WWW.TAHAWULTECH.COM

ADVISOR

RIDDLE EAST

INTERVIEWS

THREATQUOTIENT (pg 18)

> TENABLE (pg 28)

FORTINET (pg 40)

STEPHAN BERNER, CHIEF EXECUTIVE OFFICER, HELP AG ON THE TRANSITION FROM PRODUCT-BASED TO SERVICE OFFERING-BASED SECURITY (pg 12)

FUIUre-







tahawultech.com

VIRSEC Protect Your Software as it Runs.

To fully protect your software, you must first fully understand it. Only Virsec can do this, by creating a dynamic golden image of what your software is supposed to do—and immediately stop anything that it's not.



Stop Fileless Memory Attacks | Protect Legacy Applications | Reduce Patching Urgency | Engineered for Servers—Not Endpoints

"We are at the inflection point for the next paradigm shift in cybersecurity and Virsec does what is needed: protect application workloads at runtime. This is the new battleground." – John Chambers, Virsec Investor and Strategic Advisor and Former Cisco CEO



CONTENTS



7 FUTURE-PROOF

Stephan Berner, CEO, Help AG, on how the cybersecurity industry is transitioning from product-based to service offering-based.

06 NEWS We bring you the latest cybersecurity news from the region.

EDITOR'S PICK

Jason Jordaan, Instructor at SANS Institute, on ransomware and how the best defence consists of employees who are aware of the threats, and skilled cyber security defenders.

18 INTERVIEW Firas Ghanem, Regional

Firas Ghanem, Regional Director - Middle East & Pakistan at ThreatQuotient, describes how the company works with customers to improve the efficiency and effectiveness of security operations through a comprehensive approach to threats.







26 OPINION Satya Gupta, Cofounder and Chief

Technology Officer, Virsec, on Remote Code Execution.

36 SECURITY MATTERS

Industrial enterprises must adopt a multilayer approach that anticipates cyberattacks and safeguards critical assets before they are exploited, says Tim Grieveson, Chief Information Security Officer, AVEVA.



PROFESSIONAL IP SURVEILLANCE SOLUTIONS



Easy & Pro Series Range | IP Cameras & NVRs | Deep Video Compression | Superior Quality | Video Analytics Centralized Management | Starlight & Super Starlight

Monitor Your Premises From Anywhere



SWARR





UHD



EDITORIAL



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

> Anita Joseph Editor

EVENTS



STOP THE ATTACK!

Ransomware attacks are big business,

especially in the post-pandemic world. In fact, the frequency of these attacks has risen so dramatically, that organisations, both big and small, continue to reel under its impact as the year wears on. According to the mid-year update to the 2021 SonicWall Cyber Threat Report, ransomware attacks skyrocketed in the first half of 2021, eclipsing the entire volume for 2020 in only six months. In fact, through the first half of 2021, SonicWall recorded global ransomware volume of 304.7 million, surpassing 2020's full-year total (304.6

million) — a 151% year-todate increase. These stats are just the tip of the iceberg. Ransomware continues to wreak havoc on the entire business ecosystem and companies are scrambling to find a way to stop this menace.

In this issue of your favourite magazine, we discuss ransomware at length in a special feature. We have cybersecurity frontrunners debating every aspect of the problem-right from how it began, to who is to blame, down to how a multi-layered approach to security is the only way out.

Our cover story features Help AG, which focuses on the fascinating concept of

service-centric business evolution as the new era of cybersecurity. We have Stephan Berner, CEO of Help AG, discussing how instead of being focused on offering hundred products to customers, the focus is shifting towards services instead - so people can buy services with well-defined SLAs irrespective of the products that lie underneath the hood.

Our interview with Fortinet's Kalle Bjorn is all about the changing threat landscape and the company's focus on information sharing across the entire network. ThreatQuotient's Firas Ghanem

> tells us how the company works with customers to improve the efficiency and effectiveness of security operations through a comprehensive approach to threats. Marty Edwards, VP,

OT at Tenable, discusses ransomware and how Tenable is closely watching the threat environment in order to help organisations prioritise vulnerabilities that are being exploited the most.

In addition, we have the usual news updates, reports and opinion pieces to ensure that you stay ahead of all the information there is to know. Happy Reading!

FOUNDER, CPI MEDIA GROUP Dominic De Sousa (1959-2015)

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

ADVERTISING Group Sales Director Kausar Syed kausar.syed@cpimediagroup.com

Senior Sales Manager Sabita Miranda sabita.miranda@cpimediagroup.com EDITORIAL Editor Anita Joseph anita.ioseph@cpimediagroup.com

Online Editor Daniel Shepherd daniel.shepherd@cpimediagroup.com DESIGN Senior Designer Analou Balbero analou.balbero@cpimediagroup.com

> DIGITAL SERVICES Web Developer Adarsh Snehajan

Registered at Dubai Production City, DCCA PO Box 13700 Dubai, UAE

Published by

Reception: +971 4 5682993 Operations: +971 4 5682994 Accounts: +971 4 5682995

> © Copyright 2021 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.

RANSOMWARE CONTINUES TO WREAK HAVOC ON THE ENTIRE BUSINESS ECOSYSTEM.

MIMECAST ANNOUNCES INTEGRATION WITH HUMIO

"E-mail threats are becoming

day. Business email compromises,

harder to stop and proliferating each

Mimecast Limited, a leading email

security and cyber resilience company, has announced a strategic API integration with Humio, a CrowdStrike Company, the only log management platform enabling complete observability for all streaming logs

in real-time and at scale. The integrated solution is designed to deliver email-based threat intelligence with advanced detection, investigation and threat hunting. Enterprise organisations leveraging the integration gain search and correlation capabilities across all log types to better detect and respond to advanced cyber threats.

spear phishing attempts and the rise of ransomware are among the biggest challenges IT and security teams face," said Jules Martin, vice *"OUR INTEGRATION* WITH HUMIO **HELPS PROVIDE** ORGANISATIONS **INCREASED VISIBILITY WITH LIVE SEARCHES & REAL-**TIME DASHBOARDS. **EMPOWERING THREAT**

HUNTING TEAMS

TO FIND MALICIOUS

ACTIVITY BEFORE IT

LANDS IN AN INBOX."

president, Ecosystem & Alliances at Mimecast. "Our integration with Humio helps provide organisations increased visibility with live searches and real time dashboards. empowering threat hunting teams to find potentially malicious activity before it lands in an inbox. Incident response teams are empowered to work faster, a vital benefit when containing incidents before they

II II ES MARTIN **VP FCOSYSTEM** & ALLIANCES, AT MIMECAST



become a full-scale breach."

Humio's unique architecture enables customers to log everything and miss nothing, and joint customers can ingest Mimecast logs with other log sources including infrastructure, network and software. This provides customers with complete visibility across their threat landscape, coupled with fast search performance and comprehensive query language. enabling threat hunters to guickly ask any questions of their data. Humio's real time alerts and comprehensive API make it easy to integrate with leading cybersecurity platforms for efficient and automated response actions, which can be utilised to modify parameters within Mimecast for preventative protection.

FORTIGUARD LABS REPORTS TENFOLD **INCREASE IN RANSOMWARE**

DEREK MANKY. CHIEF. SECURITY INSIGHTS & GLOBAL THREAT ALLIANCES, FORTIGUARD LABS



Fortinet, a global leader in broad, integrated, and automated

cybersecurity solutions, has announced the latest semiannual FortiGuard

Labs Global Threat Landscape Report. Threat intelligence from the first half of 2021 demonstrates a significant increase in the volume and sophistication of attacks targeting individuals. organisations, and increasingly critical infrastructure. The expanding attack surface of hybrid workers and

"WE'RE SEEING AN INCREASE IN EFFECTIVE & DESTRUCTIVE CYBERATTACKS AFFECTING **ORGANISATIONS IN A SINGLE INCIDENT CREATING AN INFLECTION POINT** FOR THE WAR ON **CYBERCRIME.**"

learners, in and out of the traditional network, continues to be a target. Timely collaboration and partnership momentum across law enforcement

> as well as public and private sectors is an opportunity to disrupt the cybercriminal ecosystem going into the second half of 2021.

"We are seeing an increase in effective and destructive cyberattacks affecting thousands of organisations in a single incident, creating an important inflection point

for the war on cybercrime," biez Derek Manky, chief, Security Insights & Global Threat Alliances at FortiGuard Labs. "Now more than ever, everyone has an important role in strengthening the kill chain. Aligning forces through collaboration must be prioritised to disrupt cybercriminal supply chains. Shared data and partnership can enable more effective responses and better predict future techniques to deter adversary efforts. Continued cybersecurity awareness training as well as AI-powered prevention, detection, and response technologies integrated across endpoints, networks, and the cloud remain vital to counter cyber adversaries," he added.

BEYONDTRUST APPOINTS NEW CTO & CSO TO STRENGTHEN SECURITY LEADERSHIP

BeyondTrust, the worldwide leader

in Privileged Access Management (PAM), has announced the appointment of Marc Maiffret as Chief Technology Officer and appointment of Morey Haber as Chief Security Officer, further expanding and strengthening the company's security leadership.

Marc Maiffret brings 20+ years of executive security leadership to BeyondTrust, as a founder at eEye Digital Security, and executive leadership positions at FireEye, BeyondTrust, and SpaceX. As Chief Technology Officer (CTO), Marc will be focused on developing technology roadmaps and building the innovative technology platforms necessary to enable the delivery of

highly secure, highly scalable, best-inclass products. Marc will also take a role in BeyondTrust Labs, further enhancing BeyondTrust initiatives in security and technology research.

"Joining BeyondTrust is not only a chance to work with an amazing team, but also contribute to a company

MARC MAIFFRET

BRINGS 20+ YEARS

OF EXECUTIVE

SECURITY

LEADERSHIP AT

BEYONDTRUST. AS

A FOUNDER AT FEYE

DIGITAL SECURITY.

AND EXECUTIVE

I FADFRSHIP

POSITIONS AT

FIREEYE.

that I believe is best positioned to have a continued impact in helping customers solve real-world security problems," said Marc Maiffret, CTO. BevondTrust. "I believe that properly managing privileges, identities and access is central to defending against modern attackers. I'm excited for the opportunity to build on the innovation and remarkable progress



MARC MAIFFRET, NEW CTO AT BEYONDTRUST.

BeyondTrust has made in the last few years while helping to chart a course for what is beyond the horizon."

Morey Haber joined BeyondTrust in 2012 as a part of the eEye Digital Security acquisition, where he served as a Product Owner and Solutions Engineer since 2004. Morey has more than 25 years of IT industry experience and has authored three books: Privileged Attack Vectors, Asset Attack Vectors, and Identity Attack Vectors. Morey will carry his extensive knowledge from his most recent experience as BeyondTrust CISO and CTO into his new role as Chief Security Officer (CSO), where he will direct and oversee security and governance for the company's corporate and cloud-based solutions.

