INTRO INAUDIT CYBERELLENDE PUBQUIZ

“A BIT *OF* CYBER AWARENESS EVERY DAY KEEPS THE HACKER *AWAY*”

5 ARGUMENTEN VOOR LEUKE TRAININGEN

"A BIT OF CYBER AWARENESS EVERY DAY KEEPS THE HACKER AWAY"

1. **Tussen de stoel en het toetsenbord ...**
2. **Weten is niet hetzelfde als "doen"**
3. **Het is geen 'level-playing field'**
4. **Zelfs 'legends' moeten trainen**
5. **Training hou je alleen vol als het ook leuk is !**


EUPHORIA
SCIENCE
PANIC
LOCAL
WORLD
UNIVERSE
TRUE
RATIONAL
FAKE
NEWS
MUSIC
VOLUME
TUNING

2023-10

INAUDIT CYBERELLENDE PUBQUIZ

NET BINNEN
- 11:11 LIVE Champions League | Vermoedelijke opstelling Feyenoord voor...
- 10:25 Nederland, België en Duitsland stellen zich officieel kandidaat voor 'baanbrekend...
- 08:49 Franse media over 'ultra's' na Lens-PSV: 'Nederlandse voetbal heeft vaker...
- 07:15 PREMIUM Lazio-coach Maurizio Sarri...
- 06:54 Meer dan twintig gewonden na rellen rond duel tussen Lens en PSV: 'Dit soort...

BEKIJK ALLE ARTIKELEN

Geslaagde afpersing KNVB slaat in als bom in securitywereld: 'Dit wordt alleen maar erger'

MILJOEN EURO Het is een verstandige zet, maar tegelijkertijd een 'heel verontrustend signaal' dat de KNVB heeft besloten om losgeld te betalen aan Russische cybercriminelen. Specialisten vrezen dat meer grote bedrijven binnenkort aan de beurt zijn als de Nederlandse overheid niet snel maatregelen neemt. ,,Afpersen werkt kennelijk, en dit verhaal zal de trend alleen nog maar erger maken in de toekomst."

Sebastiaan Quekel 12 sep. 2023 Laatste update: 12-09-23, 14:35

20 REACTIES

De KNVB heeft losgeld betaald - vermoedelijk ruim een miljoen euro - om te voorkomen dat gehackte persoonsgegevens van onder meer leden op straat zouden komen te liggen. Bij de aanval zijn ook identiteitsbewijzen, woonadressen en salarisgegevens van Oranjespelers en andere professionele voetballers gestolen.

In een advertentie in deze krant stelt de bond dat betalen een moeilijke keuze was, maar dat er uiteindelijk 'onder deskundige begeleiding afspraken' met de hackers zijn gemaakt. De cyberinbraak was in april en daarvan is aangifte gedaan bij de politie. Die inbraak werd opgeëist door een criminele groepering die zichzelf Lockbit noemt. Dit beruchte Russische hackerscollectief maakt gebruik van *ransomware*, ook wel gijzelsoftware genoemd.

'Je kunt wel stoer doen'

De KNVB heeft er goed aan gedaan om in te gaan op de eisen van de hackers, zegt Lisette Meij, tech-juriste en eigenaar van Lime Legal. ,,Je kunt wel heel 'stoer' doen en zeggen dat je niet betaalt, maar uiteindelijk zijn de personen waarvan de gegevens zijn gelekt daar het echte slachtoffer van", vertelt Meij. ,,Je hoort vaak dat door het betalen je het verdienmodel in stand houdt. Maar als jij als enige partij niet betaalt, verander je het verdienmodel niet. Daarmee zorg je dus alleen dat het risico dat de gegevens van betrokken personen straks op straat liggen gigantisch is."

Hackers van Lockbit werken volgens een bepaald stramien. Als de getroffen partij niet betaalt voor het ontsleutelen van de data, bijvoorbeeld omdat er goede back-ups zijn, dan beginnen ze met openbaarmaking te dreigen. ,,Vaak wordt er dan een klein deel van de data op het darkweb gezet, met de dreiging alles te openbaren als er niet betaald wordt", zegt tech-advocaat Jan Gerrit Kroon. Dat is vermoedelijk in het geval van de KNVB gebeurd.

https://therecord.media/sbu-involved-in-alfa-bank-hack

IMAGE: BRATEEVSKY VIA WIKIMEDIA COMMONS

Daryna Antoniuk
October 23rd, 2023

News Government Nation-state

Ukraine security services involved in hack of Russia's largest private bank

Ukrainian hackers collaborated with the country's security services, the SBU, to breach Russia's largest private bank, a source within the department confirmed to Recorded Future News.

Last week, two groups of pro-Ukrainian hackers, KibOrg and NLB, hacked into Alfa-Bank and claimed to obtain the data of more than 30 million customers, including their names, dates of birth, account numbers, and phone numbers, according to a post on their official website.

Alfa-Bank was sanctioned by the United States following Russia's invasion of Ukraine last year. The bank is owned by the Russian-Israeli billionaire Mikhail Fridman, who is blacklisted by the U.S. and Europe as part of efforts to impose restrictions on Russia's economy and its wealthiest businessmen.

Hackers released some of the data online, including information about Fridman and his son, pro-Russian blogger Artemy Lebedev, and Russian rappers Timati and Basta. Alfa-Bank denied reports of the leak, according to Russian news agency TASS.

A source within Ukraine's security service who requested anonymity because he is not authorized to speak publicly about the incident confirmed to Recorded Future News that the Ukrainian agency was involved in the operation, but did not provide further details.

