

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.

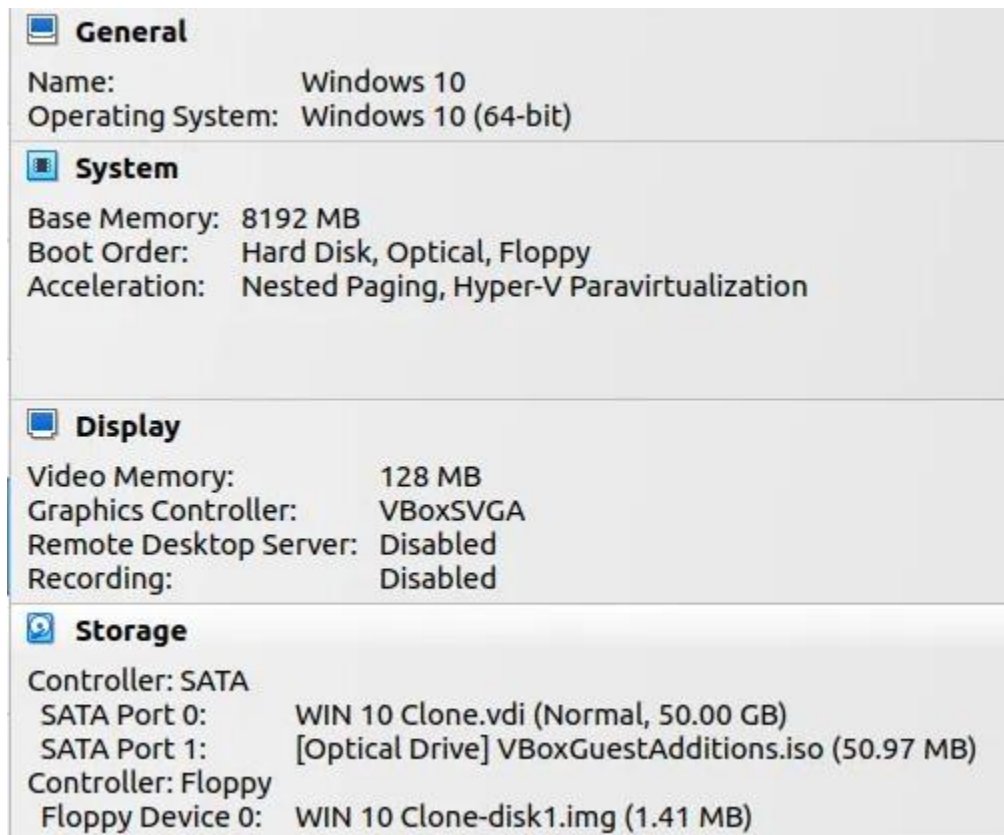
What Next

- 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



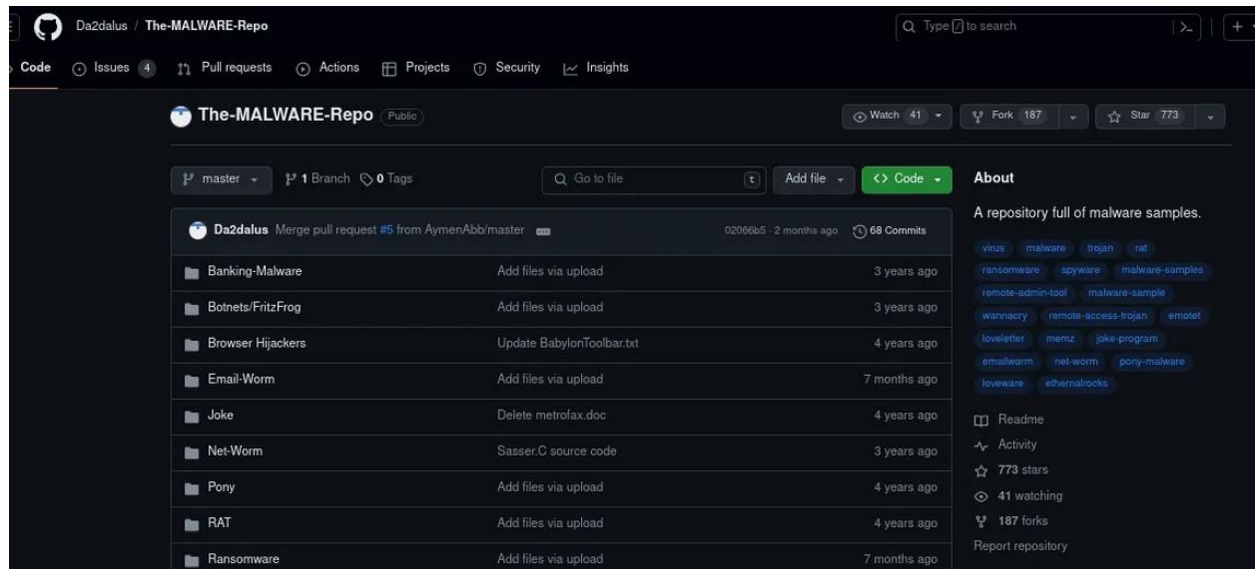
- You can give it by our need
- I Suggest you for giving 4Gb+ Ram and 50Gb Storage for better performance

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**



<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.

