ANALYZE PHISHING EMAILS

* Malware and phishing emails are both types of cyber threats, often used by malicious actors to compromise the security of individuals, organizations, or computer systems.

**MALWARE:**



1. Malware, short for malicious software, refers to any software intentionally designed to cause damage to a computer, server, client, or computer network. Malware can take various forms, including viruses, worms, Trojans, ransomware, spyware, and adware.
2. Malware and phishing emails are both types of cyber threats, often used by malicious actors to compromise the security of individuals, organizations, or computer systems.

**PHISHING EMAIL:**



1. Phishing is a type of social engineering attack where attackers impersonate legitimate entities, such as banks, companies, or government agencies, to trick recipients into revealing sensitive information, such as usernames, passwords, credit card numbers, or other personal information.
2. Phishing emails often contain urgent messages, alarming statements, or enticing offers to prompt recipients to click on malicious links or download infected attachments. These emails can be highly convincing, often using logos, email templates, and language that mimic those of legitimate organizations. Phishing emails are a common method for distributing malware or gaining unauthorized access to sensitive information.

* **Requirements:**

**Hardware:**

* Laptop / Computer
* 8 or 8+ GB of RAM
* 50 GB storage

**Software:**

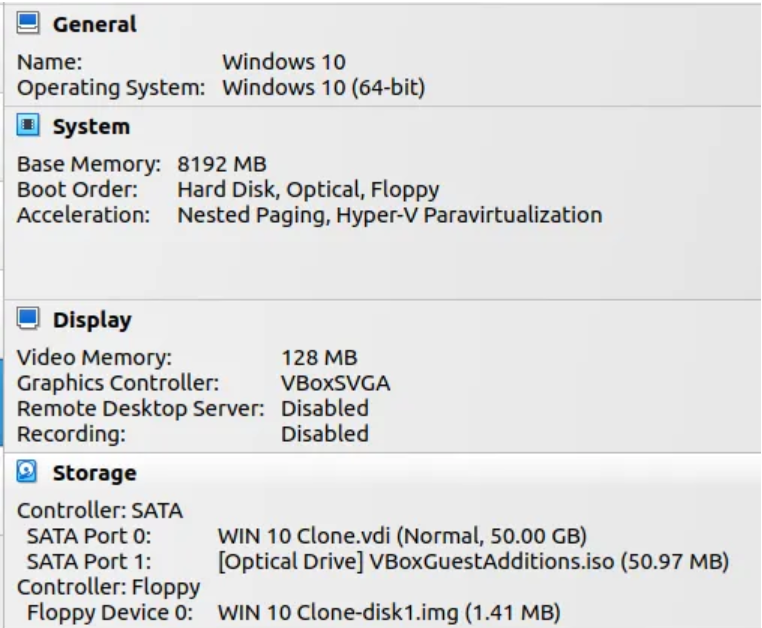
* Virtual Box
* Windows 10 install in it
* Sandbox Environment
* One Malware .exe file

**Introduction:**

I downloaded a malware sample to analyse 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.

**Practical Demo:**

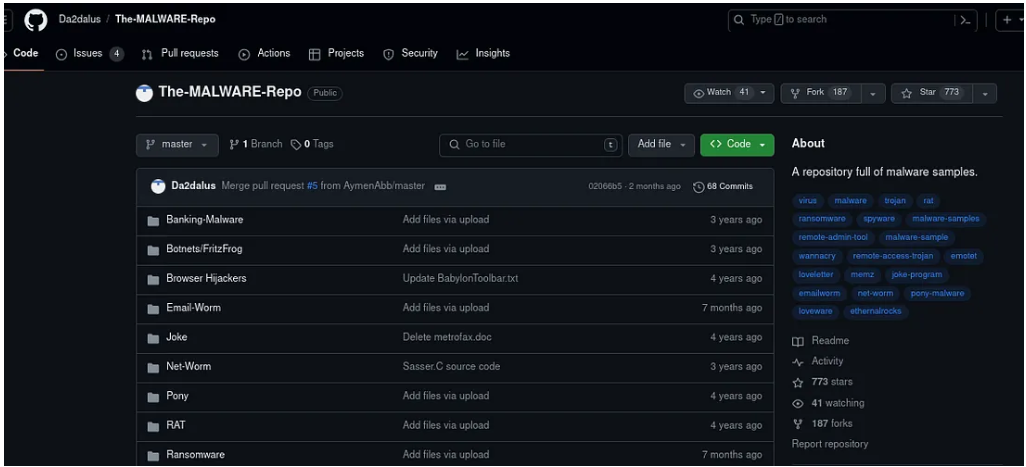
* First download the virtual box
* Install the Windows OS in it
* Give it a decent amount of specification
* Mine is here