This is not the first time Ukraine's intelligence has collaborated with hacktivists. The head of cybersecurity at the Security Service of Ukraine, Illia Vitiuk, has said previously that documents leaked by Ukrainian hackers play a significant role in the country's cyber intelligence efforts.

https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/

Cyber attacks in the Israel-Hamas war

23/10/2023

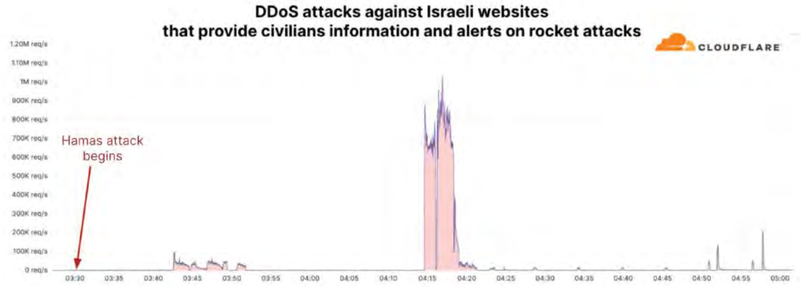

Omer Yoachimik

Jorge Pacheco

5 min read

On October 7, 2023, at 03:30 GMT (06:30 AM local time), Hamas attacked Israeli cities and fired thousands of rockets toward populous locations in southern and central Israel, including Tel Aviv and Jerusalem. Air raid sirens began sounding, instructing civilians to take cover.

Approximately twelve minutes later, Cloudflare systems automatically detected and mitigated DDoS attacks that targeted websites that provide critical information and alerts to civilians on rocket attacks. The initial attack peaked at 100k requests per second (rps) and lasted ten minutes. Forty-five minutes later, a second much larger attack struck and peaked at 1M rps. It lasted six minutes. Additional smaller DDoS attacks continued hitting the websites in the next hours.



DDoS attacks against Israeli websites that provide civilians information and alerts on rocket attacks

https://www.cpomagazine.com/cyber-security/caesars-entertainment-discloses-cyber-attack-ransom-payment-made-weeks-before-mgm-heist/

CPO MAGAZINE

HOME NEWS INSIGHTS RESOURCES

CYBER SECURITY NEWS 5 MIN READ

Caesars Entertainment Discloses Cyber Attack, Ransom Payment Made Weeks Before MGM Heist

SCOTT IKEDA · SEPTEMBER 19, 2023

As MGM casino-hotel properties in Vegas continue to struggle to get back to full operational status, Caesars Entertainment quietly disclosed its own recent cyber attack in a mandatory SEC filing. Unlike MGM, Caesars appears to have skated through their own incident by making a $15 million ransom payment to the hackers.

It also appears that the same group is behind both cyber attacks. VX-Underground has linked dark web chatter about both incidents to a newer group called “Scattered Spider” or “Roasted 0ktapus,” an affiliate of the Blackcat ransomware group that deploys their ALPHV malware during attacks. The group was first documented in December 2022 and has quickly built a reputation for skilled social engineering approaches, and are unusual in that its members are thought to be based in the US and UK.

https://tech.co/news/caesars-data-breach-state

tech.co

Caesars Data Breach Saw Hackers Steal Over 41,000 People’s Data

Think the house always wins? Casino giant Caesars would beg to differ, after admitting the scale of its recent data breach.

Written by James Laird

Updated on October 12, 2023

Casino giant Caesars has admitted that more than 41,000 of its patrons had their personal information stolen in a major September **data breach** that pre-dated that month's blockbuster MGM hack.

While the total number of victims is still be counted, Caesars has now said that 41,397 folks from the state of Maine had their details pilfered by the cybercrime gang responsible for the ransomware attack. A group called Scattered Spider has been judged responsible for the breach.

> Explaining exactly what happened in the breach, Caesars notes that it was the “victim of a social engineering attack on an outsourced IT support vendor that resulted in unauthorized access (on August 18, 2023) to Caesars' network and the exfiltration of data (beginning on or about August 23, 2023).”

Most Recent

Slack Finally Ditches X/Twitter Integration for Good
Ellis Di Cataldo - 30 mins ago

Why Is Temu So Cheap? It’s Losing Billions, That’s Why
Isobel O'Sullivan - 16 hours ago

Instagram Teases New Custom Sticker Feature You Can’t Try (Yet)
James Laird - 2 days ago

4-Day Workweek Jobs You Can Apply for in October
James Laird - 2 days ago

Fully Remote Jobs You Can Apply for in October
Adam Rowe - 4 days ago

https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware

Vox

EXPLAINERS CROSSWORD VIDEO PODCASTS POLITICS POLICY CULTURE SCIENCE MORE Give

TECHNOLOGY CYBERSECURITY PRIVACY & SECURITY

The chaotic and cinematic MGM casino hack, explained

A "limited number" of customers' Social Security numbers were taken.

By Sara Morrison | sara@vox.com | Updated Oct 6, 2023, 11:25am EDT

SHARE

Sara Morrison is a senior Vox reporter who has covered data privacy, antitrust, and Big Tech's power over us all for the site since 2019.

Did prominent casino chain MGM Resorts gamble with its customers' data? That's a question a lot of those customers are probably asking themselves after a cyberattack took down many of MGM's systems for several days. And it may have all started with a phone call, if reports citing the hackers themselves are to be believed.

MGM, which owns more than two dozen hotel and casino locations around the world as well as an online sports betting arm, **reported** on September 11 that a "cybersecurity issue" was affecting some of its systems, which it shut down to "protect our systems and data." For the next several days, reports said everything from **hotel room digital keys to slot machines** weren't working. Even websites for its many properties went offline for a while. Guests found themselves waiting in hours-long lines to check in and get physical room keys or getting handwritten receipts for casino winnings as the company went into **manual mode** to stay as operational as possible. MGM Resorts didn't respond to a request for comment, and has only posted vague references to a "cybersecurity issue" on Twitter/X, **reassuring guests** it was working to resolve the issue and that its resorts were **staying open**.

