A robot with yellow eyes and a glowing yellow eye

Description automatically generated   
  
**Russian Hacktivists, Killnet, launch DDoS attack, disrupting US Airport Websites in 2022**

A close up of a card

Description automatically generated

**INTRODUCTION**

A Distributed Denial-of-Service (DDoS) attack is a prevalent form of cybercrime where an attacker floods a server with an overwhelming amount of internet traffic, rendering legitimate users unable to access online services and websites. This attack is orchestrated by utilizing a network of compromised systems, known as a "botnet," under the control of the attacker. The botnet comprises numerous infected devices, often acquired through compromised software or malware, which are instructed to simultaneously send traffic to the target server. The substantial volume of traffic originating from multiple locations makes DDoS attacks exceedingly difficult to counteract and mitigate effectively.

The motivations driving DDoS attacks can vary significantly. Some attacks are carried out by disgruntled individuals or hacktivists aiming to make a statement or exploit vulnerabilities in cyber defenses. Others are financially motivated assaults initiated by competitors seeking to disrupt or disable a rival business's online operations. Regardless of the motive, the repercussions of DDoS attacks can be severe. They lead to a substantial decrease in legitimate traffic, resulting in potential loss of revenue, disruption of services, and damage to a company's reputation.

As the Internet of Things (IoT) expands and more devices become interconnected within networks, the potential vulnerability to DDoS attacks increases. IoT devices often have weak security measures and can be easily compromised, making them susceptible to inclusion in botnets for launching DDoS attacks. Consequently, the importance of implementing robust DDoS protection and mitigation strategies cannot be overstated. Organizations and businesses must invest in proactive measures to safeguard their online presence and infrastructure from these evolving cyber threats.  
 **RUSSIAN HACKTIVISTS DISRUPT**

**A close up of text

Description automatically generated**

A screenshot of a news article

Description automatically generated

A close up of text

Description automatically generated

A close up of text

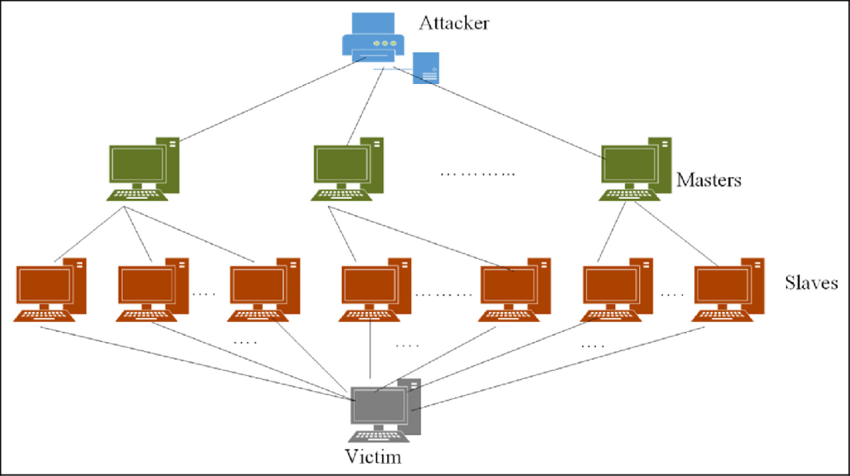
Description automatically generated

The websites for Chicago O’Hare International Airport and Hartsfield-Jackson Airport in Atlanta were temporarily blocked, triggering "connection timed out" errors for visitors. Atlanta’s airport website activated a “security service to protect itself from online attacks.” Despite the disruptions, most of the targeted sites remained operational, and the overall impact was more of an inconvenience than a security threat to passengers. The DDoS assaults could only target the airports’ websites, not the IT servers at the facilities.

