Muninn

TABLE OF CONTENTS

Pulling Focus on Cybersecurity in 2023

The cover for our Cyber Trends 2023 was created with *DALL-E 2* with input by our senior visual designer Artur Pinto. DALL-E 2 is an advanced AI model that is capable of generating high-quality and realistic images with great attention to detail and a wide range of artistic styles, all based on the user's textual input.

As our world hurtles towards an increasingly digital future, it's more important than ever to keep up with the latest trends in cybersecurity. In our Cyber Trends for 2023, we dive deep into some of the most pressing issues and latest developments in the digital world.

We start by shining a light on the demand for cybersecurity experts and how it has skyrocketed, leaving a critical shortage of skilled professionals. We expose the alarming dearth of cybersecurity staff and provide insights into the reasons behind it.

But the threat doesn't end there. In the shadowy world of hacktivism groups like Anonymous and Killnet have made headlines for causing chaos and disrupting the status quo. We investigate the impact of their attacks on businesses, governments, and individuals, and their change of strategy since Russia started their war on Ukraine.

Next, we turn our attention to the growing threat of data breaches and exfiltration, the ever-growing trend of stealing sensitive information. Cybercriminals are becoming more sophisticated in their methods, and businesses of all sizes are at risk. We shine a light

Andreas F. Wehowsky

on how to protect your organization from becoming a victim.

Alert fatigue is not a new issue, but the pandemic has accelerated this trend and it has been especially visible in our industry due to the lack of cybersecurity staff. With possible solutions at our fingertips, we are looking at some customer cases to see what can be done.

Finally, we explore the exciting world of artificial intelligence and its latest trends in chatbots, including groundbreaking systems like ChatGPT. We look at the impressive capabilities of these AI-powered chatbots and their potential impact on today's society including the darker side of this development.

As we move ahead in 2023, it's crucial to bear in mind that rapidly evolving technology and tools may be swiftly adopted by threat actors to create even more malicious attacks. These threats could be of superior quality compared to those traditionally crafted, with an infinite range of malware and malicious code variations. This only reinforces the significance of zero-day attack prevention across the entire IT infrastructure, from email and endpoint security to network and cloud security, and everything in between. The tides of power in the cybersecurity landscape are shifting, propelled by sweeping geopolitical changes, a reorganization of hacker networks, and a staggering shortage of skilled security personnel.

This affects people's and businesses' everyday life but is also the ground for Muninn's development and product roadmap. In 2023 the world needs to stay ahead of cybercriminals more than ever before and our team at Muninn is strongly committed to detect and prevent the increasing number of cyberthreats.

Cybersecurity

Staff Shortage Sparks Crisis as Organizations Struggle to Meet Growing Threats

The demand for cybersecurity and IT job positions is growing at an unprecedented rate, with companies struggling to keep up. In today's world, where valuable and private data and information are the lifeblood of any enterprise, finding and retaining specialty talent in cybersecurity has become critical.

According to the fifth annual (ISC)² Cybersecurity Workforce Study, the global cybersecurity workforce is expected to grow to 4.7 million in 2022, which represents an increase of 11.1% over the previous year. However, this increase is not enough to fill the growing gap, which now stands at 464,000 more jobs. This gap has increased by 26.2% year-over-year and is especially severe in the aerospace, government, education, insurance, and transportation sectors.

The (ISC)² study found that nearly 70% of cybersecurity workers feel that their organization does not have enough staff to be effective. This talent shortage is threatening the most foundational functions of the profession, such as risk assessment, oversight, and critical systems patching. More than half of the employees at organizations with workforce shortages believe that their company is at moderate or extreme risk of a cyberattack.

Adding to the talent gap, the number of cybersecurity attacks companies face each year is also growing. According to Accenture's State of Cybersecurity Report 2021, the average number of cybersecurity attacks per year rose by 31% from 2020 to 2021, with companies falling victim to an average of 29 attacks last year. The (ISC)² study notes that cyberattacks have become more prevalent in a year of "geo-political and macroeconomic turbulence," citing the Russian cyberattacks on the Ukrainian government at the beginning of the war as one of the major events.

On top of it the pandemic changed the world profoundly, shifting the global workforce rapidly to the online world. With billions of people abruptly transitioning to remote work, employees were forced to adopt a wide array of unfamiliar IT tools and applications. This digital transformation also presents an unparalleled opportunity for cybercriminals, who are taking advantage of the massive expansion in the threat landscape to launch a devastating barrage of cyberattacks, creating an unprecedented escalation in online security threats.

> Although more than 464,000 workers were added in the past year, the cybersecurity workforce gap has grown more than twice as much as the workforce.

Candidates are applying, but they aren't quite qualified for the job

In the fast-paced world of cybersecurity, the threat landscape is constantly evolving, and bad actors are becoming increasingly sophisticated in their attacks. This has created a dire need for knowledgeable candidates who can keep up with the changes in technology. However, despite the growing number of digital jobs, the industry is facing a critical shortage of qualified candidates to fill these positions.

One of the biggest obstacles in closing the talent gap is the unobtainable standards set for entry-level employees. Many job postings require new hires to possess advanced certifications like the Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM). While these certifications are valuable, the prerequisites for taking the exams include several years of job experience and are expensive and difficult to pass on the first attempt. Furthermore, those who do obtain these certifications tend to apply for higher-level positions rather than entry-level ones.

This approach has inadvertently barred many potential cybersecurity professionals from entering the field at the start of their careers. With so few qualified candidates available, it's crucial to find new ways to identify and train individuals who possess the necessary skills and aptitude for the job. The industry needs to be more inclusive and find innovative approaches to bridge the talent gap and meet the urgent demand for qualified cybersecurity professionals.

> The delicacy of digital assets demands a higher level of technical expertise, particularly for entry-level jobs. Aspiring candidates need to demonstrate proficiency in various programming languages, including Java, Golang, Python, and C++, alongside a thorough understanding of Linux, intrusion detection, and risk assessment. These are just a few of the many skill sets required.

Getting the job done while short-staffed

In today's digital landscape, most organizations rely on a complex web of 45 to 75 security tools to safeguard their valuable data and information. While these tools are essential, they generate a daunting number of logs and security alerts every day, often numbering in the thousands.

Analyzing and investigating each of these alerts requires individuals with the right education, experience, and expertise to make quick, informed decisions and take swift action when needed. However, as the cybersecurity threat landscape becomes increasingly complex, the pool of candidates with the necessary skills and experience to mitigate these challenges is limited, and finding a qualified candidate for an open position is often a stroke of luck.

Furthermore, as cybersecurity workers are aware of their high demand, qualified candidates demand high salaries, and in today's market, whoever is willing to pay more will win the talent race. This presents a significant challenge for organizations seeking to fill multiple positions simultaneously with highly specialized experts while remaining on a budget. The reality is that many organizations struggle to fill the gaps in their cybersecurity teams. Even though organizations invest in certain security systems, often no one is available to react to critical alerts, leaving the organization vulnerable to cyberattacks and other security breaches.

