WWW.TAHAWULTECH.COM

ADVISOR

MIDDLE EAST

INTELIGENT SECURITY

Securat

TAJ EL-KHAYAT, AREA VP, EMEA SOUTH AT VECTRA AI TELLS ANITA JOSEPH HOW THE NEW VECTRA AI PLATFORM IS REDEFINING CYBERSECURITY WITH ITS COMPREHENSIVE, END-TO-END FEATURES.

🚸 tahawultech.com



DNG RANGE THE COMPLETE SERIES



Features

- Long range connectivity upto 250meters
- Model options with different port counts and speed
- Extensive PoE power budget across various models
- · IP40 rated outdoor switches
- Surge protected
- External DIP switches to toggle function modes



D-Link

CONTENTS





- 6 News from the world of cybersecurity and beyond.
- $18\,$ Sophos analyses attacker behaviours and tools during the first half of 2023.
- 20 G42 and Microsoft unlock new opportunities for digital transformation.
- $28\,$ SANS Institute Elevates Cyber Resilience in Qatar with SANS Doha September 2023.



C P I M E D I A G R O U P. C O M



DEETUS AT SITEX THE WORLD'S LOBAL #GITEXGLOBAL

CYBER VALLEY DUBAI WORLD TRADE CENTRE STAND NO.

H25-A10 HALL 25



For more information, please contact : +971 4 568 2993 info@cpimediagroup.com



EDITOR'S NOTE



Talk to us: E-mail: anita.joseph@ cpimediagroup.com

> Anita Joseph Editor

EVENTS



THE DOUBLE-EDGED SWORD

RESHAPING THE

SECURITY LANDSCAPE

n the ever-evolving landscape of cybersecurity, the emergence of generative AI has promised new horizons and posed novel challenges. As we harness the power of artificial intelligence to bolster our defenses, we must remain vigilant about the potential risks that accompany this revolutionary technology.

Generative AI, often celebrated for its ability to generate realistic text, images, and even videos, has the potential to reshape the cybersecurity landscape. Its applications in threat detection,

anomaly recognition, and incident response are undeniable, offering the

prospect of more robust defenses against cyberattacks. However, as we delve deeper into the realm of generative AI, it becomes apparent that we are in a constant battle against adversaries seeking to exploit this technology.

One of the primary concerns surrounding generative AI is its capacity to create highly convincing fake content, which can be used for phishing campaigns, deepfakes, and social engineering attacks. Cybercriminals are quick to adapt, and they are already leveraging generative AI to craft sophisticated, tailored attacks that are difficult to detect. As the line between genuine and fake blurs, cybersecurity professionals must deploy equally advanced AI systems to counter these threats.

Furthermore, the potential for generative AI to automate the development of malware and hacking tools raises serious concerns. These AI-generated tools can adapt in real-time, making them more challenging to defend against. This necessitates a

> continuous, dynamic approach to cybersecurity, with Al-driven solutions actively monitoring and

adapting to emerging threats.

So, while Generative AI offers innovative solutions to combat cyber threats, it also empowers malicious actors to create more sophisticated and convincing attacks. As we embrace this technology, it is imperative that we remain proactive in developing robust defense mechanisms that can outsmart the AI-driven threats of tomorrow. The future of cybersecurity depends on our ability to harness generative AI for good while guarding against its potential for harm.

Published by

FOUNDER, CPI Dominic De Sousa (1959-2015)

ADVERTISING Group Publishing Director Kausar Syed kausar.syed@cpimediagroup.com EDITORIAL Editor Anita Joseph anita.joseph@cpimediagroup.com

Online Editor

PRODUCTION AND DESIGN Designer Prajith Payyapilly prajith.payyapilly@cpimediagroup.com DIGITAL SERVICES Web Developer Adarsh Snehajan webmaster@cpimediagroup.com Publication licensed by Dubai Production City, DCCA PO Box 13700 Dubai, UAE

Tel: +971 4 5682993

© Copyright 2023 CPI All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com Daniel Shepherd daniel.shepherd@cpimediagroup.com

Contributing Editor SAME & Tahawultech Veronica Martin

SOPHOS LAUNCHES INCIDENT RESPONSE RETAINER

Sophos, a global leader in innovating

and delivering cybersecurity as a service. has announced its new Sophos Incident Response Retainer, which provides organisations with speedy access to Sophos' industry-first fixed-cost incident response service that includes 45 days of 24/7 Managed Detection and Response (MDR). The retainer cuts red tape, allowing Sophos incident responders to guickly jump into active cyberattacks to investigate and remediate them. External vulnerability scanning and critical preparedness guidance are also included in the retainer, enabling organisations to proactively improve their existing security resilience by pinpointing and resolving issues that reduce the likelihood of a

breach in the first place.

At a time when attacker dwell time is steadily shortening, as revealed in a new 2023 Active Adversary Report for Tech Leaders that Sophos published, time to locate and evict adversaries is critical in limiting damage and completely stopping nefarious endgames, such as data breaches and ransomware. The report indicates that median adversary dwell time continued to plummet, from 10 days in 2022 to eight days in the first half of 2023: for ransomware alone, the time between initial access and impact dropped from nine days to just five. Adversaries also preferentially carried out attacks during targets' night and weekend hours, with only 9.6% of ransomware



incidents taking place during the targets' daytime business hours. The single most common attack times were Fridays between 11 p.m. and midnight in the targets' local time zones.

VMWARE ADVANCES AUTONOMOUS WORKSPACES WITH AI-POWERED INTEGRATIONS

Data and intelligence play a key role in

enabling automation and implementing a successful hybrid work strategy, but a holistic approach is required to maximise its advantages. Today, VMware announces modern Al integrations to the Anywhere Workspace platform, part of the VMware Cross-Cloud services portfolio, that automatically optimise employee experience, drive new vulnerability management use cases, and simplify application lifecycle management. VMware Anywhere Workspace is the only hybrid work platform that integrates digital employee experience (DEX), virtual desktop infrastructure and apps (VDI and DaaS), unified endpoint management (UEM) and security to enable a seamless and secure workspace on any device or location.

"Last year, we announced our Autonomous Workspace vision as a path forward for organisations to navigate



the challenges brought on by hybrid work," said Shankar Iyer, senior vice president and general manager, End-User Computing, VMware. "We are thrilled to unveil new advancements for our customers that expand data sources and insights, integrate with technology partners for improved security, and unify app delivery strategy across all virtual desktops and apps. These innovations continue to progress our vision of providing the next evolution of digital workspaces."

VMware continues to leverage data, intelligence, and automation to improve the employee and IT experience by introducing new Insights and Playbooks based on greatly expanded data and machine learning algorithms that enhance DEX remediation capabilities. These updates broaden access to data, help strengthen VMware Insights, and allow for remediation of more issues. VMware will now enable delivery of new app performance scores, in addition to existing mobile device, desktop, and virtual environment experience scores. If a SaaS app service goes down, IT is proactively alerted and employees are automatically notified. This allows IT to quickly resolve the outage without dealing with inbound support tickets and employees don't waste time trying to access unavailable services.

TENABLE UNVEILS COMPREHENSIVE WEB APPLICATION AND API SCANNING CAPABILITIES FOR NESSUS EXPERT

Tenable, the Exposure Management

company, has announced web application and API scanning in Tenable Nessus Expert, new features that provide simple and comprehensive vulnerability scanning for modern web applications and APIs.

Backed by Tenable Research, Nessus provides broad and accurate vulnerability coverage for web applications and APIs – spanning web application servers, content management systems, web frameworks, programming languages and JavaScript libraries. The result is fewer false positives and negatives, ensuring security practitioners know the true risks in their applications.

