Review

Comprehensive Review Analysis and Countermeasures for Cybersecurity Threats: DDoS, Ransomware, and Trojan Horse Attacks

Naveesen Ravichandran , Tahrhunraj Tewaraja , Vishendraa Rajasegaran , Sri Sharvesh Kumar , Siva Kumar Livekha Gunasekar , Siva Raja Sindiramutty *

Posted Date: 20 September 2024

doi: 10.20944/preprints202409.1369.v1

Keywords: Cybersecurity; DDoS Attacks; Ransomware; Trojan Horse; Countermeasures

Review

Comprehensive Review Analysis and Countermeasures for Cybersecurity Threats: DDoS, Ransomware, and Trojan Horse Attacks

Naveesen Ravichandran, Tahrhunraj Tewaraja, Vishendraa Rajasegaran, Sri Sharvesh Kumar, Siva Kumar Livekha Gunasekar and Siva Raja Sindiramutty *

School of Computer Science Taylor's University Subang Jaya; magan.shiva91@gmail.com

Abstract: With all the sophisticated threats to network security, intrusion detection is a section of the security technology industry that is becoming increasingly significant. In this research paper, we have discussed in detail the detection, effects, and prevention protocols of security issues. Security issues are a wide range of elements. Hence, we narrowed our research to two main sectors which are malware attacks and distributed denial of service (DDOS). To make the research more informative, we looked at three selected real-life cases of security intrusion that occurred around the world in recent years. Malware attacks and DDOS are constantly being developed creatively to challenge all the current security systems. In addition, we have analysed and highlighted the potential threats of the security issue and included proposed countermeasure ideas to avoid the security issues. The research findings also show us that malware is evolving simultaneously with our security technology growth. This gives us an understanding that prevention is significantly a continual improvement process.

Keywords: Cybersecurity; DDoS Attacks; Ransomware; Trojan Horse; Countermeasures

Distributed Denial of Service (DDOS) Background

In this part, delve into the background of distributed denial of service (DDoS). To start this discourse, I, Naveesen, shall first define DDOS in the interest of clarity. (Reblaze, 2022; Wen et al., 2023) As a subtype of denial of service (DoS) attacks, DDoS assaults are included. A DoS (Denial of Service) attack seeks to make the intended users of the targeted system unresponsive. When websites were hosted on different servers in the early days of the Internet, single-source DoS assaults were effective. Nowadays, there is a much lower likelihood of this happening because websites are hosted in the cloud, dispersed over several data centres, connected to content delivery networks and so on. Even when using techniques like amplification and reflection, it is very difficult for a single-source attack to have enough bandwidth to overwhelm a contemporary website's resources. As a result, attackers increasingly spread their attacks over several sources. DDoS assaults may mobilize a potentially huge pool of resources, which has made them a big problem today.

Now that I've explained what DDoS is, let's speak about the DDoS attack, how it is carried out, and the attack's architecture. Let me explain everything with my current, inexperienced understanding, and if I misinterpreted anything, I'd like to learn from it. (Fruhlinger, J., 2022) A DDoS attack occurs when an attacker or attackers attempt to stop a service from being delivered. To do this, access to nearly anything, including servers, devices, services, networks, applications, (Zhou et al., 2021; Zaman et al., 2011) and even specific transactions within applications, may be banned. In a DoS attack, only one system delivers the malicious data or requests, but in a DDoS attack, several systems do so. The primary method used by these attacks is to saturate a system with data requests. This can include sending a web server so many requests to display a page that it crashes under the strain, or it might involve barraging a database with queries. The available CPU, RAM, and internet bandwidth

 doi:10.20944/preprints202409.1369.v

are all used up consequently. Effects might range from minor service interruptions to the complete shutdown of websites, programmes, or even whole enterprises.

Attacks on the application layer and attacks on the network layer are the two main subcategories of DoS attacks (Uddin, Kumar and Chamola, 2024; Sindiramutty et al., 2024). Each of the several DDoS attack types describes the attack's objective as well as its specific features and tactics. (Learning Center. (n.d.)) Application layer attacks, also known as layer 7 attacks, are threats that try to overwhelm a server by sending many requests that need a lot of processing resources to process. HTTP floods, slow attacks like Slowloris or RUDY, and DNS query flood attacks are a few examples of this sort of attack. Attacks on your network at the layer 3–4 level, also known as network layer attacks, are almost invariably DDoS attempts to disrupt the "pipelines" connecting your network. NTP amplification, DNS amplification, NTP flood, SYN flood, and other sorts of attacks fall under this group of attack techniques. DDoS attacks are often high-traffic incidents, frequently measured in gigabits per second (Gbps) or packets per second (PPS). Although most network infrastructures can be destroyed with 20 to 40 Gbps, the most powerful network layer assaults may reach hundreds of Gbps.

Let's use an illustration to clarify the DDoS attack's structure. On the page I visited, I found a fantastic illustration [3]. Let's think about an analogy rather than getting into the specifics of the technology. Assume I operate a burger delivery business. When their items are prepared for pickup, customers call to place their orders. One day, a prankster calls my home several times and orders a total of 100 burgers. All my chefs are kept busy as a result, so I stop accepting new orders. The Joker, however, never consumes hamburgers. I was unable to help legitimate clients because my resources were being used by fake enquiries. Despite the inconvenience, it is simple to stop since just one individual is delivering the erroneous directives. Simply blocking their phone number will put an end to the issue. The same thing may occur on a server. One rogue client can flood a server with bogus requests, making it difficult for it to serve legitimate users. However, identifying that client is simple since the server may simply reject any inbound requests from a single fake client, precisely like in my example.

Denial-of-service (DoS) attacks, which are the forerunners of contemporary DDoS attacks, fall under this category. Now picture many pranksters calling my burger restaurant. My phone never stops ringing, and it's practically impossible to tell which consumers are real and which are scammers. Because some of the block numbers could belong to customers, I also can't just utilize them. My company is completely frozen. This is exactly what happens when a server is the target of a DDoS attack. Hackers can generate phoney traffic that appears to be originating from several devices, which eventually causes a server, network, or website to fail.

DDoS attacks are frequently carried out for several motives, including extortion, hacktivism, and rivalry. A DDoS attack's perpetrator will typically demand a ransom. The rare attack-warning ransom letter may also be issued, though. DDoS attacks are frequently utilized as a method of expression. Hacktivists can utilize DDoS attacks to openly support or criticize a rule, person, or business. According to a 2017 poll, more than 40% of businesses that have experienced a DDoS attack blame their rivals. This seems far more feasible given the current $150 price tag for a week-long DDoS attack.

This section will thoroughly investigate and discuss the most hazardous DDoS attack kinds. When the system gets a SYN packet, an incomplete communication request that no longer satisfies the actual communication needs starts a SYN assault, which results in a denial of service (DOS). To further clarify this SYN Flood Attack to you, I'll present you with a graphic that I discovered in the text. (Nafea Alhammadi, 2021; Sindiramutty, Tee, et al., 2024)

 doi:10.20944/preprints202409.1369.v

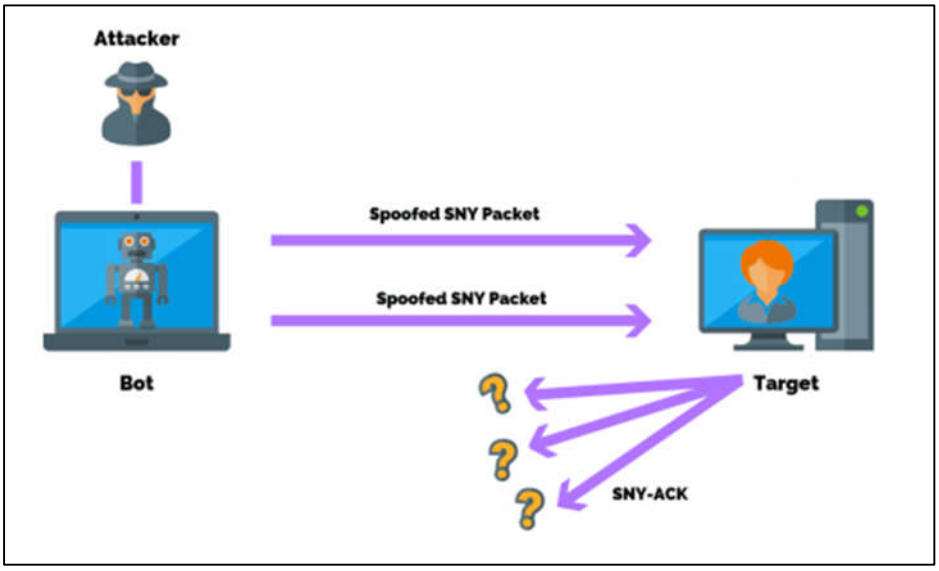


Figure 1. The Architecture of SYN Flood Attack.

The ICMP flooding will come next. A system expands and all resources start to fail when the ICMP overwhelms it with a lot of repeating echoes, at which point a lot of system traffic can no longer be processed. When examined by strengthening ICMP flood security, the Board of Directors might establish thresholds that need ICMP floods. As per usual, I'll include a pertinent graphic to help illustrate what I'm referring to in this section, ICMP flooding.

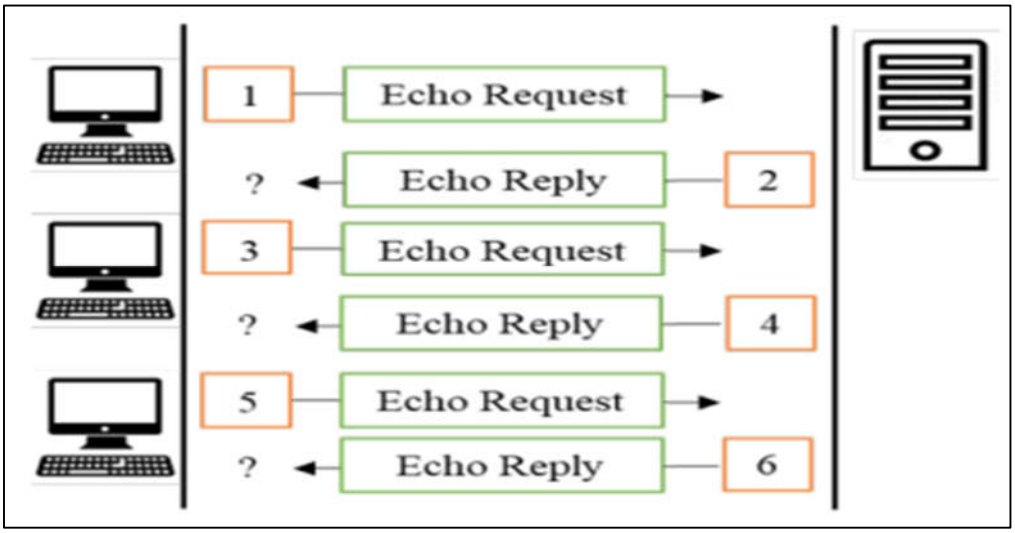


Figure 2. ICMP Flood Attack.

A UDP flood occurs when a system is overloaded with UDP packets to the point where it is unable to support any more valid connections, much like an ICMP flood. With enhanced UDP flood security, managers may establish a threshold that is greater than their ability to defend against UDP flood attacks. This is also included with a pertinent illustration that is quite apparent.

 doi:10.20944/preprints202409.1369.v

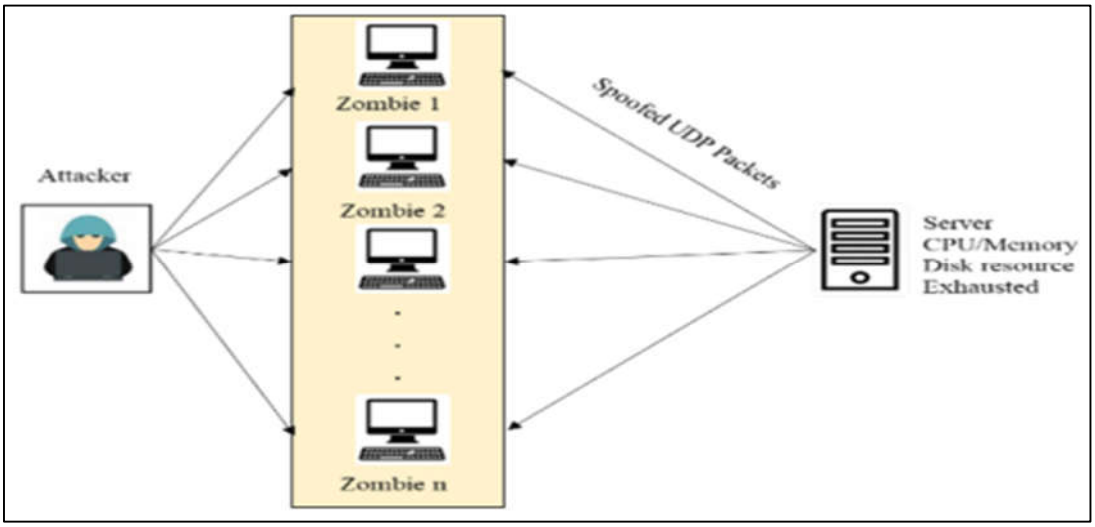


Figure 3. Architecture of UDP Flood (Nafea Ali Majeed, Zaboon and Abdullah, 2021).

The last sort of flooding attack is the misuse attack. It takes advantage of network resources, especially those that can only be shared by a small number of users or those that cannot be shared by many users (Mohiddin, Midhunchakkaravarthy and Hussain, 2023). By taking resources away from other users and using them exclusively for their own needs, the attacker in this attack does not share any resources with other users. This kind of assault frequently results in bottleneck problems, which can slow or even stop NFV network services. Here is the architecture.

