ISSUE 67 | AUGUST 2022 WWW.TAHAWULTECH.COM



HIGHLIGHTS MIMECAST

MIMECAST VEEAM SOFTWARE ESET

SECURITY FIRST

SASCHA GIESE OF SOLARWINDS TELLS ANITA JOSEPH ABOUT SECURE BY DESIGN, THE IT TRENDS REPORT AND THE HYBRID CLOUD OBSERVABILITY PLATFORM.



Make the most of WiFi 6.

Linksys Atlas Pro 6 with Intelligent Mesh[™] is a dual-band WiFi 6 system that delivers next-level streaming, data traffic and uninterrupted video conferencing to more than 30 devices per node simultaneously.

Access to 160 MHz — the least congested channels available on the 5GHz band — unleashes WiFi 6's incredibly fast connectivity.



Up to 3,5X faster speeds than WiFi 5.

Mesh WiFi 6 delivers true gigabit speeds—up to 5.4 Gbps with 6-stream connectivity—throughout your entire home or business, inside & out

160 MHz capable.

Access to the least congested channels on the 5 GHz band unleashes the true power of WiFi 6, allowing work-from-home, online learning, streaming & gaming devices to operate simultaneously without reduced bandwidth.

Linksys.com

More WiFi Channels.

Dynamic Frequency Selection (DFS) provides access to more channels, reducing interference from neighbouring networks.

Industry-leading technology.

The Qualcomm Immersive Home
216 Platform transforms home & business
WiFi to wired-like stability & speed.

Easy setup & control.

It's simple to set up and lets you manage your network or prioritise devices from anywhere, all with the free Linksys app.

*As compared from 802.11ac to 802.11ax.

30+ devices

Capacity per node.



AX5400

Accumulated speed up to 5.4 Gbps.



Covers homes with up to

2-3 bedrooms

per node (±230 m² / 1 floor).



Model# MX5500

Available in 1-, 2- or 3-Pack: MX5501, MX5502, MX5503

CONTENTS











- 6 Security news roundup from the region and beyond.
- Toufic Derbass, MEA Managing Director, Micro Focus, on the importance of face-to-face meetings post COVID.
- 22 Dan Woods, Global Head of Intelligence at F5, on the cybersecurity myths that are harming businesses.
- Edwin Weijdema, Global Technologist at Veeam Software, on the next wave of Ransomware.

NUCLIAS CLOUD BUSINESS GATEWAY

POWERFUL and ENDURING

multi-aspect protection for SMB cloud networks



DBG-2000

Why You Want It



Zero Touch Provisioning



Cloud-Based Management



Intrusion Prevention System



Dynamic Web Content Filtering



Auto VPN



Application Control



EDITOR'S NOTE



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

> Anita Joseph Editor

EVENTS





POWER OF OBSERVABILITY

Not too many of us are aware of what the

term Observability means in cybersecurity. It is actually the process of assessing the internal state of a network/system based on its external outputs. Observability leverages logs, metrics and traces — three critical components of a complex system. In simple terms, Observability is a management strategy focused on keeping the most relevant, important and core issues at or near the top of an operations process flow. The term is also used to describe software

processes that facilitate the separation of critical information from routine information.

This issue of Security
Advisor Middle East attempts to throw
more light on what is clearly emerging as
a security and business resilience tool. Our
cover story with Sascha Giese of SolarWinds
provides an expert's perspective and
discusses the Hybrid Cloud observability
solution powered by SolarWinds that offers
end-to-end visibility across on-premises
and multi-cloud and observability across
network, cloud, infrastructure, applications,
and database resources.

We also have Gordon Love, Vice
President, MEA and Emerging Markets at
Mandiant, telling us all about the company's
operations in the region and its next-gen
cybersecurity products and services.
Our interview of the month with Werno
Gevers of Mimecast spotlights the state of
email security in the region and also how
cybersecurity has now become one of the
top five priorities in the boardroom.

If you'd like to know more about how three prominent ransomware gangs

consecutively attacked the same network, read our report on the Sophos X-Ops Active Adversary whitepaper, "Multiple Attackers: A Clear

and Present Danger" to learn more. There's also another report from Nozomi Networks Labs which details how analysts have uncovered growing security concerns for both hard-coded passwords and internet interfaces for end-user credentials.

So as you can probably tell, this issue has packed a punch-it keeps you up-to-date with everything you need to know about cybersecurity and the threat landscape. So, Happy Reading!

FOUNDER, CPI Dominic De Sousa (1959-2015)

Published by



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

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com OnlineEditor Daniel Shepherd daniel.shepherd@cpimediagroup.com

Editor

Anita Joseph

anita.joseph@cpimediagroup.comm

PRODUCTION AND DESIGN
Designer
Prajith Payyapilly
prajith.payyapilly@cpimediagroup.com

DIGITAL SERVICES Web Developer Adarsh Snehajan webmaster@cpimediagroup.com

OBSERVABILITY

IS GAINING TRACTION

NOW.

Publication licensed by Dubai Production City, DCCA PO Box 13700 Dubai, UAF

Tel: +971 4 5682993

© Copyright 2022 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.