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

**Downloading Malware:**

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



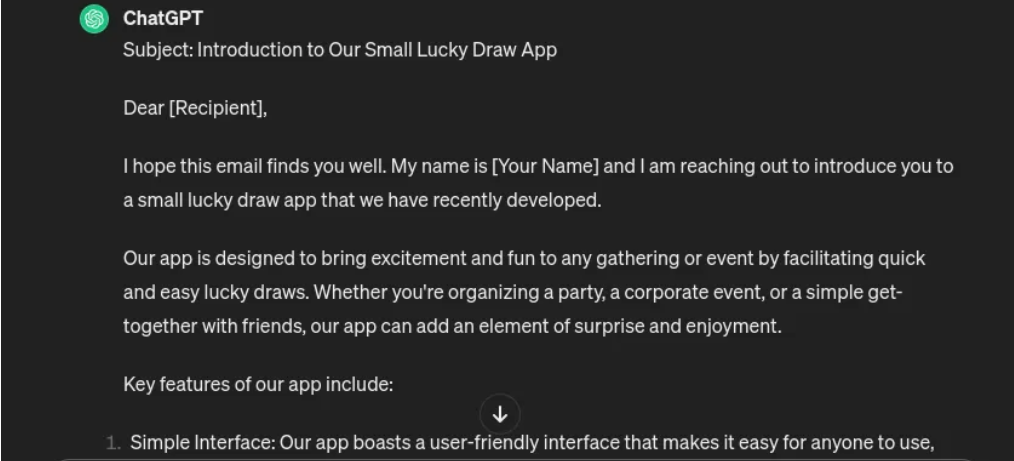
<https://github.com/Da2dalus/The-MALWARE-Repo>

**Send Email:**

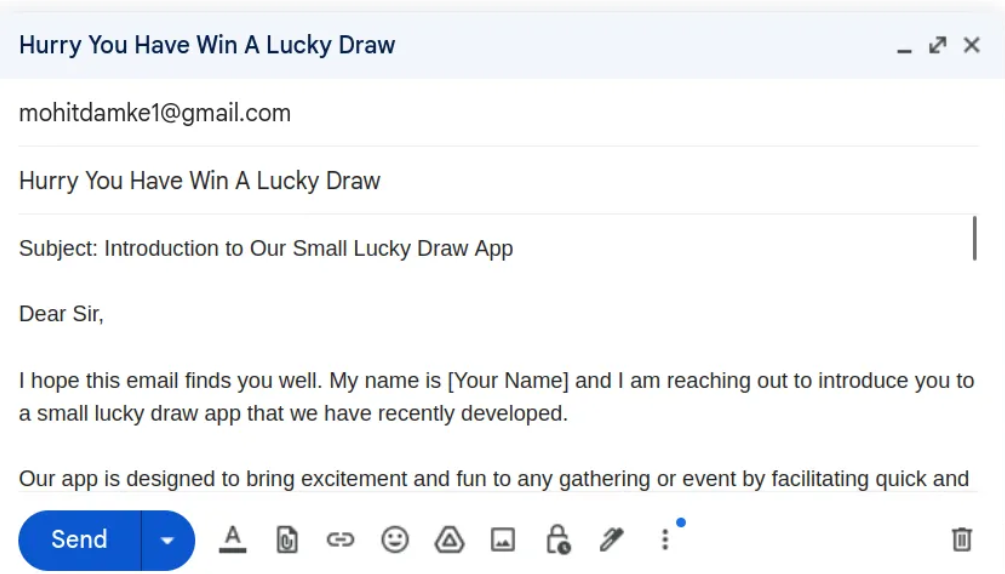
* If we want to send email so we can send it from our mail box
* But the malicious mail is not send by mail it is send by some different kind of mailbox which contain some additional option for sending mail.
* We can hide our email address from it and also hide sender information.
* We can add Phishing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

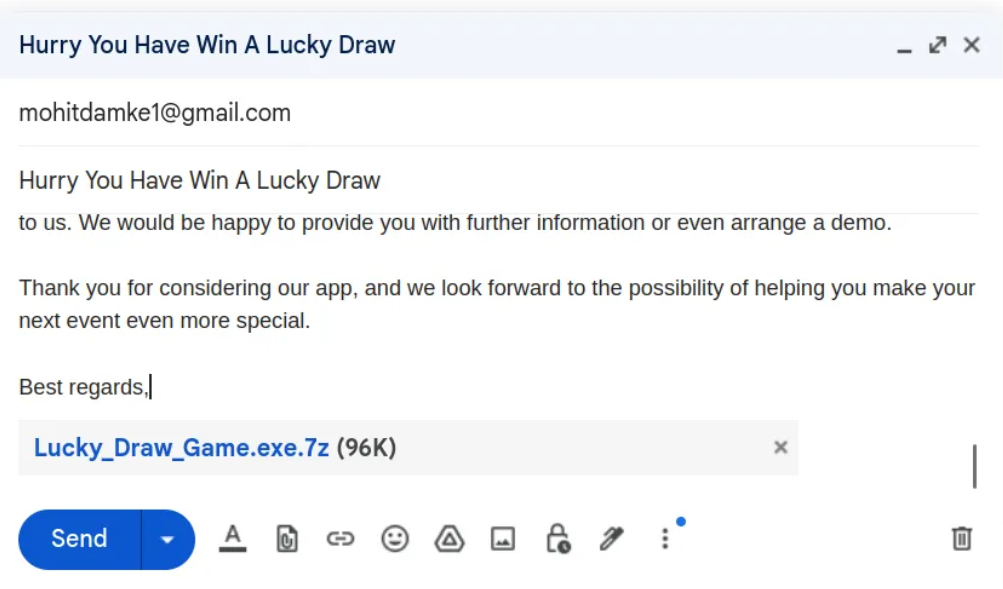
**Sending Malicious Email to Next Person:**

* Here I have sent 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.