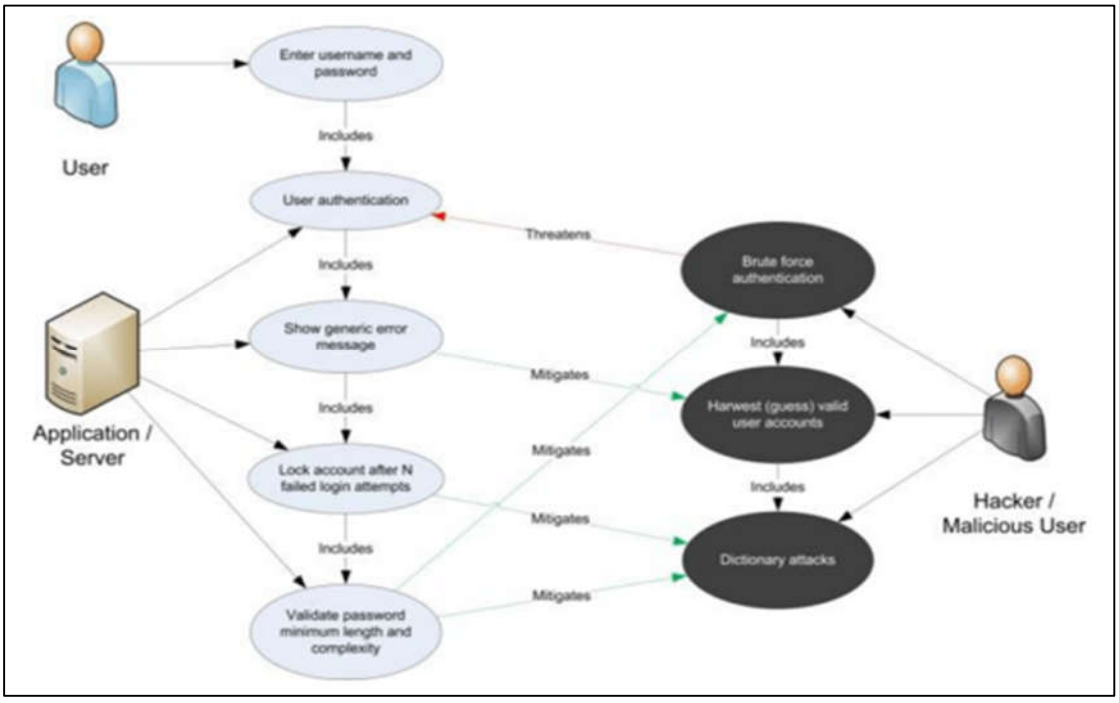


Figure 4. Misuse Flood Attack Architecture (Nafea Ali Majeed, Zaboon and Abdullah, 2021).

Case 1—DDoS

I'm Naveesen, and I'm in charge of this section's coverage of DDoS incidents that take place between 2017 and 2022. Later, I'll outline and go through the security issues that the topic I picked raises, as well as any potential security dangers that could develop if those issues aren't fixed.

 doi:10.20944/preprints202409.1369.v

On my topic, DDoS, renowned examples from the years 2017 to 2022 are currently on the rise. Let's begin the narrative. (Nicholson. P, 2018) In February 2020, a significant DDoS assault was launched on Amazon Web Services, the 800-pound giant of the cloud computing industry. This was the worst DDoS attack in recent memory, and it targeted an unidentified AWS client using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) reflection. This method relies on shoddy third-party CLDAP servers and increases the amount of data transmitted to the victim's IP address by 56 to 70 times. Over three days, the attack peaked at an astounding 2.3 terabytes per second.

Although the AWS DDoS Attack's effects were far less severe than they could have been, the attack's sheer size and its potential effects on AWS hosting customers' income and brand value are important. This assault vastly surpasses the previous record by 70%. (A10 Networks (2022)) The previous record was held on February 28, 2018, by the Memcached-based DDoS attack against GitHub, which clocked in at 1.35 Tbps. These "performance gains" in DDoS attacks have been gradually growing over the previous four years, with a sizable high-profile attack occurring every two years. The infamous Mirai botnet attacks of 2016 fit within this pattern.

Because of the "innovative" 620 Mbps multi-vector botnet attack against security expert Brian Krebs and the following disclosure of 1.2 Tbps from the French hosting business OVH, Mirai may be the most well-known collection of DDoS attacks. This DDoS assault was the first ever recorded, with a throughput of almost a terabit per second. Multiple versions of the Mirai botnet attack code were produced after attempts to conceal the creators' identities. These continue to worry us. Even though each of these DDoS attacks set new records, they all showed us how to build better defences.

The purported AWS attack allegedly included techniques such as Connection-less Lightweight Directory Access Protocol (CLDAP) DDoS reflection and amplification operations, which are typical of high-volume attacks. We continue to see reflection and amplification attacks as the weapon of choice, along with CLDAP and other usual amplification assaults such as exposed UDP Portmap, DNS, NTP, SSDP, and SNMP UDP-based services. These attacks have two major benefits: first, by amplifying the attacker's payload, they can generate 5x, 10x, or 100x the traffic from their requests; second, they can spoof to hide the attacker's identity while directing the payloads towards a specific target of their choice.

Although AWS's analysis is vague in terms of specifics, we do know that CLDAP is a well-known amplification technique and is not one of the most potent DDoS weapons available right now. The A10 threat research team looked at the threat presented by CLDAP in contrast to other DDoS weapons, and the findings paint an intriguing picture. The most current information from A10's DDoS Weapons Report for Q2 2020 indicates that CLDAP does not rank among the top five DDoS weapons. It is far less frequently used as a weapon.

We can observe that there are very few open CLDAP servers when compared to the top five. There are 116 Portmap guns for every CLDAP weapon. As the AWS DDoS assault demonstrated, although having a lower attack surface, it is still quite susceptible. To help you understand what I'm referring to in this situation, I've provided a statistic table that I discovered in the article you read.

 doi:10.20944/preprints202409.1369.v

DDoS Weapon	Number of Weapons	Weapons Frequency more than CLDAP
Portmap	1,818,848	116x
SNMP	1,673,070	107x
SSDP	1,671,128	107x
DNS Resolver	1,331,160	85x
TFTP	1,054,330	67x
CLDAP	15,651	0x

Figure 5. DDoS Weapons Analysis.

Compared to the top five countries, the United States possesses approximately 2 million DDoS weapons, but just 1,294 CLDAP weapons. This gun makes up just 0.13 per cent of the total. The lower numbers are not very surprising. It may be that enterprise IT teams that have moved application workloads to the cloud are unintentionally advertising these servers and may not be properly securing them because a small number of sizable cloud-hosting companies, like Amazon, display more weapons than typical high-profile networks (by ASN designation).

But now, I'm sort of discussing attack rates and contrasting these CLDAP attacks. Let's start our main topic by going over how they stopped the assault. (Porter, 2020) The event occurred in February and was halted by AWS Shield, a programme designed to protect customers of Amazon's on-demand cloud computing platform against DDoS assaults, malicious bots, and application vulnerabilities. Amazon described the incident in its Q1 2020 threat report. Due to the integration of AWS Shield DDoS mitigation systems with AWS edge services, the time to mitigate is reduced from minutes to less than a second. Before transmitting incoming connections to the service that is being protected, stateless SYN Flood mitigation methods inspect them through a proxy server.

What Is a CLDAP DDoS Attack?

The TCP-based LDAP protocol is complemented by a UDP-based directory lookup protocol known as CLDAP, or Connection-less Lightweight Directory Access Standard. When LDAP is used to get organizational resource data from a directory service database, CLDAP is designed to reduce connection costs (Networks, 2022; Sindiramutty, Tan, Lau, et al., 2024). However, as stated in the CLDAP RFC 3352, the CLDAP protocol was inherently designed with security weaknesses such as anonymous access, no integrity protection, and no confidentiality protection. A badly configured CLDAP server that is reachable through the internet will respond to all inquiries even if the CLDAP client is a fake. The size of the CLDAP responses might range from 56 to 70 times the size of the original request. This has a high amplification factor. Due to their high amplification factor, DDoS attackers typically employ CLDAP servers for UDP-reflected amplification attacks. At the time of writing this blog post, A10 weapons intelligence is keeping an eye on 15,651 CLDAP servers that are up and might be used to execute gigabit- or terabit-scale amplification attacks.

How to Protect Ourselves from CLDAP DDoS Attack

Because UDP port 389 serves as the UDP source port for every mirrored CLDAP packet, blocking or rate-limiting port 389 traffic from the internet is an effective DDoS mitigation strategy, especially

 doi:10.20944/preprints202409.1369.v

if CLDAP responses aren't expected to come from the internet. Alternative configurations include LDAP encryption and TCP.

Despite being the "attack of the moment," CLDAP is unlikely to be the next record-breaking DDoS attack. Instead, a DDoS amplification and reflection attack based on the most common DDoS weapons we see every quarter is more plausible. As a result, it's vital to maintain up-to-date knowledge of the most recent DDoS attack patterns, adopt zero-trust DDoS defensive best practices, and establish baselines for your traffic. To avoid being the focus of the forthcoming DDoS narrative, protect our network in advance. (Extrahop (n.d.)) Even if DoS attacks are simpler to thwart or prevent, DDoS attacks can still present a serious threat. We must make sure that the traffic's source address corresponds to the list of addresses for the site that is being claimed as its origin to avoid dial-up connections from being forged. Attacks commonly send queries to every device on the network, amplifying the attack. Limiting or eliminating broadcast forwarding wherever it is feasible might help stop attacks. Users can additionally disable the echo and charged services when it is practical. Our security staff will also be better equipped to respond quickly when DoS attacks are found by enhancing our incident response.

Furthermore, we need to make sure that our firewalls are, if possible, limiting traffic beyond the perimeter. We learn more about how regular inbound traffic appears the sooner we can spot the start of a DDoS attack. We can rapidly spot unexpected peaks thanks to real-time visibility and network detection and response (NDR), which uses machine learning to maintain a profile of how our network should look.

For everyone to start at the very beginning and work their way up to the most extreme defence, I've mentioned a few countermeasures that are open types from the very beginning. Even the simplest forms of defence, like setting a firewall and antivirus software, are necessary. This will serve as my DDoS attack defence strategy. DDoS attacks are becoming increasingly common and have the potential to cost systems billions of dollars in damage. It is challenging to fully protect against DDoS attacks since you have no control over the flow to your site. However, you will be far less likely to suffer if you utilize one of the services, avoid using inexpensive hosting, and are prepared for a DDoS attack if it occurs.

Potential Security Threats

A DDoS attack might result in a variety of consequences, depending on the nature of the attack and your level of preparedness (Mohiddin, Midhunchakkaravarthy and Hussain, 2023). The most obvious and immediate effect is that your website becomes overwhelmed and crashes. This indicates that any revenue we produce through the website won't be available to us until it is back up and operating. It also has an impact on our standing as website proprietors. Furthermore, delaying the site's restoration might hurt our SEO since we risk losing position if Google detects the issue when crawling our site (Kinsta, 2022; Sindiramutty, 2024).

A DDoS attack may increase the vulnerability of our website to hackers since all our systems are focused on putting the site back online and because the attack may have disabled security mechanisms (Kaur et al., 2024). Hackers may discover it easier to enter our site through a back door if the DDoS attack has succeeded in making it useless. Follow-up attacks like these might not always come from the same source as the requests that started the DDoS attack since an experienced hacker will know how to hide their tracks, utilize many IP addresses to attack our site, as well as conceal their genuine location.

A website that has been the subject of a DDoS attack must be rebuilt over time. It could also be expensive. If I don't know what's happened to my site and haven't prepared for the possibility of an attack, I might have to start over. If I don't deal with the assault soon away, it might have a long-term impact on my site's SEO and the profitability of my business. If my website is an e-commerce firm, its downtime might cost me money in revenue. To rebuild the website and make sure it is secure against future attacks, it could be necessary to employ a security expert or web developer.

 doi:10.20944/preprints202409.1369.v

Countermeasures—DDoS

According to my research, there are several methods we may employ to defend against a DDoS attack. Black holing, often referred to as sink holing, is the first. This will be explained in the upcoming section. This technique stops all traffic and directs it to a black hole, where it disappears. The disadvantage is that all traffic, whether good or bad, is disregarded, forcing the targeted business offline. Like this, packet filtering and rate limitation just shut everything down, denying access to authorized users.

Routers can be configured to prevent common ping attacks by banning unused protocols and invalid IP addresses (Zou, Fan and Ma, 2024; Waheed et al., 2024). However, routers typically fail to thwart more sophisticated simulated attacks as well as application-level attacks using genuine IP addresses. Firewalls can block certain attack-related traffic, but they are unable to carry out anti-spoofing, just like routers.

The intrusion detection system, which is the subject of my module, will be covered next. IDS systems will have the ability to detect anomalies, allowing them to recognize when valid protocols are being used as a cover for attacks (Driouch, Bah and Guennoun, 2024; Hussain et al., 2024; Dogra et al., 2021). They can be utilized to automatically limit traffic when combined with firewalls. On the negative side, they frequently generate false positives and need to be manually adjusted by security experts because they are not automated.

To decrease the consequences of a DDoS attack, the server must be set properly for the application. The resources that an application can utilize and how it will respond to client requests can be carefully defined by an administrator. Optimized servers have a possibility of surviving a DDoS attack when paired with a DDoS mitigation system.

The last two years, as well as the COVID-19 pandemic, have opened a brand-new amusement park for cybercriminals. The start of the pandemic caused chaos, and users were unable to prioritise their computer security over their worry about the unknown. Lockdowns around the world have caused a massive rise in online activity in many areas of daily life. Everything radically changed in the internet world, but let's encounter it, most of us were unprepared for it. Job, education, shopping for groceries, and even basic healthcare have all shifted almost purely digital. Streaming sites received so much more traffic than ever previously.

Major corporations with thousands or millions of staff members could not instantaneously safeguard every one of their devices, nor consider ways to avoid DDoS attacks. Companies that offer digital services had to modify their technologies to draw more web traffic than ever before. As per NetScout's report, fraudsters viewed this as a chance and initiated 9.7 million DDoS attacks solely in 2021. To complicate things worse, it represented a 3% decrement from 2020. To prevent DDoS attacks from rising tremendously, some cybersecurity countermeasures were implemented. You've most likely learned it a million times, but prevention seems to be the most effective method for safeguarding your resources from any type of cybercrime. If you do not even have in-house professionals, try employing a consultant or an organisation to assist you in strengthening your systems and figuring out how to avoid DDoS attacks.

According to (Team, 2022), one of the best practices that all cybersecurity experts suggest every organisation to implement is set up a DDoS response plan. Assume your corporation is the victim of a DDoS attack. Like any other cybercrime, your reaction must be quick to limit the losses and stabilize your systems. A very well-designed response plan will guide your squad and allow each other to respond swiftly in the event of a crisis. Because DDoS attacks are not comparable to other types of cyber intrusions, you need to get a precise mitigation strategy if you don't want fraudsters to capture you off guard. A DDoS attack has a significant influence on your connections than malware or a social engineering intrusion, as such your action plan must be adjusted to finest react to that instance.

First and foremost, a response plan must establish a team of individuals who will be responsible for putting it into action. Your rescue team must include individuals from different workgroups, such as the IT security department, engineering, and HR and public relations experts. Make sure that your strategy clearly defines the measures required to locate and encapsulate the source of the threat to minimize contamination. The very next phase is to evaluate the damage that has occurred before

 doi:10.20944/preprints202409.1369.v

beginning to rebuild your systems and networks. To prevent the spread of fear and panic, your HR team must assist with private memos and direct staff members regarding how to deal with the situation. Public relations professionals must handle external communications and make sure that the proper number of details meets the community.