As organizations continue to grapple with the shortage of skilled cybersecurity professionals, the question arises: how can we get the job done while being understaffed? One solution may lie in next-level automation that blends artificial intelligence (AI), machine learning (ML), and behavioral analytics. This powerful combination eliminates the need for specialized technology skills and certifications, freeing up human resources to improve security posture.

However, the shortage of qualified cybersecurity professionals cannot be ignored. A comprehensive approach that includes investment in education and training, offering competitive salaries, and automating processes can help address the shortage and better protect against cyberthreats.

The time has come for businesses to step up and secure their systems and data by putting the right people and systems in place.

References:

https://newsroom.ibm.com/2020-06-30-IBM-Study-Security-Response-Planning-on-the-Rise-But-Containing-Attacks-Remains-an-Issue

https://panaseer.com/reports-papers/report/2022-security-leaders-peer-report/

https://www.isc2.org/Research/Workforce-Study

https://elevatesecurity.com/

https://www.forbes.com/sites/forbesbusinesscouncil/2022/12/06/fixing-the-cybersecurity-staff-shortage/?sh=2fb0b3445b4a

https://www.securitymagazine.com/articles/

https://www.cybersecuritydive.com/news/cybersecurity-talent-gap-worker-shortage/639724/

https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

https://fortune.com

https://resources.infosecinstitute.com/topic/7-top-security-certifications-you-should-have/

https://www.forbes.com/advisor/education/entry-level-cyber-security-jobs-guide/

The Rise of Hacktivism

How the geopolitical situation is driving change in the digital landscape

In recent years, hacktivism has undergone a significant transformation. The once disorganized and fluid social groups like Anonymous were known for their diverse agendas and lack of long-term strategy. From taking on hate groups to pilfering government secrets, hacktivist campaigns have been making waves for years. Some of the more notable old-school examples include Operation KKK, a direct attack against Ku Klux Klan members and supporters, and Operation AntiSec, which sought to obtain and leak classified government documents. But a new breed of hacktivist groups has entered the digital stage. These new groups are more focused, structured, and sophisticated, and their operations have become a growing concern for governments and corporations worldwide.

Known as "Hacktivism 2.0," this new era of hacktivism has arisen in response to conflicts in Eastern Europe and the Middle East. These state-mobilized hacktivist groups are responsible for carrying out major cyber attacks against governments and corporations across the West. The impact of these attacks has been significant, with countries like the United States, Germany, Lithuania, Italy, Estonia, Norway, Finland, Poland, and Japan being particularly targeted.

The new hacktivist groups operate like structured organizations, characterized by a clear political ideology, a hierarchy for their members and leaders, and even a formalized recruitment process. They have a strong public relations presence, carefully crafting and publicizing their success stories to highlight their significant impact in the cyber world.

Their operations are no longer limited to petty distributed denial of service (DDoS) or defacement attacks on low-profile websites. Instead, they are capable of carrying out large-scale, disruptive attacks against their targets such as government agencies and organizations, often with an extensive public relations campaign to magnify their impact, becoming a significant threat that these groups pose to both private and public entities.

> Anonymous first became associated with hacktivism in 2008 after carrying out a series of actions against the Church of Scientology called Project Chanology. The Church responded with a cease-and-desist letter to a video of Tom Cruise praising the religion. In retaliation, 4chan users organized a raid against the Church, involving prank-calling its hotline, sending black faxes to waste ink cartridges, and launching DDoS attacks on Scientology's websites.

> NoName057(16) is among the pro-Russian groups performing DDoS attacks on websites belonging to governments, news agencies, suppliers, telecommunications companies, and more in Ukraine and neighboring countries supporting Ukraine.

Hacktivism 2.0 and the shift to Government Agendas

Two years ago, a shift in hacktivism began to emerge in the Middle East. Several hacktivist groups like Hackers of Savior, Black Shadow, and Moses Staff quietly rose to prominence, focusing solely on launching attacks against Israel. These groups did not shy away from their affiliation with the Iranian regime's anti-Israel narrative. At the same time, other groups in the region dedicated themselves to targeting pro-Iranian entities, united only by their opposition to the Iranian regime.

However, this phenomenon isn't exclusive to the Middle East. The ongoing Russian-Ukrainian war has also been shaped by hacktivism. In early 2022, the Belarusian Cyber-Partisans, a group established in 2020 to oppose the Belarussian government, began launching devastating cyberattacks to obstruct Russia's troops.

The hacktivist group that has been most vocal in its support of Ukraine is TeamOneFist, a pro-Ukraine collective that caused a blackout at the airport in Khanty-Mansiysk City, Russia, after targeting the natural gas power plant in August last year.

With the rise of hacktivism, the Ukrainian government has mobilized the IT Army of Ukraine to launch a series of cyberattacks against Russia. This new wave of hacktivism has also given rise to groups that support the Russian geopolitical narrative, including Killnet, Xaknet, From Russia with Love (FRwL), and NoName057(16), among others.

The Russian-mobilized groups initially focused on specific geographical areas but have since expanded their scope to target anyone opposing the Russian agenda, from Europe and the United States to Asia. These attacks have included significant assaults on the governments and major corporations of various countries, including the US, Lithuania, Italy, Estonia, Norway, Finland, Poland, Japan, and more. One notable example is NoName057(16)'s cyberattack on the website of the Finnish Parliament in August 2022 after Finland expressed interest in joining NATO.

KillNet

The new kids on the block

The group's expanded focus resulted in a significant increase in the range of targets, including high-profile ones like major government websites, airports, and more. While the impact of some of these attacks is difficult to gauge, many of them have proven to be successful. They have caused significant downtime for major websites, some of which provide essential public services.

The group's attacks have targeted a wide range of high-profile targets, including major government websites and airports, among others. While the full extent of the damage caused by these attacks is difficult to determine, many of them have resulted in some downtime for major websites that provide essential public services. However, most countries on the receiving end of Killnet's attacks have been able to fend off the attacks or easily recover from them.

But Killnet's reputation stems not from its hacking capabilities or advanced methods, but more from its ability to disrupt services and claim victory in grandiose ways. The group is known for its flamboyant PR tactics, including flashy announcement videos, memes, and watermark images, which are shared on social media and reported by news outlets. While Killnet has expressed interest in collaborating with the Russian government, there is currently no evidence that it is under state control.

How they organize

Hacktivist groups are gaining traction in the cyber world, with an increasing number of followers joining their cause. Bound by a shared manifesto and clear rules, these groups represent a new frontier in cyber warfare. With over 89,000 subscribers on their Telegram channel, Killnet is one of the most prominent groups, being highly organized, boasting a military-like structure with a top-down hierarchy and multiple specialized squads responsible for executing their missions.

At the heart of Killnet's operations is its former leader, KillMilk. The group employs a decentralized approach, with each small squad having its own designated commander, improving the group's overall survivability. This tactic has proven highly effective as the group continues to grow in size and power. Killnet's rules and targets are laid out on their Telegram page, along with instructions on how to join or create additional squads for those seeking more autonomy or advancement within the group.

This strategy has allowed Killnet to recruit new members at an impressive rate, further bolstering their capabilities.

Killnet's success has not gone unnoticed, and other groups are now seeking to collaborate or even join forces altogether. As the group continues to evolve, it remains to be seen how far they will go and what impact they will have on the world of cyber warfare. With their strategic organization, clear structure and growing ranks, Killnet is a force to be reckoned with.