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

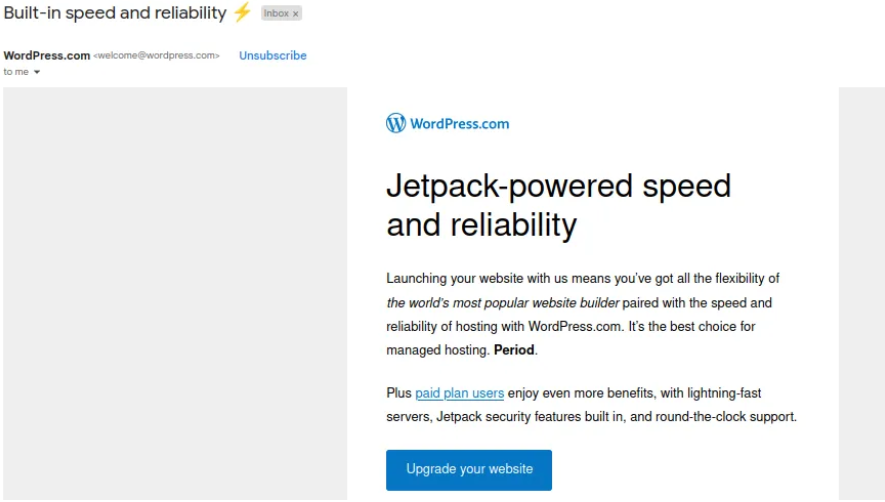




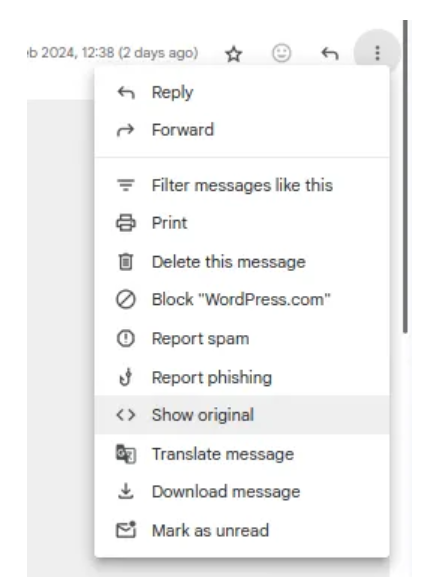
* Attached Malware File to it by changing its name to Lucky\_Draw\_Game.
* So, user will think that it is a game app but it is a malware.

**Email Analysis:**

* We can check for the email by just checking for its header.
* Let’s take an example for WordPress email.



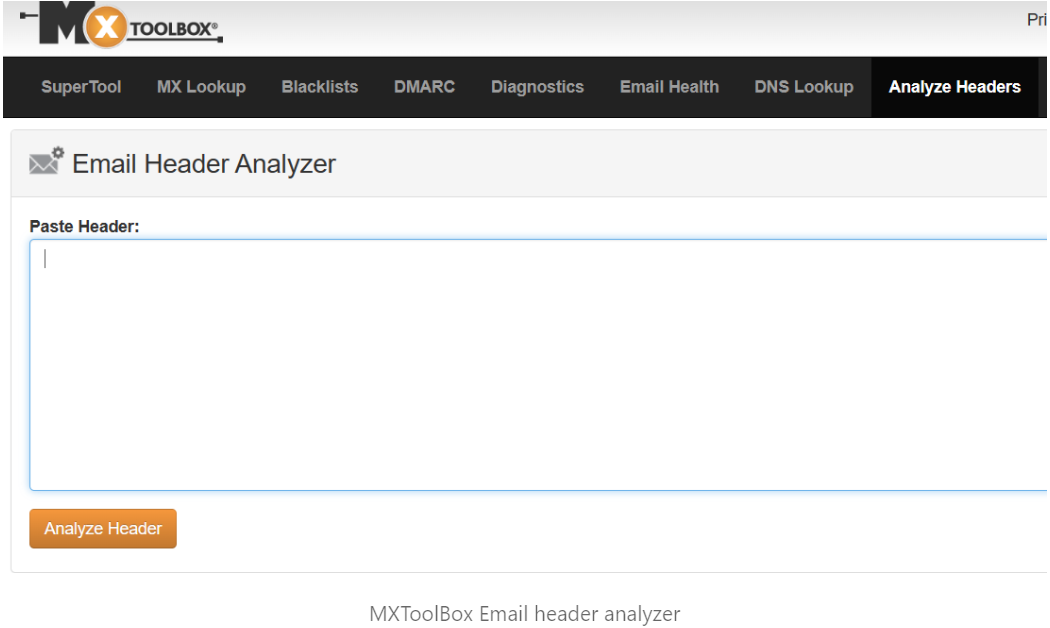
* First step is to check for the content read it carefully and notice it there are some mistakes.
* Note that it contains some attachment with it if yes so don’t open it.
* Check for the Header by clicking on 3 dots.



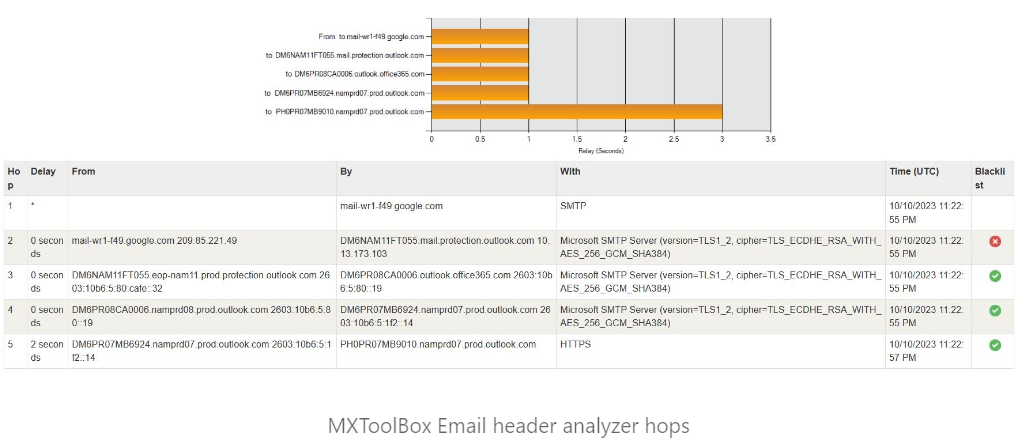
* Click on Show Original.
* Here is a bunch of information about email.