Furthermore, another countermeasure that could perhaps prevent DDoS attacks is to fortify the network security systems and infrastructure (Team, n.d.). When launching a DDoS attack on your organization, intruders regularly look for discrepancies in your system security. Your job is to make sure they do not even find that prospective point of entry by utilising all the fastest internet security practices. Begin by determining the best software solutions for your requirements. The very first lines of defence are a strong firewall, detection systems for intrusions and anti-virus applications. Consider adding additional layers of protection such as anti-spam spam detection, intrusion prevention, or online security tools, to protect against various threats.

On the other hand, users must also protect their internet infrastructure and fortify their equipment to deal with unexpected network congestion. This allows you the opportunity to investigate the abnormal traffic activity and respond before your system becomes overburdened. The industry also provides tools for preventing and stopping DDoS attacks. Consult with your cybersecurity professionals to determine the most suitable and effective alternatives for your company.

In addition, to prevent possible DDoS attacks, it is essential to monitor your network traffic (Pillai and Polimetla, 2024). However, if you do not carefully watch your internet traffic and search for evidence of a DDoS attack, you will not be able to respond in time. It is important to always keep in mind that this type of intrusion causes a rapid spike in traffic, and the offenders may evaluate your system by discharging a relatively small attack to see if it goes undetected. Those traffic spikes should indeed be interpreted as risk factors by your squad. Other signs of a DDoS attack include a huge packet for a single platform on your webpage (when you aren't planning to host any special events), occasional web glitches, and spotty internet access (Kumar et al., 2024). It is also essential to train your squad to respond immediately if such potentially malicious activity is detected. That would provide you with sufficient time to avoid a major disaster.

Besides, making the infrastructure and network able to handle any thunderous rise or unexpected spike in traffic represents one of the key Distributed Denial-of-Service mitigation best practices. While moving to the cloud for operations is beneficial in minimising threats, it does not inhibit DDoS attacks. The cloud provides more bandwidth than any on-premises quick fix. Using a worldwide Content Delivery Network is the most effective method for making infrastructure and networks more resilient (CDN). The CDN distributes data centres across large networks, caches the application, and prevents easy accessibility to the source server. Furthermore, whenever a configurable WAF is used, it provides built redundancy and instantaneously scales to accommodate whatever burden.

Next, DDoS attacks can also be avoided by implementing multi-layered DDoS protection Indusface blog (2022). Previously, DDoS attacks have mostly been Layer 3 or 4—volumetric attacks on the network or transport layers. DDoS attacks nowadays come in a variety of flavours, each of which specifically targets a different layer (network layer, transport layer, session layer, application layer) or mixture of layers. You could perhaps employ a multi-layered and pragmatic approach to DDoS detection, prevention, and safeguards. To put it another way, your DDoS mitigation alternative should provide multiple layers of defence against every form of Attack, not just volumetric types.

Another method that should be practised by every organisation to ensure DDoS attacks are prevented is to perform a vulnerability test (Kumar and Keshari, 2024). It is important to recognise your network flaws well before cybercriminal does. A vulnerability assessment includes identifying security flaws so that you may modify your infrastructure and be adequately equipped for a DDoS attack or other cybersecurity threats in a broad sense. Evaluations will assist you in safeguarding your system by looking for security flaws. This is done by conducting an inventory of all connected devices, including their objective, status monitoring, and any negative consequences associated with

 doi:10.20944/preprints202409.1369.v

them, in addition to which equipment must be ready for improvements or future analyses. This will assist you in determining your firm's vulnerability and optimise any security investments.

Outsourcing DDoS attack mitigation to the cloud has so many advantages (Guenane, Nogueira and Serhrouchni, 2015). Cloud service providers offering elevated levels of information security, such as firewalls and threat detection software, could indeed assist in protecting your investments and system from DDoS fraudsters. The cloud also has more frequency band unlike many private networks, so it is more likely to malfunction if subjected to enhanced DDoS attacks. Furthermore, reputed, and reliable cloud providers provide network redundancy, trying to replicate duplicates of your data, systems, and hardware so that if your server had become corrupted or inaccessible due to a DDoS attack, you could indeed immediately shift to secure access on backed-up versions.

Given that we are currently experiencing a DDoS attack, we are compelled to take drastic action. But as planning makes more sense than winging it, the following article includes some of the most widely utilised mitigation techniques at various levels, from a hobbyist server to an e-commerce site to an ISP (Mirre, 2021).

BGP Routing

A network of autonomous systems, or groups of IP routing prefixes, make up the internet. The most frequent owners of autonomous systems are Internet service providers, although other significant institutions, including colleges, may also be the owners of a system with a special identification number. The protocol that enables the transmission of routing data between autonomous systems is known as the Border Gateway Protocol. For instance, this protocol includes the calculation of the shortest path between autonomous units. In addition, BGP is used at Internet Exchange Points (IXP), which make up the physical network that ISPs use to route traffic between their autonomous systems. The following techniques can be used by IXPs and ISPs on the internet level to mitigate DDoS attacks (Wieren, 2019).

Blackholing

It is perhaps more specifically "Remote Triggered Blackholing" (RTBH), which is utilised inside of one or more automated systems to drop network traffic. Blackholing makes network traffic be discarded by sending it to a null route as opposed to the intended route. All traffic to or from a specific range of IP addresses is dropped because of BGP announcements to all other BGP routers. These announcements can be made upon the identification of a DDoS attack by either the victim or a network intermediary device. It should be noted that "blackholed" traffic is solely dropped based on the IP prefix of either the source or destination of the traffic; no other characteristics of the traffic are considered. As a result, lowering traffic using RTBH can effectively mitigate a DDoS attack, but, likely, decreasing traffic will also drop valid innocuous traffic (Wieren, 2019).

BGP Flowspec

The BGP extension makes it possible to filter, analyse and drop traffic by predefined flow specifications. Access Control Lists (ACLs) can be disseminated throughout all BGP Flowspec-enabled routers using BGP Flowspec. These ACLs comprise filter rules based on 12 distinct parameters, including, for example, IP addresses, ports, and TCP flags, which are present in OSI layers 3 and 4. BGP flow spec, which filters traffic based on more criteria than only IP address prefixes, has the potential to counter DDoS attacks more than RTBH. Studies have shown that using BGP flowspec, systems like RADAR and Stellar, for instance, can automate both the detection and mitigation of DDoS attacks (Wieren, 2019).

BGP, as previously mentioned, is used at a high level by IXPs and ISPs to facilitate communication between various autonomous systems. BGP thereby processes large amounts of internet data, including various types of internet traffic. It is difficult to accurately separate DDoS attack traffic from legitimate traffic, even with BGP Flowspec. Additionally, BGP Flowspecs rules are constrained by the fact that only 12 distinct parameters and no additional packet information are allowed to be used. In addition to this restriction, a BGP router is only permitted to apply a certain set of rules. For instance, a maximum of 3000 rules is indicated in the documentation of Cisco's BGP Flowspec-enabled routers. However, here we can deduce that, compared to RTBH, DDoS traffic mitigation with BGP Flowspec may be possible in a more granular manner (Wieren, 2019).

 doi:10.20944/preprints202409.1369.v

Sinkholing

Moving on, this technique works by directing only malicious traffic off from its target. Typically, it does this by identifying DDoS activity using a predefined list of IP addresses that are known to be associated with malicious operations. False positives can happen less frequently and with less collateral damage than with blackholing, but because normal users can also use botnet IPs, this is still vulnerable to false positives. Furthermore, IP spoofing, a characteristic of network layer attacks, is unlikely to be affected by sinkholing as such (Mirre, 2021).

Scrubbing

It is a step up from random full-fledged sinkholing. All ingress traffic is directed through a security service throughout the scrubbing process, which may be carried out internally or even outsourced. Using heuristics or just straightforward rules, malicious network packets are recognised based on several criteria. This includes their header content, size, type, point of origin, etc. Scrubbing must be done at an inline rate without affecting authorised users. The scrubber service, if outsourced, has the bandwidth capability to withstand the hit that we do not. There are at least two approaches, namely the BGP and DNS approaches. We shall now discuss the BGP one. When an attack is detected, we stop declaring the prefix that is currently being hit and call our scrubbing provider to begin announcing the subject prefix, receiving all its traffic, including the attack traffic. The scrubbing service cleans the traffic and sends it back to us. When we scrub internally, we must do it on our equipment, which needs to have enough bandwidth (Mirre, 2021).

At first, when greater rates of packets with source ports of protocols identified to be utilized for DoS/DDoS attacks begin arriving on our network (such as 123 or 53), we should be performing network analysis and should start signalling to our upstream providers because they can likely handle it better than us and have just as much interest in doing so as we do. However, volumetric attacks that transfer traffic in smaller packet sizes will still use more CPU power, especially on non-dedicated networking hardware. Regardless of whether we are currently under attack, we should always rule out, drop, and avoid receiving traffic that appears to originate from our network because it is obviously spoofed and cannot exist naturally (Mirre, 2021).

The Bogon Reference, which Team Cymru has long maintained, is a collection of bogons listings. Routes with bogus prefixes should never be listed within the Internet routing table. A packet having an address from a bogon range shouldn't be routed over the Internet. In DoS/DDoS assaults, these ranges are frequently used as the source addresses. Bogons are Martian packets and netblocks that the Internet Assigned Numbers Authority (IANA) has not assigned to a regional Internet registry (RIR). We should put up automated bogon lists from Team Cymru that are updated and curated to assist the bogon ingress and egress filtering via HTTP, BGP, RIRs, and DNS. If we have our own ASN, are directly linked at an IXP, lack upstream RTBH support, and have no other options, all we need to do is to determine who is forwarding the malicious traffic, drop the session if it's possible, and start receiving traffic from other peers (Mirre, 2021).

Intrusion Detection System and the Intrusion Prevention System

The systems that identify and prevent an intruder from getting through security measures. An IPS or IDS of this sort can run on a single computer or an entire network of devices (Knapp and Langill, 2011). An IDS or IPS is characterised by the fact that it often consists of numerous components and may analyse various events and objects at various locations within a network. A system that only monitors and detects intrusion rather than attempting to stop it is considered an IDS (Kizza, 2024; Khairandish et al., 2022; Kok et al., 2019). Since most systems in practice include both detection and thwarting capabilities, the terms IDS and IPS are frequently used interchangeably. From this point forward, this study will commonly refer to an IPS because it includes detecting techniques. Only the detecting component of a certain system will be specifically referred to as an IDS. Like the categorization of DDoS protection techniques, IPSs can be divided into signature-based and anomaly-based systems (A, S and B, 2024). Signature-based systems detect attacks using specific rules drawn from well-known DDoS attacks, while anomaly-based systems do (Altulaihan, Almaiah and Aljughaiman, 2024; Lim et al., 2019) so by looking for unusual behaviour on all different kinds of

 doi:10.20944/preprints202409.1369.v

system components. In anomaly-based systems, normal traffic is first collected and utilised as a comparison against incoming traffic.

The data is then subjected to statistical tests to categorise the traffic as benign or malicious. Since IPSs frequently have access to several resources in a network, anomaly-based DDoS defence methods do more frequently occur in IPSs than other DDoS defence mechanisms. When it comes to hybrid systems, both signature-based and anomaly-based strategies are used in them. A signature-based detection approach typically comes first in line in hybrid systems so that it can identify and filter out all known threats. After that, an anomaly-based system can try to filter this traffic by detecting missed DDoS attacks (Wieren, 2019; M. Saleh et al., 2022).

In general, the primary drawbacks of signature-based detection are the inability to identify unknown assaults and the difficulty in keeping a signature database current. The benefit of signature-based detection is that it produces a low percentage of false positives, nevertheless. On the other hand, anomaly-based detection has the benefit of being able to identify fresh DDoS attacks. The less precise classification of traffic and the difficulty in responding to an assault are two drawbacks of anomaly-based detection.

The focus of more recent studies has consequently been on hybrid detection systems because they can offer the benefits of both approaches. The ability to create signatures from anomalies that are discovered is a benefit of a hybrid technique since these signatures may then be applied as rules in signature-based methods. A hybrid system's drawback is that it can become challenging to implement and can also become complex (Wieren, 2019; Ramanjot et al., 2023; Saeed et al., 2022; Sangkaran et al., 2020, 2019).

IP masking

This frequently used approach relies only on the fronting service's ability to withstand the attack because it has accessibility to more bandwidth than what the attacker could provide, as well as on the user not disclosing sensitive information. All traffic passes via what is essentially a huge proxy, including possibly hazardous traffic. Before claiming it to be a win for us overall, it is important to recognise that it also has significant privacy implications because now another service terminates TLS on our behalf and sees everything that is sent to us before eventually forwarding it back (Mirre, 2021; Shah et al., 2024; Sood et al., 2022).

Network Firewall

network firewall's function is to create a barrier between two networks by filtering network packets According to that definition, BGP Flowspec qualifies as a network firewall. But unlike more conventional firewalls, which can be found on all kinds of network edges, BGP Flowspec can only be placed on BGP-enabled routers that are available at the ISP and IXP levels (Yadav and Likhar, 2024).

The setup or processing speed of the network firewalls can restrict their use against DDoS attacks. A network firewall must be able to filter packets at least as quickly as they are arriving if it is to be effective in reducing the impact of a DDoS attack (Hnamte et al., 2024). A congestion that results in a denial of service may occur if the network firewall is unable to process those packets in time. As a result, firewalls need to be carefully configured and be as quick as possible. Thus, network firewalls may be susceptible to DDoS attacks based on their behaviour and other characteristics (Wieren, 2019).

Web Application Firewall

An application used to safeguard web applications. This is especially important today since it allows system administrators to create security logic in a single location and safeguard potentially susceptible applications. Network layer attacks cannot be handled by this technology since it operates on the application layer of the OSI model and is frequently used as a component or module of a web proxy (Felix, 2024). Although not insignificant, it is vital to avoid making any assumptions and understand exactly what layer of protection using WAF offers. Applications are not typically deployed with ports directly exposed to the Internet, at least not by CBP (current best practices).

A sensible approach to proxying access to resources produces a variety of choices for authentication/authorization and protection scenarios, as well as a variety of ways to utilise the resources more efficiently. For starters, using a caching proxy server makes it simple to cache any web material that is needed. It frequently also makes it possible to set custom access controls. There

 doi:10.20944/preprints202409.1369.v

are additional hosted WAF options available, however they have the same privacy consequences as IP masking solutions. The next section will outline several techniques for reducing DDoS attacks using WAFs (Mirre, 2021).

To determine if a user request is part of a DDoS assault or not, request analysis can indeed be employed. Those queries need to adhere to a specific application layer protocol. For instance, HTTP, a widely used protocol on web servers, is a target for many DDoS attack types (Ming, Leau and Xie, 2024). HTTP request inspection can be used with WAFs like ModSecurity or Modevasive to find certain kinds of DDoS attacks (Gojali et al., 2024). These open-source WAF examples can be set up to function as a component of an Apache server.