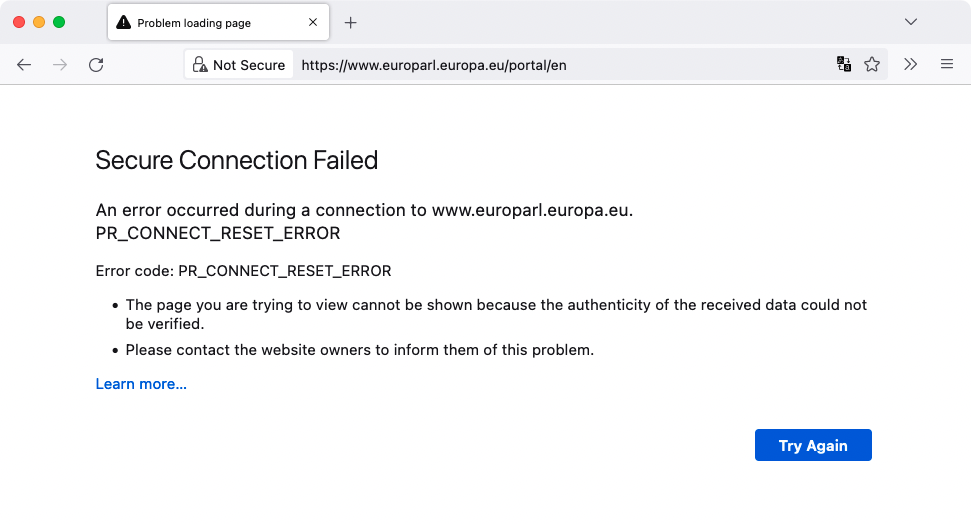
The Department of Homeland Security confirmed the attacks but did not comment on who might have been behind them. The attacks did not affect the actual operations of the airports or planes flying into and out of them. The Russian-speaking "hacktivists" from Kill Net claimed responsibility for the attacks, which took down websites at 14 airports, including Hartsfield-Jackson Atlanta International Airport (ATL) and Los Angeles International Airport (LAX).

The attacks were not trivial and could be the beginning of a larger trend, underscoring the vulnerability of the U.S. to cyberattacks attributable to actions and political events happening halfway around the world. However, it was noted that no operational systems appeared to have been taken down, and the attacks did not affect airline or airport operations.

The Russian government, possibly using private-sector hacker groups, is considered the most likely suspect behind the attacks. The coordinated nature of the incidents suggests a state-sponsored effort rather than the work of random criminals or teenage hackers. Despite the inconvenience caused, the attacks highlight the vulnerabilities in information technology and the reliance on it for daily operations, such as checking flight times or booking airport services.  
  
  
  
**DDOS ATTACK ANALYSIS**



*Fig: Summarizing overview of the operation of the DDOS Attack*



*Fig: Screenshot of the DDOS-attacked website*  
  
  
  
  
  
**EMULATION OF THE ATTACK**

My goal is to replicate the attack scenario faithfully to illustrate and gain an understanding of how the attack might have transpired. To begin, I will develop a tool for executing a Distributed Denial of Service (DDoS) attack.

I utilized Microsoft Visual Studio to craft the code required for the attack.  
  
  
A logo on a tire

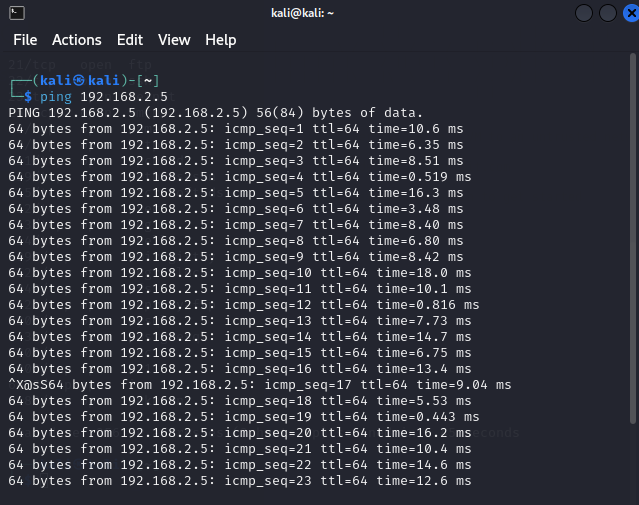
Description automatically generated *Fig: This is my Attacker Machine.*  
  
  
A screenshot of a computer

Description automatically generated

*Fig: This is my Victim Machine.*  
  
  
  
First, I will access Metasploitable 2 (Victim Machine) and use the command "ifconfig" to retrieve the IP address of the victim machine before proceeding with the DDoS attack.  
  