* While some individuals can easily interpret email headers from experience, the majority tend to copy and paste the email header into an email message header analyser for examination. One of the widely used and freely available email header analysers on the Internet is called "mxtoolbox": MX Toolbox - Email header analyser.



* Email header analysers serve a dual purpose, being employed not only for cybersecurity analysis but also by email administrators to resolve email delivery and delay issues. In the initial section of the MX Toolbox output, you will find information regarding the sequence of email server hops that processed the email. These email servers are commonly referred to as Mail Transfer Agents (MTAs). The email header should show all the MTAs the email traversed.

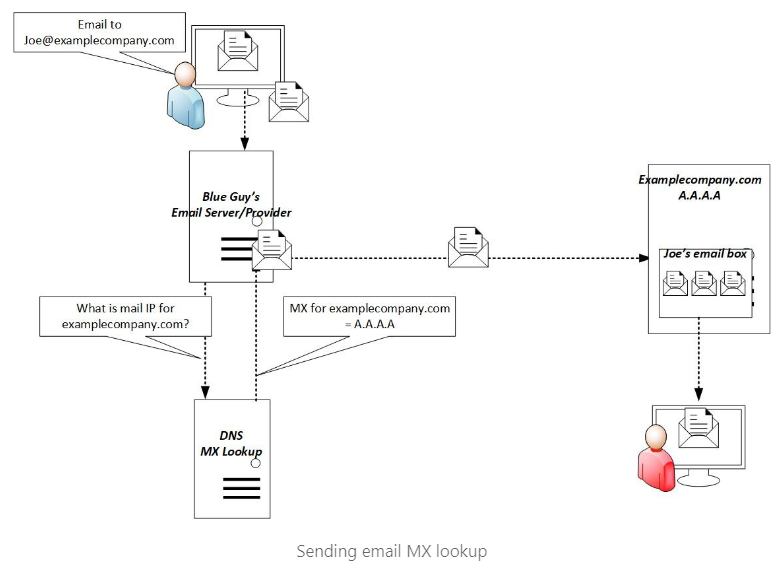


**Understanding “Sender Policy Framework” (SPF):**

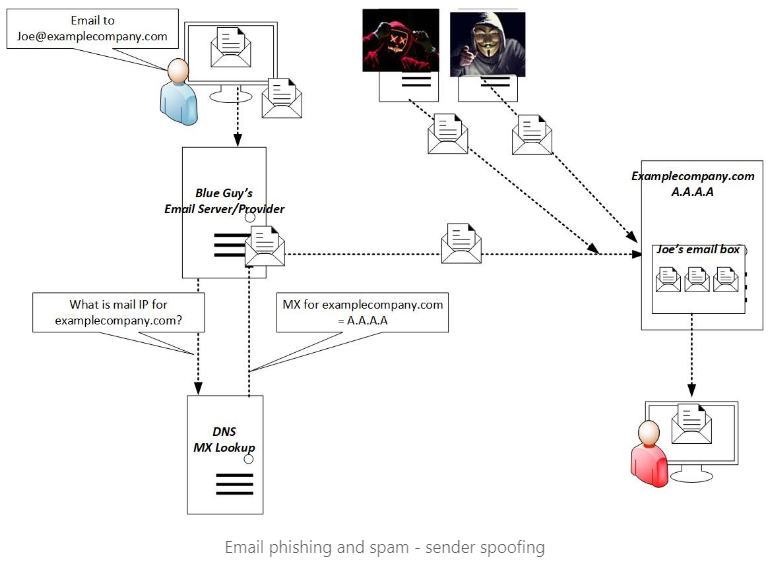
The standard email flow adheres to a straightforward process. In a simplified overview of this process, a user utilizes their preferred email client (e.g., Outlook) to compose an email. This email is subsequently dispatched from their email provider's server (MTA) to the intended destination email server.

Because internet routing operates based on IP addresses, the first task for the sending email server (MTA) is to ascertain the IP address of the mail server designated for the email recipient. This is achieved through a specific DNS query to retrieve the IP address of the email server associated with a receiving organization, for instance, an email going to joe@examplecompany.com would look up examplecompany.com. This process is known as a DNS "MX lookup" (MX being an abbreviation for "Mail eXchange").