By posing a specific challenge to the user, CAPTCHAs are frequently employed on web servers to distinguish between human users and bots. Additionally, DDoS attack requests coming from bots can be filtered using those challenges (Chahal, Bhandari and Behal, 2024). Only human-readable images may be included in the challenges offered to users, but they may also incorporate the identification of specific human behaviours. Analysing mouse movements can be used as an example of performing human behaviour detection. The benefit of WAFs is that they can identify individual DDoS attacks while other areas cannot. The drawback is that not all DDoS attack types can be mitigated because WAFs can only identify specific DDoS attacks at the application layer. Additionally, processing requests at the application level is slower than processing them at the network level. Moving the filtering component to a network level is one solution to this problem (Wieren, 2019).

Source Rate Limiting

Limiting the number of connections, a client can establish in a given period is sensible as a general precaution (Shete and Gosavi, 2021). The same holds for a cap on the number of connections a client can still have open at once, which can even thwart Slowloris, a specific kind of denial-of-service attack tool. Rate-limiting is typically configured on a proxy or WAF. However, it is possible to incorporate rate-limiting into apps. Fail2Ban is a well-known pluggable rate-limiting solution that may be used with SSHd, HTTP, or a variety of other endpoints (Mirre, 2021).

Scanning

Some studies scan the complete range for the most used amplification protocols. In other cases, only a segment and to be precise, a set of preset protocols on a particular set of IPv4 addresses in a particular area is scanned. The researchers then inform the ISPs that amplification-based attacks are likely to use those addresses (Ismail et al., 2021).

Deflecting

Honeypots are utilised to analyse and thwart actual Internet threats. The honeypots can compile a list of IPs that are attempting to utilise the honeypot as a reflector. The ISPs can then receive these IPs to add to their blacklist (Ismail et al., 2021).

Deployment

DDoS defences can also be grouped according to how they are deployed. Either the victim end or the reflector end is where the solution is implemented. Most reflector-end solutions are designed to concentrate on IP spoofing. The claim is that if the attacks are stopped at their source, victims would not need to implement many intricate solutions (Ismail et al., 2021).

Many companies either design separate traffic filtering devices or include DDoS mitigation capabilities into equipment used primarily for firewalling or load balancing. These gadgets have varying degrees of effectiveness. Nobody is perfect. While some legitimate traffic is dropped, unauthorized traffic will continue to reach the server. The server architecture must be robust enough to handle this demand while yet offering dependable client service.

DDoS attacks are deadly, covert weapons that might put a company out of business (Merkebaiuly, 2024). The threat presented by DDoS attacks is expanding along with our reliance on the Internet. I hope I didn't get off topic as usual and that I covered all the countermeasures I needed to talk about. Now that I've finished talking about DDoS attacks, my other group members will address the next topic.

 doi:10.20944/preprints202409.1369.v

Proposed Countermeasures

We advise a comprehensive technical solution that employs cooperative management, integrity of protection to defend and distributed multipoint detection to counter the DDoS attack.

1. Collaborative Management

The management server must dispatch the defence device as needed to defend against a DDoS attack with high traffic volume using unified techniques. As a result, it's important to handle devices consistently and spend defence resources sensibly. Additionally, single-point protection schemes' drawbacks should be avoided. The attack response range is widened as a result, and the backbone network's high throughput is ensured. Additionally, feedback must be gathered for filtering, comparing, and analysing.

2. Integrated protection

Attackers typically utilise DDoS attacks to deplete server or network resources before moving on to other types of attacks, such as spoofing, unlawful data collection, etc. Raising defence awareness and establishing an integrated information protection strategy, such as privacy protection, are therefore essential.

3. Distributed Multipoint Detection

Since large-scale traffic DDoS attacks might originate from various locations within networks, the attack traffic of a single location which is relatively lesser scale, is difficult to identify. So, rather than centralised single-point detection, dispersed or distributed multipoint detection is more by the traits of DDoS attacks. In conclusion, distributed attack detection mechanisms can use area nodes, which are dispersed throughout the network, to recognise attacks and take appropriate responses (Di et al., 2019).

Malware Background

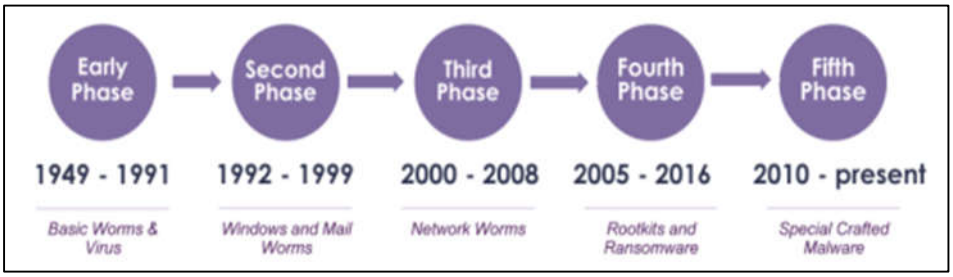


Figure 6. The timeline of malware evolution in 5 phases (Alenezi et al., 2022).

In terms of ransomware, it falls under the malware category. Malware is malicious software that is secretly installed on a computer or network to steal user data and information while also getting around the system's access controls (Iqbal et al., 2024). Malware comes in a variety of forms, each with a unique set of objectives and methods for entering a computer system (Vasani et al., 2023; Vijayalakshmi et al., 2021). As previously mentioned, ransomware is another category of malware that encrypts all the data on a system and demands payment as ransom to unlock the files. Then there is the Trojan Horse program, which impersonates a regular, trustworthy program (Riadi, Sunardi and Aprilliansyah, 2023). It deceives users into downloading it onto their devices, and when they run the program, the attack begins. Another common form of malware is viruses. It replicates itself and copies itself into other system files, along with their malicious code. Like biological viruses, they have a rapid spread and can harm a system's core operations because they are typically contained within an executable file. In addition to the one already mentioned, there are many other types of malware, but they all pose a threat to the three main principles of cyber security, namely Confidentiality, Integrity, and Availability (CIA) (Bhol, Mohanty and Pattnaik, 2023).

 doi:10.20944/preprints202409.1369.v

Five stages can be used to divide the development of malware, during which new malware subtypes can be seen to emerge (2020). Early versions of malware were created to find security holes in MS-DOS systems rather than to steal data from a system (Ling et al., 2023; Alkinani et al., 2021). A brief system crash was the most harm malware has ever done during this phase. Viruses and worms were the most common types of malware at the time, and they spread through infected floppy discs as well as the ARPANET. In the second phase, hackers focused more on creating mail worms and macro worms to infiltrate the Windows operating system (Ferdous et al., 2023). Antivirus software was created at this time to combat certain kinds of malware.

During the third phase, when internet usage is beginning to gain popularity and more people are beginning to understand how to use it, malware assaults mostly come through email attachments, unsafe downloads from suspicious websites, and open network shares (Aslan et al., 2023). Because security was less effective than it is now, cyberattacks were able to spread network worms to users quickly, which left new internet users naive about malware assaults (Tatipatri and Arun, 2024; Tiwalade et al., 2023). Rootkits and ransomware first appeared in the fourth stage. Attackers frequently use phishing emails, fraudulent downloads, portable devices, etc. to get access to their targets (Varshney et al., 2024). Most people at this age are aware of these virus assaults and take some precautions when using the internet. Now, the major goal of malware attacks is for the perpetrator to get quick money by promising to return the data of their victims in exchange for payment. Using the victim's operating system without their knowledge or agreement, a rootkit is software that gathers information covertly.

Finally, in the fifth phase, organizations build malware specifically to harm their competitors. Instead of a random cybercriminal wanting to make quick cash, one might argue that enterprises and the military have now turned malicious software into a weapon. Malware assaults might seriously harm corporations instead of damaging actual human lives since data and information are so crucial these days. Who knows, perhaps malware will affect our lives more significantly in the future.

Case 2—Ransomware

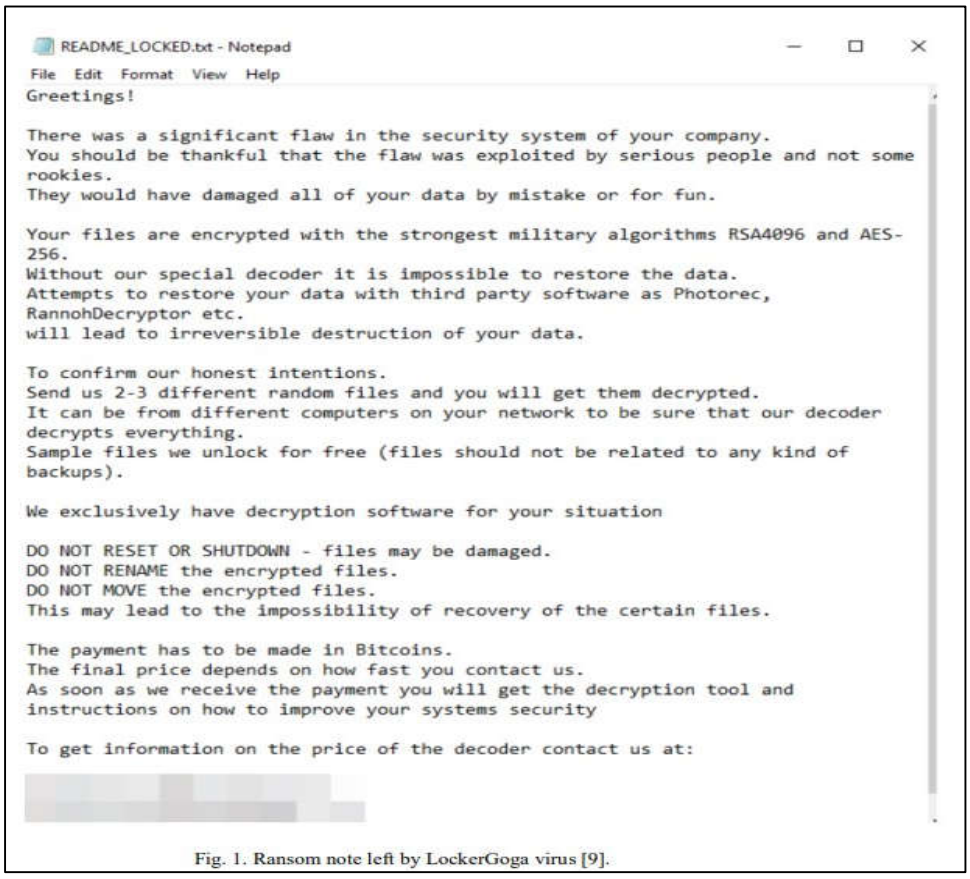
The following malware attack case is a ransomware attack that occurred on March 19, 2019, at Norsk Hydro's global headquarters in Norway. The ransomware used in this attack is known as LockerGoga, which was a brand-new variant at the time. It was discovered that the threat actor uses brute force attacks, password guessing, and phishing to acquire domain administrator access before spreading the LockerGoga ransomware. To execute an attack and encrypt the files on all connected devices, they then copy the malware to specific locations in the system. Since the attackers changed the administrator passwords and used logoff.exe to log off all users, LockerGoga differs from other ransomware in that it makes it much harder for the company to pay the demanded ransom.

Norsk Hydro's headquarters were the target of the LockerGoga ransomware attack, which resulted in production halts in the US and Europe. The business had to immediately switch to manual operations while defending against this deadly attack, shutting down the network throughout the offices (Nargiza, 2022; Chesti et al., 2020). Later, when the company management told their 35,000 employees to avoid connecting to the network and even logging into their computers for the week, they discovered that the attackers had breached their network using a ransomware program called LockerGoga. The hackers demanded a ransom, but Norsk Hydro had backups and had no plans to pay. After a week, business as usual had resumed. Units are currently operating at 70 to 80 per cent capacity using manual processes. The financial impact of the ransomware attack was estimated by Norsk Hydros in a statement to be between $35,000,000 and $41,000,000 during the first week of the response. (Nayak, 2019; Gopi et al., 2021).

When Norsk Hydro's computer systems were first subjected to the ransomware attack, the staff members observed unusual behaviour. After that, their system was locked out, and all of the computers in their office and branches in 40 other countries went dark. One of the employees discovered a text file containing a ransom demand from the attackers on the company laptop. Additionally, the attackers wanted the company to know that all of their files had been encrypted with military-grade encryption, like RSA4096 and AES265, and that any attempt to restore them using

 doi:10.20944/preprints202409.1369.v

unofficial software would result in the permanent deletion of those files. To convince Norsk Hydro that they truly had all their data, they even offered the company to send an unrelated file that would be encrypted and decrypted to test the attacker's encryption. Finally, the attackers demanded payment in Bitcoin in exchange for returning Norsk Hydro's files and giving them advice on how to make their systems more secure.


README_LOCKED.txt - Notepad

File Edit Format View Help

Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

Fig. 1. Ransom note left by LockerGoga virus [9].

Figure 7. The ransom demand text file from the attacker (What is Ryuk Ransomware? A Detailed Breakdown, 2024).

What Is LockerGoga Ransomware and How Does It Work?

LockerGoga is a ransomware assault that, like other ransomware, infiltrates a system, encrypts all the data on it, and then demands that the owner pay a ransom to have the contents decrypted. While the prior version of LockerGoga could only encrypt the files, the most recent version of LockerGoga can reset the user's password, log them out of their accounts and devices, and prevent them from signing back in, thereby denying them access to both their devices and their files. LockerGoga doesn't utilize its network, so some researchers assume that the ransomware is specifically created to assault a particular target that the attacker wishes to breach. Additionally, the malware's code is built to avoid detection by sandboxes and machine learning techniques, which might make it challenging to find in the future.

According to TrendMicro Security's investigation, LockerGoga drops and runs the ransomware via the PsExec tool on Norsk Hydro's computer system (Trend Micro, 2022). However, to use the PsExec program, the attacker would have needed the Norsk Hydro victim's login information. This raises the possibility that the attacker must have acquired the credentials via other stealthy cyberattacks like spear phishing, which primarily uses social media, emails, etc. to target specific individuals. LockerGoga's destructive routines could also provide clues on how it is distributed. LockerGoga's deployment was probably targeted and meant to interfere with business operations

 doi:10.20944/preprints202409.1369.v

because the ransomware neither provides the organization with an opportunity to restore the data nor expressly requests payment. This might also be interpreted as an effort by Norsk Hydro's competitors to sabotage their business.

As previously said, LockerGoga essentially modifies user accounts by changing passwords and logging users out of their accounts and devices. The ransomware would then change its location to a temporary folder and rename itself with the use of a command line (cmd) that does not have the file paths of the encrypted data. Immediately after, the ransomware drops a text file on the victim's desktop folder that contains a message. It is also discovered that LockerGoga uses the CreateProcessW function with command lines to list the infected machine's Wi-Fi (internet) adapter to prevent the system from being connected to any external connections. This process is completed before the ransomware renames itself and forges a new path for itself.