"Web applications are under siege and the security practitioners in charge of protecting them face numerous challenges," said Glen Pendley, chief technology officer, Tenable. "With Nessus Expert - the gold standard in vulnerability assessment - we're tackling the crux of these challenges head on by widening visibility into web applications and APIs. Whether the apps are running on-prem or in the public cloud. Nessus Expert assesses their exposures and provides security practitioners, consultants and pentesters with actionable results quickly."



vulnerability assessment solution that spans traditional IT assets and the dynamic modern attack surface, including the external attack surface, cloud infrastructure and now, web applications and APIs.

Nessus Expert is the industry's first

KASPERSKY LAUNCHES SPECIALISED SOLUTION FOR LINUX-BASED EMBEDDED DEVICES

Kaspersky has introduced support

for Linux in the Kaspersky Embedded Systems Security product. This adaptable, multi-layered solution now provides optimised security for embedded Linux-based systems, devices and scenarios, in compliance with the rigorous regulatory standards so often applicable to these systems. The product provides optimum protection for every device it secures – whatever its power level – against the latest cyberthreats directed at today's Linux systems.

A recent Fortune Business Insights' report values the global Linux market at 5.33 billion US dollars in 2021, a figure projected to grow to 22.15 billion US dollars by 2029 with a compound annual growth rate of 19.8%. Highly cost-competitive and able to work

kaspersky

across a wide range of hardware, Linux has gained popularity across commercial embedded systems in large businesses and critical infrastructure enterprises, including banks, retail firms and healthcare organisations, and Linux adoption is expected to grow significantly in coming years.

This expanding reach is naturally attracting the attention of cybercriminals, who are developing new specialised malware for these platforms. Kaspersky registered more than 14.5 million network-based automated attacks on Linux in the first half of 2023. These attacks – the result of self-distributing malware setting out to spread itself via the network – are a big favorite with attackers out to exploit vulnerabilities in embedded systems. Over the same period, Kaspersky discovered 260,000 new unique malicious files – that's an average of over 1,400 new files distributed by hackers every day. It's clear that businesses need to think very hard about protecting their Linux-based parks of embedded devices.

CISCO AND NUTANIX FORGE GLOBAL STRATEGIC PARTNERSHIP TO SIMPLIFY HYBRID MULTICLOUD AND FUEL BUSINESS TRANSFORMATION

Cisco, the leader in enterprise

networking and security, and Nutanix, Inc., a leader in hybrid multicloud computing, announced a global strategic partnership to accelerate hybrid multicloud deployments by offering the industry's most complete hyperconverged solution for IT modernisation and business transformation.

"Customers are asking for solutions that are simple, sustainable, and futureready," said Jeremy Foster, senior vice president and general manager, Cisco Compute. "This partnership answers with a complete solution spanning virtual compute, networking and storage



across customer data centers and public clouds. By combining Cisco's award-winning SaaS-managed compute portfolio with Nutanix's market-proven cloud platform software, we can help customers develop a balanced approach to power modern workloads on-prem and in the cloud."

"As organisations look to keep up with the pace of innovation, they need an integrated hardware and software platform to support application deployment anywhere," said Tarkan Maner, chief commercial officer at Nutanix. "This partnership will deliver an expanded market opportunity for both organisations as they tackle the challenges of standardising, simplifying, and securing environments across the data center, in public cloud and the edge."

HID ANNOUNCES EMPLOYEE BADGE INTEGRATION WITH WALLET APPS

HID, the world's leading provider of

trusted identity solutions, recently announced it now offers companies the integration of employee badges into digital wallets, allowing for convenient, seamless access to the workplace.

The integration of the HID Mobile Access solution with digital wallets simplifies access control to buildings and improves the user experience. Employees are not required to present physical cards but can instead identify themselves to their employers with their smartphone or smartwatch. Employees only need to activate the badge in their digital wallet and can then gain access to not just their workplace, but also to enabled corporate applications. To use this simple and digital form of authentication, all businesses need is an NFC-enabled reader.

In addition to access control, there

are several other applications for the digital employee ID card, including laptops and workstations, secure printing, special access to restricted areas, charging stations and even parking. Another important argument for integrating employee ID cards onto a mobile device is sustainability. The production of corporate ID cards and the matching sleeves consumes large amounts of plastic. In addition, companies often have to reissue the cards several times if they are lost. Digital employee ID cards, on the other hand, consume fewer resources and help companies meet their climate change goals.

"With digital employee badges, companies are adapting to the usage habits of their employees," says Gustavo Gassmann, HID Vice President of Emerging Markets, PACS. "Mobile



devices have become essential components of most people's daily lives, not just for their useful features but also for the invaluable, convenient benefits they provide. And because people always have their devices with them, accessing places and moving around different parts of the building through them makes sense."

Allied Telesis



Next Generation Industrial Switches

Our award winning family of IE switches just got better thanks to the IE220 Series

10 Gigabit uplink ports gives you the value and versatility your network requires. The ideal speed where high bandwidth backhauling and scalability is required. Coupled with IEEE 802.3bt PoE++ up to 95W to meet the demand for high power of devices connected to the network – this really is built for enduring performance in the harshest of environments, such as those found in outdoor installations. With rich functionality and advanced security features, our switches deliver the performance and reliability demanded by deployments in the age of the Internet of Things.

For more information, please contact one of our Allied Telesis Account Managers today.



Tel: +971 4 3522 433

RANSOMWARE IS INDISCRIMINATORY – PREPARE FOR EVERYTHING TO FAIL

RICK VANOVER, SENIOR DIRECTOR, PRODUCT STRATEGY, VEEAM

ansomware attacks continue to grow in frequency. As well as being more common, ransomware is also getting more potent. As per Veeam's 2023 Ransomware Trends Report 21% of companies paid the ransom but could not recover their data. The threat landscape is as volatile as it has ever been. There are more attacks taking place. They are more diverse. And they can have grave consequences for the companies they affect.

On the other hand, rather than tremble with fear at the awesome power of the cyber attacks waiting to be deployed against them, organizations must focus on what they can control – their defence. Protecting your business against cyber-attacks requires following some fundamental and consistent principles – no matter what is being thrown at you.

The ransomware wild west

There is a lawless and brutal feeling about the current cyber landscape businesses operate in. It is difficult for governments to hold cybercriminals to account and businesses are often keen to minimise public attention towards an incident that has compromised them. This contributes to a situation where almost all the focus is on the victim (the business) rather than the criminal (the attacker).

Furthermore, ransomware – and most contemporary cybercrime – is almost indiscriminatory in terms of those who suffer. The fact is that every business is a target. Yes, hacktivist organisations such as Anonymous use organised cyber-attacks as a means of exercising social justice and to call out businesses or governments they view as immoral, unlawful, or dangerous. But even the most philanthropic and virtuous companies can find themselves begging a cybercriminal gang to restore their data and systems while a hefty ransom is demanded of them to do so.

You often see a comparison made between cyber-attacks and fishing. Hence the term 'phishing' which refers to using an email or text being used as bait to trick a victim into 'biting' - in this case clicking on the link and unwittingly downloading malware onto their device. With ransomware especially we are now seeing industrial-scale attacks being carried out which are more analogous to trawler fishing. This isn't one guy with a rod casting out to get a bite off one or two fish. It's AI-infused algorithms programmed to target everyone and everything - playing a blind numbers game to catch whatever it can.

This indiscriminate nature is compounded by the fact cyber-attacks are generally difficult to contain. For example, cyber warfare between nation states is a threat to every organisation - not just those deemed to be in the firing line. We saw this with the NotPetya attack in 2017 – an attack on a specific utility company - which impacted multiple unrelated organisations through an entirely organic spread of the chaos. Attack types also continue to evolve. For example, the LokiLocker attack was one of the first reported strains of ransomware to include a disk wiper functionality. This means organisations are not only held to ransom by having services suspended and threats of data extortion. Now they are being threatened with losing vast swathes of data completely if they do not pay up.