OIL-INDUSTRY EQUIPMENT MANUFACTURER TATSUNO PROTECTS FUEL DISPENSERS WITH KASPERSKY EMBEDDED SYSTEMS SECURITY

Tatsuno Corporation, a Japanese

manufacturer of fuel dispensers and other solutions for global retail commercial fueling customers, has chosen Kaspersky Embedded Systems Security to protect the payment terminal systems installed in its fuel dispensers. Key solution benefits include support for Windows XP, strong levels of security over a long period of time, and compatibility with low-end hardware.

The payment terminal systems embedded in the gasoline dispensers made and sold by Tatsuno Corporation accept credit card payments. To guarantee the security of payment operations, it requires a number of solid security measures and processes. These include proper security for both specialised endpoints (such as dispenser payment terminals) and the networks they connect to, protection of card holder data, some means to control vulnerabilities in software and implementation of secure access methods. It also requires convenient instruments to configure and enforce strong security policies, while periodic auditing and testing of networks is essential.

In Tatsuno's preliminary tests, it found that Kaspersky Embedded Systems Security, a multi-layered solution to protect Windows-based embedded devices, either fulfils the requirements perfectly – or facilitates their execution, streamlining some aspects for IT security staff. Additionally, it would run effortlessly on the company's hardware with limited memory

kaspersky

and disk space. Kaspersky Embedded Systems Security supports Windows XP and is suitable for the long-term lifecycle of gasoline dispensers. The solution solved Tatsuno's problems, making it the ideal choice. Working with Kaspersky's system engineers, Tatsuno was able to finish product testing quickly and smoothly.

The solution was installed in the payment terminal system, embedded in Tatsuno's gasoline dispensers in April of 2020, and is currently operating without any issues. Moving forward, Tatsuno plans to install it in other systems, including its Points of Sale (POS) systems, to ensure enhanced security.

SONICWALL TURNS 30: CYBERSECURITY PIONEER MARKS THREE DECADES OF INNOVATION

BILL CONNER, PRESIDENT & CEO, SONICWALL



SonicWall is celebrating its 30th

anniversary as a cybersecurity industry leader. Throughout August, the company celebrated its heritage, product innovation, channel DNA and the many cybersecurity innovators who have helped support and transform it into the SonicWall it is today.

"Innovation and adaptability are key components to successfully evolving cybersecurity strategy through the ebb and flow of the fast-moving threat landscape," said SonicWall President and CEO Bill Conner. "SonicWall has proven across three decades that its mission is securing the long-term success of its customers, partners and employees. While the last five years were important chapters in this journey, we have more goals to achieve, milestones to mark and history to be made. SonicWall is always forward-looking. And that's how the company - and its people - has been a mainstay in the industry for more than 30 years."

To commemorate this milestone achievement, the company is honouring long-term employees and celebrate those who have deep tenure. Throughout the month of August, SonicWall featured pictures from the company, people, products, partners and customers over the course of three decades via the #SonicWall30 social media campaign. Throwback Thursdays were reserved for contests and stories depicting SonicWall's past and future.

CYBERCRIMINALS NARROW FOCUS ON SMBS: ACRONIS REPORT

A Mid-year Cyberthreats Report 2021 by

global cyber protection leader Acronis, warns that small and medium-sized businesses (SMBs) are at particular risk based on the attack trends seen during the first six months of the year. Released at Black Hat 2021 event, where Acronis was a Diamond sponsor, the report is an in-depth review of the cyberthreat trends the company's experts are tracking.

The report revealed that during the first half of 2021, 4 out of 5 organizations experienced a cybersecurity breach originating from a vulnerability in their third-party vendor ecosystem. That's at a time when the average cost of a data breach rose to around \$3.56 million, with the average ransomware payment jumping 33% to more than \$100,000.

While that represents a major financial hit to any organization, those

Acronis

amounts would sound the death-knell for most SMBs, which Acronis believes is a major concern for the second half of 2021.

"While the increase in attacks affects organizations of all sizes, something that's under-reported in the coverage of current cyberthreat trends is the impact on the small business community," explained Candid Wüest, Acronis VP of Cyber Protection Research. "Unlike larger corporations, small and medium-sized companies don't have the money, resources, or staffing expertise needed to counter today's threats. That's why they turn to IT service providers – but if those service providers are compromised, those SMBs are at the mercy of the attackers.

MCAFEE ENTERPRISE UNVEILS INTEGRATION WITH MICROSOFT DYNAMICS 365 FOR GREATER CLOUD SECURITY & COMPLIANCE

McAfee Enterprise has announced that

MVISION Cloud, part of its secure access service edge (SASE) offering - MVISION Unified Cloud Edge (UCE), now provides enhanced security coverage for Microsoft Dynamics 365, a line of enterprise resource planning and customer relationship management software applications. This solution complements Dynamics 365 capabilities by using a frictionless API-based cloud-native approach that allows IT teams to seamlessly enforce data loss prevention (DLP) policies and collaboration controls, access control, address threats from insiders and compromised accounts, audit all user activity and secure corporate data as

users collaborate in the cloud.

Microsoft Dynamics 365 is a portfolio of intelligent business applications that empowers organisation to deliver operational excellence and create more engaging customer experiences. It brings together customers and products, people and data to bridge sales and service, supply chains and store fronts with connected business applications to reach more customers in more places. McAfee is one of the only cloud access security broker (CASB) vendor who has released API-integrated enterprise data and threat protection capabilities for Dynamics 365, providing enterprise users with an added layer of security, visibility and control.

TENABLE HELPS ORGANISATIONS DISRUPT ATTACKS WITH NEW ACTIVE DIRECTORY SECURITY READINESS CHECKS

In the wake of a growing number of

both ransomware and sophisticated attacks, Tenable, Inc., the Cyber

Exposure company, has developed 10 foundational configuration checks for its solutions, including Tenable.io, Tenable.sc and both Nessus Professional and Nessus Essentials that assess Microsoft Active Directory security readiness and align remediation efforts based on the threat landscape. These checks leverage Tenable's expertise in securing

Active Directory environments through Tenable.ad and are available immediately for existing customers at

"WE'RE SEEING THE WEAPONISATION OF ACTIVE DIRECTORY BY BAD ACTORS VIRTUALLY EVERYTIME A NEW RANSOMWARE ATTACK OR HACK MAKES HEADLINES."

no extra charge. "We're seeing the weaponisation of Active Directory by bad actors virtually everytime a new ransomware attack or back makes the headlines. Securing Active Directory is one of the most critical steps virtually any organisation should take to build stronger cyber defences and a solid foundation for their digital business", said Renaud Deraison. RENAUD DERAISON, CO-FOUNDER AND CHIEF TECHNOLOGY OFFICER, TENABLE.



Co-Founder and Chief Technology Officer, Tenable. "We're helping to address this growing crisis with new Active Directory checks that make it easier than ever for customers to understand what steps they must take immediately to get their Active Directory security in order and disrupt bad actors' go-to attack paths".

The Active Directory Security Readiness Checks are now generally available in Tenable.sc, Tenable. io, Tenable.ep, Nessus Professional and Nessus Essentials.

QUALYS JOINS HANDS WITH RED HAT TO DRIVE SECURITY FOR RED HAT ENTERPRISE LINUX COREOS & RED HAT OPENSHIFT

Qualys, Inc., a pioneer and leading

provider of disruptive cloud-based IT, security and compliance solutions,

has announced it has collaborated with Red Hat to drive greater security for both the container and host operating system for Red Hat OpenShift.

Teaming with Red Hat, Qualys is offering a unique approach providing a containerised Qualys Cloud Agent that extends security to the operating system. The Cloud Agent for Red Hat Enterprise Linux CoreOS on OpenShift combined with the Qualys solution for Container Security provides continuous discovery of packages

"AS SECURITY TEAMS LOOK TO SUPPORT MODERN APPLICATIONS BUILT ON CUTTING-EDGE TECHNOLOGY LIKE RED HAT OPEN SHIFT, THEY NEED TO SECURE BOTH THE RUNNING CONTAINER IMAGES AND THE UNDERLYING OPENSHIFT CLUSTER." and vulnerabilities for the complete Red Hat OpenShift stack. Built on the Qualys Cloud Platform, Qualys' solution seamlessly integrates with customers' vulnerability management workflows, reporting and metrics to help reduce risk.

"As security teams look to support modern applications built on cutting edge technology like SUMEDH THAKAR, PRESIDENT AND CEO AT QUALYS



Red Hat OpenShift, they need to secure both the running container images and the underlying OpenShift cluster," said Sumedh Thakar, president and CEO of Qualys. "By collaborating with Red Hat, we have built a unique approach to secure Red Hat Enterprise Linux CoreOS that provides complete control over containerised workloads enhancing Qualys' ability to help customers discover, track and continuously secure containers," he added.

A SKILLED APPROACH TO RANSOMWARE

JASON JORDAAN, INSTRUCTOR AT SANS INSTITUTE, TELLS SECURITY ADVISOR ABOUT THE RAMPANT RANSOMWARE ATTACKS AND HOW THE BEST DEFENCE CONSISTS OF VIGILANT EMPLOYEES AND SKILLED CYBERSECURITY DEFENDERS.



ould you agree that ransomware is on the rise because many MSPs, especially the smaller ones, don't take the risks of ransomware seriously enough?

Ransomware is on the rise, in my opinion, because it is an incredibly profitable and low risk cybercrime activity. Everyone is a potential target. In my investigations I have seen multinationals affected by ransomware, and just as often I have seen small business affected. While many large business and organisations are aware of the threat of ransomware. I find that smaller businesses and organisations consider ransomware to be something that won't affect them because of their size. But this is far from the truth. While major ransomware incidents like the Capitol One Pipeline incident in the United States make international news, the hundreds and thousands of small and medium size business and organisations that are affected by ransomware hardly ever do. I think if businesses and organisations understand that they are all at risk, regardless of size, then maybe they would start to take ransomware more seriously than they currently do.

"IF BUSINESSES AND ORGANISATIONS UNDERSTAND THAT THEY ARE ALL AT RISK, REGARDLESS OF SIZE, THEN MAYBE THEY WOULD START TO TAKE RANSOMWARE MORE SERIOUSLY THAN THEY CURRENTLY DO."

Would you agree that a multilayered approach that prevents ransomware from reaching networks and systems is the best way to minimise risk?

Any kind of multi-layered security (or defense in depth) approach is certainly better than a single layer of security, but simply adding extra layers of security is not enough in my opinion, because your security architecture, processes, and response, need to be appropriate for the varied threats you face. While technical security measures can always be valuable, we need to remember that the threats that we face are human ones, and humans being creative, especially when it comes to criminality, will often find a way. The best defence against threats like ransomware is, in my opinion, employees that are constantly vigilant and aware of the threats, and skilled cyber security defenders.

What approach is your company adopting towards this ever-increasing threat?

The threat of ransomware has led to the SANS Institute and SANS instructor Ryan Chapman, developing a brandnew course, FOR528 Ransomware for Incident Responders, which is aimed at helping to address the threats posed by ransomware around the globe.