Countermeasures

The countermeasures against any kind of ransomware assault are often rather similar (Hansen et al., 2024; H. Ashraf et al., 2023; Humayun et al., 2020 and 2021). The most popular preventative measure to take before becoming vulnerable to attacks is to regularly back up all data to an external device. Thus, since we already have backups of all the files, we don't need to pay the attackers' ransom to unlock our files. As seen in the instance of Norsk Hydro, the attacker may encrypt our files using military-grade encryption so that their victims would have no choice but to rely on their mercy and pay the ransom. Therefore, having a backup minimises the likelihood that you will lose your data to malware attacks while simultaneously saving you money by preventing the need to pay the attackers to decrypt the data that you still have.

In addition, other security precautions like application control and behaviour monitoring might be useful in detecting unauthorised system alterations and executions. To prevent any illegal access to the network, for instance, every kind of password change that is spotted in the network should be tracked down and identified. In addition, since attackers may come from within the network as well as from the outside, it is important to keep an eye on how users and accounts behave. By taking these precautions, companies may be able to stop any stealthy actions that malware attackers may take to make their systems more vulnerable to ransomware threats in the future.

The next defence is a little less sophisticated. To stop attackers from quickly breaching the network, it may be very helpful to educate the staff about spoofed emails and unsafe websites. According to speculation in the instance of Norsk Hydro's ransomware incident, the attacker may have used the phishing tactic to get passwords and deploy their LockerGoga virus in the system. How so? Maybe a staff member unintentionally opened a questionable attachment from an email or used the company's computer and network to browse a dodgy website. The workforce might act as the first line of defence against any future ransomware attacks if they are aware of the techniques attackers may use to access the company's system.

Norsk Hydro could protect its system administration tools that the attacker may use in the future since they did not implement any countermeasures, or at least none that have been publicly revealed by Norsk Hydro (Mott et al., 2024). To limit additional exposure of sensitive and important data for the organization, Norsk Hydro may have also started using network segmentation and data classification. Network segmentation makes it more difficult and time-consuming for hackers to access the network, much less the company's system. Finally, Norsk Hydro should deactivate any outdated or third-party elements of their system that might be abused by potential attackers in the future. If Norsk Hydro were to pay the ransom money and the attacker maintained their promise of disclosing the faults and how to enhance their system, perhaps the attacker would list these problems that Norsk Hydro should address. But then again, ransomware attacks like LockerGoga are improving every day, with various varieties taking advantage of freshly found security vulnerabilities in computer systems. One might either pay the ransom to recover the encrypted files or take steps to prevent any significant data loss from the ransomware assault. Once the ransomware virus has seized control of your machine, there is nothing that can be done to remove it. Prevention is better than cure, as they say. More countermeasures are stated below:

 doi:10.20944/preprints202409.1369.v

i. If there is a highly competent attacker and a malevolent insider, keeping them from accessing the network and system is insufficient even with high-level security measures. To ascertain and comprehend what is happening in the network, it is crucial to monitor and follow an attack's Cyber Kill Chain (CKC). The system should use a variety of monitoring tools, such as an Intrusion Detection System (IDS) that can track, gather data, examine, and quickly identify an attack. Thus, every interface of the edge gateway should have an IDS sensor installed (Al-Hawawreh et al., 2019; Humayun, Sujatha, et al., 2022).

ii. In the chain of cyber defence, humans are the weakest link. We lose focus when we are busy or distracted, click on links, or access malicious attachments. To overcome this, it is required that security awareness training be provided in the Learning Management Systems (LMS) of every firm to guarantee that staff members can react appropriately to threats (Ghotbi, P, 2021). This act may assist users in changing from being targets to defenders who can recognize, avoid, and report fraudulent attachments by keeping them informed of the strategies and tactics used by cybercriminals. This contributes to the security of the company's operations, finances, and data. User awareness should emphasize safe computer procedures and precautions. Users should be trained to recognize suspicious activity because they are the last line of protection. Furthermore, to help users, increase their knowledge and awareness of typical security concerns, they should also consider adopting solutions that offer routine microlearning (Papez and Shields, 2021). Organizations should routinely check their employee's knowledge as well. It has been shown that awareness and training are insufficient if there aren't regular knowledge assessments. Running internal phishing campaigns is a common strategy to determine user preparedness and response. This technique involves sending employees a carefully designed phishing email. A warning page is displayed after a person clicks the link. This would help to educate them practically as well (Ghotbi, P, 2021).

iii. In comparison to a typical firewall, next-generation firewalls include more distinctive features, such as enhanced traffic filtering that involves a more thorough examination of packets up to the application layer in an Open System Interconnect (OSI) paradigm or the transport and framework levels. Additionally, they incorporate stateful inspection, NAT, port and protocol filtering, virtual private networks, and anti-malware security (Al-Hawawreh et al., 2019).

iv. Backup systems are another common defence against ransomware assaults. Even though almost all businesses have several backup systems, they frequently fail to function when ransomware outbreaks occur. Data on the victim's computer will initially be encrypted when it becomes infected with destructive ransomware. The ransomware will then encrypt the data kept on the NAS (Network Attached Storage) and Internet-based cloud file systems that are mounted on the victim's PC remotely. Since those remote storages are virtually often used to store backup data and since they are typically automatically mounted on the victim's machine. As a result, both the source data and the backup data are often encrypted in destructive ransomware attacks, making data recovery difficult. Given the potential of damaging ransomware and the requirement for data recovery, a safe and reliable backup system with high usability is necessary (Jin et al., 2018; Javaid et al., 2022; Jayakumar et al., 2021; Jhanjhi et al., 2020).

v. All hardware, mobile devices, operating systems, software, and applications, including cloud storage and content management systems (CMS), should be patched and kept up to date. If can, use a central patch management system. Apart from that, to stop programmes from running in frequent ransomware sites like temporary files, implement application whitelisting and software restriction policies (SRP). Furthermore, w We can also impose restrictions on Internet usage. We should consider ad-blocking software and use a proxy server when accessing the Internet. We should limit access to popular entry points for ransomware, like social networking sites and personal email accounts (Ransomware: Facts, threats, and countermeasures, 2019).

vi. Despite extensive training and ongoing talks about ransomware, businesses continue to fall prey to these attacks. To manage cyber events, the National Institute of Standards and Technology (NIST) offers a reference framework. Having a strong "react" and "recovery" plan is necessary for ransomware attacks, even though putting in place detective and protective procedures is crucial. To deal with ransomware assaults and defend against the most recent ransomware threats, it is important to have a thorough plan and step-by-step runbooks (Ghotbi, P, 2021).

 doi:10.20944/preprints202409.1369.v

vii. When ransomware is discovered in a portion of the network, breaking the network up into smaller sections enables us to keep it under control. Many legacy networks continue to operate as sizable /8 or /16 flat subnets. When ransomware infiltrates those networks, it can quickly infect many hosts. In this circumstance, it will be challenging to separate and contain the affected endpoints (Ghotbi, P, 2021).

viii. An efficient antimalware suite should be used. Security technologies are available that can spot ransomware-specific behaviour and stop the infection before any damage is done (Wisser, 2020).

ix. As was already established, the objective is to manage and contain infected hosts as soon as they are discovered. Isolating a host may be simpler in virtual settings. However, to investigate and take corrective action in physical environments, we might need to physically unplug the network connection and operate on the computer console. The remediation strategy and runbooks should be very specific about the isolation and confinement procedures for various environments (Ghotbi, P, 2021).

x. To stop infection spread, we must quickly detach the infected system from the network. In addition, we need to identify the data that was impacted since some sensitive data may call for further reporting or mitigation efforts. We can also try to find out if a decryptor is accessible. No More Ransom! and other online sites can be helpful. If not, we should try recovering files from routinely kept backups. Finally, such ransomware attacks should be reported (Ransomware: Facts, threats, and countermeasures, 2019; Fatima-Tuz-Zahra et al., 2020).

Email-based security is one of the comprehensive solutions that we suggest using. This solution includes threat-informed email protection, anti-spam solutions, and email authentication controls. More and more ransomware attacks are originating via email as their main vector. One of the first mitigating techniques is having an email protection system that obtains threat intelligence from reliable sources. Threat-intel authorities disseminate known ransomware Indicators of Compromises, which are regarded as the first line of security.

Then, to prevent phishing emails from entering the network, users need to adopt an anti-spam solution. To filter out all the potentially hazardous incoming messages, the user only needs to set up their anti-spam settings on their email provider. Consider including a tag alerting users to the risks of opening attachments and clicking links in all emails from outside sources. Along with examining several email attributes including the email header, sender's IP address, reputation, and message body, users should be able to recognise different threat techniques and trends. Additionally, users can enforce email authentication through mechanisms like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and DMARC, block any attempts to send emails from trusted domains that are not authorised, and dynamically report on lookalike domains across digital channels.

Case 3—Trojan Horse

Based on our research on the topic, of malware attacks, there have been many cases in recent years involving various countries attacked by various types of malware. Malicious software is designed particularly to infect computers and other devices where the motive behind it varies in each case. With that, one of the cases that was highlighted in recent years was the case of the city of Allentown, Pennsylvania. In 2018, Emotet began to spread in the United States of America with an attack on Allentown. According to (Petcu, 2022; Almusaylim, Zaman and Jung, 2018; Ali,S., 2022; Almoysheer, et.al. 2021; Alsharif, et.al, 2023), Emotet has been one of the longest-running cybercrime operations in recent history and this time, the target was the city of Allentown. Before getting deeper into the case, Emotet in simple terms is involved in one of the malware strains known as banking Trojans.

Not long before, in 2017, this particularly adaptable and dynamic malware that we last saw exploiting a Windows API from that in November 2017. Ever since then, Emotet's objectives and capabilities have been gradually increasing, and it has added new methods that allow it to evade sandbox and malware detection. (Micro, 2018). In February 2018, the city's vital main systems were impacted by the malware known as Emotet. This impacted both their financial and public safety

 doi:10.20944/preprints202409.1369.v

operations according to Mayor Ed Pawlowski. The mayor also said that no external banking transactions could be completed by Allentown's finance department. Furthermore, all the 185 surveillance cameras in the city were impacted during this attack and finally, the police department couldn't access Pennsylvania State Police databases. Across town, city employees were getting kicked out of the computer network and it was not a glitch. Emotet spread widely around the city's networks, self-replicating and harvesting city employees' credentials. It affected city systems running on Microsoft, and therefore, the city hired a team of Microsoft engineers to handle the issue. Yet, during the attack phase, no evidence was found to show that it compromised citizens' personal information.

City officials warned people from opening any emails or attachments from city employees since compromised Microsoft Word Documents are known as Emotet infection vectors. They avoided releasing information about what was being done as the hacker may still be able to modify the attack in response to actions taken by the Allentown city. The city reportedly declared that they paid Microsoft a $185,000 first emergency response cost to "stop this bleeding." The other $1 million would go toward recovering expenses. (Tung, 2020; Singhal et al., 2020).

From another view, this case is further explained by Microsoft who provided a case study that explains the company's response to this major Emotet attack that brought down the whole network, bypassed antivirus security, and evaded all its Windows computers. The infection started when an employee opened a malicious attachment. According to the Microsoft Detection and Response Team (DART), an attacker sent several phishing emails to Fabrikam employees using an alias to hide its identity.

When one of the receivers opened a file attached to the email, their credentials were sent to the attackers' command-and-control site, enabling the hackers access to their system. They further added that four days after acquiring control of the employee's computer, the threat actor began sending phishing emails to other persons on the Fabrikam network. This was a sneaky and successful method of infecting the network. Many typical email filters do not analyse internal communications for viruses, making phishing emails from an internal account appear much more convincing. More individuals opened attachments, and more computers downloaded malware. Everything went proceeding as planned by the threat actor. (DART, 2020).

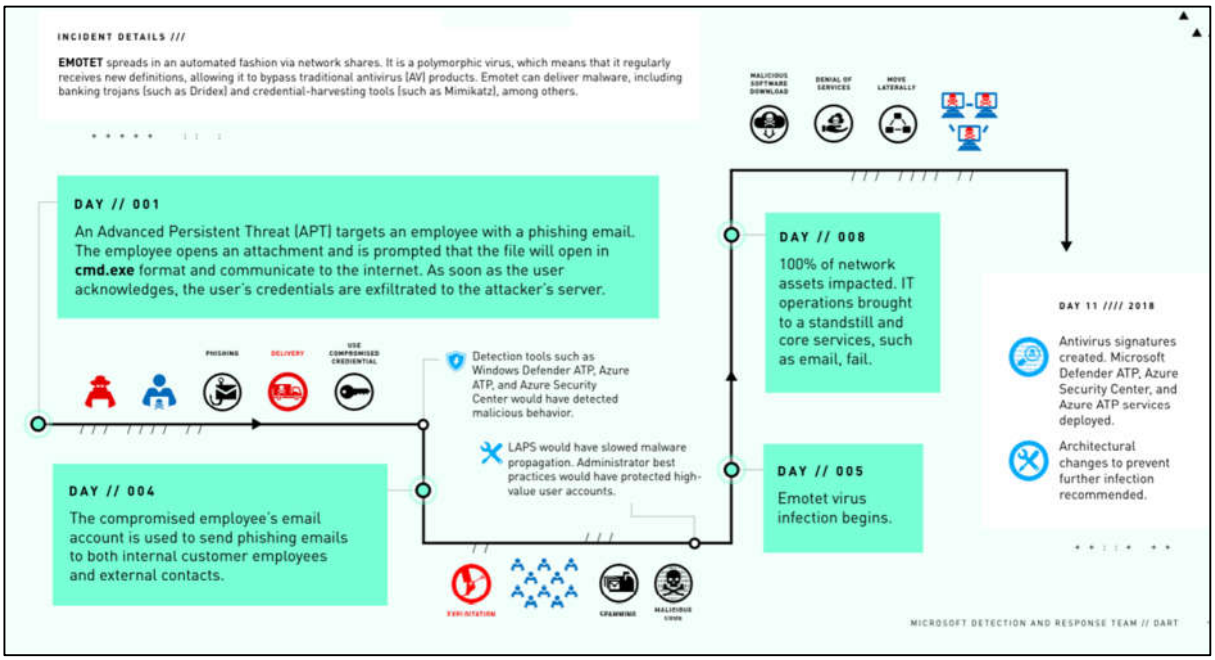


Figure 8. Incident Details.

 doi:10.20944/preprints202409.1369.v

Security Issues

Based on the case of the malware attack discussed, the security that caused the damage was a banking Trojan. Emotet is a malware type known as banking Trojans, which is one of the most deadly and destructive malware attacks. The United States Department of Homeland Security has issued a forceful statement in response to the 2018 incident. The reason for the increased attention is that Emotet is frequently used in cases of financial information theft. The principal vectors for Emotet's spreading are malicious emails in the form of spam and phishing campaigns.