It took about 10 days, but MGM announced on September 20 that its hotels and casinos were "operating normally" again, although there may be some "intermittent issues" and MGM Rewards may not be available.

"We thank you for your patience," the company said in **its statement**. It did not provide any additional information on the reason why its systems went down in the first place.

Several weeks later, on October 5, MGM provided another update with some bad news for its guests: The hackers were able to access their personal information, including names, contact information, gender, date of birth, and driver's license, passport, and even Social Security numbers, from "some customers" before March 2019. The company did not reveal just how many people that includes, but says it is providing free credit monitoring services to them, which has become the **standard response** from companies who can't secure their customers' data.

https://www.reuters.com/business/mgm-expects-cybersecurity-issue-negatively-impact-third-quarter-earnings-2023-10-05/

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Inves

Business

Casino giant MGM expects $100 million hit from hack that led to data breach

By **Zeba Siddiqui**

October 6, 2023 4:35 AM GMT+2 · Updated 19 days ago

Aa

An exterior view of MGM Grand hotel and casino, after MGM Resorts shut down some computer systems due to a cyber attack in Las Vegas, Nevada, U.S., September 13, 2023. REUTERS/Bridget Bennett/File Photo *Acquire Licensing Rights*

Oct 5 (Reuters) - MGM Resorts International (MGM.N) said on Thursday a cyberattack last month that disrupted its operations would cause a $100 million hit to its third-quarter results, as it works to restore its systems.

One of the world's largest gambling firms, MGM shut down its systems after detecting the attack to contain damage, it said. It expects to also incur less than $10 million as a related one-time cost in the quarter ended on Sept. 30.

Cyber security trends 2023

Report | October 2023

The latest threats and risk mitigation best practice – before, during and after a hack

DOWNLOAD THE REPORT

→ READ THE ACCOMPANYING PRESS RELEASE

DISCUSS WITH US ON SOCIAL MEDIA: #CYBERSECURITYTRENDS

Investments in cyber security are paying off but an evolving threat landscape will require much greater focus on early detection and response capabilities.

Improvements in cyber security and business continuity are helping to combat encryption-based ransomware attacks, yet the cyber threat landscape is continually evolving. 2023 has seen a worrying resurgence in ransomware and extortion claims, resulting in an uptick in costly incidents, demonstrating that although progress is being made, the threat posed by ransomware shows little sign of abating.

Reports note that the number of ransomware victims surged by as much as 143% globally during the first quarter of 2023 with January and February seeing the highest number of hack and leak cases in three years. Ransomware alone is projected to cost its victims approximately US$265bn annually by 2031.

Hackers are increasingly targeting IT and physical supply chains, launching mass cyber-attacks and finding new ways to extort money from companies, large and small. Most ransomware attacks now involve the theft of personal or sensitive commercial data for the purpose of extortion, adding further cost and complexity, as well as the increased potential for reputational damage and third-party liability. Allianz analysis of a number of large insurance industry cyber losses shows that the proportion of cases in which data is exfiltrated is increasing every year – from 40% of cases in 2019 to around 77% of cases in 2022, with 2023 on course to surpass last year's total.

Protecting an organization against intrusion remains a cat and mouse game, in which the cyber criminals have the advantage. Threat actors are now exploring ways to use artificial intelligence (AI) to automate and accelerate attacks, creating more effective AI-powered malware and phishing. Combined with the explosion in connected mobile devices and 5G-enabled Internet of Things, the avenues for cyber-attacks look only likely to increase in the coming years.

Preventing a cyber-attack is therefore becoming harder, and the stakes higher. As a result, early detection and response capabilities are becoming ever more important. An intrusion can quickly escalate, and once data is encrypted and / or stolen, the consequences and costs snowball – costs can be as much as, or even more than, 1,000 times higher than if an incident is not detected and contained early, Allianz analysis shows.

Ultimately, early detection and effective response capabilities will be key to mitigating the impact of cyber-attacks and ensuring a sustainable insurance market going forward.

RaaS groups responsible for majority of incidents

Ransomware-as-a-Service (RaaS) remains a key driver for the ongoing frequency of attacks. With access to RaaS kits and services, criminals lacking the skill to develop their own malware can launch ransomware attacks quickly and affordably. With prices starting from US$40 per month, RaaS kits enable cyber criminals to make millions from extortion demands with little financial investment.

"This is not a problem that is going away," says **Michael Daum, Global Head of Cyber Claims at Allianz Commercial**. "We often deal with the same attack groups. They change – they disappear, reorganize and then reappear under a different name – but the groups with the best tactics make the most money, and then they start re-selling their tools and expertise to others. They operate like successful businesses."

Ransomware attacks against large companies typically originate from a relatively small number of groups. For example, Allianz has handled several claims attributed to the likes of Black Basta, Clop and LockBit. According to the US Cybersecurity and Infrastructure Security Agency[9], LockBit was the most deployed ransomware variant across the world in 2022, with more than 1,700 attacks since 2020 in the US alone, and approximately US$91mn of ransoms paid.

"Cyber criminals' tactics continue to evolve," says Daum. "When we talk about ransomware, we are now really speaking about attackers applying various techniques in order to extort money. Where we used to see encryption, we now see attackers steal data or carry out Distributed Denial of Service (DDoS) attacks – with no encryption applied or in combination with encryption – in order to demand a ransom."