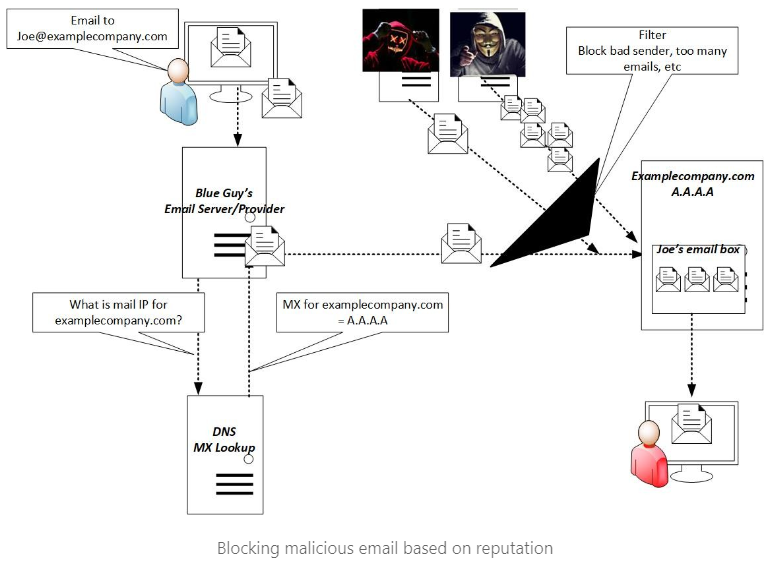
In brief, the sending MTA forwards the email to the IP address obtained from the MX lookup. This sending MTA, depicted as "Blue Guy's Email Server" in the diagram below, also operates from its own distinct IP address for sending purposes.



At this juncture, everything should be good in the email world; however, unscrupulous individuals often seek to send both malicious emails and spam to specific, targeted companies.



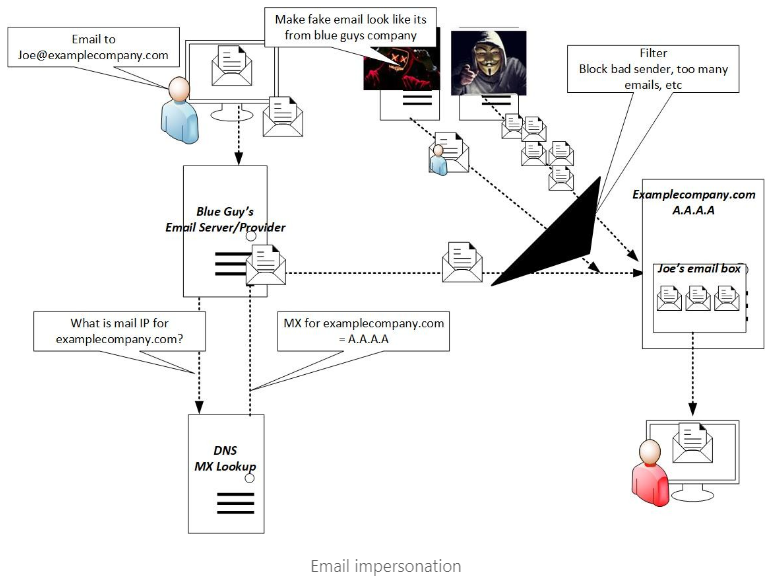
As emails contain sender domains and IP addresses, security tools began to identify and block common IP addresses and URLs associated with spam and malware. Email service providers also initiated the development of reputation-based algorithms. For instance, an email server sending a high volume of emails per hour could be flagged as a potential source of spam. Additionally, newly established email sending domains are initially treated with more scrutiny until they establish a track record of legitimacy over time.

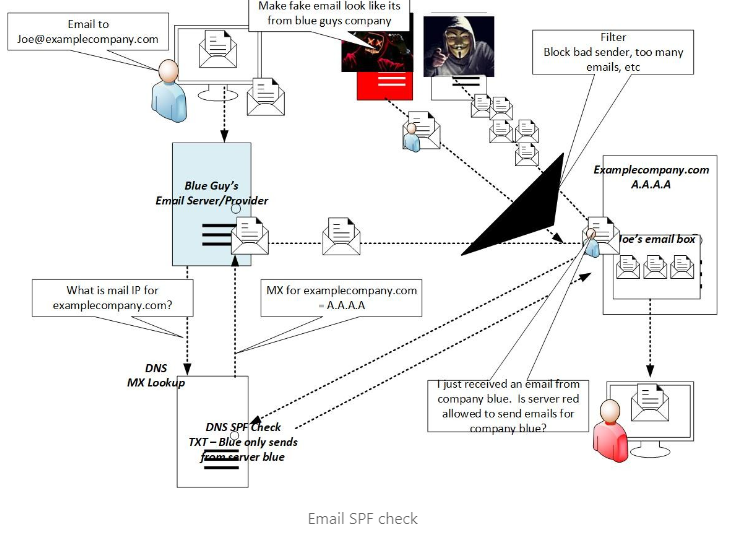


These threat/spam actors then had to devise additional tactics to complete their nefarious hacking goals. Step #1 of getting Phishing and spam emails through email filters and clicked is making them look legitimate. Some strategies for making emails look legitimate include:

* Impersonating the sender's information for a legitimate domain.
* Hacking into a legitimate sender's email account or email server.

Of these two methods, impersonating the sender's email information is easier to execute.