Consistent principles of defence

There is some good news for businesses. No matter how scalable, spreadable, or malicious an attack is, these various evolutions can be viewed as attackers simply using bigger guns and more of them. The fundamental principles of how you prepare your defences against even the most sophisticated and powerful ransomware stay relatively the same.

First, practice impeccable digital hygiene. All employees must be



trained to identify suspicious content and be warned of the impact that malpractice using work devices can lead to. For all the might at the hands of cybercriminals, in many ways their biggest weapons are unsuspecting employees who give them the keys to the back door of an enterprise network. Given the scatter gun approach now adopted by many cyber-attacks, criminals are not necessarily targeting your organisation specifically. But if you prove to be an easy hit, you'll become a victim.

With that said, all businesses must prepare for their defences to fail – no matter how robust you might think they are. Concepts such as zero trust and deploying techniques such as twofactor authentication can be useful for restricting the access an attacker has to data by taking over one individual's workstation. Ultimately, the best way to protect data is to ensure that it has been securely backed up and is fully recoverable before an incident takes place. Follow the 3-2-1-1-0 backup rule, which states there should always be at least three copies of data, on at least two different types of media, at least one off-site and one immutable or offline, with zero unverified backups or errors.

While the headlines and constant discussion around cybersecurity and ransomware can be daunting, it's important to remember than the fundamental actions required to protect data remain the same. Data Protection and Ransomware Recovery strategies ensure businesses can protect all data from cyber-attacks, server outages, accidental loss and deletion across physical, virtual, cloud, SaaS, and Kubernetes environments. Investing in a data protection strategy and taking advantage of a solution that enables continuous backup and Disaster Recovery (DR) can give businesses peace of mind that should the worst happen, they never need to pay the ransom. 1

INTELLIGENT SECURITY TALE-KHAYAT, AREA VP, EMEA SOUTH AT VECTRA AI TELLS

ANITA JOSEPH HOW THE NEW VECTRA AI PLATFORM IS REDEFINING CYBERSECURITY WITH ITS COMPREHENSIVE, END-TO-END FEATURES.

an you tell us about the origin of the Vectra AI platform? What prompted the rollout of this solution, and what are some of its key highlights?

Let's delve into the Vectra AI platform. Over the last four years, we've been diligently listening to our customers and gathering feedback from esteemed professionals such as CISOs, thought leaders, security architects, and SOC analysts. What we've learned is that our customers are seeking a solution that delivers specific outcomes to enhance their cybersecurity posture. The Vectra AI platform was developed in close collaboration with our customers to address these needs.

We've identified three critical areas where our customers want to see improvements. First, they aim to bolster their resilience against THE INTEGRATION OF AI AND ML THROUGH THE VECTRA AI PLATFORM ALLOWS ORGANISATIONS TO STREAMLINE AND STRENGTHEN THEIR SECURITY POSTURE.

the ever-evolving and increasingly sophisticated cyber threats. Second, they want to modernise their security operations centers (SOCs) using Artificial Intelligence (AI) and Machine Learning (ML) without the complexity of starting from scratch. Lastly, they are eager to respond swiftly and effectively to cyber threats, ideally stopping them in their tracks early in the attack cycle. To fulfill these objectives, we realised we needed to understand the root of the challenge. Why, despite the plethora of tools available in the market, is it still challenging to achieve these outcomes? The answer, we found, revolves around the concept of "more" or what we refer to as the "spiral of more." Organisations are grappling with expanding attack surfaces, leading to more evasive attacker techniques.

Furthermore, the abundance of security tools translates to more detections and rules to manage, which inevitably increases complexity and costs. With an overload of tools and complexity comes an inundation of alerts, creating additional workload and stress for analysts. The heart of the problem today is dealing with this spiral of more. In response, we built the Vectra AI platform, centered on delivering what we call "Integrated Attack Signal Intelligence."





Can you elaborate on "Attack Signal Intelligence"?

Attack Signal Intelligence is a term we've coined to emphasise its distinction from Threat Intelligence. While Threat Intelligence focuses on known threats, Attack Signal Intelligence empowers organisations to mitigate both known and previously unknown threats.

Our platform offers comprehensive visibility across various attack surfaces, including network, cloud, SaaS, and identity. Moreover, it seamlessly integrates with Endpoint Detection and Response (EDR) providers. By doing so, we provide an integrated signal that encompasses different parameters essential for identifying threats effectively.

VECTRA AI OFFERS INTEGRATED SIGNAL INTELLIGENCE, EMPOWERING HUMAN INTELLIGENCE AND ACCESS TO EXPERT RESOURCES.

Our AI-driven approach allows us to think like attackers, focusing on their behavior. We incorporate tactics, techniques, and procedures from the MITRE ATT&CK framework into our algorithms. This strategic approach positions Vectra AI as an essential component that mimics attacker behavior in the customer's security arsenal.

Attack Signal Intelligence excels in reducing noise and alert fatigue by emphasising malicious true positives. It helps analysts concentrate on critical, high-value detections instead of wading through a sea of alerts. Our platform's unsupervised learning, in conjunction with supervised learning, offers faster detection and a potent defense against unknown threats, including zero-day attacks.





In essence, Attack Signal Intelligence not only leverages threat intelligence but also protects against the unknown. It comprehensively considers known signatures, threat intelligence data, research, and known signatures, bolstering defenses even against highly sophisticated attackers.

That clears up the distinction between Threat Intelligence and Attack Signal Intelligence. How does the Vectra AI platform assist organisations in prioritising urgent security matters, given the abundance of security-related information?

Prioritisation of security matters is indeed a crucial challenge for many organisations. The Vectra AI platform offers an elegant solution by harnessing the power of artificial intelligence.

BY UTILISING OUR EXPERTISE, ORGANISATIONS \rightarrow CAN EFFICIENTLY NAVIGATE THE COMPLEX WORLD OF CYBERSECURITY.

It liberates SOC analysts from the burdensome task of manually sifting through vast amounts of metadata and packet captures.

Our platform empowers analysts to focus on managing events rather than drowning in them. We utilize AI for detections, triaging, and prioritising detections, guiding analysts to the most critical and time-sensitive issues. Through a sophisticated algorithm, we ensure that high-risk detections take center stage on the dashboard, allowing analysts to swiftly address them. In essence, Vectra AI simplifies and enhances human intelligence by streamlining the identification of urgent security matters. This streamlined approach enables organisations to respond more efficiently to imminent threats, while also providing a clear path for addressing less critical issues in due course.

What are the expected benefits for organisations that adopt the Vectra AI platform?

Customers and organisations adopting

ATTACK SIGNAL → INTELLIGENCE EXCELS IN REDUCING NOISE AND ALERT FATIGUE BY EMPHASISING MALICIOUS TRUE POSITIVES.

the Vectra AI platform can anticipate several key benefits. Firstly, they will enhance their resilience against evolving and sophisticated cyber threats. Our platform offers visibility across 40 attack surfaces, ensuring robust protection against a wide range of threats.

Secondly, the modernisation of Security Operations Centers (SOCs) becomes a reality. The integration of AI and ML through the Vectra AI platform allows organisations to streamline and strengthen their security posture without the need for a complete overhaul.

Lastly, organisations gain the ability to proactively address unknown threats. Vectra AI's unsupervised learning, coupled with its focus on attacker behavior, empowers organisations to protect against not only known threats but also emerging, sophisticated, and even zero-day threats.

Additionally, our platform excels in hybrid and multi-cloud environments, offering seamless coverage and a 360-degree view of security. By utilising our expertise, organisations can efficiently navigate the complex world of cybersecurity and maintain a strong defense against evolving threats.