VALUABLE SAVINGS ON TIME AND COST WITH SALICRU UPS SYSTEMS



Salicru offers a wide range of UPS systems, from 1 kVA to 1500 kVA, in the Off-Line, Line-Interactive, and On-Line categories.

SCREENCHECK ME - AUTHORISED DISTRIBUTOR FOR





N

FUTURE-PROOF

STEPHAN BERNER, CHIEF EXECUTIVE OFFICER, HELP AG, TELLS **ANITA JOSEPH** HOW THE CYBERSECURITY INDUSTRY IS TRANSITIONING FROM PRODUCT-BASED TO SERVICE OFFERING-BASED, AND HOW THIS IS OPENING UP NEW AVENUES OF OPPORTUNITY. **A SECURITY ADVISOR EXCLUSIVE.**

> re businesses transitioning from a "product-based" business model to a "serviceoffering" based model today? What are the implications of this transition for

cybersecurity, in particular?

As the threat landscape continues to evolve at exponential rates, it is extremely difficult for organisations to maintain cyber resilience by depending only on inhouse security teams. This, coupled with the global shortage of skilled resources in cybersecurity, has led to the need for partnering with expert Managed Security Service Providers (MSSPs) to ensure 24/7 monitoring and incident response. In addition, the predictability that comes with fixed SLAs for service offerings and flexible payment schemes makes it all the more a preferred option for enterprises.

The transition away from the productbased model has increased the importance of the role of MSSPs. When a customer opts to work with an MSSP, they have access to the right and requisite expertise, as well as the latest technologies, as MSSPs have been continuously investing in technologies, knowledge and talent.

Additionally, the MSSP team functions as an extension to the customers if they have in-house experts or operations, giving customers the benefit of having a collaborative model.

Finally, working with a service provider also offers predictability, not only from a service perspective, but also from a budget perspective. Customers that utilise a service provider will know what their monthly rental charge is, whereas if they onboarded the technology themselves, they may have to consider unpredictable costs related to operational expenditures, upgrades, and increases in capacity.

The last few years have seen a spike in the adoption of services like proxies, managed firewall as a service, and secure access service edge (SASE), indicating that customers – rather than onboarding technologies that they would have to manage – are opting to outsource security operations to an expert that will allow them to contract on an SLA-based offering.

Today, security solutions must be tied to both high-level corporate goals and to everyday end-user realities as a result of the potential for increased risk to enterprise assets. What is the security impact of these new end-user realities? Even with all the best security measures in place, network security is only as good as its weakest link which, in most cases,

"THE LAST FEW YEARS HAVE SEEN A SPIKE IN THE ADOPTION OF SERVICES LIKE PROXIES, MANAGED FIREWALL AS A SERVICE AND SECURE ACCESS SERVICE EDGE (SASE), INDICATING THAT CUSTOMERS ARE OPTING TO OUTSOURCE SECURITY OPERATIONS TO AN EXPERT THAT WILL ALLOW THEM TO CONTRACT ON AN SLA-BASED OFFERING." is the end user. Considering the shift to remote work due to the pandemic, and the increased adoption of the cloud, security must be completely built into the organisation's systems. You cannot simply purchase a solution and call it a day.

Today, the reality is that users are connecting from anywhere, anytime, and remote workers are accessing organisational resources from environments that are not sufficiently secure. Apps are rapidly moving to the cloud, and the traditional concept of the organisational perimeter has vanished. As a result of these factors, the attack surface of companies continues to expand, and remote assets are becoming more challenging to manage, making it increasingly difficult to have a single pane of glass view of things.

Additionally, the need to maintain uniform and granular access controls to applications in the cloud as well as onprem, has not only increased the complexity of security operations but also impacted user experience. Traditional models dependent on on-site licensing are not practical anymore, as users are everywhere and data has moved to the cloud.

Enterprises are also being pushed toward allowing customers to benefit from any available connectivity. This means supporting both wired and wireless technology. How can security be guaranteed even when the enduser device is not connected to the enterprise network?

This comes down to innovation in the security space. Technologies such as Zero Trust and security at the edge are crucial to protecting organisations today, as the castle-and-moat approach is no longer sufficient.

Zero Trust Network Access (ZTNA) augments traditional VPN technologies for application access, and removes the excessive trust once required to allow employees and partners to connect and collaborate securely.

Secure Access Service Edge (SASE) is another piece of the cybersecurity puzzle in this perimeter-less era. SASE is an emerging framework for the convergence of networking and network security services within a global cloud-based platform, providing zero trust network access, data and threat protection, and better performance with reduced complexity.

Help AG has been heavily focusing on innovating solutions to address the issue of securing users no matter where they are. Last year, we launched Help AG Secure Private Access Service (HPA), a scalable and locally delivered service that follows an identity aware ZTNA approach. HPA provides holistic security, visibility and control across environments. Also, earlier this year, we launched Cyber Edge X, a SASE offering that unifies networking and security services in a cloud-delivered architecture to protect users, applications, and data everywhere from cyber threats, ultimately enabling organisations to redefine their perimeter security in the cloud.

It is also crucial to ensure that users are activated as part of your security strategy. Even the best technologies may fall short, so it is important to build security awareness to increase the chance of your users making the right decisions, thereby becoming your first line of defence. Help AG has always been an advocate of a people-



centric approach to cybersecurity — be it our employees, business partners, or customers.

How about value-for-money & cost-effectiveness? Will these new approaches benefit enterprises & customers financially? Aside from being crucial in the perimeter-

"SASE IS AN EMERGING FRAMEWORK FOR THE CONVERGENCE OF NETWORKING AND NETWORK SECURITY SERVICES WITHIN A GLOBAL CLOUD-BASED PLATFORM, PROVIDING ZERO TRUST NETWORK ACCESS, DATA AND THREAT PROTECTION, AND BETTER PERFORMANCE WITH REDUCED COMPLEXITY."



less era, ZTNA and SASE can both reduce an organisation's IT costs. Employing SASE can help organisations manage costs better by moving away from a complex hybrid IT environment and offering a single cloudnative architecture.

Also, more and more enterprises today are leveraging MSSPs for 24x7 security operations, instead of trying to handle security operations themselves. Utilising the services of an MSSP will cut down the total cost of ownership (TCO) as the customer doesn't have to onboard resources. This brings predictability to spending, as the business's security spending shifts from a CAPEX to an OPEX model. In addition to cost-efficiency, outsourcing security operations to an MSSP allows the organisation to focus on its core business.

This brings us to Help AG's Managed Security Services (MSS). What are some of its key differentiators and how does it help customers stay ahead of cyber-attacks?

Help AG has been one of the region's most experienced and trusted cybersecurity partners for more than 15 years. When we decided to build our Managed Security Services offering, we committed to building truly global and advanced security services while molding them to suit regional market threats and requirements. With these core principles, we built our service offering from the ground up and it was received very well in the market, enabling us to become the biggest MSS provider in the region.

One core principle that sets our MSS offering apart is that our core service architecture aligns with regional compliance requirements such as local data residency, without compromising on the quality or efficiency of the service.

Additionally, Help AG has a large team of security researchers who are constantly searching for zero days and new vulnerabilities, and this knowledge is fed back into our Security Operations Center (SOC) service to ensure our customers are always one step ahead.

Moreover, we are one of the few players in the region who have an in-house threat intelligence team. We leverage intelligence gathered from our existing community and customers, coupled with threat activity monitoring of the dark web for activities that could impact the customer.

Another factor that sets our services apart is that the Help AG SOC utilises automation capabilities for enrichment and response to alerts that we observe in our customers' environments. This allows us to not only be consistent in incident handling, but also to conduct faster triage and response.

Most importantly, we are always innovating to stay ahead in protecting our customers. At Help AG, we are committed to evolving our services, collaborating with technology partners, as well as working with our customers to continually improve their security posture through both identifying new services and improving the ones we are delivering to them.

Is it more efficient & effective for organisations to handle their own cybersecurity operations, or should they outsource them to a service provider?

It does not make sense for an organisation to handle its own cybersecurity operations, and there are a number of reasons for this. The first is that the cost of building an internal SOC entails significant investment in people, processes, technology, physical facilities and physical and logical surveillance, not to mention the selection of hardware and software technology. And even when you have made all these purchases and procured them, you are still unlikely to get any value out of them, unless you have access to the right expertise and maturity in operating the processes. This is only made more difficult by the fact that the number of unfilled cybersecurity positions stands at 3.1 million according to reports.

Thus, it makes far more sense both commercially and logically, to choose a managed security service provider that has already invested in the technology, skills, and maturity of processes and operations. All these resources and abilities can be acquired by partnering with the right MSSP, and with Help AG, the cybersecurity arm of Etisalat Digital, enterprises get access to the best and largest MSS team in the region, as well as a flexible financing model, hence investing in a capability which will evolve over time.

"EVEN THE BEST TECHNOLOGIES MAY FALL SHORT, SO IT IS IMPORTANT TO BUILD SECURITY AWARENESS TO INCREASE THE CHANCE OF YOUR USERS MAKING THE RIGHT DECISIONS, THEREBY BECOMING YOUR FIRST LINE OF DEFENCE."

What is Help AG's strategy when it comes to cybersecurity as a service? Can you also give us an idea in terms of the service roadmap in the coming months?

Help AG's strategy is to shift from technology delivery to a service-centric model. We have been advocates of this from day one, and we are best-placed today to offer comprehensive cybersecurity services covering the entire lifecycle, from 'Assess' to 'Defend' to 'Respond'. Irrespective of the underlying technology or the deployment model, the customer will rest assured that they are provided a service built on best-of-breed technologies. Our vision is to offer our customers the highest level of protection and user experience, wherein we deliver top notch services in terms of people, processes and technology, on an MRC/PAYG model.

The second important aspect of our strategy is that all the services we deliver are fully compliant with UAE data regulations.

Additionally, we ensure that we have expertise and infrastructure on the ground. The concept we follow is 'think global, act local,' aiming to give customers all the benefits of the most advanced global technologies while fully provisioning them locally with expertise available on the ground.

Under our strategy, the customer also enjoys SLA-based offerings; cybersecurity expertise on demand wherein our experts work as an extension of the customer's team, and elastic capacity based on the customer's needs.

In terms of our services roadmap, we have already standardised many of our services, including 24/7 Threat Monitoring, Detection and Response, and we have applied automation to several of our existing services, including our Managed Advanced Web Application Firewall (AWAF) and SASE services. Other best-of-breed services we offer include Penetration Testing, Red Teaming, Security Awareness, Compromise Assessment, Managed Security Controls, Managed Threat Intelligence, Digital Risk Protection, SMB Security Offerings, Always-On DDoS Mitigation, Security Bundles with Service Providers and Secure Cloud Offerings.

How has Help AG invested in technologies and training to meet the security needs of the region?