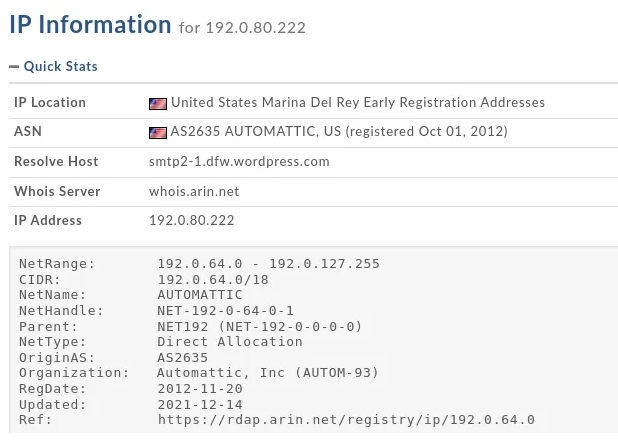
Thankfully, detecting email impersonations is a more manageable task. To counter the threat of email impersonations, email providers devised unique protection mechanisms. The first of these is SPF, which stands for "Sender Policy Framework." What SPF does is allow senders to include a special TXT record in DNS that outlines the authorized IP addresses responsible for sending emails on behalf of their particular domain. As a result, when a mail server receives an email from that domain, it can conduct a query for the sender's SPF record to cross-reference it with the sending IP address identified in the actual email received from that domain. The SPF check in the received email passes if the IP address of the sending domain's email server matches what's specified in the sending domain's SPF record. Conversely, if there's no match, the SPF check fails. 

**While SPF is highly effective, there are certain corner cases it doesn't cover. One such instance occurs when emails are forwarded through a mail server.**

**IP:**

It shows it’s IP address.

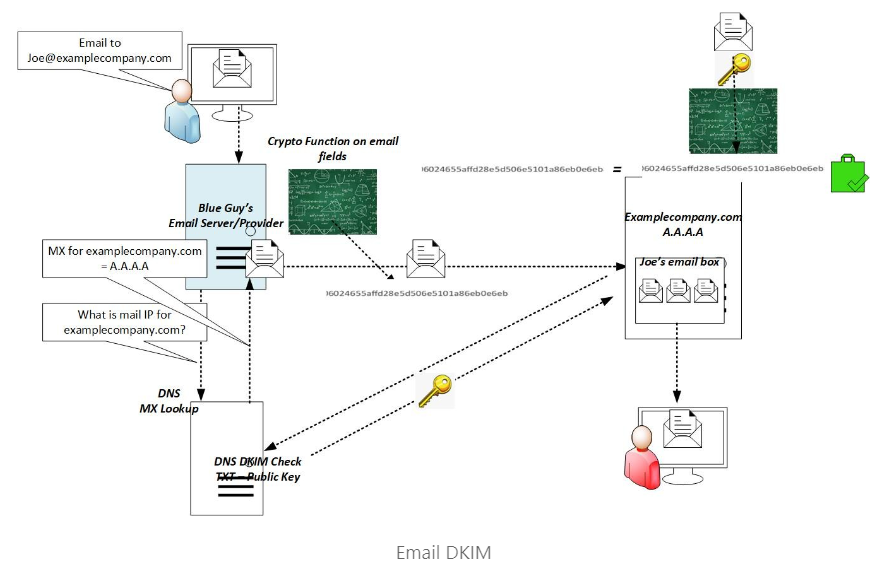




**Understanding "DomainKeys Identified Mail" (DKIM):**

Where SPF verifies that the sending IP is authorized, DKIM, on the other hand, validates whether the sending server is authorized to send emails. DKIM operates through Public/Private Key cryptography.

DKIM plays a crucial role in ensuring that the sender is authorized to dispatch messages from their domain and that the message remains unaltered in transit. However, it's important to note that DKIM primarily reduces the likelihood of spammers utilizing forged or stolen email addresses.



Nothing prevents hackers/spammers from purchasing a legitimate domain and generating valid SPF and DKIM records for them. However, hackers frequently attempt to impersonate reputable organizations to obtain user credentials, such as the inundation of emails we all see requesting password resets for banks, Google accounts, email services, and more.

* Let’s Check for the domain name register.



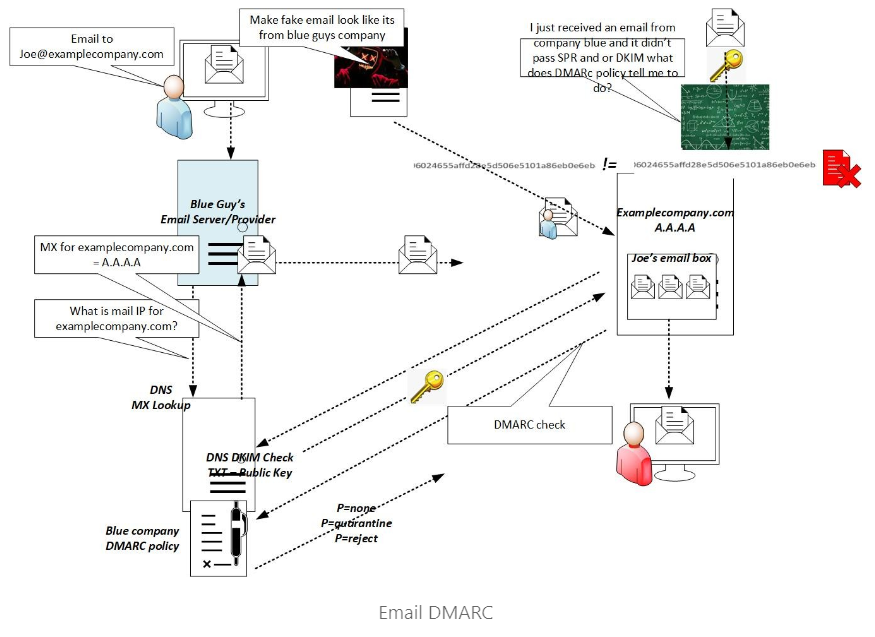




* They have hide much of the information so we are not able to get more information.
* So here we have done the basic level of email analysis.