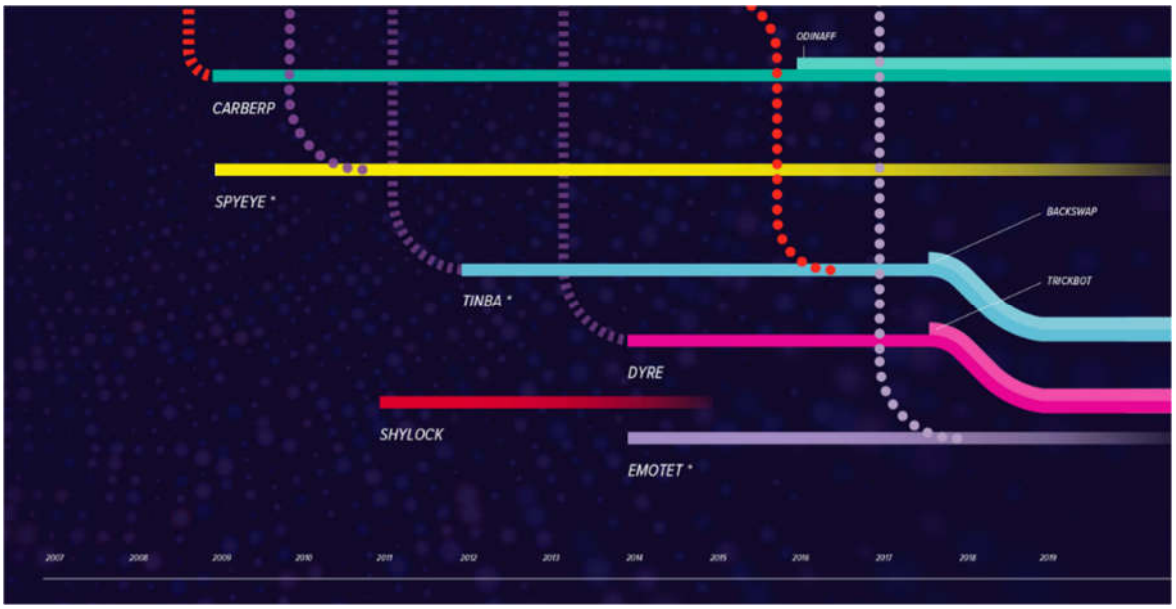


Figure 9. Comparison Table.

The question here is what a trojan is? A trojan is any harmful application that masquerades as a genuine one. They are frequently designed to steal sensitive information from users, such as login passwords, account numbers, financial information, credit card information, and so on. A banking trojan functions, similarly, portraying itself as something positive or useful to individuals while serving a far more insidious, undisclosed goal. Even a mobile app that looks to serve a legitimate purpose, such as a game, lighting, or messaging service, might be a trojan designed to steal information. Trojans escape detection by concealing elements in other files, comprising part of a rootkit. Once it gets into an individual's client machine, it performs variety of methods to create botnets, steal information or money and inject malicious code into browsers.

Hence, how did Trojan evolve? Initially, banks were very much aware of being targeted by attackers and enhanced their overall systems. Therefore, these cybercriminals came up with a new approach to attacking customers and employees individually. Rather than attacking the institution, they decided to target individuals and steal useful credentials. This is when banking Trojans became dominant among cyberattacks. Banking trojans target individuals from institutions mainly via spam, phishing, drive-by-downloads, and social engineering. This upgrade changed the scope, technical ability, and the main goal of this malware attack. The targets were not only financial institutions, but it further grew to apply on other occasions which include online advertisers, social media sites and communication platforms.

There are several potential security threats that banking trojans can cause if the issues are not resolved early. Banking Nowadays Trojans have grown into advanced industrial hacking tools, allowing attackers to capture banking passwords as victims enter them into a bank's login page. Furthermore, it may gather credit card details and other financial information as you input it into a webpage. Furthermore, it replicates all passwords you have stored in your web browser and allows you to remotely connect to your computer. Banking trojans will search your computer for financial

 doi:10.20944/preprints202409.1369.v

data and steal your files if not detected in time. It can search your organization's network and extend to other computer systems in a larger danger scenario.

According to (Kessem, 2020), the primary objective of banking Trojans used to be to steal money from business accounts, however, that objective has since been broadened. Reviewing the financial crime scene for 2019 reveals a glaring pattern for the leading banking Trojan gangs: These malware botnets are now being utilized for targeted, high-stakes ransomware assaults as well as data theft and bank account theft. The security industry has started to refer to these coordinated operations as a potential threat since they aren't intended to target only specific individuals, but rather businesses of all sizes so that the attackers can demand higher ransom payments.

Countermeasures

According to the case study on the city of Allentown, they had paid Microsoft to handle this malware attack which consumed the network bandwidth until using it for anything was made possible. In response, Microsoft's Cybersecurity Solutions Group's Detection and Response Team (DART) was in charge of taking the necessary countermeasures towards the spread of banking Trojans, Emotet. It was not an easy task as by that time, all the computers and important systems were already failing and completely overrun by Emotet.

First, DART distributed trial licences for Microsoft malware detection technologies such as Defender Advanced Threat Protection, Azure Security Centre, Azure Advanced Threat Protection, and others. Next, The DART crew on site utilized remote tools to access Fabrikam's network and set up buffer zones that partitioned computers with administrator capabilities to prevent Emotet from spreading and intentionally invading systems throughout the network.

Their actions managed to remove Emotet with antivirus and the team also uploaded antivirus signatures for the malware for destruction of Emotet. It is not sufficient to depend entirely on antivirus software to defend against Emotet and other Trojans. For end users, identifying the polymorphic malware is just the beginning. There is just no solution that offers Emotet or other Trojans that are continually evolving complete security. You can only reduce the danger of infection by using technical and organisational measures.

Trojans get their name since require an individual's consent to execute on their devices, either when you run a program by yourself or when you open a file or picture that contains the programme. (Kaspersky, 2021; Shahid et al., 2021). Considering this, the primary and effective way of prevention against Trojans is to never open any email attachments sent to you or run a program if you are uncertain about the source, that also involves all documents downloaded from peer-to-peer programs or Internet sites. However, in today's modern globalized world, this would be extremely difficult and nearly impossible, so additional enhanced security precautions must be taken. In addition, phishing is a technique of social engineering that is frequently used to retrieve sensitive user details such as usernames and passwords as well as credit card details. Likewise, phishing has the potential to download a Trojan onto your device. It entails an intruder impersonating a trustable entity and convincing the victim to click on an email, SMS, or text message, which stimulates the Trojan horse. As a result, one should avoid an attachment in an email sent by an anonymous sender.

Besides, you should always keep your computer's software up to date to prevent trojan horse attacks. This is especially true for critical programmes such as your windows operating system and web application. Cybercriminals employ recognised security flaws in these kinds of programs that can assist the Trojan in its task, and even if the supplier fixes the small hole, it won't affect you only if you keep your software updated. Always maintain a firewall running to retain your Wi-Fi connection as safe as possible. Firewalls, both software and hardware, are outstanding at attempting to control suspicious web traffic and can frequently prevent Trojan horses from installing into your device in the first place.

Moreover, each of these small details is beneficial, but to remain truly secure, you must download antivirus software or a Trojan exfoliator. When kept updated, this software will inspect your system to verify that you may have not downloaded a Trojan and will instantaneously inspect any programme or file you run to safeguard it. There seem to be free Trojan removers available on

 doi:10.20944/preprints202409.1369.v

the Web, but very few are constantly updated, while others are Trojans. Choose a brand-name virus protection with a trial version to effectively safeguard your device. This will enable users to experience the advantages of a program prior to purchasing it.

In our opinion, Fabrikam and the institutions in the city in Allentown had poor practice on security management as their email filters couldn't scan internal mail. This gave Emotet an easy invasion to spread internally without triggering alerts. A proper mail filter mechanism and multi-factor authentication could have made it harder for Emotet to make use of the harvested credentials from employees. Solutions for email security can be broken down into three which are to weed out spam mails, verification of the message itself and finally end-to-end encryption.

The latest Sender Policy Framework (SPF) is a standard that ensures that incoming mail from a domain originates from an IP address that has been allowed by a domain's administration and enables the identification and blockage of fake email addresses. Additionally confirming that the email originated from a trusted mail server is made possible by DomainKeys Identified Mail (DKIM).

Every email communication can have a digital signature added to the headers due to DKIM. Once verified, this signature can be compared to a public cryptographic key that is stored in the Domain Name System (DNS) record for the company. Transport Layer Security is the third essential element of spam-proof email for the financial services sector (TLS). As a solution, Allentown should begin utilising DKIM to cryptographically sign email messages to guarantee that they haven't been altered while in transmission, SPF records to identify approved mail servers, and TLS encryption to secure channels end-to-end. (Mairs, 2018).

Malware must be investigated to comprehend how it functions, spreads, and infects. Organisations, businesses, agencies, and governmental bodies must teach their employees about malware. An excellent method to learn how to avoid our systems from becoming infected with this malware is to educate yourself about it (Herati, D. A. et al., 2018; Ghosh et al., 2020; Gaur et al., 2023; Ghani et al., 2022; Gouda et al., 2022).

The most common issue with updating our system is that most businesses, organisations, and companies continue to use outdated operating systems, software, and services. For instance, some universities and colleges continue to use outdated versions of various operating systems like Microsoft Windows XP, 7, and 8. Other operating systems like Linux, OS X, and others operate similarly to this. Consider a machine running Microsoft Windows XP in a business or organisation. This outdated operating system is more prone to security threats than more recent versions, like Microsoft Windows 10, which has the most recent security updates.

It is impossible to provide security at a 100 per cent level because the digital world is always threatened by new malware strains and other threats, as well as attacks based on various criteria. Another crucial issue is the need to update software with the most recent security fixes that the product's creator offers. Here, hackers may choose to target certain applications and infect them with malicious code; then, when users update or install from untrusted sources, the machine will get infected. Because of this, it's crucial to update these programmes with the most recent security updates from their official website. Cybercriminals and others who conduct experiments study on vulnerabilities and find security gaps in operating systems as well as software will find that Microsoft Software was, is, and will continue to be a prime target.

Users of digital systems, those who use Microsoft products like Windows in its various versions, Office, and other products, or the Android operating system, which is used in handheld devices like smartphones, tablets, smartwatches, and other devices, are particularly vulnerable to malware, both known and unknown. They should be knowledgeable about malware prevention and system security. One of the most important preventative measures is to upgrade your operating system or other software on schedule whenever you receive a notification about a new release or update from official sources.

Most software firms and organisations have their unique release dates for both new goods and security or other patches for already existing software. Users, primarily system administrators who oversee the data and systems, must be aware of these crucial details regarding the release date of new software versions and patches. Administrators of databases, operating systems, networks, and

 doi:10.20944/preprints202409.1369.v

security should be able to handle the tasks that fall under their purview (Herati, D. A et al., 2018; Humayun et al., 2022).

As was previously mentioned, malware can propagate through a variety of channels, such as spam email. These days, it's crucial for a firm to have messaging security measures in place for the system securing emails that are sent and received. There are many different types of these security products on the market, and some businesses, like Google, use them for Gmail so that you cannot send an email attachment that contains or has harmful executable files. These security measures may be ineffective against zero-day malware or attacks that are fresh and undiscovered by the security software because they only know about known files (malware) (Herati, D. A et al., 2018).

Another method of preventing and protecting the system from malware is by using endpoint security solutions. Many endpoint security products are available on the market for securing the system and keeping an eye on its operations. Kaspersky is a good example of a company with high-quality endpoint security products. The host-based intrusion detection systems, host-based intrusion prevention systems, honeypots, and firewalls for protecting the systems against known and unknown malware or other sorts of threats may also be considered as a somewhat higher level of these endpoint security solutions (Herati, D. A. et al., 2018).

To protect the interconnected systems in an organisation, network security and prevention play a crucial and necessary role. To fully safeguard the entire system against malware, malicious traffic, known or unknown threats, and vulnerabilities, the data should be monitored and regulated by a firewall or other centralised or decentralised security mechanisms. Firewalls, honeypot/honeynet systems, intrusion detection systems, and intrusion prevention systems all play significant roles in network security. Today's honeypot systems for malware mostly concentrate on catching and hunting for novel, unknown, zero-day malware (Herati, D. A. et al., 2018; Nayyar, Gadhavi and Zaman, 2021).

It's wise to always have backup plans. It is beneficial for all other types of risks as well, such as those caused by natural disasters like floods, loss, fire, earthquake, damage, stolen, and so on. If you maintain the discipline of consistently backing up your data, disaster recovery is simple. It is preferable to have backups that are independent from the system itself, in a different place, or, if possible, online backups that are accessible from anywhere at any time and lower the risk of data loss (Herati, D. A. et al., 2018).

There are several comprehensive solutions that we would be suggesting to counter the malware attack. One of them is the need to always proceed with caution when downloading software and opening files. We shouldn't install shady software or open attachments from unidentified sources. Trojans abound in software pirated copies. Such a download provider has no obligation to give us security. Bear in mind that if something is free, the provider has nothing to lose. Therefore, if the Download Copy contains malicious programmes, we are on our own. A pirated piece of software can infect your PC with malware. Additionally, some apps lack Publisher Details. Our device OS may suffer if we install such codes from an Unknown Origin. In the past, we could scan a program installation file. However, current malware is always changing.

Therefore, malware could trick our anti-virus software. Therefore, use caution when installing any apps on your computer. Sometimes even software that appears to be "authentic" can be problematic. In addition, we should always be careful when sharing files. Movie torrenting and other peer-to-peer file-sharing services might make it simple to unintentionally download malicious software. Therefore, we should use extreme caution when downloading materials, especially from unreliable sources. We should also be cautious of external devices that are already infected with malware. Malicious software can be stored on any external drive or peripheral device.

As a result, we need to take care of your external gadgets. If a PC connected to our memory cards or drives also has a virus, our devices become contaminated. Therefore, it is important to remember that such a malware transfer is two-way. Consequently, both your computer and your external gadgets should be protected. Moreover, either by downloading files or entering information, we should always look at the address bar. Some trojans function in a manner akin to phishing scams. A

 doi:10.20944/preprints202409.1369.v

hacker can make a website that appears to be from a brand you deal with regularly. Make sure the website that appears in the address bar is the one you want to access.