In addition to our experience and expertise, we have a focus on thought leadership and early adoption of new, innovative technologies. Take secure cloud enablement as an example; cloud became a huge buzzword during the global pandemic, but prior to that, the region's pace of cloud adoption had been slow. Staying ahead of this trend, Help AG was pioneering secure cloud enablement long before the pandemic. We were already consulting, designing and putting architectures in place with our clients, helping them securely move their workloads to private cloud, public cloud and hybrid environments.

From the start, Help AG has been an organisation that invests heavily in its own people and in training and enablement so that we can provide the right level of service to our clients in the region. With our significant internal capabilities, including very strong delivery, support and managed service capabilities, we take full responsibility and accountability for training our staff.

Hikvision Temperature Screening Thermal Solutions

36.5° C

SAFER, FASTER, SMARTER





Temperature Screening Thermal Cameras

For more information, please scan the QR-Code to visit our Temperature Screening Thermal Solution page.



AN INTELLIGENT APPROACH TO CYBER THREATS

FIRAS GHANEM, REGIONAL DIRECTOR - MIDDLE EAST & PAKISTAN AT THREATQUOTIENT, TELLS SECURITY ADVISOR HOW THE COMPANY WORKS WITH CUSTOMERS TO IMPROVE THE EFFICIENCY AND EFFECTIVENESS OF SECURITY OPERATIONS THROUGH A COMPREHENSIVE APPROACH TO THREATS



Firas Ghanem



hat is the biggest cyber threat facing CIOs and organisations in the region?

We see social engineering leading the list of threats. In 2020, almost a third of the breaches incorporated social engineering techniques. We also saw ransomware and vulnerabilities. This year, according to a recent study published by Kaspersky Labs, more than 2.5 billion phishing cases have been reported from Egypt, Saudi Arabia, Qatar, Kuwait, Bahrain and Oman. The report also incorporated an interesting fact: Back in October 2020, cybercriminals successfully stole user login credentials from thousands of Arabic language users, using fake Netflix customer support pages. So, these are some of the major cyber threats that we see today.

Do you think there is a greater need now for organisations to adopt a more open and extensible threat intelligence platform, and how does ThreatQuotient step into this?

Yes, there is a serious need for organisations to do this. In order to



understand and stop threats more effectively and efficiently, your existing security infrastructure and people need to work smarter, not harder. ThreatQuotient can serve as an open and extensible threat intelligence platform that accelerates security operations through streamlined threat operations and management. The integrated, selftuning threat library, adaptive workbench and open exchange allows organisations to quickly understand threats, make better decisions and accelerate detection and response.

In fact, using ThreatQ as a threat intelligence platform equips customers with a threat library that automatically scores and prioritises threat intelligence based on the parameters they set. Prioritisation is calculated across many separate sources, both external and internal, to deliver a single source of truth using the aggregated context provided. This removes noise, reduces risk of false positives, and enables users to focus on data that really matters.

What do you think companies can do to gain more from the existing security investments, both in people and technology?

ThreatQuotient's strategy for this year is to focus on automation specifically for detection & response needs. We

> "AT THREATQUOTIENT, WE COMBINE AUTOMATION & HUMAN INTELLIGENCE FOR PROACTIVE DETECTION AND RESPONSE. WE HAVE CUSTOMER-DEFINED CONFIGURATIONS & INTEGRATIONS, AS WELL AS A CUSTOMISABLE WORKFLOW AND CUSTOMER-SPECIFIC ENRICHMENT, TO STREAMLINE ANALYSIS THREAT & EVENT DATA..."

believe in a smart way of approaching automation and in automating only what is relevant. This allows you to define when exactly you'd want to run an automated action, and what to lean following it. An example of that is if you have a series events identifying potential malware samples, and some of those samples are determined by the ThreatQ Threat Library to be related to known high profile adversaries and campaigns, then the automated actions taken will differ based on that context.

In short, at ThreatQuotient, we combine automation and human intelligence for proactive detection and response. We have customer-defined configurations and integrations, as well as a customisable workflow and customerspecific enrichment to streamline analysis of threat and event data, for faster investigation and automation of the intelligence lifecycle.

How does ThreatQuotient work with clients for a more proactive threat detection and response process?

At ThreatQuotient, we have created ThreatQ and ThreatQ investigations, to help security operations prioritise efforts, improve detection and accelerate response. Our platform gives SOC analysts, incident responders and threat analysts unmatched flexibility, visibility and control that they can't get elsewhere. We accomplish this through providing context and ensuring relevance - as defined by the customer and not a vendor. ThreatQ works with your existing processes and technologies to make your people and technologies more efficient. The platform gives security operation teams the ability to answer who, what, where, why and how questions about alerts and threats. For example: What does this alert mean, how should we defend against this malware family, is that indicator part of an opportunistic drive-by or something more targeted, and have we seen it before?

With ThreatQ, these questions can be answered quickly and with more confidence.



o discussion on security will be complete without touching upon the modernday cybercriminal's

Brian Chappell, director - Product Management at Byonn the Byonn of th

preferred playground and the single most frustrating mode of attack that plagues organisations, both big and small, today: Ransomware. This, as we know it, is an age-old criminal extortion tool where hackers encrypt critical data, rendering it inaccessible, and promising the victim to restore it once the ransom amount has been paid. We also know that in the days following the COVID-19 pandemic, this mode of attack has risen alarmingly, because in the sudden transition to the online space, companies, struggling to stay afloat, failed to address their critical security loopholes, providing attackers a lucrative, get-rich-guick-opportunity.

What we don't know is how much it's actually impacting us. If statistics are anything to go by, ransomware attacks are estimated

"THE ROOT CAUSE OF RANSOMWARE IS THE CYBERCRIMINALS WHO CREATE AND DISTRIBUTE IT IN THE FIRST PLACE, SO IF YOU ARE DETERMINED TO FIND ONE **GROUP TO BLAME, THAT'S WHERE YOU SHOULD START."**

to cost the world around \$6 trillion annually by the end of this vear. Ransomware costs businesses more than \$75 billion per year, and that's only an unofficial estimate. Cybersecurity firm Cybersecurity Ventures predicts that in 2021, globally, a new organisation is expected to fall victim to a ransomware attack every 11 seconds. One could go on, but this is just the tip of the iceberg-a simple google search will reveal sobering facts about this increasingly preferred and devastating mode of cyber-attack.

HOW DOES IT BEGIN?

According to Maher Jadallah, senior director - Middle East & North Africa. Tenable. ransomware typically compromises enterprises by one of two attack methods:

By exploiting vulnerabilities within the hardware, operating systems, software, applications, etc. of the devices they target. We all know that patching is essential, but given the sheer volume of new vulnerabilities identified, knowing where to start can be challenging. Organisations need to find and fix the vulnerabilities that ransomware targets with priority placed on the high-risk flaws that are being actively exploited.

By leveraging misconfigurations David Brown, security operations director at Aton pat related to hardware, operating systems, software, applications, etc. Just as there are thousands of vulnerabilities to patch, there are thousands of security settings to be configured, many of which are not secured correctly. With simple gueries, an attacker can determine what is running on the device they've compromised, allowing them to know exactly which misconfigurations to look for.

LIKELY TARGETS

There is no fixed criterion for choosing a target organisation. It could be because an organisation has a smaller security team or a broad-based team of staff that does a lot of file sharing, making it easier

to identify vulnerabilities quickly. Or it could be because attackers think an organisation might pay the ransom amount quickly, in order to have their critical data restored as quickly as possible-this could include key government offices and large corporates. But it doesn't end there As Maher Yamout senior security researcher at Kaspersky puts it: "One approach that we have seen grow in popularity, and that greatly concerns us, is supply chain attacks, whereby the partners and suppliers of an intended victim are targeted. The REvil campaign, for example, compromised an MSP provider and then distributed ransomware to its customers' networks."

WHO'S TO BLAME?

Everyone knows what ransomware is-they're still unclear about how it begins and thrives. Almost invariably, blame falls on the Managed Service Providers (MSPs), especially the smaller ones. "Smaller MSPs may not have the IT security budgets that bigger MSPs have. The truth is that MSPs are a prime target for cyberattacks; by compromising a single MSP, attackers can gain access to the networks the MSP serves. Targeting a smaller MSP improves the success rate of a cyberattacker, says Manikandan Thangaraj, vice-president, ManageEngine.

"Everyone wants to find "the primary cause" of ransomware - it's easy to say that it's all down to users, because they're the ones who fall for phishing attacks; it's easy to find fault with IT for failing to patch; and it's easy to blame outside sources such as contractors or managed service providers (MSPs) for what you see as inadequate



support," says Paul Ducklin, principal research scientist at Sophos. "To be clear, the root cause of ransomware is the cybercriminals who create and distribute it in the first place, so if you are determined to find one group to blame, that's where you should start," he adds. He points out that in real life, "there are many ways that ransomware gets in, and the crooks who launch ransomware attacks know all of them, so if one approach doesn't work, they'll typically just try another until they find a foothold inside your network."

Jonathan Couch. senior vice-president, Strategy, at ThreatQuotient, says that while MSPs not taking ransomware seriously enough is definitely a contributor to the continuing rise of ransomware, the more comprehensive reason is that ransomware continues to

"EVERY MSP OUT THERE SHOULD BE KICKING INTO HIGH GEAR AND RE-CALCULATING THEIR RISK ASSESSMENTS, ENSURING THEIR INCIDENT RESPONSE **PRACTICES ARE STRONG. AND DOING AN HONEST** ASSESSMENT OF WHAT THEY CAN AND CAN'T DO..."

generate revenue for criminal groups. "Organisations big and small are slow to adapt to the threats and they don't try to anticipate the next move or the next types of ransomware and how they will operate. Very few MSPs, and especially the smaller ones, take a wholistic approach for customers. This would be to ensure proper data architecture (offline backups,

Naher Vamout, senior security researcher at Haspersy,

.....

Maher Jadallah, senior director - Middle East & North Africa - High and the senior director - Middle - High and the senior director - Middle - High and the senior - High and the senior - Middle - High and the senior - High and the senior

network segregation between functions etc.) and many don't provide any kind of significant email security (stopping the attack before it starts and protecting users from installing malware on their systems)," he adds.

David Brown, security operations director at Axon Technologies has a different take. He attributes the rise in ransomware to the fact that:

The increased value of cryptocurrency used to pay for the ransom is a direct driver of criminal activity.

With the availability of ransomwareas-a-service, this subscription-based malicious business model enables even novice cybercriminals to launch ransomware attacks.

More organisations are missing basic cyber hygiene controls such as backup, patching, security hardening, configuration, and monitoring controls due to their expanded digital footprint and usage of cloud assets.

More organisations are paying the ransom because they do not have the backups to restore their data.

Concurring with him is Brian Chappell, director – Product Management at BeyondTrust. "I'd say ransomware is on the rise because most organisations don't take the risk seriously enough. Despite the moves toward approaches like Zero-trust, there's still a lot of the fortress-mentality where firewalls and proxies are relied upon to secure the network and users are given excessive privileges to 'simplify' privilege management – while actually introducing complexity in monitoring and responding to "TO IMPLEMENT AN EFFECTIVE RANSOMWARE PROTECTION STRATEGY, YOU NEED TO SECURE YOUR APPLICATIONS, PROTECT ACCESS TO YOUR APPLICATIONS, AND PREVENT LATERAL MOVEMENT ON THE NETWORK."

what users do with that privilege," he points out.