Killnet activities world-wide

Norway – In a coordinated effort, Killnet hackers launched a series of DDoS attacks against Norwegian organizations on June 28, 2022. The targets of the attacks and the extent of the damage caused remain unclear. However, the National Security Authority of Norway released a statement confirming that no private data was compromised during the attacks. .

Italy – In May 2022, Killnet launched a highly publicized attack on the Eurovision song contest. Russia was prohibited from competing in the competition, so the hacking group attempted to carry out a DDoS attack. The attack was ultimately blocked by Italy's police department, but the country didn't escape unscathed. Killnet retaliated by hitting the Senate and National Health Institute websites with similar attacks. Despite being thwarted, the attack demonstrated the group's boldness and their willingness to take on high-profile targets.

USA – The group's actions have included a distributed denial of service (DDoS) attack on Bradley International Airport in Connecticut, which was confirmed by US authorities in March of 2022.

Killnet has also claimed responsibility for a cyberattack on Lockheed Martin, a major US defence corporation. The attack was carried out in retaliation for the US supplying HIMARS systems to Ukraine, which Killnet sees as an act of aggression against Russia. The group's founder, known as "Killmilk," has accused Lockheed Martin of sponsoring "world terrorism" and being responsible for "thousands and thousands of human deaths." Killmilk announced prior to the attack that it would be a new type of cyberattack targeting the company's production systems as well as information about its employees.

Japan –The group targeted several high-profile Japanese websites in September, in response to Japan's support for Ukraine in the escalating Russian-Japanese conflict over the Kuril Islands.

Killnet's attacks were highly effective and caused significant disruptions to key Japanese websites. The group successfully targeted the e-government website, the public transportation websites for Tokyo and Osaka, the JCB payment system, and Mixi, which is Japan's second largest social media site.

Germany: German government and politicians' websites have been targeted by Killnet, as well as those of other high-profile organizations. The attacks were in response to the German government's decision to supply military equipment to Ukraine.

January 26th 2023 the German Federal Office for Information Security (BSI) announced a wide-ranging DDoS attack against various agencies and companies in Germany. Airports, companies in the financial sector, and federal as well as state administrations were particularly affected. Killnet had reportedly announced the attacks in advance as retaliation for Germany's decision to send Leopard 2 battle tanks to Ukraine.

Finding new talent

Once opening their doors for everyone interested, Hacktivist groups now are taking a more exclusive approach to recruitment, seeking out only the most skilled and knowledgeable hackers or experts in specific fields to join their ranks. This approach is aimed at minimizing the risk of mistakes that could expose the group's entire operation. By handpicking the most capable members, these groups hope to build a team that can operate with precision and efficiency. However, some groups are struggling to find enough skilled hackers, leading to a recent trend of relaying DDoS attack instructions to the masses and enlisting the help of a wider pool of less-skilled individuals to carry out their attacks.

New World Order

The past few years have been marked by an upswing in conflict across Eastern Europe and the Middle East, with far-reaching consequences for people's lives and geopolitical situations around the globe. One of the most striking effects of these conflicts has been the escalation of tensions in the world of cyberspace.

Where once the term "hacktivism" was little more than a buzzword, today it represents a serious and growing threat to global organizations. Hacktivist groups have become increasingly organized, structured, and sophisticated, ushering in a renaissance era for this type of activity. Of particular concern is the fact that many of these groups have clear affiliations with specific states, serving the interests of those governments at the expense of other countries and organizations.

While hacktivism initially emerged as a phenomenon associated with specific conflict areas, it has rapidly spread to other parts of the world. This proliferation is expected to continue, with hacktivist operators enhancing their arsenals and unleashing increasingly sophisticated and damaging state-level attacks. What's more, an increasing number of governments are taking note of the success of state-mobilized hacktivist groups and may seek to create their own, making it clear that this phenomenon is here to stay.

Whether you view hacktivism as a legitimate form of dissent or a dangerous threat to cybersecurity, it is impossible to deny the profound impact it has had on politics and activism. By blurring the line between virtual and real-world activism, hacktivism has forced society to re-evaluate what it means to engage in dissent and activism in the digital age, and to confront the new and often unpredictable challenges of this new era.

References:

https://en.wikipedia.org/wiki/Anonymous_(hacker_group)

https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos

https://thecyberexpress.com/the-scariest-ransomware-groups-in-2023/

https://www.helpnetsecurity.com/2023/01/18/cybersecurity-in-2023-russian-escalation-chinese-espionage-iranian-hacktivism/

https://www.bloomberg.com/news/articles/2022-06-30/russian-hackers-target-norway-in-latest-volley-of-cyber-attacks

https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/

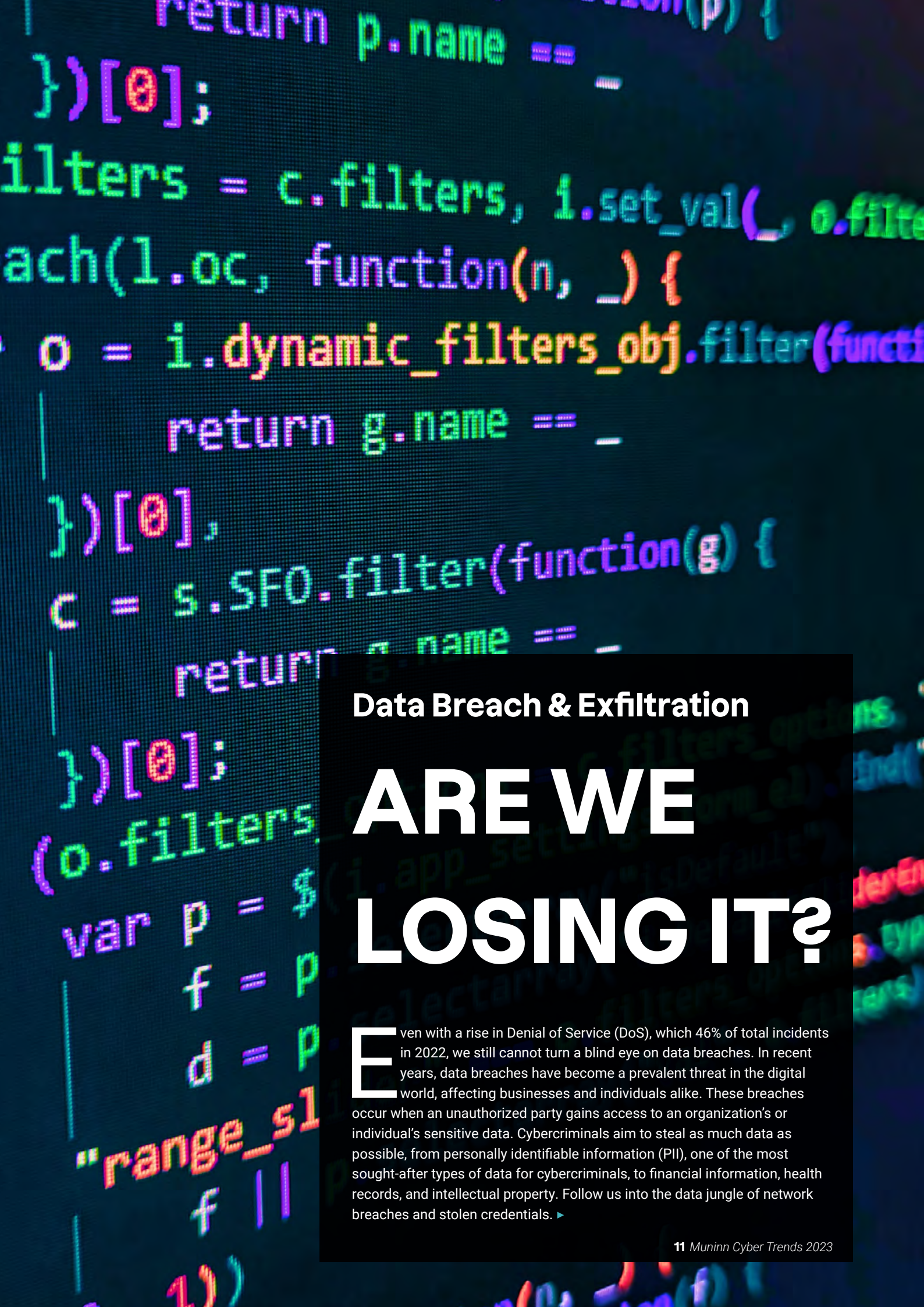
https://en.wikipedia.org/wiki/Killnet#cite_note-14