RaaS kits enable cyber criminals to make millions from extortion demands, with prices starting at

US$40 per month

LockBit was the most deployed ransomware variant across the world in 2022, with

1,700+

attacks since 2020 in the US

US$91mn

approximate cost of ransoms paid

https://fd.nl/samenleving/1493776/timide-ogende-pepijn-21-is-volgens-om-een-van-de-grootste-cybercriminelen-van-nederland

22 okt 16:00

Timide ogende Pepijn (21) is volgens OM een van de grootste cybercriminelen van Nederland

Carel Grol

Pepijn werkte voor een cyberveiligheidsbedrijf, maar was in zijn eigen tijd een criminele hacker. ANP / Richard Brocken

In het kort

- Pepijn had in een turbulente jeugd een grote uitvlucht: de computer.
- Hij werd hacker en eiste losgeld van bedrijven die hij met software had gegijzeld.
- Het Openbaar Ministerie eist zes jaar celstraf tegen de man van 21.

De computer was de enige constante factor in het jonge leven van Pepijn. Hij was niet sportief, had geen vrienden, zijn ouders waren gescheiden, zijn stiefvader gewelddadig. Pepijn was suïcidaal en werd uit huis geplaatst. Gamen werd zijn uitvlucht.

Op zijn tiende kon hij al programmeren. Vier jaar later werd hij, tijdens een onlinespelletje, door iemand uitgedaagd. Zoals jongetjes op straat elkaar imponeren met hun voetbalvaardigheden, zo kreeg van Pepijn van deze onlinepersoon de vraag of hij iets kon doen, een kleine handeling, die het netwerkverkeer even verstoorde: een soort computervariant op een voetbaltruc.

Dat lukte. Zo werd Pepijn hacker. Aanvankelijk legde hij wel eens een lek bloot in een spelletje. Maar binnen een paar jaar werd de geïsoleerde tiener een bijna obsessieve verzamelaar van data. En een inbreker. Hij zocht zwakke plekken in websites van bedrijven en hogescholen. Vervolgens trok hij persoonsgegevens van hun site. Dan mailde hij: ik heb jullie data. Voor hem was het spielerei. Daarna vroeg hij vindersloon.

wo 14 december 2022 07:03

5 minuten

Jongeren zijn vaker betrokken bij cybercrime-zaken. Dat blijkt uit cijfers die het Openbaar Ministerie op verzoek van de NOS heeft verzameld. Vorig jaar was in bijna de helft van de cybercrime-zaken een verdachte jonger dan 21 jaar. In 2018 ging het nog om 33 procent. Theo van der Plas, programmadirecteur Digitalisering en Cybercrime bij de politie, vertelt erover in het *Radio 1 Journaal*.

"Ze worden niet alleen steeds jonger, maar er komen ook steeds meer jonge cybercriminelen bij", zegt Van der Plas. Volgens hem komt dat deels doordat het een eenvoudige vorm van criminaliteit is om in te stappen. "Jongeren voelen zich veilig achter het internet. Je hoeft slachtoffers niet in de ogen te kijken om dit te kunnen plegen."

Bendes

Tegelijkertijd neem de ernst toe: jongeren richten volgens het OM vaak ernstige schade aan. Ook Van der Plas beaamt dat het niet meer om "eenzame jongeren op een zolderkamer" gaat. Het gaat steeds meer om georganiseerde bendes: "Cybercrime heeft zich vermengd met de georganiseerde misdaad, er wordt tonnen in verdiend."

Ook ziet hij steeds vaker dat dit soort criminaliteit online wordt verheerlijkt, vooral door influencers en rappers. "Jongeren zien een filmpje op TikTok en denken 'dat is makkelijk verdienen'. Dat baart ons zeker zorgen."

Aanpak begint bij ouders

Volgens Van der Plas kan de politie de aanpak niet alleen af en moeten ook gemeenten, scholen en ouders zich bewust worden van het probleem. "Als je zoon elke maand met nieuwe dure schoenen thuiskomt, is er wel iets aan de hand. Ouders moeten meekijken wat hun kinderen online doen."

"Daarnaast moeten scholen er aandacht aan besteden en moeten bedrijven ervoor zorgen dat het plegen van bijvoorbeeld Whatsappfraude niet mogelijk is." Maar ook de politie zelf is aan zet: "We proberen aangiften meer aan elkaar te koppelen, zodat we patronen herkennen en de grote daders sneller op het spoor komen." Soms kunnen tientallen tot zelfs honderden aangiften naar een of twee achterliggende daders leiden. "Zo komen we bij de grote vissen terecht, en niet enkel bij de geldezels."

Ook ziet de politie dat mensen snel kunnen afglijden van cybercrime naar reguliere criminaliteit. "Crimineel geld maakt crimineel geld", aldus Van der Plas. "Jongeren rollen van de cybercrime in het drugscircuit. Dat willen we natuurlijk niet."

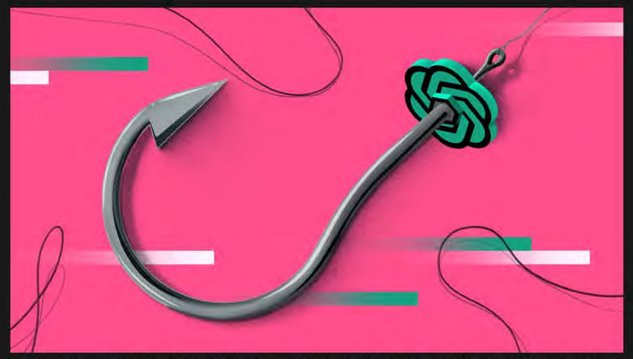
https://www.nporadio1.nl/nieuws/binnenland/3e791bd5-95be-4e85-b362-4ca5e54aabba/jonge-cybercriminelen

30 juni 16:57

Hoe ChatGPT tegen wil en dank co-piloot wordt van de cybercrimineel

Ardi Vleugels, Jan Fred van Wijnen

De nachtmerrie van elke cybersecurity-expert is een razendsnelle computer die meedenkt met kwaadwillenden. Is dat met ChatGPT realiteit geworden?