In summary, Vectra AI offers integrated signal intelligence, empowering human intelligence, and access to expert resources. These factors collectively enable organisations to fortify their cybersecurity posture, modernise their operations, and stay ahead of emerging threats in an everchanging digital landscape. **1**



DWELL TIME SHRINKS **TO 8 DAYS** IN 2023: SOPHOS



ophos, a global leader in innovating and delivering cybersecurity as a service, recently released its Active Adversary Report for Tech Leaders 2023, an in-depth look at attacker behaviours and tools during the first half of 2023.

After analysing Sophos Incident Response (IR) cases from January to July 2023, Sophos X-Ops found that median attacker dwell time—the time from when an attack starts to when it's detected shrunk from 10 to eight days for all attacks, and to five days for ransomware attacks. In 2022, the median dwell time decreased from 15 to 10 days.

In addition, Sophos X-Ops found that it took on average less than a day approximately 16 hours—for attackers to reach Active Directory (AD), one of the most critical assets for a company. AD typically manages identity and access to resources across an organisation, meaning attackers can use AD to easily escalate their privileges on a system to simply log in and carry out a wide range of malicious activity.

"Attacking an organisation's Active Directory infrastructure makes sense from an offensive view. AD is usually the most powerful and privileged system in the network, providing broad access to the systems, applications, resources and data that attackers can exploit in their attacks. When an attacker controls AD, they can control the organisation. The impact, escalation, and recovery overhead of an Active Directory attack is why it's targeted", said John Shier, field CTO, Sophos.

"Getting to and gaining control of the Active Directory server in the attack chain provides adversaries several advantages. They can linger undetected to determine



their next move, and, once they're ready to go, they can blast through a victim's network unimpeded. Full recovery from a domain compromise can be a lengthy and arduous effort. Such an attack damages the foundation of security upon which an organisation's infrastructure relies. Very often, a successful AD attack means a security team has to start from scratch". The dwell time for ransomware attacks also declined. They were the most prevalent type of attack in the IR cases analysed, accounting for 69% of investigated cases, and the median dwell time for these attacks was just five days. In 81% of ransomware attacks, the final payload was launched outside of traditional working hours, and for those

$\begin{array}{l} \mbox{ATTACKING AN ORGANISATION'S ACTIVE} \\ \rightarrow \mbox{DIRECTORY INFRASTRUCTURE MAKES SENSE FROM} \\ \mbox{AN OFFENSIVE VIEW.} \end{array}$

that were deployed during business hours, only five happened on a weekday.

The number of attacks detected increased as the week progressed, most notably when examining ransomware attacks. Nearly half (43%) of ransomware attacks were detected on either Friday or Saturday.

"In some ways we've been victims of our own success. As adoption of technologies like XDR and services such as MDR grows, so does our ability to detect attacks sooner. Lowering detection times leads to a faster response, which translates to a shorter operating window for attackers. At the same time, criminals have been honing their playbooks, especially the experienced and well-resourced ransomware affiliates, who continue to speed up their noisy attacks in the face of improved defences. But, it doesn't mean we're collectively more secure. This is evidenced by the levelling off of non-ransomware dwell times. Attackers are still getting into our networks, and when time isn't pressing, they tend to linger. But all the tools in the world won't save you if you're not watching. It takes both the right tools and continuous, proactive monitoring to ensure that criminals have a worse day than you do. This is where MDR can really close the gap between attackers and defenders, because even when you're not watching, we are", said Shier.

The Sophos Active Adversary Report for Business Leaders is based on Sophos Incident response (IR) investigations spanning the globe across 25 sectors from January to July 2023. Targeted organisations were located in 33 different countries across six continents. Eightyeight percent of cases came from organisations with fewer than 1,000 employees.

The Sophos Active Adversary Report for Tech Leaders provides security professionals with actionable threat intelligence and insights to better operationalise their security strategy.

GGAA AND MICROSOFT UNLOCK NEW OPORTUNITIES FOR DIGITAL TRANSFORMATION

42 and Microsoft have embarked on the next phase of their ongoing strategic collaboration and announced a multifaceted plan to make available sovereign cloud offerings, co-innovate and deliver

advanced AI capabilities, and expand the existing data center infrastructure in the UAE.

Microsoft's sovereign cloud offering will allow UAE public sector and regulated industries to use new platform capabilities for securing sensitive data, providing access to the latest cloud and AI features available on Azure public cloud and helping them comply with local privacy and regulatory requirements. G42's deep understanding of UAE sovereignty requirements and technical capabilities are central to customising the offering to help address customer's specific needs.

By combining their expertise and existing capabilities, the companies will also focus on bringing cutting-edge, AI-enabled industry specific solutions for health and life sciences, energy, sustainability and projects of national significance, for example the COP28 conference being held in the UAE this year.

In addition to setting new milestones for public sector cloud computing security and innovation, G42 and Microsoft will further empower the wider technology ecosystem by delivering new in-country services, extend go-tomarket opportunities for partners, and unlock considerable value for Microsoft's partner ecosystem to deliver industryspecific solutions to local entities. The partnership will also see Microsoft expanding its Azure services footprint in the UAE via Khazna Data Centers, a joint venture company between G42 and e&.

His Excellency Dr. Mohamed Al Kuwaiti, Head of Cyber Security for United Arab Emirates Government & Director of The National Data Center under The Supreme Council for the National Security, praised the partnership between Microsoft and G42 stating that it will further contribute to creating a safer and more resilient digital environment that the public sector and regulated industries can utilise to enhance efficiency, as well as enable citizens to access services seamlessly, which will lead to flourishing innovation without compromising security and data privacy while bolstering the country effort to manage cyber risks effectively, ensure continued services to society,

support economic growth, and uphold the reputation of the United Arab Emirates.

Microsoft

Peng Xiao, Group CEO of G42, described the joint sovereign cloud and Al offering with Microsoft as a significant step forward in the company's mission to accelerate innovation and drive meaningful technological advancements across key sectors. "This strategic collaboration with Microsoft isn't just about technology; it's about creating a holistic ecosystem for societal resilience and growth. By combining our respective expertise and shared forward-thinking approach, we aim to not only transform industries but also create positive economic opportunities and lasting impacts on the well-being of individuals, communities, and society as a whole."

Judson Althoff, Executive Vice President and Chief Commercial Officer at Microsoft, noted that organisations all over the world are turning to advancements in generative AI technology to imagine new ways to solve business, societal, and sustainability challenges. "Microsoft's partnership with G42 will empower customers across the public sector with next-generation Al solutions built on the most trusted, comprehensive, and integrated cloud platform. With data privacy, security, and compliance as our core priorities, we have a unique opportunity to help organisations responsibly innovate for the benefit of citizens and residents across the UAE."

Samer Abu-Ltaif, Corporate VP and President for Central and Eastern Europe, Middle East and Africa at Microsoft, said that the UAE has distinguished itself as an early adopter of the latest technologies, creating the ideal environment for developing and deploying cutting-edge solutions. This has given organisations across every industry the confidence to explore solutions that will drive their digital transformation agendas, improve efficiency and enhance agility. "By strengthening our collaboration with G42, we are supporting the UAE's vision of empowering individuals and businesses to innovate AI solutions that not only drive sustainable economic growth, but also tackle ongoing challenges in our communities."

This announcement marks the first significant outcome since G42 and Microsoft announced their intention to partner earlier this year, in April 2023. The two companies plan to further strengthen their collaboration in the upcoming months.



CISCO APPOINTS OLIVER TUSZIK AS NEW EUROPE, MIDDLE EAST AND AFRICA PRESIDENT

liver Tuszik has been announced as the next President of Cisco Europe, Middle East, and Africa (EMEA), With over 10 years of experience in Cisco, Tuszik most recently held the position of Senior Vice President of the Cisco Global Partner Sales and Routes to Market business, where he supported Cisco's expansive global ecosystem of partners and advocated for customer needs. Prior to this, Tuszik has over 25 years of leadership experience across Europe for Cisco, as CEO of Computacenter in Germany, and in various other IT companies. For Tuszik it is a homecoming, as he successfully led Cisco Germany between 2013 and 2018.