However, as Sam Curry, chief security officer at Cybereason says, "it's not so much that MSPs don't take security seriously. It's more about lacking the resources and knowledge to improve their security enough to lower their own risks. Every MSP out there should be kicking into high gear and re-calculating their risk assessments, ensuring their incident response practices are strong, and doing an honest assessment of what they can and can't do for themselves, let alone for their customers. To do security right, MSPs need prevention and detection, of course, but also business preparation, segmentation, backup and recovery plans and contingencies for the tough decisions when things happen."

Manikandan Thangaraj, vice-president, ManageEngine

WHAT CAN BE DONE?

Experts offer several solutions. From frequent file-backs ups to anti-malware software, to user training, the answers are many. However, in recent years, there is common consensus about the need for a "layered" approach to malware and ransomware, in particular. ••••••

"A multi-layered (defence-indepth) approach is correct," says David Brown. "Each layer in the security stack allows for the potential to Detect, Degrade, Deceive, Disrupt, and, lastly, Deny the threat from reaching its objectives. If your security technologies can holistic integrate out of the box, this is typically better than buying best-of-breed technologies across each layer that cannot integrate. No matter how many times a solution uses the terms AI or Blockchain, it's probably not the correct choice if it's not part of a holistic layered or in-depth solution."

Says Werno Gevers, cybersecurity expert at Mimecast Middle East: "To protect against ransomware

sam curry, chief security officer at Cybereason

and other cyberattacks, Middle East organisations need to develop a layered security strategy that hardens

Paul Ducklin, principal research scientist at Sophos

the email perimeter and protects

against email-borne threats. This

remains the favoured attack vector for

cybercriminals. Such a strategy should

to augment the native security of

as Microsoft 365."

business email platforms such

"Data should be

archived regularly to

an independent and

separately secured

environment, and

a robust email

continuity plan

needs to be

in the wake of a

successful attack."

are increasingly employing

more sophisticated attacks and

defeating existing defences because

of which organisations need to cover

META & CEE at Barracuda Networks.

multiple bases in their efforts to mitigate

the threat, says Toni El Inati - RVP Sales,

Ransomware attackers

established to

ensure the business

can continue running

include additional security solutions

is especially important as email

is therefore to protect user credentials from email attacks," he adds. "This involves blocking phishing attacks before they reach users' inboxes, trainings employees to recognise phishing attempts, and having tools and procedures in place to effectively execute incident response," he adds.

"The first step in protection

Toni El Inati says that to prevent data exfiltration and encryption, it is important to protect the top attack vector for data breaches – web applications. "To implement an effective ransomware protection strategy therefore, you need to secure your applications, protect access to your applications, and prevent lateral movement on the network."

Kaspersky's own approach towards ransomware is a multi-layered, next-generation protection that lets products detect ransomware at both the delivery and execution stages of the attack. Maher Yamout points out: "In Kaspersky's products a component called Mail AV, for example, analyses the whole context of a message, including email attachments, and applies strong heuristics to the content. Exploit Prevention (EP) is another special component that prevents ransomware penetration through software vulnerabilities. Among the most important applications protected by EP are browsers, office applications and PDF readers."

For Maher Jadallah, securing the Active Directory is the most important step an organisation can take. "Over and over again we see forensic proof that, regardless of the entry point a ransomware attacker targets, Active Directory is always involved as a next step in the attack to move laterally and gain

.

••••••

privileges in order to deploy ransomware. For example, RYUK and XingLocker (a variant of MountLocker) specifically need Active Directory to be involved, otherwise these attacks fail. Attackers know how to enumerate and analyse Active Directory, so they rely on it for a successful breach and deployment of their malicious software." Active Directory is at the centre of authentication and resource access for most organisations, which is another key reason attackers love to leverage it.

But that's not all. "If you've focused your energy on looking out only for ransomware, you won't get your first chance to spot the attack until much later than you would have if you had a defence-in-depth policy - and you'll probably end up missing many other, equally dangerous, network attacks altogether," Ducklin observes.

"At Sophos, you will often hear us talking about "synchronised security," by which we mean that detecting and blocking network intrusions (and, perhaps most importantly of all, finding out how they happened so that the same (or other) crooks can't simply walk back in later on) requires a joined-up approach that collects threat intelligence from multiple sources."

LIVING WITH IT

What's so alarming about ransomware is that the more the number of devices and data that is introduced, the more prolific and rampant it becomes. And with a future that looks increasingly digitised, it wouldn't be out of place to assume that ransomware is here to stay.

However, all's not lost, as long as organisations realise that security is a shared responsibility and have a solid response plan in place.

"THE BETTER **SECURITY TEAMS ARE GOOD AT OUICKLY DETECTING SUSPICIOUS OR MALICIOUS ACTIVITY AND ENSURING THEIR COMPANY HAS** THE VISIBILITY, INTELLIGENCE. **AND CONTEXT TO UNDERSTAND AND ELIMINATE THE THREAT BEFORE IT RISES TO THE LEVEL OF A SIGNIFICANT** ATTACK."



•••••

• • • • • • • •

toni El Inati - RVP Sales, META & CEE at Barracuda Nethorita

"Protecting a network from ransomware attacks isn't the duty of the IT team alone—it's a shared responsibility. Just one wrong click on a single device connected to the network can lead to all data being encrypted, locked, or both," reminds Manikandan Thangaraj.

According to Curry: "A modern protection set must prevent everything possible, including ransomware, and still have a detection component for finding the low and slow spread of malicious tools by humans. The better security teams are good at quickly detecting suspicious or malicious activity and ensuring their company has the visibility, intelligence, and context to understand and eliminate the threat before it rises to the level of a significant attack."

•••••

That's something we need to aim for, right away.

REMOTE CODE EXECUTION: THE NEW CYBERSECURITY BATTLEGROUND

SATYA GUPTA, CO-FOUNDER AND CHIEF TECHNOLOGY OFFICER AT VIRSEC, ON WHY THE REMOTE CODE EXECUTION (RCE) IS A DEADLY CYBER-ATTACK WEAPON THAT MUST NEVER BE UNDERESTIMATED.



his week, CheckPoint published a new report that chronicled the UAE threat landscape over the past six months. In the report, the company identified that the most common vulnerability exploit type was Remote Code Execution (RCE), which impacted 62% of businesses.

This finding is not at all surprising. From an attacker's perspective, an RCE vulnerability in a workload – a workload being the infrastructure on which data center software runs-- is the gift that keeps on giving, in countless attacks, not only in the UAE but across the globe. Metaphorically speaking, RCE vulnerabilities are like the rocket that will launch any cyber-attack warhead such as the ransomware (e.g. LockBit, DarkSide, REvil, Sodinokibi, etc. etc.) warhead. Most recently, an RCE vulnerability in an email application was implicated in the highly publicized SolarWinds supply chain attack. RCE vulnerabilities were also the root cause of the Hafnium and Kaseya attacks. Very early and automated protection in response to an RCE attack is essential for effective enterprise protection.

RCE: How it Works

When a craftily constructed payload is delivered to an application with a lurking RCE vulnerability, the application relinguishes execution control to the attacker. The application is said to have reached the "Exploitation" state in the cyber kill chain. Wresting execution control from an application allows the attacker to not only install more tools required to perpetuate the attack but also establish a two-way communication path back to the attacker's command control center. At this point, the attacker has achieved full keyboard control on the victim. Now the victim workload is totally at the attacker's mercy and can perform any malicious action of the attacker's choosing. These actions could include running ransomware, exfiltrating critical data, scraping user credentials, pivoting to other workloads, perform crypto mining activities, join a botnet, etc.

Underestimating the enemy

It is often said that adversaries use the same techniques repeatedly. Assuming threat actors will leverage the same techniques continuously is not only naïve but is also a little selfFROM AN ATTACKER'S PERSPECTIVE, AN RCE VULNERABILITY IN A WORKLOAD IS THE GIFT THAT KEEPS ON GIVING, IN COUNTLESS ATTACKS, NOT ONLY IN THE UAE, BUT ACROSS THE GLOBE.

serving for classes of cyber security products that leverage signatures and threat feeds. Most adversaries are well funded, skilled, motivated, and highly effective. All they need is early awareness of an RCE vulnerability and an enterprise that is hosting the vulnerable application. Once they are in the enterprise data center, the attack metastasizes in seconds. If the attacker is able to reach the Command and Control state in the kill chain, there is going to be no stopping the adversary.

RCE Vulnerabilities are particularly potent against conventional endpoint, perimeter, and threat hunting security tools. Even though these security tools

claim they work in the application's runtime, their runtime clock starts after the attack has reached the "Actions on Objectives" state in the kill chain; long after the attacker has achieved keyboard control over the victim workload. These security tools work by tracking how many anomalous activities have occurred over a fixed period of time. They declare the victim is under attack if a pre-defined threshold of anomalous activities is exceeded. A skilled attacker can float under the radar and be able to totally bypass protection offered by conventional security tools. At SolarWinds, the attack continued unabated from September 2019 to Dec 2020 (15 months) before a security vendor published a specific indicator of compromise (IOC).

To achieve true protection against an attack that leverages an RCE vulnerability, the security control must kickstart protection before the attack reaches the "Command Control" stage of the kill chain. An attack that has crossed the Command Control (C2) stage of the kill chain is unstoppable. Irreparable harm is guaranteed to occur.

What the Cybersecurity Future Holds

Continued dependence on security controls that are fueled by threat feeds, even if these tools advertise cool AI/ ML capabilities, is a losing battle. Vulnerabilities will continue to proliferate, and no amount of prior knowledge or threat hunting can keep up. For every hour it takes a bad actor to create new malware, it takes many thousands of hours for cyber defenders to perform static and dynamic analysis on it to extract a foolproof IOC.



WHAT ORGANISATIONS CAN DO TO DEFEND IT & OT NETWORKS FROM RAMPANT RANSOMWARE ATTACKS

MARTY EDWARDS, VP, OT AT TENABLE, TELLS ANITA JOSEPH HOW RANSOMWARE ATTACKS ARE BECOMING ALL-PERVASIVE AND HOW TENABLE IS CLOSELY WATCHING THE THREAT ENVIRONMENT, IN ORDER TO HELP ORGANISATIONS PRIORITISE VULNERABILITIES THAT ARE BEING EXPLOITED THE MOST. ansomware is taking centre stage todaywhat's your take on the ransomware attack scenario in the region?

Ransomware is certainly becoming one of the predominant threats that we face these days. Everybody has talked about and focused on the nation-state aspects of cybersecurity for far too long, and now we see the shift towards highly organised criminal organisations. I am extremely concerned because I think criminals always go where they can make the most money and critical infrastructure is a very attractive target for them. I think they're going to continue to pivot and target organisations where they can make the most money.