De simpelste en meest voorkomende online fraude is niet het kraken van een bank. Dat is het opstellen van een phishingmail. Illustratie: Adrià Voltà voor Het Financieele Dagblad

In het kort

- ChatGPT, het AI-programma voor levensechte gesprekken, is volgens de makers geprogrammeerd om geen onethische of criminele dingen te doen.
- Toch blijkt het simpel om het programma te misleiden, waardoor het kwaadaardige hackers wél assisteert.
- Het is al voldoende om ChatGPT mee te nemen in een rollenspel. Zoals een internetbeveiliger die het personeel wil trainen in het herkennen van een phishingaanval.

Tom Wolters zit voor het vragenvenster van ChatGPT, de superslimme zoekmachine die gesprekken voert alsof het een echt mens is. De makers van het Amerikaanse bedrijf OpenAI stellen dat het is geprogrammeerd om geen kwaadaardige dingen te doen. Zoals een kind vertellen dat Hitler een toffe peer is, of een recept geven om thuis een atoombom te maken. Maar sinds de introductie, najaar 2022, is het een mondiaal spelletje om ChatGPT om de tuin te leiden. Zodat het tips geeft om cryptomunten te kraken of de wereld over te nemen.

https://fd.nl/bedrijfsleven/1478223/hoe-chatgpt-tegen-wil-en-dank-co-piloot-wordt-van-de-cybercrimineel

The Biggest AI Moment Ever for Cybercrime Just Happened

Author: Raef Meeuwisse, author, Artificial Intelligence for Beginners
Date Published: 24 March 2023

A monumental development has just taken place in the AI realm, and if you work in cybersecurity, you will soon realize its implications.

My own expertise stems primarily from cybersecurity but I have spent the past few years buried in various strands of research and this includes tooling up to understand AI.

Many of you will also have a growing awareness of AI and most have by now at least sampled ChatGPT, an awesome text-based chatbot AI capable of real-time interactions and boasting deep knowledge across more disciplines than any human in history. This already presents some problems for cybersecurity, as various functions from this AI can be called via APIs (Application Programming Interfaces) at very low cost.

The misuse of ChatGPT and other commercial AI platforms is at least restricted by policies – but that still requires any unethical or illegal use to be detected. These AIs will not intentionally set out to break any laws but those without any ethics are busy finding ways to circumvent the rules.

Let me cut to the endgame here before I explain how it happened. Imagine what would happen if cybercriminals could get an AI as capable as ChatGPT 3.5 or 4.0, but instead of a vast data center, be able to run a wholly independent instance on a standalone machine – where they can decide what rules or policies it abides by?

It is technically illegal for cybercriminals to reuse this work, but alas through the effort of several parties, it has proven possible to take an AI model with the power of ChatGPT 3.5 (an AI that requires a massive data center just to get its basic functions running) and create a much tinier and more efficient version that has been able (in a small number of tests conducted so far) to outperform it.

Here is what happened:

We have long been warned that once AI arrived, its development would be exponential.

A group of researchers at a Stanford-based research team were able to use just 175 different manually created tasks (self-instruct seed tasks), and using these in combination with an API connection to ChatGPT 3.5 (the DaVinci version for those interested), they were able to get into a cycle of automated generation until they reached a sample size of 52,000 conversations.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/the-biggest-ai-moment-ever-for-cybercrime-just-happened

Wednesday, October 25, 2023

https://securityboulevard.com/2023/06/palo-alto-networks-finds-cyberattack-patterns-changing/

Palo Alto Networks Finds Cyberattack Patterns Changing

by Michael Vizard on June 12, 2023

An analysis of cyberattacks published by the Unit 42 research arm of Palo Alto Networks found a significant increase in attempts to mimic generative artificial intelligence (AI) sites on the web using typosquatting techniques.

Cybercriminals are attempting to take advantage of the popularity of platforms like ChatGPT to distribute malware to end users that are not looking closely at the URL of the site they have landed on, the report warned.

The report also noted that while cybercriminals are not yet widely using generative AI to create cyberattacks, there has been an increase in attacks aimed specifically at operational technology (OT) platforms. In the last year, Unit 42 reported a 28% increase in the ratio of malware aimed specifically at vertical industries using OT technologies.

Anand Oswal, senior vice president and general manager for network security at Palo Alto Networks, said that while attacks against OT technologies are not new, the level of increase suggested that cybercriminals are increasing their focus on critical infrastructure.

Overall, the report also noted that 13% of the network traffic generated by malware is now encrypted using the secure socket layer (SSL) protocol and that cryptominer traffic has doubled in the last year.

Finally, the report also found exploitation of known vulnerabilities increased 55% compared to 2021 and that PDFs remain the most widely used vehicle for delivering malware via email attachments.

In general, the challenge cybersecurity teams encounter is not so much that cybercriminals are developing new malware and techniques but that they continually evolve existing ones. Most malware is a derivative of a previous exploit, while typosquatting has been exploited by cybercriminals for decades. The issue is that the overall size of the attack surface that needs to be defended continues to expand as more devices are connected to the internet to access a range of cloud services.

