b0:3c0:3309:2057 with SMTP id j4-20020a056808118400b003c033092057mr1579956oil.
 26.1707980883498;
 Wed, 14 Feb 2024 23:08:03 -0800 (PST)
 ARC-Seal: i=1; a=rsa-sha256; t=1707980883; cv=none;
 d=google.com; s=arc-20160816;
 b=xQnH1a/dRXPI4aB3z+Eh0hNC2t3060ZfysAWPeZuha5LBVR7tmw7RAZj0xmqIj4a0
 muc2W0VHSWu0sKeHKnupoYpms0K9zhYCzKRo26Ymp/Pa0tWgZSxHBFM+3aH8gVCu3cF
 /4uesAoY/ZxZLQNUpBe6smxMg6u0XdtetUh+MOVUHLURD15P0wIEdfYKwfWZmobEXI8
 +yIGL9Kuym5ltk4gjL2EhgotTKeoBkUPQPiXsM+g01/UXH3Cjefs9BbJqgB/iLeXbD94
 AcsnTYfrV65SblFakCYLaRx/ShYg1xTECNxFzb95fxig0T8Bk2ULbsrPtdqu3uB9LSJB
 hp5g==
 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
 h=content-transfer-encoding:mime-version:precedence:list-archive
 :list-subscribe:list-unsubscribe-post:list-unsubscribe:list-help
 :message-id:subject:from:to:date:dkim-signature;
 bh=T0svl0Rv8Ku7/06hGBVxIUGVkdRp38P8A0R2W4WCc=;
 fh=V6yAsV32y/GzlsxL5xk4Atddn0Q7z6YC7KmI+huPh6s=;
 b=XwDye5PPthfZCxJ318Kn7u/9vML5dEd4UYkaWpr3Lw6DRNRI0Vxe4qwUPdE3DIJN5
 oC7rmv45mXifiKz0YWE9mlLz1Ma3IxwA/dUkDxH6P/oy00j8GPBL0wmg8y0cQFkcZ3U
 dcdQDK4rI2nKMDQSV4mFLyLPmuHM2pMMjR2akQGVcd5YswWgjM8/9HZAxumGsiiaJE
 9hBsTGR2UWK6xhggLQFCboMBKxmxe845hoAKD6/D4/VM/e4RdnXsRyp2X8gBCN0iXE
 0R50Lz9YmJuGzxpCg0aI2mEg0KdE0AABj7a0y6x73CoFno0qnN1v6v0I9w9EbTqa7M
 6XLA=;
 dara=google.com
 ARC-Authentication-Results: i=1; mx.google.com;
 dkim=pass header.i=@wordpress.com header.s=automatic1 header.b="NoiC2N/X";
 spf=pass (google.com: domain of mohitdamkel@gmail.com@b.wordpress.com designates 192.0.80.222 as permitted
 sender) smtp.mailfrom="mohitdamkel@gmail.com@b.wordpress.com";
 dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=wordpress.com
 Return-Path: <mohitdamkel@gmail.com@b.wordpress.com>
 Received: from smtp2-1.dfw.wordpress.com (smtp2-1.dfw.wordpress.com. [192.0.80.222])
 by mx.google.com with ESMTPS id m3-20020a0568080f0300b003c0456cd04asi1316063oiw.0.2024.02.14.23.08.03
 for <mohitdamkel@gmail.com>
 (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
 Wed, 14 Feb 2024 23:08:03 -0800 (PST)
 Received-SPF: pass (google.com: domain of mohitdamkel@gmail.com@b.wordpress.com designates 192.0.80.222 as permitted
 sender) client-ip=192.0.80.222;
 Authentication-Results: mx.google.com;
 dkim=pass header.i=@wordpress.com header.s=automatic1 header.b="NoiC2N/X";
 spf=pass (google.com: domain of mohitdamkel@gmail.com@b.wordpress.com designates 192.0.80.222 as permitted
 sender) smtp.mailfrom="mohitdamkel@gmail.com@b.wordpress.com";
 dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=wordpress.com
 DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=wordpress.com; s=automatic1; t=1707980883;
 bh=lZ45eLtc4zr5FDE17TawP4h9PCT9rZp06NHgWp5q2E=; h=Date:To:From:Subject:List-Help:List-Unsubscribe:
 List-Subscribe:Post:List-Subscribe:List-Archive:From; b=NoiC2N/X/5q/ktx4nx9nsxjhRPBX2H0mje+3qxlj/
 9Y3A1vLS3I2EaNb8IjhMIhWj
 h7bYZx9CeJCT0e0NgBvWP8qcCDy4RcnBtga10kwVXlJGSUqW8J0w/UDuNHu2HXUZY
 03Aw1y0544e6jbTqHt9czvBjrh7CkDzNDE06ke/izB2M2FTmVo+rFfxgZpAd5j2
 wEeRkM7BC4UBvFb7ia3pv1ren3R2Wr9Q8muMg21bWe65D7ukxzdVlt3Z+e/ggBgs7d
 ckH5usqasBv1M5gXka3m6AljA7TuiNUZMyCs5ztXNFqDGwm7mQvl0AmrunbZQtfk