Is the critical infrastructure of organisations being actually affected by rampant ransomware attacks and what can organisations do if they find themselves the target of a ransomware attack?

Before the convergence of IT & OT networks, all the operational technology – the computers that actually operate your factory or operate your water treatment facility or your power grid or refinery or what have you – were predominantly isolated or air gapped. But that's no longer the case. For business reasons we've interconnected these different networks, and you have to be very concerned with the detection of ransomware or detection of any kind of security threat, no matter what network it's on.

I would say that if you find ransomware on your network, then it's almost too late to be testing your backup and restore procedures. You should have a plan and you should anticipate a worst-case scenario, for example that you're going to be infected with ransomware. So, make sure that you have your backup and recovery plans. plus your disaster recovery plans, in good shape, and regularly test them. I can't believe how many people take backups of their data, but they never test restoring them. So, the way I describe it to people is that you should treat it no different from anticipating a fire - for example, in your server room. If you have a fire in your server room, and it destroys your computers, how many days does it take your business to get back up and running? Ransomware should be no different, and we should have a plan in place to limit the damage and recover quickly.

What do you think is the biggest challenge that organisations in the region face in the fight against ransomware. Why does this happen and how does the challenge come about? It's complex, and I think that there's no easy answer. Some organisations do an extremely good job at proactive cyber security measures to try and combat things like ransomware. But then you have other organisations that perhaps haven't even started with a basic level of security. I wouldn't want to paint any organisation as being good or bad. Ransomware is evolving in complexity and we are seeing increased instances of Ransomware as a Service - this means you have experts that write the actual code, but then they sell that as a service to some other criminals that may not have the cyber skills, but are more efficient at moving money and targeting organisations, or getting that initial system foothold. So, they're all working together, and that means they're bringing the best of the best to the fight. As defenders, we have to counter that with the best of the best, as well.

How does Tenable step in to help fight ransomware in the region?

It's multifaceted. First and foremost, the majority of ransomware is based on known and existing vulnerabilities. So, if you have a good programme in place to detect where your assets are vulnerable, then you are in the position to prioritise these to fix the highest priority ones first. We do this for you – we watch the threat environment and we help you prioritise which vulnerabilities are being exploited the most. We do that everywhere in your IT network. And in your OT environment, we also have threat detection capabilities. So, we're actually monitoring all networks and we can tell you if we see threats in any area.

Are businesses doing enough to address the issue? How do you see the whole ransomware ecosystem playing out? It's no longer sufficient to just have a

"IT'S NO LONGER SUFFICIENT TO JUST **HAVE A STANDALONE SECURITY PRODUCT INSIDE YOUR OT ENVIRONMENT. OR A STANDALONE** SECURITY PRODUCT FOR VULNERABILITY **MANAGEMENT, OR A STANDALONE** SECURITY PRODUCT FOR ACTIVE DIRECTORY SECURITY **MANAGEMENT. AND** SO ON."

standalone security product inside your Operational Technology environment, or a standalone security product for vulnerability management, or a standalone security product for active directory security management, and so on. We need to get all that information into the same place, so that it can be analysed to give you a holistic picture of what's happening from a security standpoint on your networks. These converged networks are complex and they're connected in ways that many organisations don't even understand, until we help them through that journey.

And so, I think that you need to partner with a security provider that can give you a broader view. This ransomware threat is not going away. Fortunately, our governments are holding diplomatic discussions on international law enforcement and are trying to do better at holding criminals accountable for their actions. But I think it's such a lucrative environment right now, that it's only going to get worse. In fact, we haven't seen the worst of it yet.

SOPHOS REPORT REVEALS STEALER CAMPAIGN DISGUISED AS PIRATED SOFT WARE

STEALER IS DELIVERED TO TARGETS BUNDLED WITH RANSOMWARE AND OTHER MALICIOUS CONTENT, SAYS **SEAN GALLAGHER,** SENIOR THREAT RESEARCHER AT SOPHOS.





ophos, a global leader in next-generation cybersecurity, has published new research, "Trash Panda as a Service:

Raccoon Stealer Steals Cookies, Cryptocoins and More," detailing how a stealer disguised as pirated software grabs cryptocurrencies and information while dropping malicious content, such as cryptominers, on targeted systems.

"With much of daily and professional life now reliant on services delivered through a web browser, the operators behind information-stealing malware are increasingly targeting stored web credentials that provide access to a lot more than they could get by just stealing stored password hashes," said Sean Gallagher, senior threat researcher at Sophos.

"The campaign we've been tracking shows Raccoon Stealer grabbing passwords, cookies, and the 'autofill' text for websites, including credit card data and other personally identifying information that may be stored by a browser. Thanks to a recent 'clipper' update that changes the clipboard or destination information for a cryptocurrency transaction, Raccoon Stealer also now targets crypto-wallets, and it can retrieve or load files – such as additional malware – on infected systems. That's a lot of stuff that cyber criminals can easily monetise for a service that is 'rented out' at \$75 for a week's use."

Raccoon Stealer is usually spread by spam E-mail. However, in the campaign Sophos investigated, it is distributed through droppers that the operators disguised as cracked software installers. These droppers bundle Raccoon Stealer with additional attack tools, including malicious browser extensions, YouTube click-fraud bots, and Djvu/Stop, a ransomware targeted primarily at home users.

The operators behind this Raccoon Stealer campaign also used the Telegram chat service for the first time for command-and-control communications, according to Sophos researchers.

"Information stealers fill an important niche in the cyber crime ecosystem. They offer a quick return on investment and represent an easy and cheap entry point for bigger attacks," said Gallagher. "Cyber criminals often sell stolen identity credentials on 'dark' marketplaces, allowing other attackers, including ransomware operators or Initial Access Brokers, to take advantage of them for their own criminal intentions - such as breaking into a corporate network through a workplace chat service. Or attackers can use credentials for further attacks targeting other users on the same platform. There is a constant demand for stolen user credentials especially credentials providing access to legitimate services that attackers can use to easily host or spread more



"RACCOON STEALER ALSO NOW TARGETS CRYPTO-WALLETS, AND IT CAN RETRIEVE OR LOAD FILES – SUCH AS ADDITIONAL MALWARE – ON INFECTED SYSTEMS." malware. Information stealers may look like lower-level threats, but they're not."

Sophos recommends that organisations that use online services for workplace chat and collaboration use multi-factor authentication (MFA) to protect employees' accounts and ensure that all employees have up-to-date malware protection on any computer they access remote work-related services from.

Sophos Intercept X protects users by detecting the actions and behaviors of malware like Raccoon Stealer, including scanning for suspicious activity in memory and protecting against fileless malware.

Sophos advises consumers to install a security solution on the devices that they and their families use for online communications and gaming, such as Sophos Home, to protect everyone from malware and cyberthreats. It is also good security practice to avoid downloading and installing unlicensed software from any source. Always check first to make sure it's legitimate.



AMIVIZ JOINS HANDS WITH PICUS SECURITY TO ENHANCE THREAT PREPAREDNESS OF PARTNER NETWORK

PICUS'S RICH THREAT LIBRARY CONTAINS OVER 10,000 THREAT SAMPLES AND ATTACK SCENARIOS, INCLUDING THE MOST PREVALENT MALWARE AND ADVERSARIAL TECHNIQUES.

miViz, the Middle East region's first enterprise B2B marketplace, has announced that it has expanded its portfolio of cyber security solutions by partnering with Picus Security.

Picus Security's Complete Security Control Validation platform tests and measures the effectiveness of security tools to prevent and detect the latest cyber threats. It also provides vendor-specific mitigation content and insights to address weaknesses and gaps in coverage and visibility.

Due to the rapid speed at which threats evolve, it is vital that all organisations should be able to determine the state of their security posture at any time. By partnering with Picus, AmiViz offers its community of reseller partners and their customers an automated solution to continuously assess the preparedness of network, endpoint, and email controls to safeguard against attacks and breaches. Picus' rich threat library contains over 10,000 threat samples and attack scenarios, including the most prevalent types of malware and adversarial techniques.

According to AmiViz, security needs

to be a board-level conversation. The Picus platform enables security teams to quantify risks, helping business leaders to understand how well prepared their organisation's controls are to defend critical assets against current and emerging threats.

AmiViz, with its one-of-a-kind enterprise marketplace, offers Picus Security the ability to identify and recruit reseller partners across the Middle East. AmiViz's Virtual Customer Experience Centre is equipped to help resellers showcase Picus's technology to clients remotely by providing a unique customer-specific environment in the cloud.

"Keeping up with the latest cyber threats is a huge challenge for all organisations," says Tim Ager, VP of Sales for EMEA at Picus Security.

"By partnering with AmiViz, we're delighted to introduce the benefits of an automated and continuous approach to security validation to businesses across the Middle East and demonstrate why the Picus platform stands out from the crowd offering a comprehensive solution that not only simulates the latest attacks but also helps to improve controls to better defend against them."

About AmiViz

AmiViz is the first B2B enterprise marketplace focused on the cybersecurity industry in the Middle East, designed specially to serve the interests of enterprise resellers and vendors. Driven by innovation and AI-powered technology, the platform provides a unique collaboration platform through a mobile app on iOS and Android, as well as a webbased platform to enterprise resellers, consultants, system integrators, channel partners and vendors.

AmiViz offers its one-of-a-kind consumer-style e-commerce platform with a fusion of human touch, offering products and services that cater to localised market conditions and regulations across the Middle East.

About Picus Security Inc.

Picus Security is a leading Breach and Attack Simulation vendor, enabling organisations to test, measure & improve the effectiveness of their cyber security controls through automated and continuous offensive and defensive security testing.

The company has been named by Frost & Sullivan as one of the most innovative players in the BAS market. 1



 \bigcirc

 \bigcirc

 \bigcirc

 \bigcirc

 \bigcirc







17-20 OCT 2021 -

WHERE BUSINESS, INNOVATION, AND THE FUTURE WILL BE DECIDED

140 COUNTRIES PRESENTING THEIR TECHNOLOGIES, MAKE SURE YOU'RE THERE TOO

SECURE YOUR SPACE NOW: marketing@gitex.com

MELTIN



G | T E X 2 0 2 1 G | T E X . C

∑ 0

ONE IN 10 CYBERSECURITY INCIDENTS IN ORGANISATIONS CONSIDERED SEVERE: KASPERSKY

KASPERSKY ANALYSED ANONYMISED CUSTOMER CASES IDENTIFIED VIA THE KASPERSKY MDR SERVICE IN Q4 2020 TO SEE HOW WIDESPREAD AND SEVERE RESOLVED INCIDENTS WERE.

ccording to anonymised metadata voluntarily provided by Kaspersky MDR customers, one-in-10 (9%) prevented cybersecurity incidents could cause major disruption or unauthorised access to the customer's assets. The vast majority of incidents (72%) were of medium severity. This means that if these threats had not been detected by the service, they would have affected the performance of the assets or could lead to single data misuse cases.