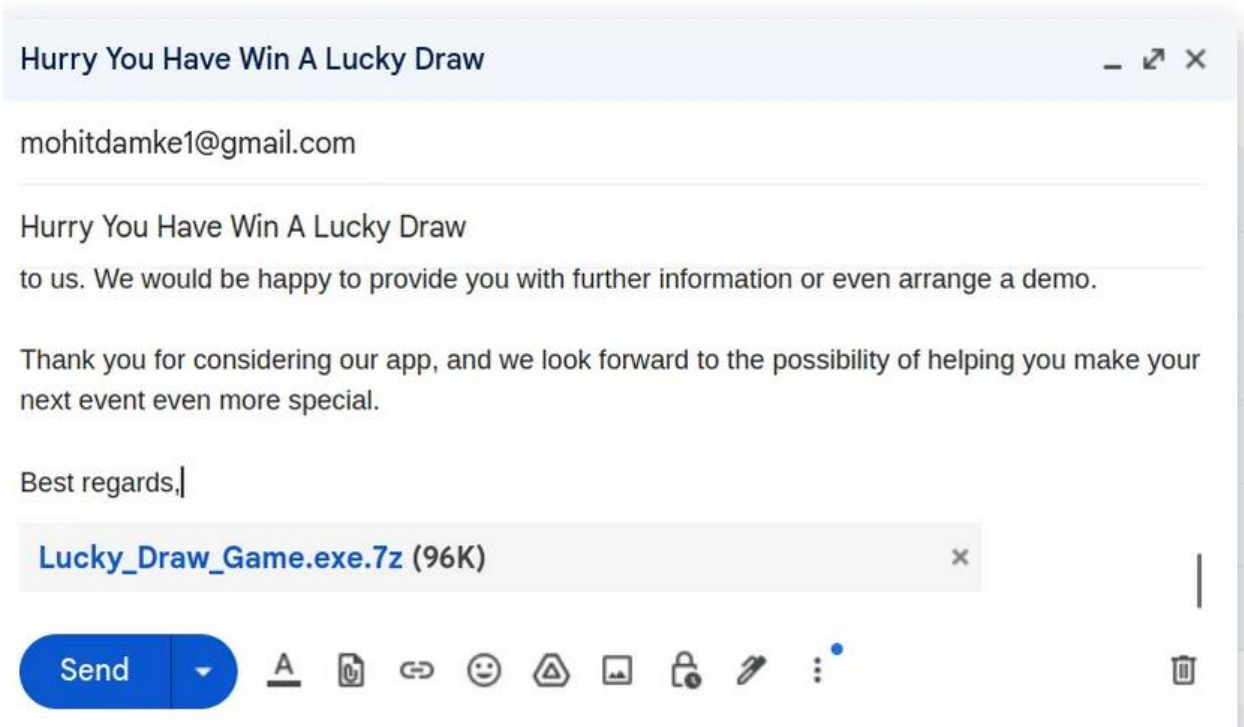
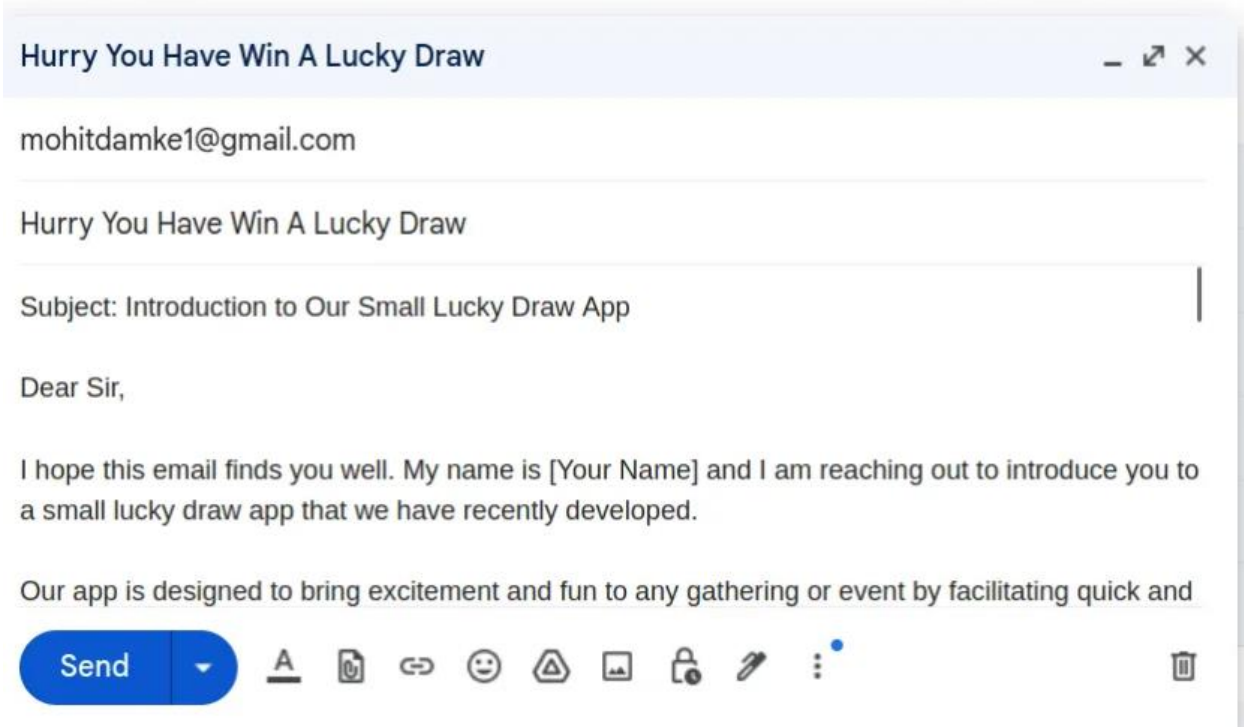
Key features of our app include:



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.