**Understanding "Domain-based message Authentication Reporting and Conformance" (DMARC):**

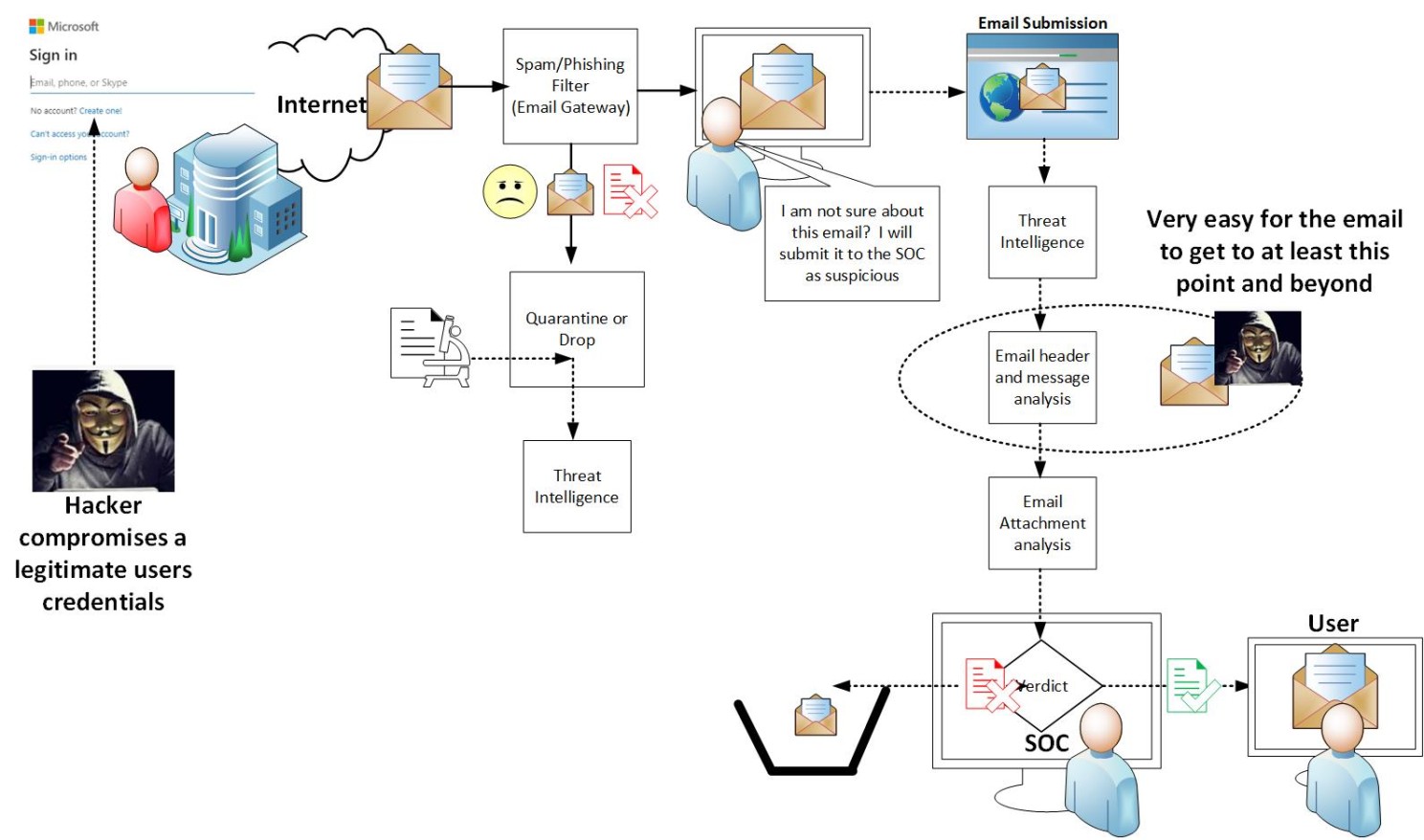
Lastly there is DMARC, which stands for "Domain-based Message Authentication, Reporting, and Conformance." Organization's setup a DMARC entry for their domain to instruct receivers of emails from their domain (legitimate or spoofed) on what to do if SPF and/or DKIM checks fail when the receiver checks them.