Palo Alto Networks has been making a case for unifying the management of cybersecurity via a cloud service that spans both IT and OT technologies. It's not clear how quickly organizations are centralizing the management of cybersecurity, but reducing the total number of point products that cybersecurity teams need to deploy, manage and update reduces the total cost of cybersecurity. It also provides more flexibility in terms of being able to invoke additional capabilities as required.

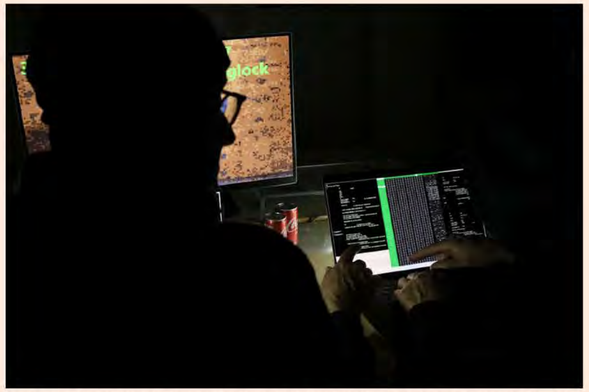
In the meantime, most cybersecurity teams are going to accomplish a lot more by focusing on the fundamentals than spending too much time worrying about the launch of more esoteric cyberattacks. Most cybercriminals are not going to put extra time and effort into launching a complicated, unique cyberattack when the simple ones they already have at their disposal remain effective. The challenge cybersecurity teams face now is finding a way to automatically combat as many known threats as possible. This will allow them to use the limited resources they have to identify how the techniques and tactics that cybercriminals use are evolving to evade existing controls.

https://fd.nl/bedrijfsleven/1493504/gijzelsoftware-raakt-nederlands-bedrijfsleven-minder-hard

22 okt 16:54

Gijzelsoftware raakt Nederlands bedrijfsleven minder hard

Stijn van Gils, Jan Fred van Wijnen



Door betere beveiliging en back-ups van data verdwijnt de noodzaak om te betalen voor ontgrendeling. Foto: Heiène van Rijn/ANP

In het kort

- Bedrijven in Nederland zijn minder kwetsbaar voor cyberaanvallen.
- Adviesbureaus voor cybersecurity zien hun omzet in deze activiteit teruglopen.
- Bedrijven beschermen hun netwerken beter en hebben vaker back-ups van hun data.

Nederlandse bedrijven betalen minder vaak losgeld aan hackers om hun computers te ontgrendelen. In veel gevallen hebben ze reservekopieën van hun data, die ze terugzetten op niet-geïnfecteerde computers. Als er al wordt betaald, is het meestal alleen voor geheimhouding van gevoelige data. Ook is het niveau van beveiliging in Nederland hoger dan in de rest van Europa. Dit zeggen verschillende bureaus voor cyberveiligheid en verzekeraars tegen computerschade.

Het gevolg is dat het werk voor cyberadviseurs in Nederland verandert. De vraag naar hulp bij onderhandelingen met hackers en het herstellen van een versleuteld netwerk is bij sommige bureaus teruggelopen. 'De laatste tijd zaten onze medewerkers vaker zonder incidenten', zegt Arwi van der Sluijs, directeur van cyberbeveiliger NFIR. 'We hebben zelfs even verlies gedraaid.'

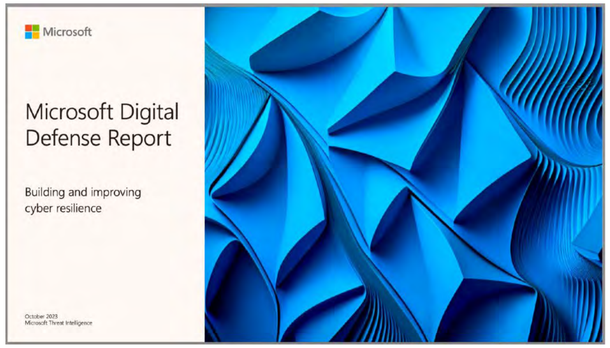
Dit is een trendbreuk. De laatste jaren groeide de markt voor digitale hulpverlening juist vanwege agressieve cyberbendes. De bureaus die een computernetwerk herstellen en beveiligen na een aanval, zagen hun medewerkers steevast overuren draaien. Verzekeraars van computerschade werden zo voorzichtig, dat het moeilijk was om nog een verzekering tegen computergijzeling af te sluiten.

https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-

This year's report draws on insights from these and other sources across Microsoft and the ecosystem:

Telemetry sources: Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Microsoft Entra ID (formerly Azure AD), Microsoft Defender Threat Intelligence

More about this diagram



IBM **Security**

Cost of a Data Breach Report 2023

IBM

Figure 5. Mean times to identify and contain breaches stayed roughly the same.
Compared to 2022, both the mean time to identify (MTTI) and the mean time to contain (MTTC) breaches saw only marginal changes. Mean time to identify refers to the time it takes an organization to uncover a security breach. Mean time to contain refers to the time required to resolve a security breach once it has been identified.

In 2022, it took organizations 207 days to identify a breach. In 2023, it took only 204 days. On the other hand, organizations required an average of 73 days to contain breaches in 2023, while they required just 70 days on average in 2022. The highest mean times to contain and identify breaches both occurred in 2021, at 212 and 75 days, respectively.