IP

- It shows his IP address

SPF: PASS with IP 192.0.80.222

Here is information we get from the ip

IP Information for 192.0.80.222

— Quick Stats

IP Location	 United States Marina Del Rey Early Registration Addresses
ASN	 AS2635 AUTOMATTIC, US (registered Oct 01, 2012)
Resolve Host	smtp2-1.dfw.wordpress.com
Whois Server	whois.arin.net
IP Address	192.0.80.222

NetRange:	192.0.64.0 - 192.0.127.255
CIDR:	192.0.64.0/18
NetName:	AUTOMATTIC
NetHandle:	NET-192-0-64-0-1
Parent:	NET192 (NET-192-0-0-0-0)
NetType:	Direct Allocation
OriginAS:	AS2635
Organization:	Automattic, Inc (AUTOM-93)
RegDate:	2012-11-20
Updated:	2021-12-14
Ref:	https://rdap.arin.net/registry/ip/192.0.64.0

- We get to know that the ip is genuine and comes from original source

Domain

- Lets Check for the domain name register

DKIM: 'PASS' with domain wordpress.com

- Here is the domain of wordpress
- Lets check for more information

Whois Record for WordPress.com

— Domain Profile

Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) +1.2086851750
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	8,751 days old Created on 2000-03-03 Expires on 2033-03-03 Updated on 2023-08-28
Name Servers	NS1.WORDPRESS.COM (has 1,576,071 domains) NS2.WORDPRESS.COM (has 1,576,071 domains) NS3.WORDPRESS.COM (has 1,576,071 domains) NS4.WORDPRESS.COM (has 1,576,071 domains)

WHOIS RECORD
WHOIS RECORD FOR WORDPRESS.COM
Created on 2000-03-03

•

 **DomainTools** PROFILE ▾ CONNECT ▾ MONITOR ▾ SUPPORT Whois Lookup

Registrant City:
Registrant State/Province: CA
Registrant Postal Code:
Registrant Country: US
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: REDACTED FOR PRIVACY (DT)
Registry Admin ID:
Admin Name:
Admin Organization: Automattic, Inc.
Admin Street:
Admin City:
Admin State/Province: CA
Admin Postal Code:
Admin Country: US
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: REDACTED FOR PRIVACY (DT)
Registry Tech ID:
Tech Name:
Tech Organization: Automattic, Inc.
Tech Street:
Tech City:
Tech State/Province: CA
Tech Postal Code:
Tech Country: US
Tech Phone:
Tech Phone Ext:

They have hide much of the information so we are not able to get more information

- So here we have done the basic level of email analysis

IP & Domain Analysis Websites

- Here are some of the websites where you can do analysis
- **WHOIS Lookup:**



- WHOIS lookup services like whois.net or whois.domain tools.com allow you to find detailed information about domain names, including registrant details, registration and expiration dates, and name server information.