FiazHacks.com

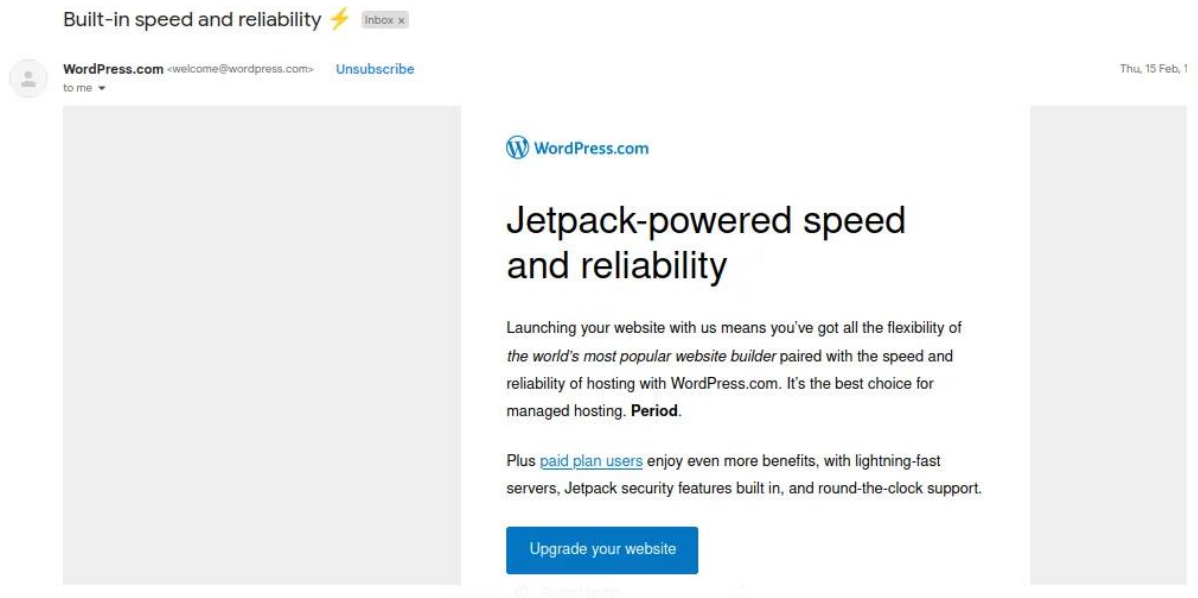


Attached Malware File to it by changing its name to **Lucky_Draw_Game**

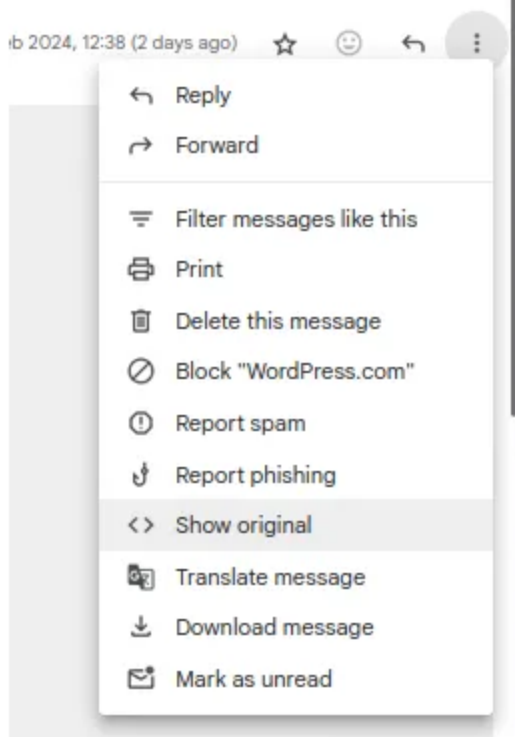
- So user will think that it is a game app but it is a malware
- **NOTE : The Mail is not been sent properly scanner has scan malware file and it disable to download the file and so we cannot download the file but we can test it manually**