Tuszik's appointment comes as Cisco accelerates efforts to securely connect technology, people, governments, and businesses across the world. As IT and ecological priorities become more prevalent, all industries have had to reconsider business models and supply chains to become more agile, resilient, and sustainable. In his new role, Tuszik will be enabling this through Cisco's ecosystem, partners, and customers to advance significant digitisation and innovation across EMEA.

"I have had the privilege to work with the largest organisations and brightest minds around the globe, and by far EMEA has the biggest untapped opportunity on the world stage. The power, innovation capability and talent diversity of the countries is unmatched." said Oliver Tuszik. President of EMEA, Cisco. "Technology is the most critical component to accelerate digitisation and enable industry transformation for the region. From secure and sustainable infrastructure to transformative technologies in AI, to empowering the future of work, Cisco is literally at the heart of making it possible."

"Oliver has had an incredible impact in his ten years at Cisco. He has repeatedly proven to be one of the most inspirational leaders at the company and is one of the strongest advocates for our customers and partners that I have come across. I can't wait to see what our amazing team in the region will accomplish under his leadership," said Jeff Sharritts, Executive Vice President and Chief Customer and Partner Officer, to whom Tuszik will report. **1**



Bedata ready.

Commvault is a worldwide leader in delivering data readiness. Our intelligent data management solutions work on-prem and in the cloud, allowing you to store, protect, optimize, and use your data. Always.

commvault.com



FOUR WAYS UAE BUSINESSES CAN USE GAMIFICATION TO ADDRESS CYBERSECURITY TALENT SHORTAGES

ANITA JOSEPH CAUGHT UP WITH **MOHAMMAD ISMAIL**, VP MIDDLE EAST, AFRICA & TÜRKIYE AT DELINEA, TO FIND OUT MORE ABOUT GAMIFICATION AND HOW IT CAN HELP BRIDGE THE CYBERSECURITY TALENT GAP

s of the end of last year, the International Information Systems Security Certification Consortium (ISC2) put the global cybersecurity skills gap at 3.4 million. In countries like the UAE, which have traditionally been in threat actors' sights to a higher-than-average degree, this gap could become even more problematic as almost half of cybersecurity professionals are reportedly considering leaving their role due burnout. Facing a constantly evolving threat scape, UAE organisations cannot afford to lose this talent and should therefore look at new ways to improve the security skills of all employees, as many cyberattacks start with stealing credentials using increasingly sophisticated techniques.

Game on!

We have known for many years that endusers are cybersecurity's weakest links, but let's face it: cybersecurity training can be boring and dry, with employees spending an hour or more reviewing a PowerPoint deck may not deliver the best outcomes.

But what if we made a game out of it? Gamification – the integration of game-like mechanics and incentives into traditionally non-gaming environments – is built on the premise that competition and engagement lead to better learning and increase the likelihood that the acquired knowledge is retained and applied and is being used in a range of business areas such as sales and marketing, across industries from retail to healthcare. When applied to cybersecurity, this means employees have to deal with real-life-like situations, but with the option of going back, reviewing and changing their actions. This helps them remember and apply what they learned the next time they encounter a threat such as a phishing email. It also has the benefit of reducing the workload of the IT staff.

Continuous training for technology professionals

Gamification is not just for employees outside the IT department. IT and security professionals must keep pace with their evolving adversaries, so they are ready to defend and respond. For example, when a new vulnerability is discovered, gamification can help teams learn about it, how it is exploited, and what they can do to reduce its risk to the organisation. A similar approach, for example, was used to educate technical professionals when the Log4j vulnerability emerged.

Collaboration across functions

Gamified training can also be used to break down silos and ensure that collaboration becomes a habit across business units. To this end, it is important that each team is made up of employees from all departments, with a varied skill set so that everyone can learn from everyone else. This concept also applies to levels of knowledge and ability, so that one line-of-business employee may learn something about operations from another in a similar discipline, just as more inexperienced IT and security professionals may learn from higher flyers in their departments.

New careers

Gamification gives people a platform to shine. It is not uncommon to use points-based leader boards to show achievements during activities and these can be used to discover new talent among existing employees. It is also worth considering that students currently in higher education have been learning in different ways than the traditional frontal session and would be more interested working for an organisation that can offer "less traditional" training opportunities.

Game over!

We know that processes and technologies are nothing without the people that use them. Since the goal is enhancing an organisation's security posture, gamification helps in many ways and even allows discovering hidden cybersecurity talent. By making training fun, simulations, hackathons, and ethical hacking platforms make knowledge stick, which helps reduce risks now and in the long term - adding real value. Skills gaps have two sides: lack of staff and more work for current employees to do. By ensuring that cybersecurity awareness is retained by non-technical staff and that non-security staff can highlight their potential, gamification addresses both sides of the gap equation. 🚦

VMWARE PUTS POWER OF GENERATIVE AI WITHIN REACH OF ANY ENTERPRISE

VMWARE PRIVATE AI IS BRINGING COMPUTE CAPACITY AND AI MODELS TO WHERE ENTERPRISE DATA IS CREATED, PROCESSED, AND CONSUMED. Mware, Inc. has introduced new Private AI offerings to drive enterprise adoption of generative artificial intelligence and tap into the value of trusted data. Private AI is an architectural approach that unlocks the business gains from AI with the practical privacy and compliance needs of an organisation.

To make Private AI a reality for enterprises and fuel a new wave of AIenabled applications, VMware announced:

- VMware Private Al Foundation with NVIDIA, extending the companies' strategic partnership to ready enterprises that run VMware's cloud infrastructure for the next era of generative Al.
- Error! Filename not specified. VMware Private AI Reference Architecture for Open Source to help customers achieve their desired

Al outcomes by supporting best-inclass open source software (OSS) technologies today and in the future.

VMware Private AI is bringing compute capacity and AI models to where enterprise data is created, processed, and consumed, whether that is in a public cloud, enterprise data center, or at the edge. With these new offerings, VMware is helping customers combine the flexibility and control required to power a new generation of AI-enabled applications that will help dramatically increase worker productivity, ignite transformation across major business functions, and drive economic impact. A McKinsey report estimates generative AI could add up to \$4.4 trillion annually to the global economy.

A multi-cloud environment is the foundation for this new class of AIpowered applications because it makes private yet highly distributed data easier to harness. VMware's multi-cloud approach provides enterprises with greater choice and flexibility where AI models are built, customised with an enterprise's private data, and consumed, while still enabling required security and resiliency across any environment.

"The remarkable potential of generative

Al cannot be unlocked unless enterprises are able to maintain the privacy of their data and minimise IP risk while training, customising, and serving their Al models," said Raghu Raghuram, CEO, VMware. "With VMware Private AI, we are empowering our customers to tap into their trusted data so they can build and run AI models quickly and more securely in their multi-cloud environment."

Enterprises today face a hard choice when it comes to generative AI. They can either take advantage of public AI models to build their generative AI applications, but with the attendant risks of data exposure and uncertain training sources. Or they can attempt a "do-it-yourself" model, a strategy which lacks cost-efficiency and time- tovalue. VMware AI Labs developed VMware Private AI specifically to solve this problem.

"Al has traditionally been built and designed by data scientists, for data scientists," said Chris Wolf, vice president of VMware Al Labs. "With the introduction of these new VMware Private Al offerings, VMware is making the future of Al serve everyone in the enterprise by bringing the choice of compute and Al models closer to the data. Our Private Al approach benefits enterprise use cases ranging from software development and marketing content generation to customer service tasks and pulling insights from legal documents."