 A screenshot of a computer

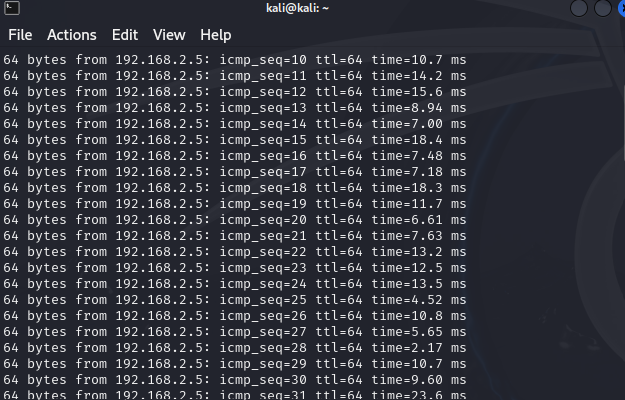
Description automatically generated  
  
After executing the command, we obtained the IP address as 192.168.2.5.  
  
  
Afterward, we accessed the IP address location from the attacker's machine. Now, this is the web server we are going to attack.  
  
A screenshot of a computer

Description automatically generated  
  
Afterward, I'll set up a script to initiate a DDoS (Distributed Denial of Service) attack using hping3. Before proceeding with this, we'll use the ping command to gauge the response time of the IP address and verify the bidirectional connectivity.

  
  
After running the ‘ping’ command, we can see that the IP address connection is good and fast.

Now here is the command I used with hping3 to initiate the DDoS attack:  
  
 A screenshot of a computer

Description automatically generated  
  
Let’s break down the command I used with hping3:  
  
"**sudo**": It's like using your super admin cap. It provides you the ability to perform unique tasks on your computer.  
  
"**hping3**": The secret phrase that instructs your computer to transmit messages.  
  
"**-p 80**": This is when it gets interesting. You wish to send your message to port 80, according to this. That's like delivering a message to a specific door where online content often enters the internet.  
  
"**-c 1000**": The number of packets to send (in this example, 1000) before quitting is specified by this option. 1000 TCP packets will be sent to the designated destination by hping3.  
  
"**-S**": The TCP SYN flag is set in TCP packets by using this option. To establish a connection with another TCP endpoint (like a web server), utilize TCP SYN packets.  
  
"**--flood**": With this option, hping3 is instructed to transmit packets without waiting for a response. In essence, it sends a deluge of TCP SYN packets to the target.  
  
"**192.168.2.5**": Hping3 will send the TCP SYN packets to this target IP address. In this instance, hping3 will overload port 80 (HTTP port) on the target (192.168.2.5) with TCP SYN packets.

  
  
Finally, when running the 'ping' command after the attack, we can observe that the connection to the IP address is deteriorating, becoming slower and less responsive.  
  
  
In conclusion, the emulation of a Distributed Denial of Service (DDoS) attack using Microsoft Visual Studio and hping3 provides a practical understanding of how such attacks can occur and their impact on network performance. By replicating the attack scenario, we were able to observe the initial fast and responsive connection to the victim machine's IP address, which gradually deteriorated into a slower and less responsive connection after the DDoS attack was initiated. This exercise underscores the importance of understanding and mitigating the risks associated with DDoS attacks, as highlighted by Microsoft's response to recent DDoS attacks targeting the HTTP/2 protocol.  
  
  
  
 **END OF THE ATTACK**  
 **PROTECTION MECHANISM  
  
General recommendations**   
  
To prevent DDoS attacks, consider implementing the following general recommendations:

1. **Minimize the Attack Surface**: Limit the exposure of your application or resources to unnecessary ports, protocols, or applications. Use firewalls or Access Control Lists (ACLs) to control inbound traffic and restrict direct Internet traffic to critical parts of your infrastructure.

2. **Scale Up Your Bandwidth and Server Capacity**: Ensure your hosting provider offers redundant Internet connectivity and consider employing Content Distribution Networks (CDNs) and smart DNS resolution services. This helps in handling large volumes of traffic and mitigating DDoS attacks.