https://www.bleepingcomputer.com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/

https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows

https://www.computerweekly.com/news/365530999/Killnet-DDoS-attacks-disrupt-Nato-websites

https://www.jpost.com/israel-news/moses-staff-hackers-strike-again-attack-israeli-engineering-companies-683855



Data Breach & Exfiltration

ARE WE LOSING IT?

Even with a rise in Denial of Service (DoS), which 46% of total incidents in 2022, we still cannot turn a blind eye on data breaches. In recent years, data breaches have become a prevalent threat in the digital world, affecting businesses and individuals alike. These breaches occur when an unauthorized party gains access to an organization's or individual's sensitive data. Cybercriminals aim to steal as much data as possible, from personally identifiable information (PII), one of the most sought-after types of data for cybercriminals, to financial information, health records, and intellectual property. Follow us into the data jungle of network breaches and stolen credentials. ▸

Recent statistics and a Muninn customer case on data exfiltration

The leading types of attacks involved in data breaches are constantly evolving. The top five varieties currently include stolen credentials, ransomware, and phishing. Despite the existence of around 180 distinct action types, the majority of breaches (73%) are attributed to the top ten varieties.

When it comes to analyzing cyberattacks, timing is just one piece of the puzzle. By examining the Event Chain data and tracing the path of an attack, we can gain a more nuanced understanding of the breach. According to Verizon's data breach report, the majority of successful attacks involve only a few key actions, namely Phishing, Downloader, and Ransomware. However, breaches that utilize five or more actions are a rarity. As defenders, our ultimate goal is to elongate the attack chain. With each additional step, defenders gain the opportunity to intervene, detect, respond, and recover. Attackers know this, and they are less likely to attempt longer attack chains as a result. Therefore, by extending the attack path, we increase our chances of thwarting cyberattacks before they can do any significant damage.

By analyzing industry-specific data, we may gain a more precise understanding of the current situation:

- **83%** of organizations had more than one data breach in 2022.
- **82%** of all breaches involved 'the human element' (the use of stolen credentials, phishing, misuse or human error) in 2022
- Approximately **47%** of all cybersecurity incidents involved Personally Identifiable Information (PII), **46%** of involved Authentication Credentials and **7%** involved Payment Card Data.
- **60%** of data breaches lead to increases in prices passed on to customers in 2022.
- The global average cost of a data breach was **$4.35M USD** in 2022.
- Approximately **814,000** phishing websites were created in 2022.

References:

https://www.tekspace.com.au/blog/cyber-security-stats-2022/

https://www.blackfog.com/the-state-of-ransomware-in-2022/#:~:text=We%20recorded%2028%20ransomware%20attacks,known%20UK%20snack%20food%20manufacturer.

https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-data-exfiltration

https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/

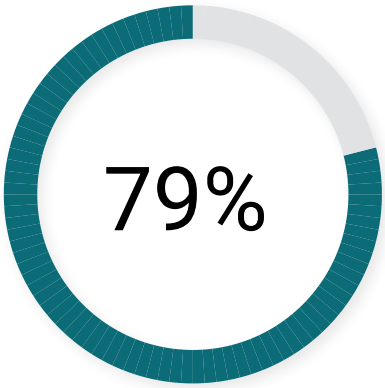
https://www.ibm.com/au-en/reports/data-breach

Financial Sector:

Financial breaches involving servers increased from 50% in 2016 to 90% in 2022. However, the type of attack known as “Server-Web application” has seen a significant rise from 12% to 51% during this period, becoming one of the top three attack patterns. These attacks often involve the use of stolen credentials, which is the main data stolen in this industry, and brute force hacking and credential stuffing are the most common techniques used to obtain such credentials. It is noteworthy that web application attacks and stolen credentials are often intertwined.

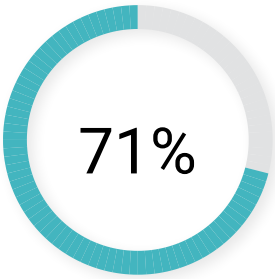
System Intrusion has surged from 14% in 2016 to 30% in the previous year. While organized crime was only responsible for 49% of breaches in 2018, it has risen significantly to 79% in recent years. As a result, ransomware attacks have become more prevalent due to their high-profit potential and low risk. It is expected that criminals will continue to use ransomware as an attack vector in the future.

Top Attack Patterns

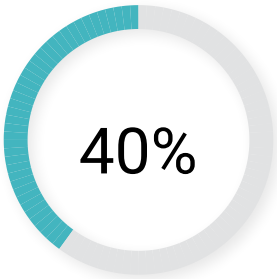


Basic Web Application Attacks, System Intrusion and Miscellaneous Error represent 79% of breaches.

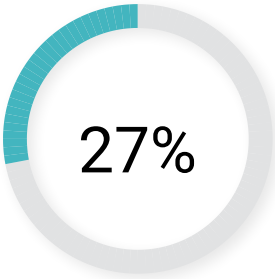
Data Compromised



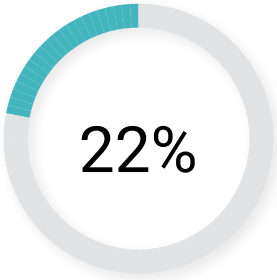
Personal



Credentials



Other



Bank

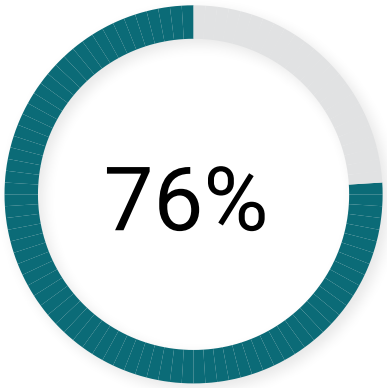
Healthcare:

Internal actors have always had a primary role in security breaches in the healthcare industry. But the game has changed, and the old guard is losing its grip. Although employees are still causing breaches, they're now more than 2.5 times more likely to make a mistake than to intentionally misuse their access. The most common errors are mis delivery and loss, but since 2019, the industry began seeing the rise of basic web application attacks, which have become a serious problem for everyone, not just in healthcare.