MXToolbox:

MXToolbox offers a variety of tools for analyzing domains and IP addresses, including DNS lookup, blacklist check, and email header analysis.

IPVoid:



The screenshot shows the IPVoid homepage. At the top is a dark blue header with the IPVOID logo in white. Below the header is a navigation bar with dropdown menus for IP, DNS, TEXT, URL, ENC/DEC, RANDOM, EXTRACT, and MORE, along with social media links for Twitter and Facebook. The main content area has a white background. It features a title 'IP Address Tools Online' and a subtext 'We offer a vast range of IP address tools to discover details about IP addresses.' Below this is a search bar with the placeholder 'Search Tools..'. At the bottom of the main content area is a green button labeled 'WINDOWS SOFTWARE' and 'File Lines Manipulator - Manipulate Text Lines of Files→'.

IPVoid provides tools for IP and domain analysis, including blacklist check, IP geolocation, and reverse DNS lookup.

Shodan:



The screenshot shows the Shodan homepage. The top navigation bar is dark with the SHODAN logo, 'Explore', 'Pricing', and a search bar. To the right is a red search button with a magnifying glass icon. The main area has a black background. It features a title 'Search Engine for the Internet of Everything' and a subtext 'Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.' Below this is a green 'SIGN UP NOW' button. To the right is a world map with colored dots representing connected devices.

Shodan is a search engine that lets you find specific types of computers (routers, servers, etc.) connected to the internet using a variety of filters. It's particularly useful for analyzing devices connected to the internet by their IP addresses.

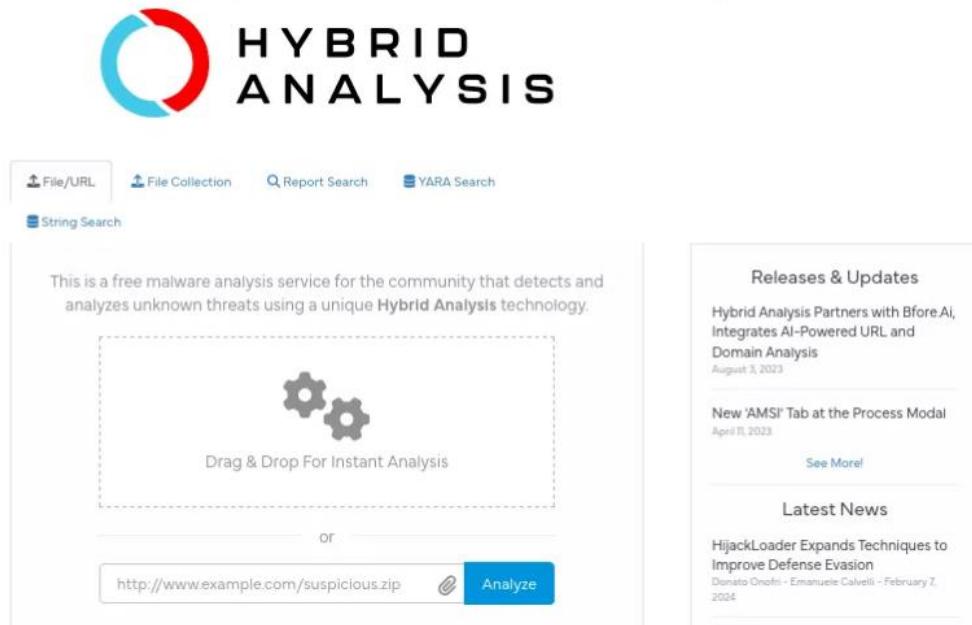
Malware Analysis

VirusTotal:



VirusTotal is a free online service that analyzes files and URLs for viruses, worms, trojans, and other kinds of malicious content. It aggregates multiple antivirus engines and scan results from various sources to provide comprehensive insights into the potential threats of a file or URL.