Cyber attacks are growing in complexity and employing evasive techniques to

avoid detection by security solutions. Detection and prevention of such threats requires seasoned threat hunters who can spot suspicious actions before they cause damage to a company. Kaspersky analyzed anonymised customers' cases identified via the Kaspersky MDR service in Q4 2020 to see how widespread and severe resolved incidents were.

The research revealed that almost every industry, except mass media and transportation, saw high severity incidents during the analysed period. Most often critical incidents affected organisations from the public sector (41% of all high severity incidents were detected in this industry), IT (15%) and financial (13%) verticals.

Almost a third (30%) of these critical incidents were human-driven targeted attacks. Almost one quarter (23%) of high severity incidents were classified as high impact malware outbreaks, including ransomware. In 9% of cases, cyber criminals gained access to a company's IT infrastructure using social engineering techniques.

Kaspersky experts also noted that current APTs were typically detected together with artifacts of previous



advanced attacks, suggesting that if an organisation responds to a sophisticated threat, it's often attacked again, likely by the same actor. Also, in organisations experiencing APTs experts often discovered signs of simulation of adversarial behavior, such as red teaming, or an assessment of a company's operational security capabilities through a sophisticated attack simulation.

"Our study found that targeted attacks are rather common — more than one quarter (27%) of organisations faced them. The good news is that organisations that are likely to experience such incidents know about this risk and are prepared for them. These organisations employ services that help them assess their defensive capabilities, such as red teaming, as well as seek help from experts who can stop criminals, " said Gleb Gritsai, Head of Security Services, Kaspersky. ALMOST A THIRD (30%) OF THESE CRITICAL INCIDENTS WERE HUMAN-DRIVEN TARGETED ATTACKS. ALMOST ONE QUARTER (23%) OF HIGH SEVERITY INCIDENTS WERE CLASSIFIED AS HIGH IMPACT MALWARE OUTBREAKS, INCLUDING RANSOMWARE.

To protect your organisation from APTs and other advanced attacks, Kaspersky recommends the following:

Dedicated services can help against high-profile threats. The Kaspersky Managed Detection and Response service can help identify and stop attacks in their early stages, before the attackers achieve their goals.

Use a dedicated set for effective endpoint protection, threat detection and response products to timely detect and remediate even new and evasive threats. Kaspersky Optimum Framework includes the essential set of endpoint protection empowered with EDR and MDR.

Provide your SOC team with access to the latest threat intelligence and regularly upskill them with professional training.

Provide your staff with basic cybersecurity hygiene training, as many targeted attacks start with phishing or other social engineering techniques.

PREDICTIVE CYBERSECURITY IS THE NEED OF THE HOUR

AS INNOVATIVE TECHNOLOGIES ARE WEAPONISED BY CYBERCRIMINALS, INDUSTRIAL ENTERPRISES MUST ADOPT A MULTILAYERED APPROACH THAT ANTICIPATES CYBERATTACKS AND SAFEGUARDS CRITICAL ASSETS BEFORE THEY ARE EXPLOITED, SAYS **TIM GRIEVESON,** CHIEF INFORMATION SECURITY OFFICER, AVEVA.



Tim Grieveson

he exponential development of computing devices has expanded access capabilities for cybercriminals to detect and exploit vulnerabilities

in innovative ways. With a mediumgrade smartphone now more powerful than the most advanced computers were only a few years ago, for example, cybercriminals can launch powerful and sophisticated attacks at a relatively low cost from a mobile unit while also working from home. That ease of access goes some way to explain why there is a cyberattack every 39 seconds. As industrial organisations embrace digitalisation, inadequate security protection can open up their systems to malicious actors. Criminals today use a wide variety of methods, from commonly used techniques such as phishing and computerised password hacking to more sophisticated operations such as watering hole attacks that deliver malware to visitors.

Increasingly, the same innovative technology that is being used to deliver innovative solutions for common benefit is being deployed in destructive ways to inflict catastrophic damage to infrastructure, business systems, and ultimately, the citizenry.

Two sides to the same coin

Artificial intelligence (AI) is just such an example of dual-use expertise. While the technology has already improved business operations in several ways, AI is already being weaponised for illicit gain.

Attackers may seek to control of the data sets that train the AI, for example, by subtly altering parameters or modifying scenarios to avoid detection of underlying data exploits. Similarly, pattern recognition can be used to identify access points for injectables for remote execution at a later date, or even to improve social engineering by targeting workers at their most vulnerable moments. A simple mention on a social media website about grid maintenance could alert cybercriminals to a potential weakness.

At the same time, AI can also be deployed for protection. The best line of defense is often to retaliate in kind. AI is already being adopted in network monitoring and data analytics, where it is used to determine a baseline of normal behavior and identify inconsistencies of different kinds, such as unusual traffic patterns or anomalous server access. As the algorithm learns and progresses, predictive analytics can be deployed to flag up such intrusions early on, while deploying defensive responses and raising supervisory alarms.

As technologies such as AI rapidly evolve to become integrated into the industrial passage, cybersecurity issues will remain a key area of concern. Security professionals must assume that AI and other technologies can and

"GLOBAL CYBERCRIME IS EXPECTED TO INFLICT \$6 TRILLION IN TOTAL DAMAGES THIS YEAR, RISING TO \$10.5 TRILLION ANNUALLY BY 2025. A SIGNIFICANT PERCENTAGE OF THOSE ATTACKS ARE LIKELY TO HIT INDUSTRIAL ORGANISATIONS."

will be used for criminal benefit. Global cybercrime is expected to inflict \$6 trillion in total damages this year, rising to \$10.5 trillion annually by 2025. A significant percentage of those attacks are likely to hit industrial organisations. A comprehensive approach that anticipates and predicts cyberattacks can safeguard organisations from security issues. AVEVA partners with worldwide industry leaders to deliver the best-in-class solutions that drive digital transformation that also

comply with the highest cybersecurity standards across its software. For industrial organisations on the road to digitalisation, cybersecurity concerns can be addressed in three significant ways, through a combination of intelligent design, cloud computing, and machine learning.

Embed security across software solutions

Cybersecurity must be placed at the forefront of digitalised processes and baked into any solutions being deployed across



the enterprise. Industrial software solutions must incorporate security protection across the system design and development process, from the very start through to rigorous testing and validation to eliminate any vulnerabilities and exhaustively address cybersecurity challenges.

Automated software upgrades

Process interruptions and downtime must be eliminated to maintain operational continuity, particularly as industrial organisations too, embrace remote operations. Keeping security infrastructure up-to-date patches critical vulnerabilities and strengthens industrial assets against cybercriminals. Automated upgrades equip industrial IT infrastructure with the latest security capabilities and bypass conventional barriers to software adoption, in the process empowering industries to leverage leading technologies and quickly respond to evolving market demands.

Deploy AI technology against cyber threats

Tools such as the Unified Operation Center (UOC), AVEVA's market-leading performance management tool, can easily combine IT and OT products for enhanced cybersecurity protection. By using machine learning and artificial intelligence to provide a centralised view of systems across the enterprise, decision-making is streamlined so even the slightest anomaly is detected early, well before it can escalate into something bigger and more damaging.

As technologies evolve and cybercriminals abuse them for illicit gain, traditional one-off approaches are no longer sufficient to protect organisations. Instead, businesses must take a systematic, multilayered approach that anticipates cyberattacks and protects data and other critical assets before they are exploited.

ARE YOU AN AMAZON CUSTOMER? WATCH OUT FOR THESE SCAMS!



Amer Owaida

mazon is the largest online marketplace in the world boasting over US\$386 billion in revenue in 2020 with 200 million subscribers

to its Amazon Prime service just in the United States. And that's just a fraction of the whole customer base that it serves around the globe year-round. Of course, such a huge customer pool attracts cybercriminals who are looking to make bank by scamming unsuspecting victims with a variety of tricks that they have in their arsenal of scams.

Fake Order Phishing Email

As with any major service, Amazon is no stranger to being spoofed or impersonated by enterprising fraudsters who are looking to dupe people out of their personal information, or to access credentials to their accounts. The emails you may receive MOST PEOPLE ARE FANS OF THE CONVENIENCE AMAZON BRINGS TO ONLINE SHOPPING, AND THAT'S PRECISELY WHAT CYBERCRIMINALS ARE BETTING ON, SAYS **AMER OWAIDA**, SECURITY WRITER AT ESET.

can take on various forms, however they usually impersonate a common Amazon dispatch email, that regular customers have encountered many times over. For example, you might receive one confirming a purchase that you didn't make and tries to trick you into clicking on various links that look like contact information to Amazon's customer service. These links can then redirect to something looking like the official Amazon login page, however, when you try to sign in you will have divulged your credentials to the scammer. Alternatively, by clicking on the link or attachment in the email you may download a malicious payload to your device that will attempt to download keylogging software that will try to harvest your credentials to any services you use.

Generally speaking, unless the fraudster behind the scam did an immaculate job with the counterfeit email there are several warning signs that will give it away as an attempt at phishing. If the email contains, typos, grammar mistakes, or an attachment it is most assuredly a scam. When checking out a link that you've received in an email, by hovering your cursor over it, check whether the address is something.amazon.com where something is one of many valid Amazon subdomains – for example, pay. amazon.com or www.amazon.com. If you suspect that you're being phished you should contact Amazon directly, since it takes these issues seriously.

Gift Card Scams

Gift card fraud is another perennial problem that you can encounter. The conartists may utilise different strategies to dupe their victims, however, the ultimate goal remains the same - trick them into purchasing and sending Amazon gift cards. Popular tactics usually include evoking a sense of urgency or pressure in order to make victims act quickly rather than give deep thought to the contents of the message or phone call. Victims may receive unsolicited email messages or phone calls about a pressing issue involving their social security numbers or benefits and to resolve it they'll have to pay a penalty using gift cards. Alternatively, victims may be told that a family member is in trouble and needs financial help. There are multiple scenarios at play where fraudsters can also impersonate Amazon itself, claim to be someone from the management of the victim's employer, you name it.

However, fortunately, most of these scams can be uncovered quite easily if you keep a cool head. Government officials will never ask you to pay a fine or penalty with a gift card, so you can be 100% sure that if you get such a request it's a scam. As for the rest of the scenarios, to verify the claims you just need to call your family member to see if they're in trouble or the person from your company that requested the gift cards. And of course, it goes without saying that you should contact all of the aforementioned people or institutions through the verified official channels.

Payment Scams

Payment scams come in many shapes and sizes, and while

the form may differ, in the end, the scammers behind them are after only one thing the contents of your bank account. There are multiple ways that this can occur. One tactic that is often utilized is trying to convince you to pay outside Amazon's secure platform. The crooks will try to lure you in various



ways by offering a discounted price, for example, however, if you relent, the most probable outcome is that you'll both lose your money and won't get the product. And additionally, you won't be able to lodge a complaint with Amazon since you paid the fraudulent charges outside the confines of their platform. Other flavors of payment scams to watch out for include paying to claim a prize that you've supposedly won or to a seller whose identity you can't verify, and avoid offers that seem too good to be true or that you find suspicious.