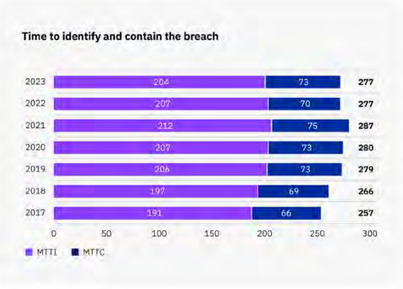


Figure 5. Measured in days

Cost of a data breach by country or region

Figure 3. Measured in USD millions

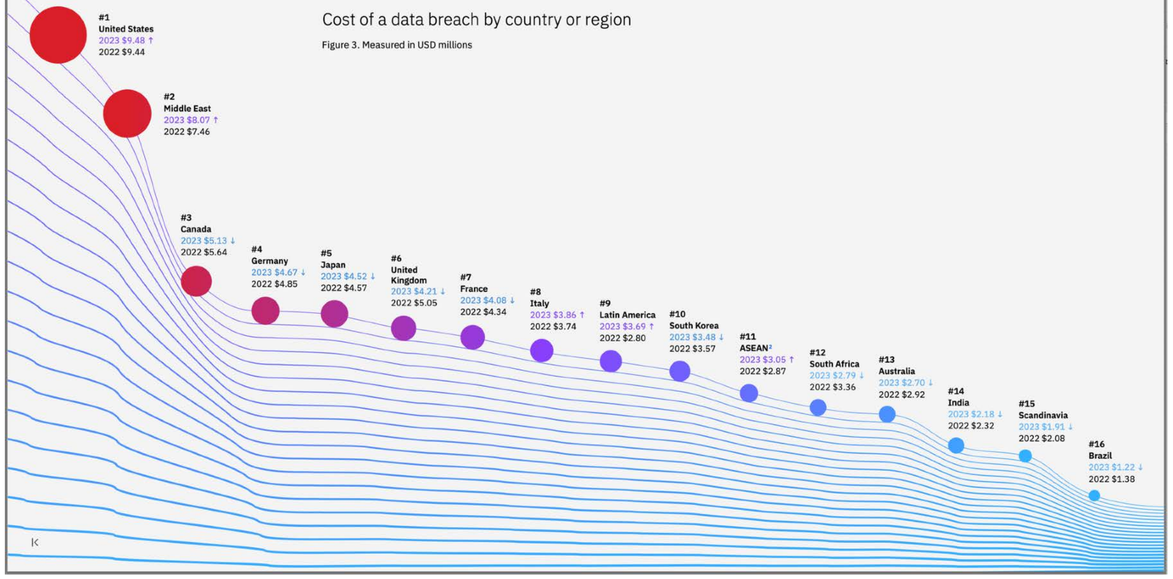


Figure 6. Lost business costs hit a five-year low.
Last year's report saw detection and escalation costs rise to become the costliest category of data breach expenses, indicating a shift toward longer and more-complex breach investigations. The trend continued this year as detection and escalation costs remained in the top spot and rose from USD 1.44 million to USD 1.58 million, demonstrating a change of USD 140,000 or 9.7%. Detection and escalation costs include activities that enable a company to reasonably detect a breach and can include forensic and investigative activities, assessment and audit services, crisis management, and communications to executives and boards.

The other key cost segments of a data breach—lost business cost, post-breach response and notification—also saw changes compared to 2022. Lost business costs dropped 8.5%, from USD 1.42 million in 2022 to USD 1.30 million in 2023. Lost business costs include activities such as business disruptions and revenue losses from system downtime, the cost of lost customers and acquiring new customers, and reputation losses and diminished goodwill.

Notably, the notification cost segment rose from USD 310,000 in 2022 to USD 370,000 in 2023, which represents a 19.4% increase. Post-breach response costs rose by just USD 20,000. Notification costs include activities that enable the company to notify data subjects, data protection regulators and other third parties.