Conclusion

In a nutshell, the state of the problem, which has recently become one of the hottest information security topics, is briefly introduced in this study. First, we discussed recent occurrences regarding the cyberattack topics that we have selected, which include malware attacks and distributed denial of service (DDOS). We have thoroughly examined the most recent cases touching the issue we have chosen. We have also identified the methods that the cybercriminals employed to attack their intended victim. This knowledge was obtained through a thorough analysis of the instances we covered. Additionally, we have recognised the security concerns related to the malware, vulnerabilities, and threats present in the cases that we have selected. The potential security risks that could result from those cyberattacks have also been mentioned. In addition, we talked about the countermeasures against and prevention of distributed denial of service (DDOS). Here, we've outlined some fundamental ideas for countering or mitigating distributed denial of service (DDOS). Finally, we talked about countermeasures against malware attacks and ways to prevent them. Here, we've outlined some essential ideas for fending off malware attacks.

Cyberterrorism or cyber warfare, such as that carried out by hacktivists, can also be linked to cyberattacks. To put it another way, motives can differ. In other words, motives can differ. These motivations can be divided into three primary categories which are criminal, political, and personal. Thus, it would be wise for any person to take any appropriate safety precautions seriously, for them from becoming the victim of a cyberattack.

Reference

8 tips for DDoS protection, mitigation, and defense : Indusface blog (2022) Indusface. Available at: https://www.indusface.com/blog/ddos-protection-mitigation-and-defense-8-essential-tips/#1_Mitigate_DDoS_Attacks_with_Multi-Layered_Multi-Module_Defense

A, P.S., S, S.P. and B, H. (2024) 'DDoS and Botnet Attacks: A Survey of Detection and Prevention Techniques,' *2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS)* [Preprint]. https://doi.org/10.1109/adics58448.2024.10533615.

Alenezi, M.N. et al. (2022) 'Evolution of Malware Threats and Techniques: a Review,' *International Journal of Communication Networks and Information Security (IJCNIS)*, 12(3). https://doi.org/10.17762/ijcnis.v12i3.4723.

Al-Hawawreh, M., Hartog, F.den and Sitnikova, E. (2019) "Targeted ransomware: A new cyber threat to edge system of Brownfield Industrial Internet of Things," IEEE Internet of Things Journal, 6(4), pp. 7137–7151. DOI: https://doi.org/10.1109/jiot.2019.2914390.

Alkinani, M.H. et al. (2021) '5G and IoT Based Reporting and Accident Detection (RAD) System to Deliver First Aid Box Using Unmanned Aerial Vehicle,' *Sensors*, 21(20), p. 6905. https://doi.org/10.3390/s21206905.

Almusaylim, Z.A., Zaman, N. and Jung, L.T. (2018) 'Proposing A Data Privacy Aware Protocol for Roadside Accident Video Reporting Service Using 5G In Vehicular Cloud Networks Environment,' *2018 4th International Conference on Computer and Information Sciences (ICCOINS)* [Preprint]. https://doi.org/10.1109/iccoins.2018.8510588.

Ali, S., Hafeez, Y., Humayun, M., Jhanjhi, N. Z., & Le, D. N. (2022). Towards aspect based requirements mining for trace retrieval of component-based software management process in globally distributed environment. Information Technology and Management, 23(3), 151-165.

Almoysheer, Najd, Mamoona Humayun, and N. Z. Jhanjhi. "Enhancing Cloud Data Security using Multilevel Encryption Techniques." Turkish Online Journal of Qualitative Inquiry 12, no. 3 (2021).

Alsharif, Mohammed H., Abu Jahid, Anabi Hilary Kelechi, and Raju Kannadasan. "Green IoT: A review and future research directions." Symmetry 15, no. 3 (2023): 757.

Altulaihan, E., Almaiah, M.A. and Aljughaiman, A. (2024) 'Anomaly Detection IDS for detecting DOS attacks in IoT networks based on machine learning algorithms,' *Sensors*, 24(2), p. 713. https://doi.org/10.3390/s24020713.

Aslan, Ö. et al. (2023) 'A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions,' *Electronics*, 12(6), p. 1333. https://doi.org/10.3390/electronics12061333.

BasuMallick, C. (2022) What is a trojan horse? meaning, examples, and prevention best practices for 2022, Trojan Horse Meaning, Examples, Prevention. Available at: https://www.spiceworks.com/it-security/application-security/articles/what-is-trojan-horse/

Bhol, S.G., Mohanty, J. and Pattnaik, P.K. (2023) 'Taxonomy of cyber security metrics to measure strength of cyber security,' *Materials Today Proceedings*, 80, pp. 2274–2279. https://doi.org/10.1016/j.matpr.2021.06.228.

Chahal, J.K., Bhandari, A. and Behal, S. (2024) 'DDoS attacks & defense mechanisms in SDN-enabled cloud: Taxonomy, review and research challenges,' *Computer Science Review*, 53, p. 100644. https://doi.org/10.1016/j.cosrev.2024.100644.

Chesti, I.A. et al. (2020) 'Evolution, Mitigation, and Prevention of Ransomware,' *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* [Preprint]. https://doi.org/10.1109/iccis49240.2020.9257708.

DART, M.D.and R.T. (2020) FULL OPERATIONAL SHUTDOWN. rep. ZDNET. Available at: https://www.zdnet.com/article/microsoft-how-one-emotet-infection-took-out-this-organizations-entire-network/

Driouch, O., Bah, S. and Guennoun, Z. (2024) 'CANSat-IDS: An adaptive distributed Intrusion Detection System for satellites, based on combined classification of CAN traffic,' *Computers & Security*, 146, p. 104033. https://doi.org/10.1016/j.cose.2024.104033.

Dogra, V., Singh, A., Verma, S., Kavita, Jhanjhi, N.Z., Talib, M.N. (2021). Analyzing DistilBERT for Sentiment Classification of Banking Financial News. In: Peng, SL., Hsieh, SY., Gopalakrishnan, S., Duraisamy, B. (eds) Intelligent Computing and Innovation on Data Science. Lecture Notes in Networks and Systems, vol 248. Springer, Singapore. https://doi.org/10.1007/978-981-16-3153-5_53

Dsm (no date) DDoS prevention: The 5 best tips, DSM. Available at: https://www.dsm.net/it-solutions-blog/prevent-ddos-attacks

Express Data Path", UNIVERSITY OF TWENTE STUDENT THESES, pp.1-57. Available at: http://essay.utwente.nl/80125/ (Accessed November 5, 2022).

Fatima-Tuz-Zahra, N. et al. (2020) 'Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning,' 2020 2nd International Conference on Computer and Information Sciences (ICCIS) [Preprint]. https://doi.org/10.1109/iccis49240.2020.9257607.

Felix, N.O.O. (2024) 'TCP/IP stack transport layer performance, privacy, and security issues,' World Journal of Advanced Engineering Technology and Sciences, 11(2), pp. 175–200. https://doi.org/10.30574/wjaets.2024.11.2.0098.

Ferdous, J. et al. (2023) 'A review of State-of-the-Art malware attack trends and defense Mechanisms,' IEEE Access, 11, pp. 121118–121141. https://doi.org/10.1109/access.2023.3328351.

Froutan, P. (2004) How to defend against ddos attacks, Computerworld. Computerworld. Available at: https://www.computerworld.com/article/2564424/how-to-defend-against-ddos-attacks.html

Fruhlinger, J. (2022). DDoS attacks: Definition, examples, and techniques. [online] CSO Online. Available at: https://www.csoonline.com/article/3648530/ddos-attacks-definition-examples-and-techniques.html.

Gaur, L. & Jhanjhi, N. Z. (Eds.). (2023). Digital Twins and Healthcare: Trends, Techniques, and Challenges. IGI Global. https://doi.org/10.4018/978-1-6684-5925-6

Ghosh, G. et al. (2020) 'Secure surveillance system using chaotic image encryption technique,' IOP Conference Series Materials Science and Engineering, 993(1), p. 012062. https://doi.org/10.1088/1757-899x/993/1/012062.

Ghani, Norjihan Binti Abdul, Suraya Hamid, Muneer Ahmad, Younes Saadi, N. Z. Jhanjhi, Mohammed A. Alzain, and Mehedi Masud. "Tracking Dengue on Twitter Using Hybrid Filtration-Polarity and Apache Flume." Comput. Syst. Sci. Eng. 40, no. 3 (2022): 913-926.

Gouda, Walaa, Maram Almurafeh, Mamoona Humayun, and Noor Zaman Jhanjhi. "Detection of COVID-19 based on chest X-rays using deep learning." In Healthcare, vol. 10, no. 2, p. 343. MDPI, 2022.

Ghotbi, P. (2021) Ransomware: Statistics, latest threats and countermeasures, Online Masters Programs from St. Bonaventure University. Available at: https://online.sbu.edu/news/ransomware-statistics-latest-threats-countermeasures (Accessed: November 6, 2022).

Glamoslija, K. (2021) How to defend your PC and devices against a trojan horse virus, SafetyDetectives. Safety Detectives. Available at: https://www.safetydetectives.com/blog/what-is-a-trojan-horse-and-how-to-protect-against-it/

Gojali, A.M. et al. (2024) ANALYSIS OF THE EFFECTIVENESS OF THE COMBINATION OF FAIL2BAN AND MODSECURITY IN MITIGATION OF DDOS ATTACKS ON WEB SERVERS. http://eksplorasi.org/index.php/nre/article/view/214.

Gopi, R. et al. (2021) 'Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things,' Multimedia Tools and Applications, 81(19), pp. 26739–26757. https://doi.org/10.1007/s11042-021-10640-6.

Guenane, F., Nogueira, M. and Serhrouchni, A. (2015) 'DDOS Mitigation Cloud-Based Service,' 2015 IEEE Trustcom/BigDataSE/ISPA [Preprint]. https://doi.org/10.1109/trustcom.2015.531.

H. Ashraf, F. Khan, U. Ihsan, F. Al-Quayed, N. Z. Jhanjhi and M. Humayun, "MABPD: Mobile Agent-Based Prevention and Black Hole Attack Detection in Wireless Sensor Networks," 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-11, doi: 10.1109/ICBATS57792.2023.10111277.

H. Ashraf, M. Hanif, U. Ihsan, F. Al-Quayed, M. Humayun and N. Jhanjhi, "A Secure and Reliable Supply chain management approach integrated with IoT and Blockchain," 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-9, doi: 10.1109/ICBATS57792.2023.10111371

Humayun, M., N. Z. Jhanjhi, B. Hamid, and G. Ahmed. "Emerging smart logistics and transportation using IoT and blockchain. IEEE Internet of Things Magazine, 3 (2), 58-62." (2020).

Humayun, M., Khalil, M. I., Alwakid, G., & Jhanjhi, N. Z. (2022). Superlative feature selection based image classification using deep learning in medical imaging. Journal of Healthcare Engineering, 2022(1), 7028717.

Hansen, P. et al. (2024) 'Guarding the Galaxy: Satellite Ransomware and Countermeasures,' 2024 IEEE Aerospace Conference [Preprint]. https://doi.org/10.1109/aero58975.2024.10521045.

Herati, D. A, Bojamma, A. M and Gandhi, I. (2018) "Countermeasures to Ransomware Threat", ResearchGate, pp.1-7. Available at: https://www.researchgate.net/publication/324690703_Countermeasures_to_Ransomware_Threats (Accessed: November 5, 2022).

Hnamte, V. et al. (2024) 'DDoS attack detection and mitigation using deep neural network in SDN environment,' Computers & Security, 138, p. 103661. https://doi.org/10.1016/j.cose.2023.103661.

How to prevent ddos attacks (2022) Embroker. Available at: https://www.embroker.com/blog/how-to-prevent-ddos-attacks/

Humayun, M., Ashfaq, F., et al. (2022) 'Traffic management: Multi-Scale vehicle detection in varying weather conditions using YOLOV4 and spatial pyramid pooling network,' *Electronics*, 11(17), p. 2748. https://doi.org/10.3390/electronics11172748.

Humayun, M., Sujatha, R., et al. (2022) 'A Transfer Learning Approach with a Convolutional Neural Network for the Classification of Lung Carcinoma,' *Healthcare*, 10(6), p. 1058. https://doi.org/10.3390/healthcare10061058.

Hussain, K. et al. (2024) 'Threats and Vulnerabilities of Wireless Networks in the Internet of Things (IoT),' *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)* [Preprint]. https://doi.org/10.1109/khi-htc60760.2024.10482197.

Iqbal, A. et al. (2024) 'Unveiling the connection between malware and pirated software in Southeast Asian countries: a case study,' *IEEE Open Journal of the Computer Society*, pp. 1–10. https://doi.org/10.1109/ojcs.2024.3364576.

Ismail, S, Hassen, H, Just, M & Zantout, H. (2021) "A review of amplification-based distributed denial of service attacks and their mitigation," Computers & Security, 109, article no:102380. DOI: https://doi.org/10.1016/j.cose.2021.102380.

Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, Shahbaz Khan, and Rajiv Suman. "An extensive study on Internet of Behavior (IoB) enabled Healthcare-Systems: Features, facilitators, and challenges." BenchCouncil Transactions on Benchmarks, Standards and Evaluations 2, no. 4 (2022): 100085.

Jayakumar, P., Brohi, S. N., & Jhanjhi, N. Z. (2021). Artificial intelligence and military applications: Innovations, cybersecurity challenges & open research areas.

Jhanjhi, N. Z., Sahil Verma, M. N. Talib, and Gagandeep Kaur. "A canvass of 5G network slicing: Architecture and security concern." In IOP Conference Series: Materials Science and Engineering, vol. 993, no. 1, p. 012060. IOP Publishing, 2020.

Jin, Y, Tomoishi, M, Matsuura, S and Kitaguchi, Y. (2018) "A secure container-based backup mechanism to survive destructive ransomware attacks," 2018 International Conference on Computing, Networking and Communications (ICNC), pp. 1-6. DOI: https://doi.org/10.1109/iccnc.2018.8390376.

Kaspersky (2021) Avoiding a trojan virus: Keeping the gates closed, www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/preemptive-safety/avoiding-a-trojan-virus

Kaur, K. et al. (2024) 'Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies,' *Frontiers in Computer Science*, 6. https://doi.org/10.3389/fcomp.2024.1420680.

Kessem, L. (2020) Banking trojans and ransomware—a treacherous matrimony bound to get worse, Security Intelligence. SecurityIntelligence. Available at: https://securityintelligence.com/posts/banking-trojans-and-ransomware-a-treacherous-matrimony-bound-to-get-worse/

Kizza, J.M. (2024) 'System Intrusion Detection and Prevention,' in *Texts in computer science*, pp. 295–323. https://doi.org/10.1007/978-3-031-47549-8_13.

Khairandish, M. O., M. Sharma, V. Jain, J. M. Chatterjee, and N. Z. Jhanjhi. "A hybrid CNN-SVM threshold segmentation approach for tumor detection and classification of MRI brain images. IRBM, 43 (4), 290–299." (2022).

Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). A review of intrusion detection system using machine learning approach. International Journal of Engineering Research and Technology, 12(1), 8-15.

Knapp, E.D. and Langill, J.T. (2011) Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems. http://cds.cern.ch/record/1988553.

Kumar, S. and Keshari, A.K. (2024) 'An effective DDOS attack mitigation of IoT using Optimization-Based adaptive Security model,' Knowledge-Based Systems, p. 112052. https://doi.org/10.1016/j.knosys.2024.112052.

Kumar, S. et al. (2024) 'A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services,' Computer Science Review, 53, p. 100661. https://doi.org/10.1016/j.cosrev.2024.100661.

Learning Center. (n.d.). What does DDoS Mean? | Distributed Denial of Service Explained | Imperva. [online] Available at: https://www.imperva.com/learn/ddos/denial-of-service/#:~:text=DDoS%20meaning%3A%20What%20is%20DDoS.

Ling, X. et al. (2023) 'Adversarial attacks against Windows PE malware detection: A survey of the state-of-the-art,' Computers & Security, 128, p. 103134. https://doi.org/10.1016/j.cose.2023.103134.

Lim, Marcus, Azween Abdullah, N. Z. Jhanjhi, Muhammad Khurram Khan, and Mahadevan Supramaniam. "Link prediction in time-evolving criminal network with deep reinforcement learning technique." IEEE Access 7 (2019): 184797-184807.

Mairs, T. (2018) 3 mandatory email security best practices for the Financial Services Industry, SparkPost. Available at: https://www.sparkpost.com/blog/3-email-security-best-practices-financial-services-industry/

Merkebaiuly, M. (2024) 'Overview of Distributed Denial of Service (DDoS) attack types and mitigation methods,' InterConf, (43(193)), pp. 494–508. https://doi.org/10.51582/interconf.19-20.03.2024.048.

Micro, T. (ed.) (2018) Malware attack will reportedly cost Allentown, PA.. US$1 million, Security News. Trend Micro. Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malware-attack-will-reportedly-cost-allentown-pa-us-1-million

Ming, L., Leau, Y.-B. and Xie, Y. (2024) 'Distributed Denial of Service attack in HTTP/2: Review on security issues and future challenges,' IEEE Access, p. 1. https://doi.org/10.1109/access.2024.3371013.

Mirre, A. (2021) "Protecting internet networks against DOS attacks", digilib.k.utb.cz, pp. 8-47. Available at: https://digilib.k.utb.cz/bitstream/handle/10563/46175/mirre_2021_dp.pdf?sequence=-1 (Accessed: November 5, 2022).

Mohiddin, S.K., Midhunchakkaravarthy, D. and Hussain, M.A. (2023) 'TSWA: a unique approach to overcome interest flooding attacks in the cloud using a combination of TSW and attack detection,' *Multimedia Tools and Applications*, 83(11), pp. 32673–32713. https://doi.org/10.1007/s11042-023-16660-8.

M. Saleh, N. Jhanjhi, A. Abdullah and R. Saher, "IoTES (A Machine learning model) Design dependent encryption selection for IoT devices," 2022 24th International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea, Republic of, 2022, pp. 239-246, doi: 10.23919/ICACT53585.2022.9728960.

Mott, G. et al. (2024) ''There was a bit of PTSD every time I walked through the office door': Ransomware harms and the factors that influence the victim organization's experience,' Journal of Cybersecurity, 10(1). https://doi.org/10.1093/cybsec/tyae013.

Nafea Alhammadi(2021) Researchgate.net. Available at: https://www.researchgate.net/publication/356786133_A_Review_of_the_Common_DDoS_Attack_Types_and_Protection_Approaches_Based_on_Artificial_Intelligence

Nafea Ali Majeed, Zaboon, K.H. and Abdullah, A.A. (2021) 'A Review of the Common DDoS Attack: Types and Protection Approaches Based on Artificial Intelligence,' Research Gate, pp. 08–14. https://doi.org/10.54216/fpa.070101.

Nayak, T. (2019, June 3). The LockerGoga Ransomware Attack: A worst-case scenario for industrial operations. AXA XL. https://axaxl.com/fast-fast-forward/articles/the-lockergoga-ransomware-attack_a-worst-case-scenario-for-industrial-operations

Nayyar, A., Gadhavi, L. and Zaman, N. (2021) 'Machine learning in healthcare: review, opportunities and challenges,' in Elsevier eBooks, pp. 23–45. https://doi.org/10.1016/b978-0-12-821229-5.00011-2.

Nicholson, P. (2018). 5 Most Famous DDoS Attacks | A10 Networks. [online] A10 Networks. Available at: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/.

PAPEZ, N and SHIELDS, r. (2021) Ransomware countermeasures—mitigation strategies: Proofpoint US, Proofpoint. Available at: https://www.proofpoint.com/us/blog/security-awareness-training/countermeasures-ransomware (Accessed: November 6, 2022).

Petcu, A.G. (2022) Emotet malware over the years: The history of an infamous Cyber-Threat, Heimdal Security Blog. Heimdal Security. Available at: https://heimdalsecurity.com/blog/emotet-malware-history/

Pillai, S.E.V.S. and Polimetla, K. (2024) 'Mitigating DDoS Attacks using SDN-based Network Security Measures,' 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS) [Preprint]. https://doi.org/10.1109/icicacs60521.2024.10498932.

Porter, J. (2020) Amazon says it mitigated the largest ddos attack ever recorded, The Verge. The Verge. Available at: https://www.theverge.com/2020/6/18/21295337/amazon-aws-biggest-ddos-attack-ever-2-3-tbps-shield-github-netscout-arbor

Ransomware: Facts, threats, and countermeasures (2019) CIS. Available at: https://www.cisecurity.org/insights/blog/ransomware-facts-threats-and-countermeasures (Accessed: November 6, 2022).

Ramanjot, Mittal, U., Wadhawan, A., Singla, J., Jhanjhi, N. Z., Ghoniem, R. M., ... & Abdelmaboud, A. (2023). Plant disease detection and classification: A systematic literature review. Sensors, 23(10), 4769.

Ransomware: Facts, threats, and countermeasures (2019) CIS. Available at: https://www.cisecurity.org/insights/blog/ransomware-facts-threats-and-countermeasures

Reblaze (2022). What is DDoS? [online] Available at: https://www.reblaze.com/wiki/ddos/what-is-ddos/#:~:text=What%20is%20DDoS%3F

Riadi, I., Sunardi, N. and Aprilliansyah, D. (2023) 'Analysis of Anubis Trojan attack on Android banking application using mobile security labware,' *International Journal of Safety and Security Engineering*, 13(1), pp. 31–38. https://doi.org/10.18280/ijsse.130104.

Shahid, H. et al. (2021) 'Energy Optimised Security against Wormhole Attack in IoT-Based Wireless Sensor Networks,' *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, 68(2), pp. 1967–1981. https://doi.org/10.32604/cmc.2021.015259.

Shete, V and Gosavi, S. (2021) "Cloud Computing—Threats On Cloud Storage" Mahratta, 1(2), pp.1-15. Available at: http://www.mahratta.org/CurrIssue/2021_Sept_2/Vol%202_Paper19_Vaidehi_Cloud%20Computing%20-%20Threats%20On%20Cloud%20Storage.pdf (Accessed: November 6, 2022).

Saeed, Soobia, Afnizanfaizal Abdullah, N. Z. Jhanjhi, Mehmood Naqvi, Mehedi Masud, and Mohammed A. AlZain. "Hybrid GrabCut Hidden Markov Model for Segmentation." Computers, Materials & Continua 72, no. 1 (2022).

Saeed, S., Haron, H., Jhanjhi, N. Z., Naqvi, M., Alhumyani, H. A., & Masud, M. (2022). Improve correlation matrix of discrete fourier transformation technique for finding the missing values of mri images. Mathematical Biosciences and Engineering, 19(9), 9039-9059.

Sangkaran, Theyvaa, Azween Abdullah, and N. Z. Jhanjhi. "Criminal community detection based on isomorphic subgraph analytics." Open Computer Science 10, no. 1 (2020): 164-174.

Sangkaran, Theyvaa, Azween Abdullah, N. Z. JhanJhi, and Mahadevan Supramaniam. "Survey on isomorphic graph algorithms for graph analytics." International Journal of Computer Science and Network Security 19, no. 1 (2019): 85-92.

Shah, I. A., Jhanjhi, N. Z., & Brohi, S. N. (2024). Use of AI-Based Drones in Smart Cities. In I. Shah & N. Jhanjhi (Eds.), Cybersecurity Issues and Challenges in the Drone Industry (pp. 362-380). IGI Global. https://doi.org/10.4018/979-8-3693-0774-8.ch015

Shah, I. A., Jhanjhi, N. Z., & Ujjan, R. M. (2024). Drone Technology in the Context of the Internet of Things. In I. Shah & N. Jhanjhi (Eds.), Cybersecurity Issues and Challenges in the Drone Industry (pp. 88-107). IGI Global. https://doi.org/10.4018/979-8-3693-0774-8.ch004

Shah, I. A., Jhanjhi, N. Z., & Ray, S. K. (2024). Artificial Intelligence Applications in the Context of the Security Framework for the Logistics Industry. In M. Ghonge, N. Pradeep, N. Jhanjhi, & P. Kulkarni (Eds.), Advances in Explainable AI Applications for Smart Cities (pp. 297-316). IGI Global. https://doi.org/10.4018/978-1-6684-6361-1.ch011

Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Gharib, A. H., & Yun, K. J. (2024). Applications of Blockchain Technology in Supply Chain Management. In N. Jhanjhi & I. Shah (Eds.), Cybersecurity Measures for Logistics Industry Framework (pp. 248-304). IGI Global. https://doi.org/10.4018/978-1-6684-7625-3.ch009

Sood, M., Angra, P., Verma, S., & Jhanjhi, N. Z. (2022). Efficient feature grouping for IDS using clustering algorithms in detecting known/unknown attacks. In Information security handbook (pp. 103-116). CRC Press.

Sindiramutty, S.R. (2024) 'Autonomous Threat Hunting: a future paradigm for AI-Driven Threat intelligence,' arXiv (Cornell University) [Preprint]. https://doi.org/10.48550/arxiv.2401.00286.

Sindiramutty, S.R., Tan, C.E., Lau, S.P., et al. (2024) 'Explainable AI for cybersecurity,' in Advances in computational intelligence and robotics book series, pp. 31–97. https://doi.org/10.4018/978-1-6684-6361-1.ch002.

Sindiramutty, S.R., Tan, C.E., Tee, W.J., et al. (2024) 'Modern smart cities and open research challenges and issues of explainable artificial intelligence,' in Advances in computational intelligence and robotics book series, pp. 389–424. https://doi.org/10.4018/978-1-6684-6361-1.ch015.

Sindiramutty, S.R., Tee, W.J., et al. (2024) 'Explainable AI in healthcare application,' in Advances in computational intelligence and robotics book series, pp. 123–176. https://doi.org/10.4018/978-1-6684-6361-1.ch005.

Singhal, V. et al. (2020) 'Artificial Intelligence Enabled Road Vehicle-Train Collision Risk Assessment Framework for Unmanned railway level crossings,' IEEE Access, 8, pp. 113790–113806. https://doi.org/10.1109/access.2020.3002416.

Tatipatri, N. and Arun, S.L. (2024) 'A Comprehensive Review on Cyber-attacks in Power Systems: Impact Analysis, Detection and Cyber security,' IEEE Access, p. 1. https://doi.org/10.1109/access.2024.3361039.

Tiwalade Modupe Usman, Yakub Kayode Saheed, Djitog Ignace, Augustine Nsang, Diabetic retinopathy detection using principal component analysis multi-label feature extraction and classification, International Journal of Cognitive Computing in Engineering, Volume 4, 2023,Pages 78-88, ISSN 2666-3074, https://doi.org/10.1016/j.ijcce.2023.02.002.

Tung, L. (2020) Microsoft: How One EMOTET infection took out this organization's entire network, ZDNET. Available at: https://www.zdnet.com/article/microsoft-how-one-emotet-infection-took-out-this-organizations-entire-network/

Uddin, R., Kumar, S.A.P. and Chamola, V. (2024) 'Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions,' Ad Hoc Networks, 152, p. 103322. https://doi.org/10.1016/j.adhoc.2023.103322.

Varshney, G. et al. (2024) 'Anti-phishing: A comprehensive perspective,' Expert Systems With Applications, 238, p. 122199. https://doi.org/10.1016/j.eswa.2023.122199.

Vasani, V. et al. (2023) 'Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion,' Electronics, 12(20), p. 4299. https://doi.org/10.3390/electronics12204299.

Vijayalakshmi, B., Ramar, K., Jhanjhi, N. Z., Verma, S., Kaliappan, M., & Vijayalakshmi, K. & Ghosh, U.(2021). An attention-based deep learning model for traffic flow prediction using spatiotemporal features towards sustainable smart city. International Journal of Communication Systems, 34(3), e4609.

Waheed, A. et al. (2024) 'Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure,' Preprints [Preprint]. https://doi.org/10.20944/preprints202407.2338.v1.

Wen, B.O.T. et al. (2023) 'Detecting cyber threats with a Graph-Based NIDPS,' in Advances in logistics, operations, and management science book series, pp. 36–74. https://doi.org/10.4018/978-1-6684-7625-3.ch002.

What is Ryuk Ransomware? A Detailed Breakdown (2024). https://www.sentinelone.com/cybersecurity-101/threat-intelligence/ryuk-ransomware/.

Wieren, H.D.van. (2019) "Signature-based DDoS attack mitigation: Automated Generating Rules for extended berkeley packet filter and express data path, Signature-Based DDoS Attack Mitigation: Automated Generating Rules for Extended Berkeley Packet Filter and

Wisser, W. (2020) Lockergoga ransomware: How to decrypt files and remove virus, MySpyBot. Available at: https://myspybot.com/lockergoga-ransomware/#preventiontips (Accessed: November 6, 2022).

Yadav, R.S. and Likhar, P. (2024) 'Firewall: A Vital Constituent of Network Security,' in Information Technology Security, pp. 47–67. https://doi.org/10.1007/978-981-97-0407-1_3.

Zaman, Noor, and Azween B. Abdullah. "Position responsive routing protocol (prrp)." In 13th International Conference on Advanced Communication Technology (ICACT2011), pp. 644-648. IEEE, 2011.

Zhou, Z. et al. (2021) 'A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic,' *Neural Computing and Applications*, 36(1), pp. 1–14. https://doi.org/10.1007/s00521-021-06389-6.

Zou, Y., Fan, W. and Ma, Z. (2024) 'Unveiling Vulnerabilities in Bitcoin's Misbehavior-Score Mechanism: Attack and Defense,' *ACM Library* [Preprint]. https://doi.org/10.1145/3664476.3664509.