An Interconnected and Open Ecosystem Supports Customers' Al Strategies

VMware Private AI Reference Architecture for Open Source integrates innovative OSS technologies to deliver an open reference architecture for building and serving OSS models on top of VMware Cloud Foundation. At VMware Explore, VMware is showcasing collaborations with leading companies from across the AI value chain:

• Anyscale: VMware is bringing the widely adopted open source Ray unified compute framework to VMware Cloud environments. Ray on VMware Cloud Foundation makes it easy for data scientists and MLOps engineers to scale AI and Python workloads much more easily by utilising their current compute footprints for ML workloads instead of defaulting to the public cloud.

- Domino Data Lab: VMware, Domino Data Lab and NVIDIA have teamed up to provide a unified analytics, data science, and infrastructure platform that is optimised, validated, and supported, purposebuilt for AI/ML deployments in the financial services industry.
- Global Systems Integrators: VMware is working with leading GSIs such as Wipro and HCL to help customers realise the benefits of Private AI by building and delivering turnkey solutions that combine VMware Cloud with AI partner ecosystem solutions.
- Hugging Face: VMware is collaborating with Hugging Face to help launch SafeCoder today at VMware Explore. SafeCoder is a complete commercial code assistant solution built for the enterprise that includes service, software and support. VMware is utilising SafeCoder internally and publishing a reference architecture with code samples to enable the fastest possible time-to-value for customers when deploying and operating SafeCoder on VMware infrastructure.
- Intel: VMware vSphere/vSAN 8 and Tanzu are optimised with Intel's AI software suite to take advantage of the new built-in AI accelerators on the latest 4th Gen Intel Xeon Scalable processors.

In addition, VMware is announcing a new VMware AI Ready program, which will connect ISVs with tools and resources needed to validate and certify their products on VMware Private AI Reference Architecture. The program will be available to ISVs focused on ML and LLM Ops, data and feature engineering, developer tools for AI, and embedded AI applications. This new program is expected to be live by the end of 2023.

THE EVENT FEATURES TWO PRACTICAL COURSES LED BY CERTIFIED INSTRUCTORS AND REAL-WORLD CYBERSECURITY EXPERTS.

SANS INSTITUTE ELEVATES CYBER RESILIENCE IN QATAR WITH SANS DOHA SEPTEMBER 2023

t the heart of Qatar's digital revolution, SANS Institute – the world's foremost authority in cvbersecurity training – unveils SANS Doha September 2023. From September 16-21, this seminal event at the InterContinental Doha - The City will prepare Qatar's next-gen cyber guardians. The second training event hosted by SANS in Qatar this year, SANS Doha September 2023, is designed to equip participants with the essential skills to adeptly address both security challenges and prospects within cloud ecosystems, as well as those needed to safeguard Industrial Control Systems (ICS) networks.

As part of its National Vision 2030, Qatar has been actively working on building a strong cyber posture, particularly due to the increasing digitalization of various sectors. To support the growing digital economy, the nation is dedicated to developing the necessary human talent for a skilled cybersecurity workforce through training graduates, upskilling cyber professionals, and reskilling employees. Consistent recognition of how vital it is to protect critical infrastructure and sensitive data has also contributed to the region's cyber awareness.

"New technologies introduce new risks. More businesses in Qatar are moving sensitive data and shifting mission-critical workloads to the cloud, across multi-cloud platforms, without fully understanding the security concerns. While cybersecurity capabilities in Qatar have witnessed a remarkable surge, cyber-attacks are always evolving. In turn, defense tactics must evolve faster and hit stronger," says Ned Baltagi, Managing Director, Middle East, Africa and Turkey, at SANS Institute.

SANS Doha September 2023 features two practical courses led by certified instructors and real-world cybersecurity experts, Kenneth Hartman and Kai Thomsen. Kenneth Hartman will cover SEC488: Cloud Security Essentials, enabling professionals to use the services of any of the leading cloud service providers (CSPs) with confidence by identifying and mitigating different risks in various services offered by CSPS and implementing appropriate security controls in the cloud.

Kai Thomsen will lead ICS515: ICS Visibility, Detection, and Response. The course will qualify participants with the core skills necessary for any ICS cybersecurity program, teaching professionals to understand their networked ICS environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This is also critical in understanding and running a modern-day complex automation environment and achieving root cause analysis for non-cyber-related events that manifest over the network.

Additionally, Thomsen will host a SANS Doha Community Night session

on September 18 from 4:30 - 5:30 PM, where he will outline the current OT threat landscape and share recommendations on preparing against ICS attacks. Participants, as well as those with an avid interest in cybersecurity, can leverage the opportunity to learn more about trends, best practices, and the latest cybersecurity developments with an industry-leading practitioner and network with like-minded individuals in the cybersecurity community, either in-person or virtually.

Classes will run from 8:00 AM to 4:30 PM AST, including breaks. With flexible training formats available, participants can also opt for a virtual, Live Online program if they cannot attend in person.

"Educating the cyber workforce in the region is illimitable, and training programs such as SANS Doha September play a pivotal role in bridging the cybersecurity skills gap in the Middle East. Based on student feedback following our previous edition of SANS Doha, held in May this year, the training was extremely successful, valuable and relevant. Participants were especially appreciative of the exceptional caliber of our instructors, and the quality of training they delivered during the course," Baltagi concluded.

Upon completion of the course, participants can immediately apply what they have learned to secure their organizations and progress in their cyber careers.

NETSKOPE THREAT LABS: SOURCE CODE MOST COMMON SENSITIVE DATA SHARED TO CHATGPT

ChatGPT popularity by region Daily percentage of users within the region interacting with ChatGPT 2.4% Middle East 1.8% Australia 1.8% Asia 1.6% Africa 1.5% Latin America 1.3% Europe North America 0.8%

etskope, a leader in Secure Access Service Edge (SASE), has unveiled new research showing that

for every 10,000 enterprise users, an enterprise organisation is experiencing approximately 183 incidents of sensitive data being posted to the app per month. Source code accounts for the largest share of sensitive data being exposed.

The findings are part of Cloud & Threat Report: AI Apps in the Enterprise, Netskope Threat Labs' first comprehensive analysis of AI usage in the enterprise and the security risks at play. Based on data from millions of enterprise users globally, Netskope found that generative AI app usage is growing rapidly, up 22.5% over the past two months, amplifying the chances of users exposing sensitive data.

Growing AI App Usage

Netskope found that organisations with 10,000 users or more use an average of 5 AI apps daily, with ChatGPT seeing more than 8 times as many daily active users as any other generative AI app. At the current growth rate, the number of users accessing AI apps is expected to double within the next seven months. Over the past two months, the fastest growing AI app was Google Bard, currently adding users at a rate of 7.1% per week, compared to 1.6% for ChatGPT. At current rates, Google Bard is not poised to catch up to ChatGPT for over a year, though the generative AI app space is expected to evolve significantly before then, with many more apps in development.

Users Inputting Sensitive Data into ChatGPT

Netskope found that source code is posted to ChatGPT more than any other type of sensitive data, at a rate of 158 incidents per 10,000 users per month. Other sensitive data being shared in ChatGPT includes regulated dataincluding financial and healthcare data, personally identifiable information – along with intellectual property excluding source code, and, most concerningly, passwords and keys, usually embedded in source code.

"It is inevitable that some users will upload proprietary source code or text containing sensitive data to AI tools that promise to help with programming or writing," said Ray Canzanese, Threat Research Director, Netskope Threat Labs. "Therefore, it is imperative for organisations to place controls around AI to prevent sensitive data leaks. Controls that empower users to reap the benefits of AI, streamlining operations and improving efficiency, while mitigating the risks are the ultimate goal. The most effective controls that we see are a combination of DLP and interactive user coaching."