3. **Implement Rate Limiting**: Limit the amount of traffic your server can accept to prevent overloading. More advanced techniques involve analyzing packets to accept only legitimate traffic.

4. **Use a Web Application Firewall (WAF):** Protect against application-level attacks like SQL injection or cross-site request forgery by using a WAF. Customize mitigations against illegitimate requests.

5. **Make Your Network Resilient**: Distribute your data centers across different networks and locations, and ensure servers are not all in the same physical location. This helps in avoiding traffic bottlenecks and makes your infrastructure more resilient against DDoS attacks.

6. **Take Advantage of Anti-DDoS Hardware and Software**: Utilize products designed to mitigate specific types of DDoS attacks and harden your IT infrastructure by adjusting settings, removing unused ports, and enabling timeouts for partly open connections.

7. **Continuously Monitor for Unusual Activity**: Regularly monitor your network for signs of a DDoS attack and take action to mitigate it as soon as possible.

8. **Ensure High Levels of Network Security**: Implement firewalls, intrusion detection systems, anti-virus and anti-malware software, endpoint security, web security tools, and network segmentation to protect against DDoS attempts.

9. **Limit Network Broadcasting**: Disable or limit network broadcasting between devices to prevent amplification of DDoS attacks. Consider disabling services like Echo and Chargen.

10. **Have a DDoS Strategy**: Develop a comprehensive strategy that includes intrusion prevention, threat management, mitigation strategies, and continuous monitoring. This approach makes it harder for attackers to execute a DDoS attack.

By combining these strategies, you can significantly reduce the risk and impact of DDoS attacks on your network and infrastructure.

## **CONCLUSION**

In the wake of the recent DDoS attacks on U.S. airport websites by the pro-Russian hacktivist group Kill Net, it's clear that cybersecurity threats, including DDoS attacks, pose significant risks to both individuals and organizations. These attacks can disrupt services, cause financial losses, and damage reputations, making it crucial for businesses and individuals to take proactive measures to protect themselves.

A close-up of a text

Description automatically generated

Moreover, organizations should adopt a multi-layered approach to counter DDoS attacks effectively. This involves minimizing the attack surface, employing segmentation principles to reduce the attack surface and filter legitimate traffic, and ensuring ample redundant internet connectivity to handle large volumes of traffic. Utilizing services like AWS Shield can provide additional layers of protection, monitoring traffic, confirming an attack, identifying the source, and mitigating the situation by rerouting malicious traffic away from the network.

A close-up of a text

Description automatically generated

## **REFERENCES**

[1] https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/

[2] https://aws.amazon.com/shield/ddos-attack-protection/

[3] https://securityscorecard.com/blog/best-practices-to-prevent-ddos-attacks/

[4] https://www.indusface.com/blog/best-practices-to-prevent-ddos-attacks/

[5] https://phoenixnap.com/blog/prevent-ddos-attacks

[6] https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks\_508c.pdf

[7] https://www.esecurityplanet.com/networks/how-to-prevent-ddos-attacks/

[8] https://www.embroker.com/blog/how-to-prevent-ddos-attacks/

[9] https://www.cdnetworks.com/cloud-security-blog/how-to-prevent-a-ddos-attack/

[10] https://www.geeksforgeeks.org/hping3-command-in-linux/

[11] https://www.icontime.com/support/knowledge-base-search/42-troubleshooting-tips/  
  
[12] https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/

[13] https://aws.amazon.com/shield/ddos-attack-protection/

[14] https://blogs.blackberry.com/en/2022/11/ddos-attack-8-simple-prevention-and-mitigation-strategies

[15] https://www.indusface.com/blog/best-practices-to-prevent-ddos-attacks/

[16] https://pressable.com/blog/ddos-attack-prevention/

[17] https://www.loginradius.com/blog/engineering/how-to-mitigate-ddos-attack/

[18] https://securityscorecard.com/blog/best-practices-to-prevent-ddos-attacks/

[19] https://pantheon.io/blog/ddos-attacks-prevention