Hybrid Analysis:



The screenshot shows the Hybrid Analysis website. At the top is a logo consisting of a red and blue circle with the text "HYBRID ANALYSIS" in bold capital letters. Below the logo are several search and analysis options: "File/URL", "File Collection", "Report Search", "YARA Search", and "String Search". The main content area features a large text block: "This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology." Below this is a "Drag & Drop For Instant Analysis" section with two gears and a "Drag & Drop" placeholder. Below that is a "Or" section with a "http://www.example.com/suspicious.zip" input field and a "Analyze" button. To the right, there are two columns: "Releases & Updates" and "Latest News". The "Releases & Updates" column has a section for "Hybrid Analysis Partners with Bfore AI, Integrates AI-Powered URL and Domain Analysis" dated "August 3, 2023", and a "See More!" link. The "Latest News" column has a section for "HijackLoader Expands Techniques to Improve Defense Evasion" dated "Donato Onofri - Emanuele Calvelli - February 7, 2024".

- Any.Run is an interactive malware analysis platform that allows users to execute and observe the behavior of malware samples in real-time. It provides a sandboxed environment for analysis.
- Hybrid Analysis is a dynamic malware analysis service that allows users to submit files and URLs for analysis. It provides detailed reports on the behavior of malware samples in a controlled environment, including information on network activity, file modifications, and system impact.

Any.Run:



The screenshot shows the Any.Run website. At the top is a navigation bar with links: "WHY US", "SERVICE", "TRACKER", "REPORTS", "PRODUCTS", "INTEGRATIONS", "PRICING", "BLOG", "CONTACTS", "MEDIA KIT", and "TRIAL". To the right of the navigation is a "Meet a brand new ANY.RUN's Threat Intelligence service" section with a "See how it works" button. The main content area features a large "ANY RUN" logo with "INTERACTIVE MALWARE HUNTING SERVICE" below it. To the right is a section titled "MALWARE HUNTING WITH LIVE ACCESS TO THE HEART OF AN INCIDENT" with a "REGISTER FOR FREE" button. The background has a dark blue gradient with vertical light blue lines.

- Any.Run is an interactive malware analysis platform that allows users to execute and observe the behavior of malware samples in real-time. It provides a sandboxed environment for analysis.

environment where users can interact with malware and monitor its activities, including network connections, file operations, and registry changes.

Joe Sandbox:

Joe Sandbox is an automated malware analysis platform that provides in-depth reports on the behavior and characteristics of malware samples. It uses advanced techniques such as code emulation, dynamic instrumentation, and memory analysis to uncover the capabilities and intentions of malicious code.

Practical Malware Analysis

- Lets Take one Malware and Analysis it with the help of **VirusTotal**
- I have one malware and lets check it
- Here is Malware



Annabelle.exe

Lets Check

- Lets Check it by uploading it on **VirusTotal**

The screenshot shows the VirusTotal homepage and a detailed analysis page for a file. The homepage features a large 'VIRUSTOTAL' logo with a blue square icon, a search bar, and a 'Choose file' button. The analysis page for 'Annabelle.exe' shows a 'Community Score' of 59/72, with 59 security vendors and 3 sandboxes flagged as malicious. The file is a 15.94 MB EXE file. The 'DETECTION' tab is selected, showing various threat labels and categories. The 'Community' tab shows 24+ related items. A 'Join the VT Community' button is present. The bottom section displays security vendor analysis for AhnLab-V3, ALYac, and Arcabit, along with a 'Do you want to automate checks?' button.

So here we get result

- 59 out of 72 security vendors and 3 sandboxes flagged this file as malicious
- That's How you can analyze any file

Conclusion

Operation ClickBait has been more than just a side project—it's been a deep dive into the world of email-based threats. From decoding phishing tactics to analyzing embedded malware, this lab gave me firsthand experience in tracking and understanding how attackers operate.

It also taught me the value of a **structured, isolated lab environment** where I could safely test samples, extract indicators of compromise, and build practical defensive strategies. Beyond technical skills, it helped reinforce a strong analytical approach to identifying and mitigating threats.

In a time when email remains one of the most exploited vectors for cyberattacks, **Operation ClickBait** has given me the tools, confidence, and curiosity to keep exploring, learning, and defending.

FiazHackshield