Blocking or Granting Access to ChatGPT

Netskope Threat Labs is currently tracking ChatGPT proxies and more than 1,000 malicious URLs and domains from opportunistic attackers seeking to capitalise on the Al hype, including multiple phishing campaigns, malware distribution campaigns, and spam and fraud websites.

Blocking access to AI related content and AI applications is a short-term solution to mitigate risk, but comes at the expense of the potential benefits AI apps offer to supplement corporate innovation and employee productivity. Netskope's data shows that in financial services and healthcare – both highly regulated industries – nearly 1 in 5 organisations have implemented a blanket ban on employee use of ChatGPT, while in



the technology sector, only 1 in 20 organizations have done likewise.

"As security leaders, we cannot simply decide to ban applications without impacting on user experience and productivity," said James Robinson, Deputy Chief Information Security Officer at Netskope. "Organisations should focus on evolving their workforce awareness and data policies to meet the needs of employees using AI products productively. There is a good path to safe enablement of generative AI with the right tools and the right mindset."

In order for organisations to enable the safe adoption of AI apps, they must center their approach on identifying permissible apps and implementing controls that empower users to use them to their fullest potential, while safeguarding the organisation from risks. Such an approach should include domain filtering, URL filtering, and content

NETSKOPE FOUND THAT ORGANISATIONS WITH 10,000 USERS OR MORE USE AN AVERAGE OF 5 AI APPS DAILY, WITH CHATGPT SEEING MORE THAN 8 TIMES AS MANY DAILY ACTIVE USERS. inspection to protect against attacks. Other steps to safeguard data and securely use AI tools include:

- Block access to apps that do not serve any legitimate business purpose or that pose a disproportionate risk to the organisation.
- Employ user coaching to remind users of company policy surrounding the use of AI apps.
- Use modern data loss prevention (DLP) technologies to detect posts containing potentially sensitive information.

Read the full Cloud & Threat Report: AI Apps in the Enterprise here. For more information on cloud-enabled threats and the latest findings from Netskope Threat Labs, visit Netskope's Threat Research Hub. To receive Netskope Threat Labs blog posts, subscribe here.

In conjunction with the report, Netskope today announced new solution offerings from SkopeAI, the Netskope suite of artificial intelligence and machine learning (AI/ML) innovations. SkopeAI leverages the power of AI/ML to conquer the limitations of complex legacy tools and provide protection using AI-speed techniques not found in other SASE products.

HOW DO YOU STOP INITIAL ACCESS BROKERS?

LAYALE HACHEM, SENIOR SOLUTIONS ENGINEER – BEYONDTRUST

hen the Arab Gulf reaion began its mass cloud migration in 2020, the technology landscape changed. And, reacting swiftly as it always does, the cyberthreat landscape changed in parallel. Today, cybercrime is an industry. We see B2B suppliers and customers. We see cloud offerings like ransomware-as-a-service (RaaS). The lone-wolf threat actor has been replaced by a workforce of specialists each playing their part in nefarious operations.

Legitimate businesses, beware. One such specialism that is rising in prominence is that of the initial access broker (IAB). As the name may suggest, IABs concern themselves with establishing a foothold within a corporate IT environment and selling that foothold. They use a range of methods, like spam and phishing, to steal credentials. They often bypass multifactor authentication (MFA). From there, it is off to the dark-Web market to make easy cash by selling their wares to others looking to make easy cash, from RansomOps gangs to supply-chain attackers.

You do you

The IAB model allows threat gangs to bridge skills gaps. An IAB may have assembled a team that is very good at establishing access. They will be skilled in social engineering and all the techniques involved in harvesting login details. They may not be so skilled in using these privileges to perform lateral movement. They may know little about how to build a ransomware payload. Those that are skilled in these latter areas may either not have the social-engineering skills to score credentials quickly or may simply want to speed up operations.

It is evident that each side of the IAB equation gains great advantages that eliminate waste in labor hours. They reduce risk and increase profits for everybody. Amid their newfound popularity, IABs are keeping authorities busy. In April, dark-Web marketplace Genesis Market was shut down by international law-enforcement agencies in Operation Cookie Monster. Similar operations had previously targeted Hydra Market and BreachForums. But these are just the markets. The sellers can skip town and go elsewhere. So how do we stop IABs? There are four main ways.

1. Enforce the principle of least privilege

By granting only those privileges needed to perform a role, organisations ensure that if a user is tricked by an IAB, the harvest will be lean. IABs do their homework and will target users with administrator rights, so it is wise to ensure that users who are not system admins in their day job are not given such access. Admin rights are a springboard for lateral movement, further credentials theft, and the elevation of privileges. Guard them well.

2. Revamp MFA

IABs have learned to compromise MFA, but that does not mean we must abandon it as a protection measure. It is still a useful tool against stolen credentials or credential-stuffing attacks. MFA fatigue attacks use push notifications and SIM-jacking to compromise this extra layer of security but Fast Identity Online (FIDO2) protects against this by using local authentication and asymmetric public-key cryptography. This delivers decentralized authentication, which is resistant to MFA fatigue and other forms of MFA bypassing.

3. Jettison VPN and RDP

VPN and RDP can often be unnecessary for remote work. What users need is straightforward access to the systems that are relevant to them. By granting this access in a controlled and auditable way, organisations stay a step ahead of IABs by preventing them from exploiting VPN access to flat networks or public-facing RDP servers. Such exploits allow free and rapid movement around IT environments. Enterprises should pay particular attention to the access granted to third parties who will be using personal or unmanaged devices.

4. Eliminate dormant accounts

Default, dormant, orphaned — these accounts are nectar to IABs, providing a pre-provisioned identity that allows an infiltrator to wander around unchallenged. They may belong to humans or machines, but when compromised, they can lead to increased dwell time; and if they have levels of privilege attached, a lot of damage can occur before the attacker is discovered. These accounts must be brought under strict management, and if they are not needed, they should be deleted. Often, default, dormant, or orphaned accounts are not enrolled in MFA. An IAB can use credential stuffing and self-enrolment in MFA to set up OTP delivery to a device of their choosing and gain access on a whim.

The game has changed but the fundamentals remain

So, the good news is that while initial access brokers are certainly a gamechanger for the threat-actor community, the risks they pose to the legitimate business are no different than they have always been. It is imperative that businesses have the security capabilities to notice they have been targeted and that access to their systems is going under the hammer at dark-Web auction houses.

Awareness begins with proactive management of identities and privileges, but to be truly cognizant of the threats to an environment, security teams should consider an identity threat detection and response (ITDR) approach. ITDR builds on privileged access management (PAM) by integrating threat intelligence, best practices, tools, and processes that allow the timely detection and investigation of high-risk anomalies, as well as a response that can save the organization from damage to assets and reputation.

Unfortunately, we live in a world where we cannot escape the digital realm. But we also live in a world that is wise to the dangers. IABs may be on the prowl, but with the right maneuvers, we can give them the slip. **1**

IABS MAY BE ON THE PROWL, BUT WITH THE \rightarrow RIGHT MANEUVERS, WE CAN GIVE THEM THE SLIP.





MANAGEENGINE NAMED A CHALLENGER IN THE 2023 GARTNER MAGIC QUADRANT FOR PRIVILEGED ACCESS MANAGEMENT

COMPANY RECOGNISED FOR ITS COMPLETENESS OF VISION AND ITS ABILITY TO EXECUTE

anageEngine, the enterprise IT management division of Zoho Corporation, has announced that it has been named a Challenger in the 2023 Gartner Magic Quadrant for Privileged Access Management (PAM). A Gartner Magic Quadrant is a culmination of research in a specific market, providing consumers a wide-angle view of the relative positions of the market's competitors. ManageEngine, which has been recognised in this Magic Quadrant report for the fourth time in five years, was assessed alongside 10 PAM vendors for its completeness of vision as well as its ability to execute.