● 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	<ccpBFShx1YxpugLVOLCG2IMImSvf73McA0PMfpeDrk@wordpress.com>
Created on:	15 February 2024 at 12:38 (Delivered after 0 seconds)
From:	"WordPress.com" <welcome@wordpress.com>
To:	mohitdanke1@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+885xDLRvTolzJQy8x8DuL57t0Wd3pyAR5ZT50nCP13H3Efa3z56
 X-Received: by 2002:a05:6808:1184:b0:3c0:3309:2057 with SMTP id j4-20020a056808118400b003c033092057mr1579956oill.
 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+Eh0hNC2t3060ZfysrAWPeZuha5LBVR7tmw7RAZj0xmIj4a0
 muc2W0VH5Wu0sKeHCknupoYPms0K9zhYczkRo26Ymp/Pa0tWgZSxHBFM+3aNBgVCu3cF
 /4uesA0y/ZxLQNMupBe6smxMg6u0XdteUn+M0VUHLURDI5P0wIEdfYkFwZmobEXI8
 +YIGl9KuyM5ltk4gJL2EhogtKEoBkUPQP1XsM+g0i/UXH3Cjefs98Bjqq8/1LeXbD94
 AcsnTyfrv6555blFAKCYLaRx/ShYg1XTECNXfZb95fX1gDTE8k2ULBsrPtDqu3uB9LSJB
 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=T0svRv8Ku7/Q6bGBVxIUGVkdzDrP38P8A0R2W4WCc+;
 fh=V6yAsV3Zy/Z6l5xL5xk4Atddn007z6YC7kmI+huPh6s+;
 b=Xu0DyeSPPhfZCxDi8Kn7uX/9vMLSDed4UYkaWpr3Lw6DRNRIOVxe4qWUpDE3DIJNS
 oC7rmv45mXiFiKz0YWE9mmLZl1Ma3IwA/dUkDxH6P/oy00j8GPB0wmgBy0cOfkcZ3U
 dcdQDK4r7IznKMDKQSV4mFLyLPmuHM2pMMJRZak0Gvd5YswwWgJM8/9HZAxumG5iaJE
 9hBsTGR2UWK6xhggLQFCboMBKxmme845hoAKD6/D4/VM/e4RdNXsRYp2XBg6BCN01XE
 0R50Lz9YmJugzXp1Cg0aIZmEg0KdE0AAUBj7a0y6x73CoFnoQnN1v6v0I9w9EhTqa7M
 6XLA==;
 dara=google.com
 ARC-Authentication-Results: i=1; mx.google.com;
 dkim=pass header.i=@wordpress.com header.s=automattic1 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 m3-20020a0568080f0300b003c0456cd04asi316063oiw.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 permitte
 sender) client-ip=192.0.80.222;
 Authentication-Results: mx.google.com;
 dkim=pass header.i=@wordpress.com header.s=automattic1 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=automattic1; t=1707980883;
 bh=1Z4SeLtc4zr5FDEI7TawP4h9PCT9rZp06NHgWVpS2E=; h=Date:To:From:Subject:List-Help:List-Unsubscribe:
 List-Unsubscribe-Post:List-Subscribe:List-Archive:From; b=NoiC2N/X5q/KtK4nx9nsxjhrPBXZH0mje+3qxlj/
 9Y3AlvLS3IZEanB8IjhlMIHwj
 h7byZx9CeJC7o0eNgBvWP8qcDy4RcnBtga10kwVXlJGSUqWw8J0w/UDUNHuZHXUZy
 0JAwly0544e6jbtqht9czvBjrh7cKdZbzNDE06Ke/izB2M2FTtmVo+rRFxgZpAd5j2
 wEeRkM7BC4UBvFb7ia3pv1ren3R2Wr9Q8muMGz1bWe65D7ukxzdvLt3Z+e/ggBgs7d
 ckh5usqas8VU1MSgXKa3m6AljA7Tu1NUZHyCs5ztXNFqDgwm7mQvLoAmrunlbzQTfk

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)