Hackers are increasingly targeting healthcare, launching run-of-the-mill attacks and more impactful ransomware campaigns. With ransomware comes the associated risk of actor disclosure, which is bad news for anyone who wants to keep their data safe.

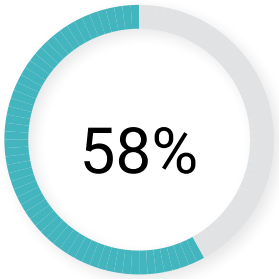
The statistics show that still more often personal data than medical data is compromised. This raises some important questions. Has the industry failed to secure personal data while tightening controls around medical data? Are actors indiscriminately encrypting records without considering the consequences? Only insiders can answer these questions for certain.

Top Attack Patterns

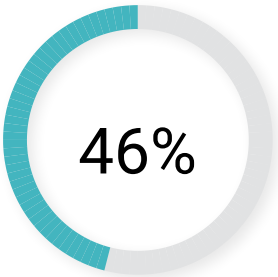


Basic Web Application Attacks, System Intrusion and Miscellaneous Error represent 76% of breaches.

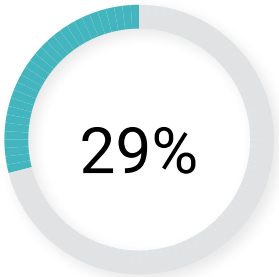
Data Compromised



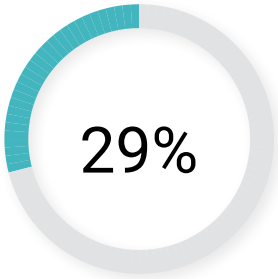
Personal



Medical



Credentials



Other

Manufacturing:

Top attack patterns: System Intrusion, Basic Web Application Attacks and Social Engineering represent 88% of breaches

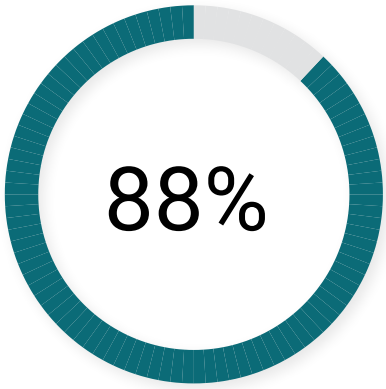
Data compromised: Personal (58%), Credentials (40%), Other (36%), Internal (14%) (breaches)

The manufacturing industry, known for its efficient production of vital components for modern living, has become an attractive target for cybercriminals. In addition to espionage, criminals are now targeting manufacturing firms with Denial of Service (DoS) attacks, credential attacks, and ransomware. Primarily targeted for its sensitive schematics and trade secrets, recent trends indicate a shift towards financially motivated attacks.

DoS attacks have become a significant concern for manufacturing companies as they disrupt productivity and impact availability, leading to losses. Although the percentage of incidents related to DoS attacks dropped in 2018, it has been increasing once again, up until the present day.

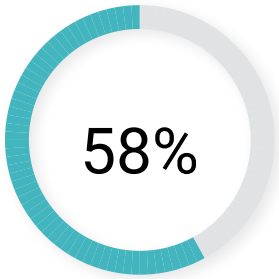
Manufacturing companies are also vulnerable to common breaches like stolen credentials (39%), Ransomware (24%) and Phishing (11%), which can cause significant damage to the industry. As the manufacturing industry continues to rely on technology and integrate IT with the OT (operational technology) side, safeguarding against cyberattacks has become much more crucial. Cybersecurity is a top priority for this industry and failing to do so could result in a halt in production and massive losses, putting entire companies at risk.

Top Attack Patterns

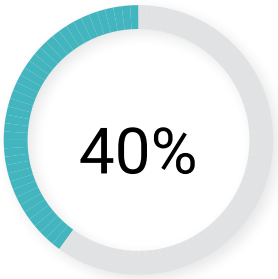


Basic Web Application Attacks, System Intrusion and Miscellaneous Error represent 88% of breaches.

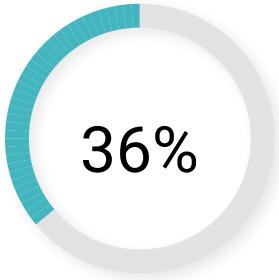
Data Compromised



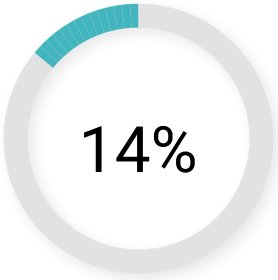
Personal



Credentials



Other



Internal

Data Breach

A Muninn Case

When we are looking at the evidence, data breaches and data exfiltration are a recurring challenge that organizations from various industries face on a daily basis. To bring this reality to light, we have compiled some examples from our own findings. In one particular case, a breach occurred via an end point device.

To illustrate the sequence of events, we have reconstructed a timeline. At that point all network traffic was being monitored, including remote devices, using the Muninn Endpoint Agent on all Windows clients.

Reconnaissance, the preliminary stage of a cyberattack, involves the gathering of vital information about a target system or network. With the rise of cybercrime, this process has become increasingly sophisticated, utilizing various tactics like scanning, footprinting, and enumeration to identify potential vulnerabilities. In this critical phase, attackers seek to gather as much information as possible, including IP addresses, operating systems, network topology, software versions, and user accounts. The information obtained through reconnaissance is then used to plan and execute subsequent stages of an attack, making it a crucial step in the success of any cyberattack. As cyberthreats continue to escalate, proactive measures such as reconnaissance are essential for organizations to protect themselves and mitigate potential vulnerabilities.

2 WEAPONIZE

This phase typically involves crafting a payload, such as a malicious email attachment, a software exploit, or a malware package, that can be delivered to the target system or network to initiate the attack. In our case the attack was initiated through a phishing email. The actual breach was detected with a series of notifications, including the notification 'Local blacklisted executable detected'.

3 EXPLOIT

This example of a cyberattack just got started: After the company whitelisted some legitimate executable files that were related to specific agents installed on their endpoints, they thought they were in the clear. But the remaining notifications were unexpected and a warning sign of potential illegal activities happening on their local machines.

Upon further investigation, it was discovered that a certain user had executed several system commands under C:\Windows\System32, including cmd.exe, findstr.exe, wmic.exe, and netsh.exe.

Now, wmic.exe is normally used by system administrators to retrieve a vast amount of information about local or remote computers using a command-line interface for Windows Management Instrumentation.

But this user submitted the following command:

C:\WINDOWS\system32\cmd.exe /d /s /c "C:\ WINDOWS\system32\wbem\wmic.exe os get /value

This was very suspicious since the list of system information was completely irrelevant to an ordinary user.