"With identities and privileged accounts evolving as the new perimeter and economic headwinds driving efficiencyrelated security initiatives, IAM leaders need a comprehensive strategy to understand and manage all kinds of privileged access in their organisations

> MANAGEENGINE, WHICH HAS BEEN RECOGNISED IN THIS MAGIC QUADRANT REPORT FOR THE FOURTH TIME IN FIVE YEARS, WAS ASSESSED ALONGSIDE 10 PAM VENDORS.

while mitigating associated business and operational risks," said Kumaravel Ramakrishnan, director of marketing at ManageEngine.

"PAM360 fits the philosophy of value-oriented IT management, helping enterprise security teams manage administrative privileges end to end. We believe that this recognition from Gartner is a testament of our continued commitment to building a unified PAM platform that will be a key cog in the IAM strategy of enterprises of any size," he added.

Recent product innovations in ManageEngine PAM360 include:

- Trust scores for users and endpoints, which offer real-time risk assessment to identify and pre-empt anomalous activities.
- Policy-based access controls, which enable administrators to predefine a set of access policies and grant conditional access to mission-critical endpoints based on trust scores and other crucial parameters.
- Self-service privilege elevation for Linux environments, which enables administrative users to configure an allow-list of sensitive commands and let users execute those commands with elevated privileges.

MOST ATTACKS ON INDIVIDUALS IN THE MIDDLE EAST INVOLVE SPYWARE

ositive Technologies analysed attacks on individuals in Middle Eastern countries between 2022 and 2023. Malware

was used in 70% of successful attacks. More than half of these attacks involved spyware. The vast majority of attacks used social engineering techniques. In 20% of phishing campaigns, the attack was multi-pronged, exploiting multiple social engineering channels simultaneously.

According to our data, cybercriminals employed malware in 7 out of 10 successful attacks on individuals in the Middle East region. More often than not, the attackers infected users' devices with spyware (three out of five malware attacks). This type of malware collects information from the infected device and then passes it on to the attacker. Depending on the task, spyware can steal personal and financial data, user credentials, as well as files from the device's memory.

Positive Technologies Information Security Research Analyst Roman Reznikov comments: "By using spyware, attackers can compromise not only



personal and payment information and personal accounts, but also corporate credentials, network connection information, and other sensitive data. The stolen data is then offered for sale on the dark web forums. As a result, a skilled attacker can gain access to an organisation and carry out a successful attack, leading to nontolerable consequences: disruption of technological and business processes, theft of funds, leakage of confidential information, attacks on customers and partners."

In the vast majority (96%) of successful attacks on individuals in the Middle East countries, social engineering techniques were employed. Most often, these were mass attacks in which the criminals aimed to reach the maximum number of victims. To achieve this, they actively leveraged current news about significant global and regional events, including the 2022 FIFA World Cup Qatar.

In every fifth (20%) phishing campaign, the attack was multi-pronged, exploiting multiple social engineering channels simultaneously. Criminals led the victims through a series of steps until the device was infected and data stolen. For instance, users could be lured through social media accounts that contained links to a messenger channel from which the victim would install a malicious application.

One of the reasons for the success of social engineering is the numerous data leaks from various organisations. According to our research on the cybersecurity threatscape in the Middle East, 63% of successful attacks on

ONE OF THE REASONS FOR THE SUCCESS OF SOCIAL ENGINEERING → IS THE NUMEROUS DATA LEAKS FROM VARIOUS ORGANISATIONS. individuals in the region resulted in leaks of confidential information. The majority of stolen information consisted of personal data (30%) and account credentials (30%). Cybercriminals were also interested in payment card data (10%) and user correspondence (8%).

On the dark web, malicious actors sell information about users and also provide stolen data archives for free. Criminals use the compromised information in subsequent attacks on users. For example, a successful attack on a bank could result in fraudulent actions against its customers.

Cybersecurity experts recommend that users follow cyberhygiene rules. Companies also need to ensure the security of employee and customer data. Data breaches cause reputational and financial damage and put at risk users whose information has been compromised. To maintain cyberresilience, it's essential to regularly assess the effectiveness of security measures and pay special attention to verification of non-tolerable events.

SCAMMERS CAPITALISE ON THE YEAR'S **BIGGEST SMARTPHONE RELEASE**

n anticipation of the imminent release of Apple's iPhone 15, Kaspersky experts have uncovered a range of scams that exploit the excitement surrounding this event. These scams encompass various fraudulent schemes, each carrying distinct risks for unsuspecting consumers, including potential data leaks and financial losses.

In one prevalent deceptive maneuver. scammers entice users with the chance to purchase the iPhone 15 ahead of its official launch. This scheme capitalizes on users' eagerness to be among the first to possess Apple's latest device. Such a scam typically unfolds as follows: scammers claim they can provide pre-release iPhones and promise users the opportunity to acquire them, often at an attractive price. To secure their 'exclusive' purchase, victims are required to make an upfront payment or divulge their financial information. Additionally, users are asked to provide personal identification details such as their name, address, and phone number. Following the submission of payment, the scammers vanish, leaving victims without the promised iPhone and deprived of their funds. Beyond the financial risks, this scam also raises significant privacy concerns, as the pilfered data may potentially be sold on the Dark Market.

Another scam presents participants with the chance to win the new iPhone 15. provided they pay a nominal upfront fee. The typical progression of this scheme unfolds as follows: users are drawn in by the allure of a free iPhone 15, perfectly complementing their anticipation for the impending release. To enter the giveaway, participants are instructed to pay a small fee, often disguised as a "processing" or "registration" fee. After

SPECIAL OFFER

Mobile Phones > PRE ORDER > IPHONE 15 ATTENTION: THIS OFFER ENDS IN: 04:25



Apple Pay - Pay with your iPhor in stores, apps, and on the web.

IPHONE 15.

using Face ID

The iPhone 15 is just around the corner, with Apple all but certain to unveil the next generation of its best iPhones in September 2023.

Indeed, the iPhone 15, iPhone 15 Plus, iPhone 15 Pro and iPhone 15 Pro Max rumors have been swirling ever since the iPhone 14 line launched last year, with analysts and eagle-eyed tipsters sharing consistent leaks concerning the specs, pricing and availability of all four phones NOW ITS YOUR CHANCE TO PRE ORDER

An example of a phishing page offering iPhone 15 pre-order

the payment participants receive nothing in return. The promised iPhone remains elusive, resulting in financial losses for those involved.

"In the digital age, scammers are constantly adapting and exploiting our excitement for the latest tech trends. It's crucial for consumers to stay vigilant, verify offers, and safeguard their personal information. Remember, if something seems too good to be true, it often is," comments Tatyana Kulikova, security expert at Kaspersky.

To avoid falling victim to such scams, Kaspersky experts recommend:

- Verify the Source: Ensure you are dealing with reputable and authorized sellers, especially for pre-release purchases.
- Avoid Upfront Payments: Exercise caution with offers demanding

upfront payments for giveaways or pre-release products.

• Use Official Channels: Rely on Apple's official website or authorized retailers for genuine purchases.

Sec. inc.

-

- Check Reviews: Before making any online purchases, research the seller and review customer feedback.
- Enable Two-Factor Authentication (2FA): Safeguard your online accounts, especially those linked to payment methods, with 2FA.
- Use Security Solution: An • automated security solution, like Kaspersky Premium, will protect you from all known and unknown scams.
- Stay Informed: Stay current on • common scams and cybersecurity best practices. 1



D

L

L

Technologies

Cyber and ransomware attacks are the enemy of today's data-driven business





Preserve data integrity and confidentiality with layers of security and controls

00	—
60	-
60	_

Isolation Physical and logical separation of data within a vault



Intelligence

Machine learning and analytics help ensure recoverability

Cyber Recovery

www.cbt.ae
 04 2101900
 info@cbt.ae