**A main reason why you need to analyse more than just email headers**

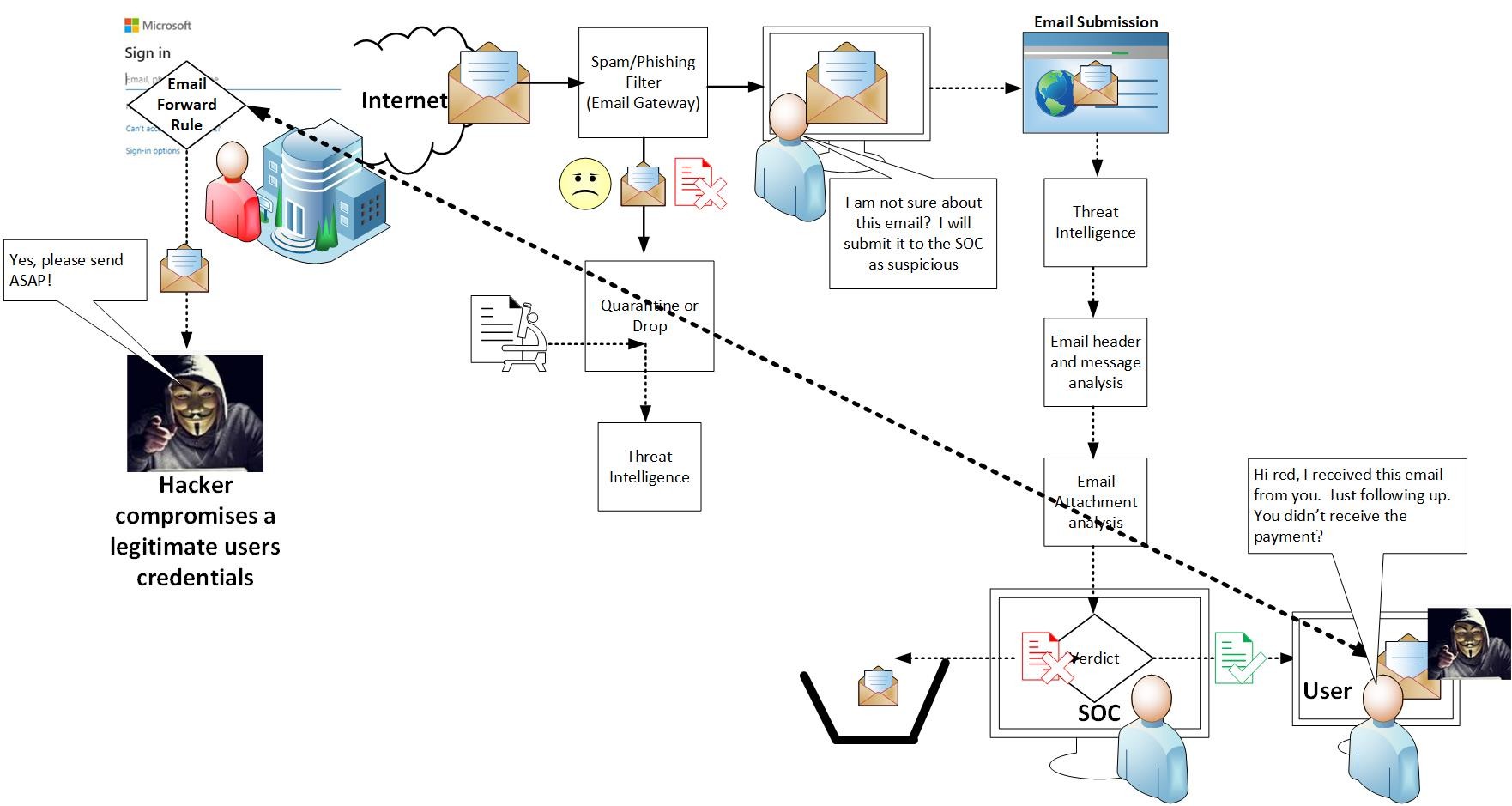
Hackers often employ a common tactic: compromising the credentials of legitimate users and reputable companies. This is particularly concerning because when an email originates from a genuine company, it tends to bypass automated spam filters and security checks, such as SPF, DKIM, and DMARC.

This underscores the importance of conducting thorough email body and attachment analysis, as well as providing comprehensive user training to thwart email phishing attempts effectively.



Dealing with emails from legitimate hacked accounts

Another technique hackers employ involves configuring email auto-forwarding rules on the compromised email accounts. By doing so, they gain control over the communication flow directed toward phishing victims. The result of this email box auto-forwarding manipulation is, the legitimate owner of the email account does not realize that their email account has been compromised.



How email auto forwarding rules play into phishing attacks

**Malware Analysis:**

Virus Total:

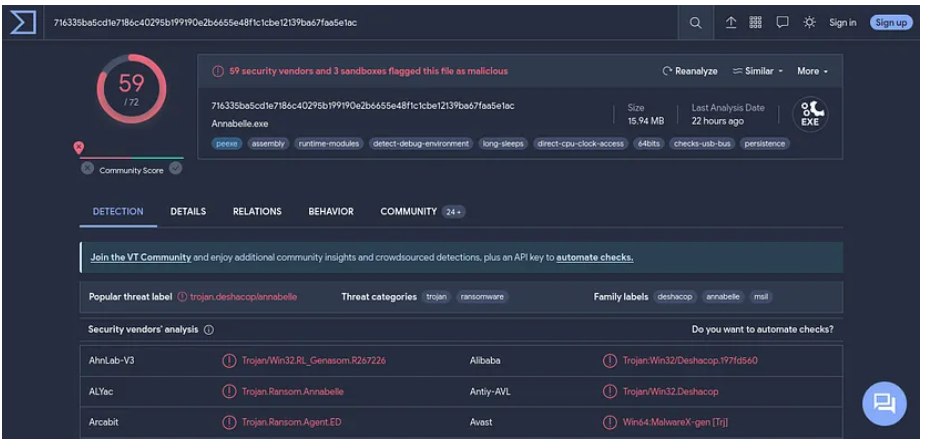


VirusTotal is a free online service that analyses files and URLs for viruses, worms, trojans, and other kinds of malicious content. It aggregates multiple antivirus engines and scan results from various sources to provide comprehensive insights into the potential threats of a file or URL.

* Let’s Take one Malware and Analysis it with the help of VirusTotal.
* I have one malware and let’s check it.
* Here is Malware.



* Annabelle.exe



* So here we get result.
* 59 out of 72 security vendors and 3 sandboxes flagged this file as malicious.
* That’s How you can analyse any file.