The infected machine wasted no time in hunting down hosts on the network with SMB file shares. As it searched a significant amount of notifications, all with the ominous label of 'Lateral movement using SMB admin shares'. All of this occurred within a single minute.

The malware was spread throughout the network with efficiency and high speed.

Within seconds of the previous barrage of notifications, the infected machine went on a rampage, unleashing over 100 'Remote execution using RPC' commands towards other hosts on the network that had accessible file shares - in just a matter of minutes.

This kind of behavior at such a rapid pace is a clear indicator that the infected machine was attempting to remotely execute malicious applications or deploy malware on other machines in the network.

But that's not all. Shortly after, the malware was executed on the other network hosts that had just been discovered, triggering a deluge of 'SMB Suspicious File Renaming' notifications:

All original files were renamed as hexadecimal values.

After gaining unauthorized access to a system, the attacker typically seeks to establish persistence to ensure continued access, even after the initial breach has been discovered and remediated.

During the maintain phase, the attacker may use various techniques to maintain their foothold on the system, such as installing backdoors, creating new user accounts, or modifying system configurations. They may also attempt to cover their tracks to avoid detection by system administrators or security personnel.

SUMMARY

Being able to gain full insights into all actions within a network makes it possible to follow such an attack right from the start. Depending on the organization's policies an attack can been prevented altogether and at any given level of the attach's progress. AI and machine learning can adjust to and analyze network patterns and respond accordingly stopping the attack at the very first step, in the above case the endpoint user. The infected laptop could be neutralized before any damage can be done, malware spread, and the loss of valuable data and downtime can be prevented.

Cybercriminals have a clear pattern of exfiltrating data and often do it through the very protocols we use every day. DNS and HTTPS, two commonly used protocols that firewalls and other blocking devices often overlook.

Muninn's innovative technology is designed to detect any suspicious activity in DNS communication, such as an unusually large amount of data being transmitted or a high volume of DNS requests per second. When such activity is detected, Muninn swiftly raises the alarm with its "DNS Tunneling" alert, giving cybersecurity staff a fighting chance to thwart the attackers and safeguard their valuable data.

Digging Deeper

DNS Tunneling — The Covert Threat to Network Security

What is DNS?

Have you ever heard of DNS tunneling? Simply put, DNS, the Domain Name System, is here to simplify online traffic. Acting as the phone directory of the internet, DNS provides users with a seamless way to access their desired websites.

While most users prefer to type in the domain or URL of the website they want to visit, the internet's infrastructure relies on IP addresses to direct traffic to its destination. DNS acts as a mediator, providing conversions between domain names and IP addresses. Without DNS, finding anything online would be a nearly impossible task. To access a website, one would need to know the precise IP address of the server hosting it - a feat that is not only impractical, but virtually impossible.

How does DNS Tunneling Work?

DNS traffic is one of the most trusted forms of communication on the internet. In fact, organizations often allow it to pass through their firewalls, both inbound and outbound, because it is a critical component for their internal employees to access external sites, and for external visitors to use their websites.

Unfortunately, this trust is also what makes DNS tunneling such a dangerous threat to organizations. Malicious actors can exploit

DNS requests to establish a command-and-control channel for their malware, allowing them to receive inbound DNS traffic carrying commands for the malware, and exfiltrate sensitive data or respond to requests from the malware operator with outbound traffic.

This insidious technique works because DNS is an incredibly flexible protocol, with very few restrictions on the data such a DNS request can contain. Since domain names can encompass almost anything, these fields can be exploited to transmit sensitive information. Attackers can also use DNS servers under their control to ensure they receive the requests and respond in the corresponding DNS replies.

In reality, a cybercriminal will register a malicious domain, such as malware.com. The domain's name server directs to the cybercriminal's server, where the malware is installed and waiting.

The next step involves infecting a computer with malware which will penetrate the organization's firewall. While most traffic is restricted by the firewall, DNS requests are generally allowed to pass through. The infected computer is therefore able to send queries to the DNS resolver, which in turn sends requests for IP addresses to top-level and root domain servers.

The DNS resolver then routes queries to the cybercriminal's server, where the tunneling program is implemented. This creates a connection between the cybercriminal and the victim via the DNS resolver, allowing the attacker to use the tunnel for malicious purposes, such as exfiltrating sensitive information.

Because there is no direct connection between the cybercriminal and the victim, tracing the cybercriminal's computer becomes a difficult task.

Due to the ease with which DNS tunneling attacks can be executed and the broad toolkit available, even unsophisticated attackers can use this technique to bypass an organization's network security measures and sneak data out undetected.

Some traffic actions that indicate a DNS Tunneling Attack could be:

- **Unusual Domain Requests**
- **Requests for Unusual Domains**
- **High DNS Traffic Volume:**

While each of these factors on their own may be harmless, if an organization is encountering several or all of these anomalies, it could be a revealing sign of DNS tunneling malware that has infiltrated and is actively operating within their network.

In such case the Muninn Dashboard would show a high alert categorized under DNS Tunneling including a short and longer description such as:

DNS Tunneling
Possible DNS Tunnel, large consecutive DNS responses detected from 10.0.0.105. Detected on:. Total Large Bytes: 1879

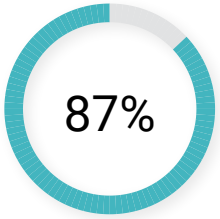
Or an even more detailed report such as:

conn10.0.0.11910.0.1.7Ports 5353 -> 5353 Sent/recv 654<->5890 bytesid. orig_p = 5353,resp_pkts = 9,resp_ip_ bytes = 5890,id.vlan = -,orig_bytes = 626,id.resp_p = 5353,id.vlan_inner = -,local_orig = T,orig_ip_bytes = 654,orig_ pkts = 1,missed_bytes = 0,history = D^d,tunnel_parents = -,duration = 10.876185,local_resp = T,uid = CbXy1o1bdTb38zL1el,resp_bytes = 5638,vlan = 1,inner_vlan = -,service = dns,conn_state = SF,proto = udp,id. orig_h = 10.0.0.119,id.resp_h = 10.0.1.7

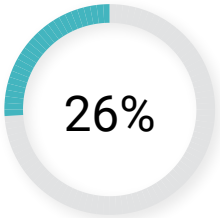
By delving into the available and detailed information, a user can investigate these traffic actions and determine whether they pose a genuine threat or simply fall within the realm of regular DNS traffic. In addition, machine learning has the ability to adapt to these network behavior patterns and can thwart data exfiltration right from the outset by flagging unusual behavior.

DNS tunneling may be a covert technique, but it is no match for organizations that are prepared. By implementing the right security measures and training employees, organizations can stay one step ahead of the bad guys and protect their sensitive data as well as their customer's data.

Facts on DNS attacks



Of organizations experienced DNS attacks



Of organizations reporting sensitive customer information stolen

Reference

https://www.efficientip.com/news/2021-idc-dns-threat-report-release/

How to Tame the Cybersecurity Alert Monster

When Too Much of a Good Thing is Bad

We all can agree that visibility of all actions taken within your network is key to successful cyberdefence. In recent years, security tools and programs have made significant advancements in detecting and preventing advanced security threats worldwide. However, can too much of a good thing become bad? With a shortage of cybersecurity staff and an overwhelming number of notifications and alerts, new challenges arise.