The obvious advice, in this case, is to stick to Amazon's platform for all orders and payments. Even the company itself warns against sending money outside the confines of its platform: "Don't send money (by cash, wire transfer, Western Union, PayPal, MoneyGram, or other means, including by Amazon Payments) to a seller who claims that Amazon or Amazon Payments will guarantee the transaction, refund

your funds if you're not satisfied with the purchase, or hold your funds in escrow."

Dodgy Phone Calls

Sometimes scammers will resort to more "analog" means to try and hoodwink their victims – fake support calls. The content of the calls might vary; however, they often sound like a pre-recorded message impersonating Amazon claiming it has registered something wrong with your account, something that would pique your interest – a fishy purchase, lost package, etc. According to a warning issued by the United States Federal

Trade Commission, the message will then either inform you to press 1 to speak to a customer support agent or give you a number to call back. If you engage in conversation, the scammers will most likely try to wheedle sensitive data out of you like your personal information or your payment data.

The most sensible thing to do, before going into full-blown panic mode, is to check if there is anything suspicious going on by contacting Amazon through the direct channels listed on the support section of their website. The company does acknowledge that in some cases it may make outbound calls but it will never ask customers to reveal any sensitive personal information in order to verify their identity.

Summing it Up

When it comes to online shopping and its related activities the saying "trust but verify" remains as true as ever. To sum it up, most of the scams can be avoided if you remain vigilant, curious, and keep your wits about you. If you receive any unsolicited E-mails, be extra careful to verify their provenance and never divulge personal sensitive information to anyone claiming to be a "customer support representative or agent."

SHARING THREAT INTELLIGENCE



Kalle Bjorn

ive us an overview of the cyber security landscape right now, particularly in the last one year.

We've obviously seen a lot of changes in the last one-and-a-half years and there's been varying degrees of readiness, shifting to remote work. This has seen quite a bit of focus on the access part-obviously work from home requires secure access. Now, if you're looking at solutions for traditional VPNs, that's something that is beginning to evolve into the zero-trust network access, which is not just a simple password with a VPN access-that's outdated. Today's world requires a lot more-solutions that **ANITA JOSEPH** CAUGHT UP WITH **KALLE BJORN,** SR DIRECTOR, SYSTEMS ENGINEERING – MIDDLE EAST AT FORTINET, TO DISCUSS THE CHANGING THREAT LANDSCAPE AND THE COMPANY'S FOCUS ON INFORMATION SHARING ACROSS THE ENTIRE NETWORK.

are really identifying the new risks and devices that are authorised to access the new environment. Then again, today, the trust checking needs to be done continuously-it's not just a simple password at the beginning, but a constant monitoring of what the user is doing, what are they accessing and then regulating the access per session, per application using contextual rulesets, instead of just saying that the user can access everything in the data centre-that's not a good option anymore. That's obviously the biggest change there is

obviously the biggest change there is. On the other side, if you look at it from the bad actors' point of view, obviously there's been some big incidents that have made the news recently-it's clear that attacks are becoming more and more complex. Protecting the environment well has also become more difficult-especially the distribution of users. What's effectively happened is that every network that 15 years ago had a single edge connecting them to the rest of the world-still has that edge, but we've seen the creation of other multiple edges such as cloud edge, on/off net edge, work-from-home edge etc, that a lot of the organisations are now moving to, or are considering moving to-that's one aspect. Also, 5G is going to be a big

factor for new services and solutions and this is really all about the connectivity and the number of devices that are going to be connecting to the environment. Ensuring that these systems are secure and safe is going to be a big challenge.

How have the security priorities of organisations changed since the pandemic?

Security has become a lot more important-of course, it was important earlier and was easier to manage because everything was physically present in one location. But with this distribution of users, that's really highlighted the need for ensuring that every possible edge we have is really properly safe and secure. It was very simple when you knew who was coming into the office and what devices they were bringing in, but its different today, with home offices and different kinds of devices and accesses that beings about a lot of new risks. On the other side, it is also interesting to see that a lot of organisations have really responded fast to the requirements of making everything safe and secure.

What about the kind of attacks-have they also changed with time?

What we've seen is a lot of targeted

attacks now and again, as people are at home by themselves, there's a lot more communication happening over emails than face-to-face, as it used to previously and that has given an opportunity for bad actors to create more targeted campaigns because you're simply not face-to-face with your colleagues, you expect that they'll email you things. This is something that really can be an issue. So, email has become the easiest way to deliver malware as far as attacks are concerned and so protecting email services has always been very critical.

How are Fortinet's products keeping up with these changes?

For us, the company is fully focused on security-I would say that the main focus has always been to ensure that the products are able to share information with each other. We're talking about threat intelligence sharing where information exchange is extremely important. Say, if you have an incident that happens in one location, you want to make sure that whatever threat intelligence you collect from there is distributed across the entire network. Normally, you don't always have single vendor solutions covering the entire network so we need to ensure that there is a level of integration between our products and any 3rd party products our customers are using. This is done through Fortinet Security Fabric.

Our fabric covers everything from end-point network access to cloud to 5G. The new FortiGate 7121F consolidates networking and security through a security-driven networking approach to deliver full visibility, the highest scalability and advanced security to protect businesscritical applications in the distributed and hybrid 5G ecosystem. Through the breadth of the Security Fabric, Fortinet provides end-to-end security for 5G private and public network ecosystems, while also providing flexible connectivity and threat intelligence capabilities.

001001100000

1000100110101001010010100001111011010 1000001111010100010001110001000100110 .0110100100110010011100010011000001111 1001101010010100101000011110110100100 00011110101000100011100010001001101010 010010011 cyber threat intelligence 00 01000011110110100100110010011100010011 11100010001001101010010100101000011110 00100110000011110101000100011100010001 001111011010010011001001110001001100000 00100010011010100101001010000111101101 011000001111010100010001110001000100110 11011010010011001001110001001100000111 00000111101010001000111000

5G provides users and organisations ultra-fast internet speed while offering lower latency for their employees working from anywhere. The latest FortiExtender 511F-5G wireless WAN brings sub 6Ghz 5G connectivity to power SD-WAN and SASE solutions. FortiExtender is simple to setup and plug into Fortinet's

> *"FORTIGATE 7121F* CONSOLIDATES **NETWORKING AND** SECURITY THROUGH **A SECURITY-DRIVEN** NETWORKING **APPROACH TO DELIVER FULL VISIBILITY. THE HIGHEST SCALABILITY AND ADVANCED** SECURITY TO PROTECT BUSINESS-CRITICAL APPLICATIONS."

industry-leading Secure SD-WAN solution to provide flexible WAN connectivity for hybrid WAN to deliver better user experience. FortiExtender also enables thin edges with 5G connectivity to FortiSASE for cloud-delivered security and inspection, providing ultra-fast and safe wireless WAN connectivity for a diverse set of industries including retail, OT and healthcare.

As an integral part of the Fortinet Security Fabric, the FortiGate 7121F and industry-leading FortiGate portfolio adds to the Fortinet Security Fabric's ability to create value for both industrial enterprises and mobile network operators, delivering consistent security across 5G private and public networks, OT, the multiaccess edge compute and public private cloud environments. Fortinet's Security Fabric provides scalable security from the RAN to the core to the multiaccess edge compute (MEC). This allows industrial enterprises to achieve digital innovations, agility, improved safety and compliance while optimising performance and eliminating latency. 🙎

RING CUSTOMERS AROUND THE WORLD CAN NOW ACCESS VIDEO **END-TO-END ENCRYPTION**

JOSH ROTH. CTO. RING. DISCUSSES HOW THE ENCRYPTION ALLOWS CUSTOMERS WITH ELIGIBLE RING DEVICES TO ADD AN EXTRA LAYER OF SECURITY THAT ONLY ALLOWS THEIR VIDEOS TO BE VIEWED ON THEIR ENROLLED MOBILE DEVICE.



Josh Roth

t Ring, we're always looking at how we can continue to innovate for our customers, and security and privacy sit at the core of that. We build privacy and security into the process - designing our devices and services with these pillars front of mind, while putting our customers in control. Every day, our teams work hard to deliver on this commitment to our customers. Privacy choices are important and everyone thinks about their privacy in a different way. That's why we continue to innovate on our customers' behalf, and to offer a range of settings to help people customize their experience, while staying safe and secure.

Video End-to-End Encryption Launches Globallv

Earlier this year, we announced a technical preview of video End-to-End Encryption in the U.S. Today, we're proud to announce that we're moving it out of technical preview and expanding the feature's availability to customers around the world.

We believe that our customers should control who sees their videos. By default. Ring already encrypts customer videos when they are uploaded to the cloud (in transit) and stored on Ring's servers (at rest). Now, customers around the world, with eligible Ring devices, can opt into video End-to-End Encryption, to add an extra layer of security that only allows their videos to be viewed on their enrolled mobile device. This advanced security option is simple to set up via the Control Centre in the Ring App and offers additional peace of mind and protection.

"WE ARE ALWAYS LOOKING AT WAYS TO EMPOWER OUR CUSTOMERS WIT GREATER CHOICE WHEN IT 🚄 **COMES TO THEIR PRIVACY** AND SECURITY, WITHOUT **MPROMISING ON** CONVENIENCE."

Extra Security, Same Emphasis on User Control

We are always looking at ways to empower our customers with greater choice when it comes to their privacy and security, without compromising on convenience. This week, we are rolling out a range of features that do just that.

Starting today, customers can choose a compatible authenticator app, in addition to existing methods like SMS, as their second method of verification when logging into their Ring accounts. We're also starting to roll out CAPTCHA in the Ring App and Neighbors App as another safeguard that helps prevent automated login attempts from bad actors, providing yet another layer of security for our customers. Visit our Help Center page about authenticator app support to learn more.

Finally, we will be launching a new, automated self-service process to allow customers to securely and conveniently transfer ownership of used Ring devices without having to make a call to Customer Support. Now, the new device owner can simply scan the device during setup, and follow the instructions on the Ring App, which will also alert the previous owner. This process ensures that all videos and events from the previous owner's account are no longer linked to the device before the ownership is transferred to the new customer. While our customer support team is always happy to help customers with any questions, this new automated process adds another easy DIY option. 1



Monitor. Manage. Secure IT.

• • • • | | | ---

- » Over 300,000 customers in 190 countries from SMB to Fortune 500[®]
- » 498 of the Fortune 500 are customers
- » #1 in Network Management*
- » 50+ IT management products

solarwinds.com

Join SolarWinds at GITEX!

Dubai | 17-21 October | Stand H8-A30



NETWORK MANAGEMENT



SYSTEMS MANAGEMENT



SECURITY AND COMPLIANCE



DB Instances

IT SERVICE MANAGEMENT

Query Advice



DATABASE MANAGEMENT



Greatest Upward Wait Time Trends

APPLICATION MANAGEMENT

* IDC Worldwide Network Management Software Tracker 2H 2020



Security-Driven Networking, everywhere you need it.

Protect the possibilities with Secure SD-WAN.