Admin, Fax, Ext:
Admin Email: REDACTED FOR PRIVACY (DT)
Created on 2000-03-03



DomainTools

PROFILE ▾

CONNECT ▾

MONITOR ▾

SUPPORT

Whois Lookup



```
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

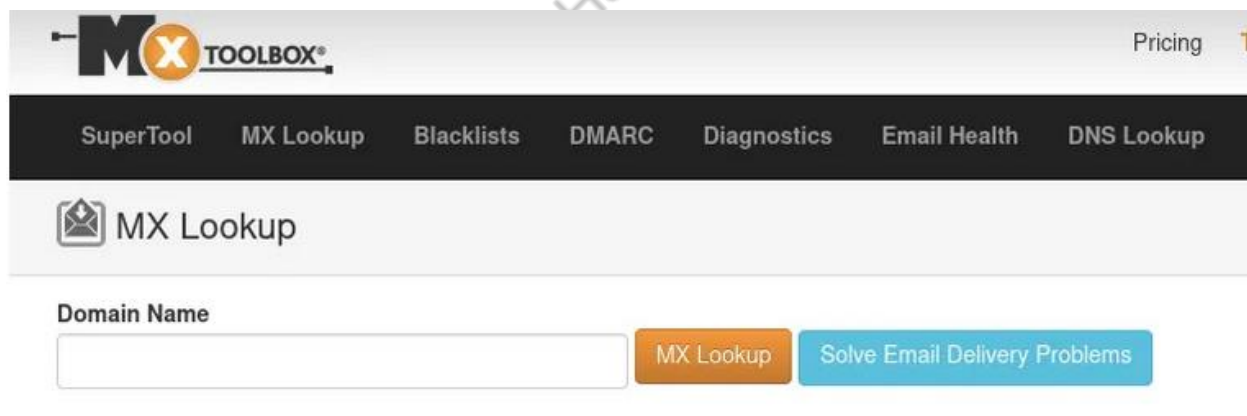
IP & Domain Analysis Websites

- 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.

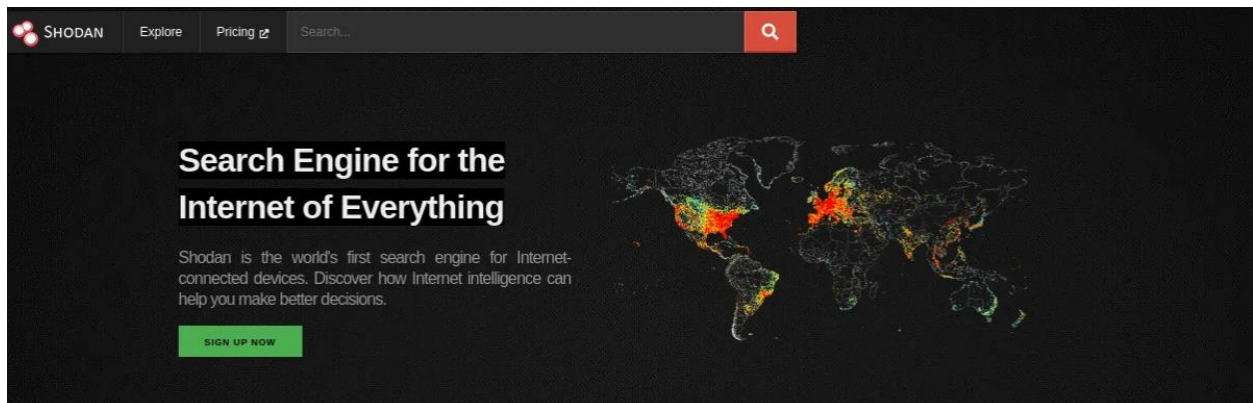
IPVoid:



The screenshot shows the IPVoid website homepage. At the top is a dark blue navigation bar with the 'IPVOID' logo on the left and a list of tool categories: IP, DNS, TEXT, URL, ENC/DEC, RANDOM, EXTRACT, and MORE, each with a dropdown arrow. Social media icons for Twitter and Facebook are on the right. Below the navigation bar is a white section with the heading 'IP Address Tools Online'. Underneath, it says 'We offer a vast range of IP address tools to discover details about IP addresses.' and 'IP blacklist check, whois lookup, dns lookup, ping, and more!'. A search bar with the placeholder text 'Search Tools..' is centered. At the bottom of this section, there is a green button labeled 'WINDOWS SOFTWARE' followed by a link: '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 website homepage. At the top is a dark navigation bar with the 'SHODAN' logo on the left, followed by 'Explore' and 'Pricing' with an external link icon. A search bar with a magnifying glass icon is on the right. The main content area has a dark background. On the left, the heading 'Search Engine for the Internet of Everything' is displayed in white. Below it, a paragraph reads: 'Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.' A green 'SIGN UP NOW' button is