A poll conducted in 2020 asked 427 security professionals about the volume of alerts at their companies. A staggering 70 percent reported that their alerts had more than doubled in the last five years. What's more, a total of 93 percent claimed that they couldn't address all the alerts in a single day. This data paints a clear picture: the cybersecurity world is experiencing alert fatigue.

Alert fatigue is not just a term confined to the world of cybersecurity. It's a phenomenon that's prevalent in various fields, including intensive care units (ICUs). With the advancements in technology and limited resources, nurses in ICUs are bombarded with an overwhelming amount of information that they don't have the time or resources to address. Similarly, in the cybersecurity world, alert fatigue is a state of mind where security analysts receive too many alerts or false positives from various sources like device monitoring, email filtering, internet security, network firewalls, and more. The never-ending list of potential threats makes it challenging for security teams to identify and respond to actual security risks and threats.

The above mentioned survey revealed that 99% of security teams reported multiple issues related to receiving high volumes of security alerts, including*:

- Missing major issues that are hidden in the noise,
- Wasting time chasing down false positives
- And taking too long to triage alerts.

To address this challenge and combat alert fatigue, organizations can implement several key strategies. The first strategy is reducing the volume of alerts by filtering and prioritizing them. By streamlining the alerts, analysts can focus on the most critical issues. The use of artificial intelligence and machine learning, like Muninn Detect, can automate this process and ensure that only the most important alerts are flagged, saving time and increasing efficiency.

Another important strategy is improving the accuracy of alerts. False positives are a major contributor to alert fatigue. They can cause analysts to become desensitized to notifications and disregard them, which can result in overlooking the real threats. Implementing more advanced detection techniques, such as behavior-based detection systems, can help reduce the number of false alarms. These systems can identify patterns and anomalies in user behavior, making it easier to pinpoint genuine threats.

On top of that organizations must provide their security analysts with the tools and resources they need to manage their workload effectively. For example, implementing a centralized dashboard can help prioritize and manage alerts efficiently. This approach provides a comprehensive view of the security landscape, enabling analysts to focus on the most critical issues.

In today's rapidly evolving cyberlandscape, ensuring that security analysts are well-equipped with the necessary skills and knowledge to manage and respond to alerts is more important than ever. Analysts need to be equipped with the skills and knowledge necessary to manage and respond to alerts effectively and manage their workload.

In addition to training, automating incident response processes can be a powerful tool in the fight against alert fatigue. By automating routine tasks such as malware detection and containment, security analysts can focus on more complex threats and investigative work. This not only reduces the risk of human error but also ensures consistent and effective incident response.

Reference

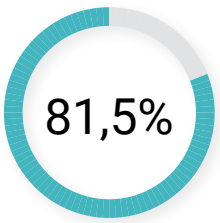
https://www.tekspace.com.au/blog/cyber-security-stats-2022/

Data on false positives from our Muninn data base

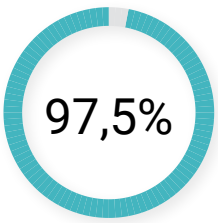
We have analyzed three customer cases to demonstrate how Muninn can effectively minimize noise and false alarms, providing only relevant alerts to the IT security manager. Our evaluation included examining the most frequent high alerts prior to implementing Muninn and comparing them to the alerts received a few weeks after implementing our sensors and establishing a baseline.

HIGH Notifications	Customer Case #1		Customer Case #2		Customer Case #3	
	Before Baselining	After Baselining	Before Baselining	After Baselining	Before Baselining	After Baselining
SMB Ransomware filename detected	1	0	11	0	0	0
Port scan detected	1	0	0	0	0	0
Remote execution using RPC	5	1	20	1	0	0
Lateral mov. using SMB admin shares	1	4	0	0	0	0
Address scan detected	19	0	1	0	0	0
DNS Tunneling	0	0	6	0	0	0
Global address scan	0	0	2	0	0	0
SMB Suspicious File Renaming	0	0	0	0	1	0
ARP scan detected	0	0	0	0	0	0
HTTP Authentication Bruteforce	0	0	0	0	40	0
SMB Sensitive File	0	0	0	0	0	0
SSH Failed Attempts	0	0	0	0	0	0
Selective Port Scan	0	0	0	0	0	0
Total	**27**	**5**	**40**	**1**	**41**	**0**

REDUCTION IN FALSE POSITIVES



Customer Case #1



Customer Case #2

Customer Case #3

OpenAI

Will ChatGPT democratize cybercrime?

OpenAI's ChatGPT, an AI-powered natural language processing tool, has made waves since its launch in November, attracting over 1 million users for a range of applications, including creative pursuits like poem writing and email campaigns, as well as code generation for websites and apps. In response to worries that it could be used for cheating, some schools have banned the use of ChatGPT and Google, who followed the trend introducing their own AI-powered chatbot called BARD.

OpenAI has confirmed that the popular online tool lacks internet access, thereby limiting its ability to provide real-time answers to user queries. Instead, the program generates modified or inferred code based on preset parameters. While ChatGPT strives to help across a range of topics, its content filters serve to prevent it from responding to questions that could pose security risks, such as code injection. However, the exploration of bypassing these filters and the potential using ChatGPT to create polymorphic malware over the last few months has moved this topic from a hypothetical scenario to a very real concern.

This is adding a potential dark side to ChatGPT, where it can be used to carry out a range of malicious activities, including phishing scams, spam messages, social engineering attacks, fraudulent customer support, and the spread of false information. Just weeks after ChatGPT debuted Check Point, a software company based in Israel, decided to combine ChatGPT and another AI-based system that translates natural language to code, to create a phishing email with a malicious Excel file. The file was weaponized with macros that downloads a reverse shell, which is one of the favorites among cybercrime actors. Check Point did not write a single line of code and instead let the AIs do all the work.

The cybersecurity community, which has historically been wary of the potential consequences of modern AI, is now also taking note due to fears that a tool like ChatGPT could be exploited by hackers with limited resources and no technical expertise f.ex. to accelerate the process of extracting usernames when enumerating against a login screen or produce authentic phishing emails.

In the case of phishing scams, ChatGPT cannot only be trained to write codes but also to create emails that appear even more authentic, especially when English isn't the receivers first language. This allows even cybercriminals with very little knowledge to distribute spam messages and spread malware, collect data, and cause harm to systems and networks. ChatGPT's ability to mimic human-like interactions can also be used in real-time and makes it a powerful tool for social engineering attacks by impersonating customer support or via a live chat on social media.

Others believe that tools like ChatGPT will be a sizable force multiplier when it comes to cyber defense and will change the game when it comes to trying to learn the secrets of malicious code, as we do not have many malware analysts in the world right now.

In the grand scheme of things, the use of ChatGPT for malicious cyberactivities looms as a major concern, but not one that is set in stone. Undoubtedly, ChatGPT's capacity to mimic human-like language has the potential to become a potent weapon for cybercriminals, unleashing a wave of phishing scams that could cripple organizations and individuals alike. Yet, with the right awareness and security protocols in place, the risk of such attacks can be mitigated. However, it is incumbent upon the tech industry to keep a watchful eye on the development and potential abuse of these advanced AI language models, and to pioneer robust safeguards that can identify and thwart malicious exploitation.