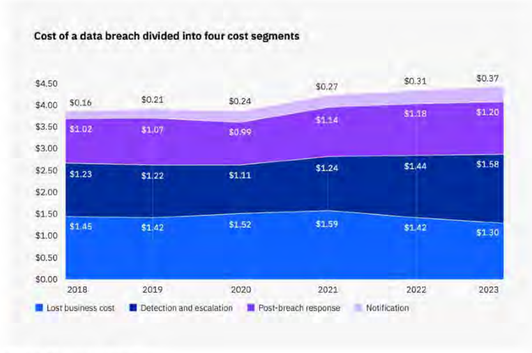


Figure 6. Measured in USD millions

Bron: IBM Security - Cost of a Data Breach Report 2023

Cost and frequency of a data breach by initial attack vector

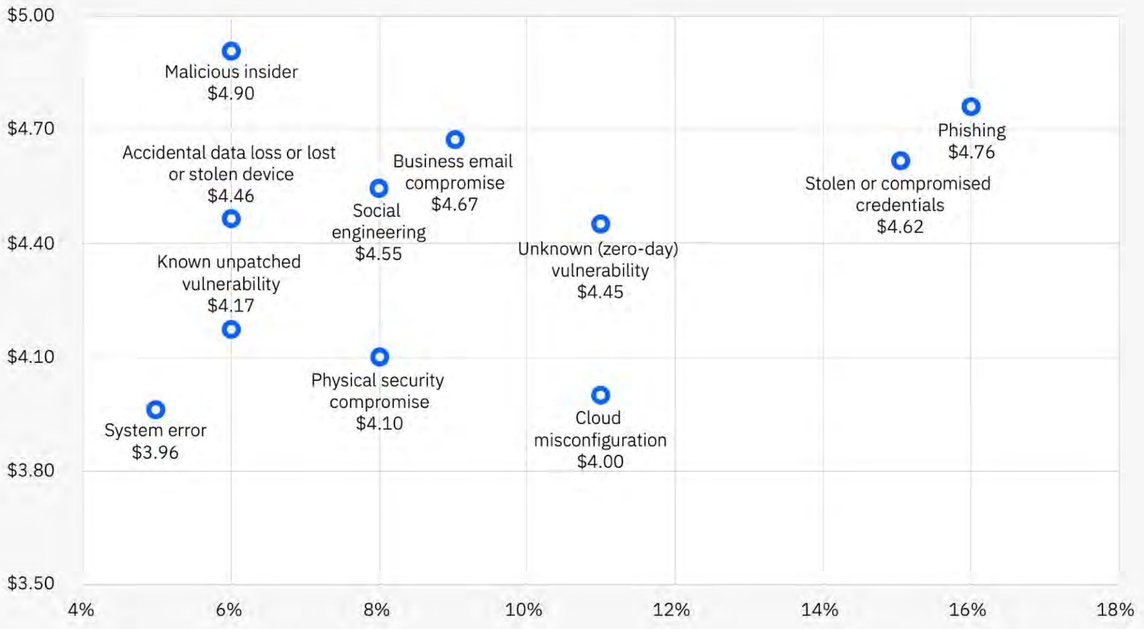


Figure 10. Measured in USD millions

Impact of key factors on total cost of a data breach

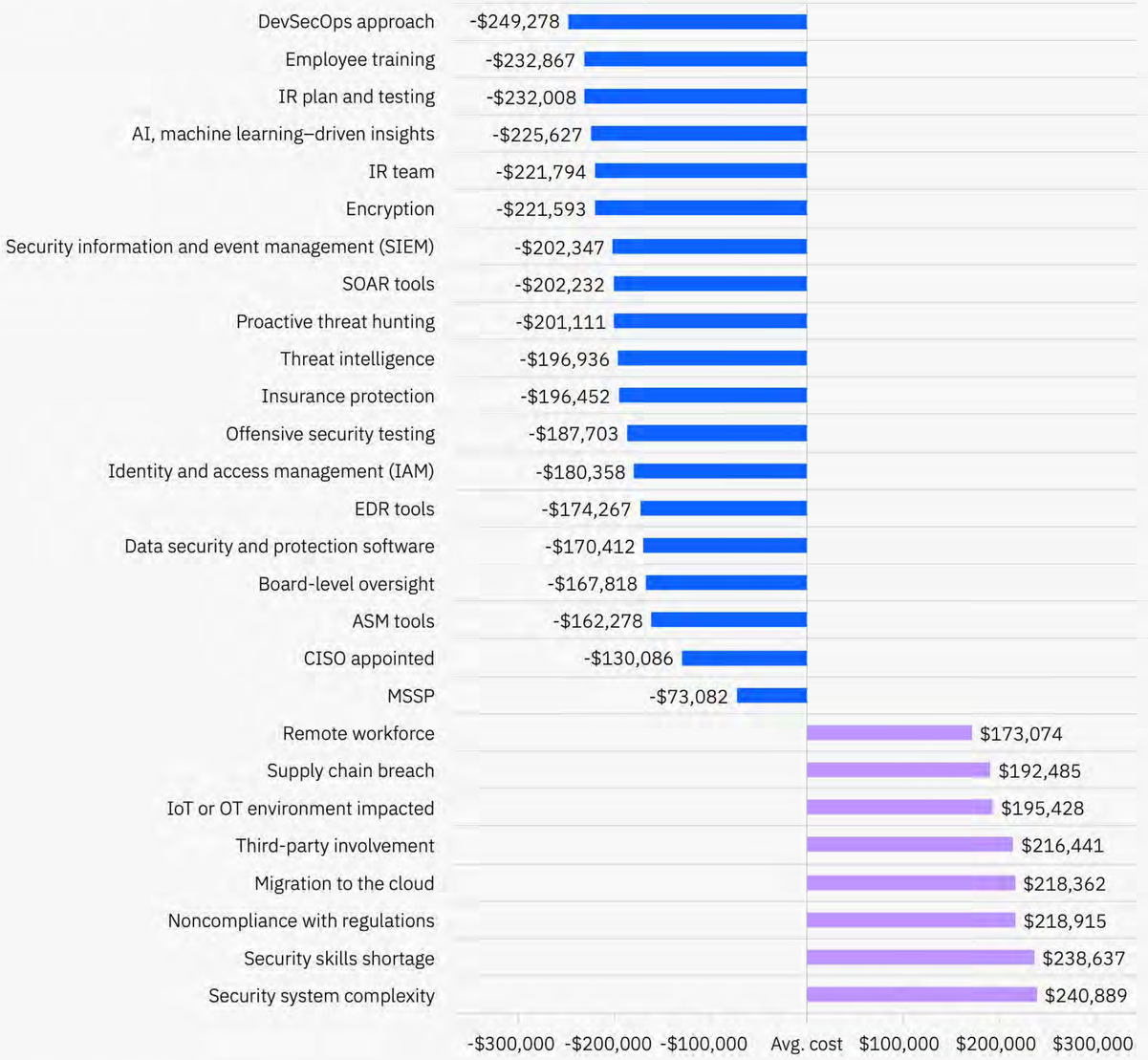


Figure 16. Measured in USD

OUR MISSION

We aim to make the digital world safer by reporting vulnerabilities we find in digital systems to the people who can fix them. We have a global reach, but do it Dutch style: open, honest, collaborative and for free.

OUR STATISTICS

Year	# of cases	# of vulnerable IPs notified
2020	14	58,358
2021	25	99,006
2022	42	244,788
2023	32	285,607

TEAM

DIVD is a platform for security researchers to report vulnerabilities, supported by volunteers.

CODE OF CONDUCT

How and why we scan and report.

NEWS & EVENTS

Just getting started with some presentations here and there

LET THE GAMES BEGIN

OVER NAAR MENTIMETER !