positioned below the text. On the right side of the page, there is a world map with a network overlay, where various regions are highlighted in red, orange, and yellow, representing discovered 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.

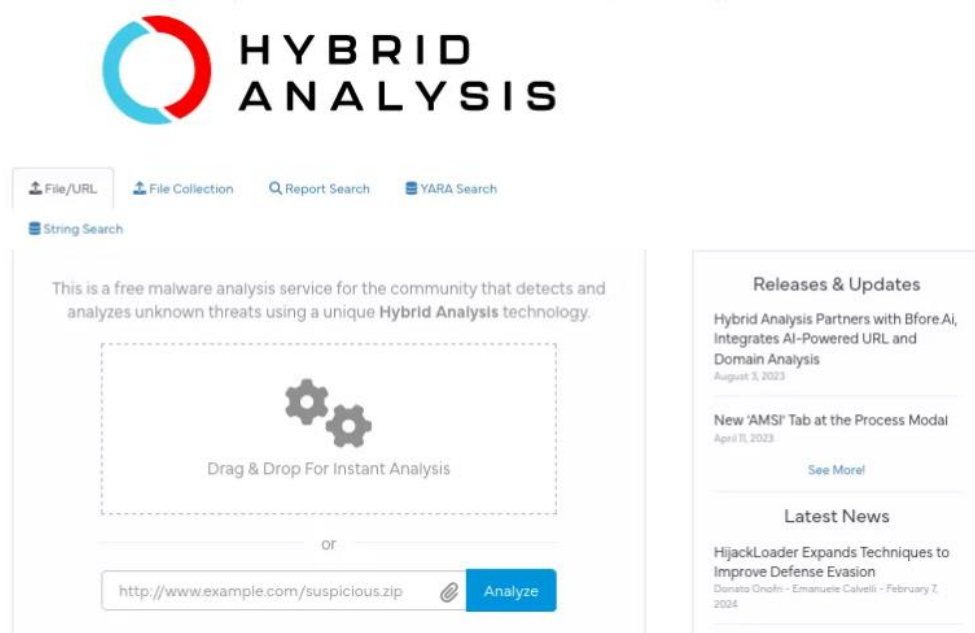
Malware Analysis

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:



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:



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 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 image shows the VirusTotal website interface. At the top, the VirusTotal logo is displayed. Below the logo, a message states: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." There are three main input options: "FILE", "URL", and "SEARCH". A "Choose file" button is prominently displayed in the center.

The lower portion of the image shows the analysis results for a file with the hash 716335ba5cd1e7186c40295b199190e2b6655e48f1c1cbe12139ba67faa5e1ac. The file is named "Annabelle.exe" and has a size of 15.94 MB. It was last analyzed 22 hours ago. A "Community Score" of 59 out of 72 is shown. A notification indicates that 59 security vendors and 3 sandboxes flagged this file as malicious. The file is categorized as a trojan.deshacop/annabelle ransomware. A table lists the security vendors that detected the file:

Vendor	Detection	Vendor	Detection
AhnLab-V3	Trojan/Win32.RL_Genasom.R267226	Alibaba	Trojan/Win32/Deshacop.197fd560
ALYac	Trojan.Ransom.Annabelle	Antiy-AVL	Trojan/Win32.Deshacop
Arcabit	Trojan.Ransom.Agent.ED	Avast	Win64:MalwareX-gen [Trj]

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