References:

https://www.sciencefocus.com/future-technology/gpt-3/

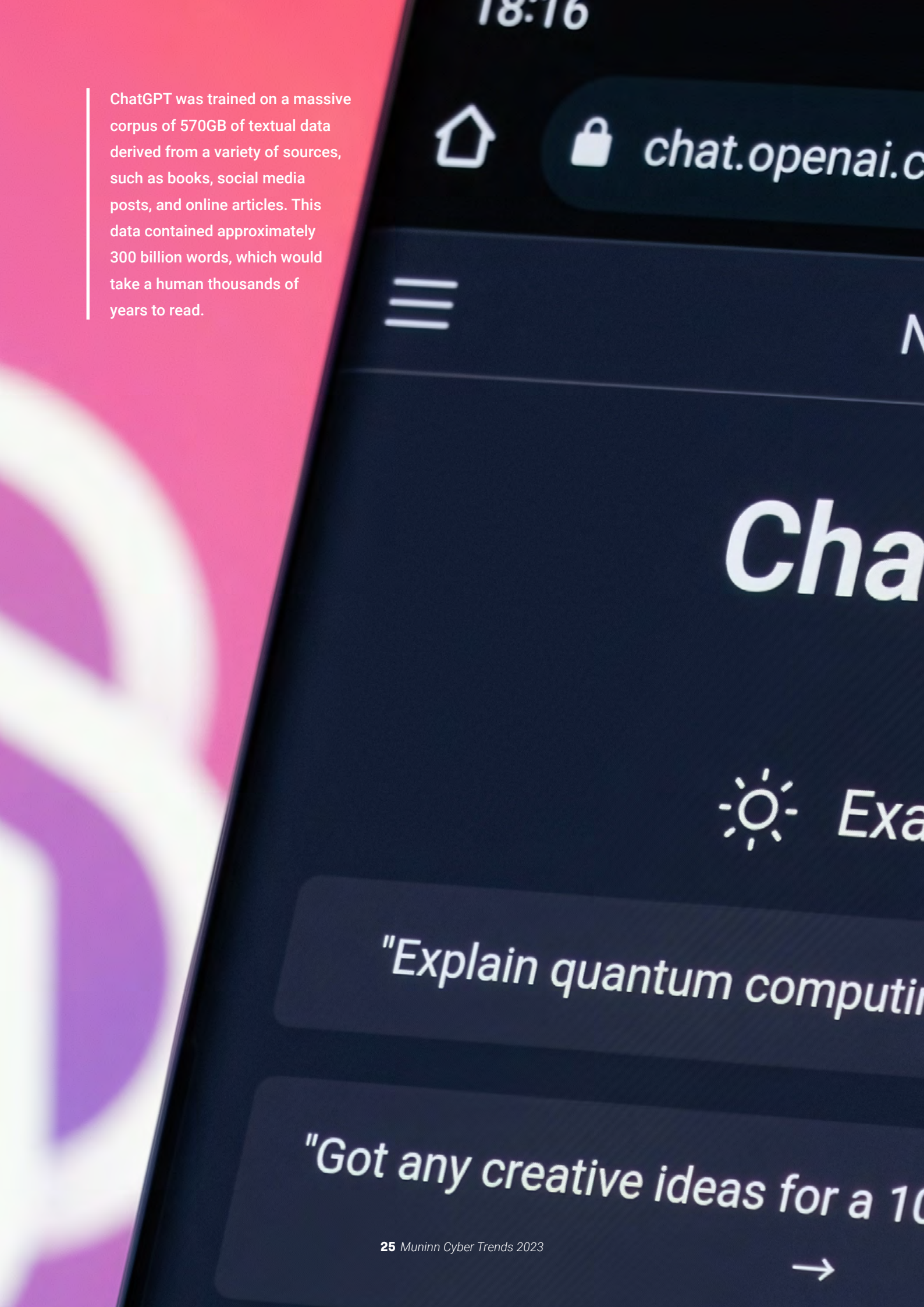
https://www.washingtonpost.com/politics/2023/01/26/yes-chatgpt-can-write-malware-code-not-well/

https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/

https://www.bloomberg.com/news/articles/2023-01-11/chatgpt-poses-propaganda-and-hacking-risks-researchers-say

https://www.cyberark.com/resources/threat-research-blog/chatting-our-way-into-creating-a-polymorphic-malware

ChatGPT was trained on a massive corpus of 570GB of textual data derived from a variety of sources, such as books, social media posts, and online articles. This data contained approximately 300 billion words, which would take a human thousands of years to read.




“The future of cybersecurity holds limitless possibilities but it’s not just about technology, it’s about people - their creativity, their resilience, and their ability to adapt to changes.”
Andreas F. Wehowsky

The Evolution of Cybersecurity

With ever-increasing ferocity, cybercriminals and state-sponsored attackers are homing in on critical infrastructure, aiming to wreak havoc and cause chaos. But according to the top security experts, what we're witnessing is just the tip of the iceberg. A whopping 80% of CISOs believe that the world is now embroiled in a "perpetual state" of cyberwarfare, with no end in sight. In 2023, we can expect to see an even higher number of attacks on hospitals and government institutions. But also new focus on data exfiltration in ransomware attacks, the rise to a new social engineering battleground and in response to that an increase in consumer concerns about online security and privacy.

With this increased focus, companies and organizations will most likely focus on third-party vendor risk management. Many organizations rely on third-party vendors for critical services and support, but these vendors also present a significant risk for cybersecurity breaches. By raising the requirements and implementing stronger vendor risk management strategies, organizations can better protect themselves against potential cyberthreats and ensure the security of their sensitive data.

But as we find solutions to what is happening today, we cannot ignore what might happen tomorrow. In the last few years and even months significant strides have been made in the field of AI and cybersecurity, but there is still a long way to go to unleash the yet unknown and full potential of AI within cybersecurity.

Therefore, Muninn is establishing the Muninn Innovation Lab (MIL), where we will be developing and implementing new and innovative solutions to address cybersecurity challenges such as false positives, malicious encrypted network traffic, sophisticated and stealthy attacks, and overwhelming volume of network traffic data. At MIL we seek innovative ideas utilizing big data, machine learning, deep learning and other advanced analytics techniques to detect and prevent cyberattacks with a cross-functional structure meaning that individuals from different departments with diverse skill sets will collaborate in the projects. But our laboratory is not just an ivory tower. In collaboration with Christian D. Jensen, Ph.D. and Sajad Homayoun, Ph.D. from Cybersecurity Engineering section of Technical University of Denmark (DTU), MIL has already tackled real-world industry challenges aimed at reducing the number of false positives using advanced machine learning techniques and was awarded an IFD industrial postdoc researcher grant in 2022 for the project.

With this sense of curiosity, the strive to find solutions and our determination in the field of cybersecurity, we at Muninn are eager to discover the opportunities and challenges that the upcoming year has in store.

www.muninn.ai

info@muninn.ai

+45 70 60 59 08