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com

LOOKOUT NAMED STRONG PERFORMER IN 2022 GARTNER PEER INSIGHTS VOICE OF THE CUSTOMER FOR SECURITY SERVICE



Lookout, a leader in endpoint

and cloud security solutions, has announced that it has been named a "Strong Performer" in the Gartner® Peer Insights "Voice of the Customer" for Security Service Edge (SSE). Gartner Peer Insights is a reviews and ratings platform for technology end users to provide candid customer feedback and for technology decision makers to learn about a company's products and services. The "Voice of the Customer" is a document that synthesises these user reviews into insights for IT decision makers.

To prevent data leakage in this cloud-first, hybrid workforce era, you need an integrated cybersecurity solution that offers advanced capabilities, rapid onboarding and a seamless user experience," said Pravin Kothari, executive vice president, Product and Strategy, Cloud Security, Lookout. "There's no stronger validation of our product's capabilities and value than positive customer endorsements. Lookout employees are deeply committed to meeting the needs and objectives of our customers, and we're honored to be recognised in the Gartner Peer Insights report."

ACTIVE ADVERSARIES EXPLOIT STOLEN SESSION COOKIES TO BYPASS MULTI-FACTOR AUTHENTICATION: SOPHOS

Sophos, a global leader in next-

generation cybersecurity, has announced in the Sophos X-Ops report, "Cookie stealing: the new perimeter bypass," that active adversaries are increasingly exploiting stolen session cookies to bypass Multi-Factor Authentication (MFA) and gain access to corporate resources. In some cases, the cookie theft itself is a highly targeted attack, with adversaries scraping cookie data from compromised systems within a network and using legitimate executables to disguise the malicious activity. Once the attackers obtain access to corporate web-based and cloud resources using the cookies, they can use them for further exploitation such as business email compromise, social engineering to gain additional system access, and even modification of data or source code repositories.

"Over the past year, we've seen



SEAN GALLAGHER

attackers increasingly turn to cookie theft to work around the growing adoption of MFA. Attackers are turning to new and improved versions of information stealing malware like Raccoon Stealer to simplify the process of obtaining authentication cookies, also known as access tokens," said Sean Gallagher, principal threat researcher, Sophos. "If attackers have session cookies, they can move freely around a network, impersonating legitimate users."

RANSOMWARE VARIANTS ALMOST DOUBLE IN SIX MONTHS: FORTIGUARD LABS REPORT

Fortinet, a global leader in broad,

integrated, and automated cybersecurity solutions, has announced the latest semiannual FortiGuard Labs Global Threat Landscape Report.

"Cyber adversaries are advancing their playbooks to thwart defense and scale their criminal affiliate networks," says **Derek Manky, Chief Security Strategist & VP Global** Threat Intelligence, FortiGuard Labs. "They are using aggressive execution strategies such as extortion or wiping data as well as focusing on reconnaissance tactics pre-attack to ensure better return on threat investment. To combat advanced and



sophisticated attacks, organisations need integrated security solutions that can ingest real-time threat intelligence, detect threat patterns, and correlate massive amounts of data to detect anomalies and automatically initiate a coordinated response across hybrid networks."

CRYPTO-CRIMINAL ACTIVITY HAS FALLEN IN 2022 WITH ILLICIT CRYPTOCURRENCY VOLUMES DOWN 15% YOY: CHAINALYSIS REPORT

After cryptocurrency-based crime

hit an all-time high in 2021, with illicit addresses receiving \$14 billion over the course of the year, there now appears to be a slowdown in illicit crypto-related activities this year, aligning with the broader decline of cryptocurrency markets. However, while legitimate cryptocurrency transaction volumes have dropped 36% year-over-year, criminal activity appears to be more resilient, with comparative illicit volumes down just 15%.

"Our data suggest that fewer people than ever are falling for cryptocurrency scams. One reason for this could be that with asset prices falling, cryptocurrency scams — which typically present themselves as passive crypto investing



opportunities with enormous promised returns — are less enticing to potential victims. We also hypothesise that new, inexperienced users who are more likely to fall for scams are less prevalent in the market now that prices are declining, as opposed to when prices are rising and they're drawn in by hype and the promise of quick returns," said Kim Grauer, Director of Research at Chainalysis.

AXIS COMMUNICATIONS TO SHOWCASE FUTURE OF SURVEILLANCE TECHNOLOGY AT INTERSEC SAUDI ARABIA



Axis Communications will be

participating in Intersec Saudi Arabia, which will take place in Riyadh from 13 to 15 September 2022. The security systems leader will be showcasing four themes at the exhibit: smart cities, critical infrastructure, hospitality, and the power of edge. Visitors can expect to see how the many dimensions of Axis's innovative, scalable products, solutions and services apply to these four themes.

"If you're in the commercial security, cyber security, and perimeter and physical security industry, Intersec Saudi Arabia is the place to be. We're particularly excited about exhibiting in Riyadh - Saudi Arabia's largest and most advanced city – as it presents the ideal platform for our team to strengthen our presence in the region and showcase our cutting-edge surveillance solutions. In line with Vision 2030, we'll demonstrate how our intelligent technology can be put to work in reshaping cities across Saudi Arabia," said Anan Elyan, Sales Manager of Western Arabia at Axis Communications.

MANAGEENGINE INTEGRATES WITH SECTIGO TO AUTOMATE CERTIFICATE LIFECYCLE MANAGEMENT

ManageEngine, the enterprise

IT management division of Zoho Corporation, has announced the integration between its key and certificate lifecycle management solution, Key Manager Plus, and Sectigo, an industry-leading identity-first security Certificate Authority. A testament to Sectigo's push for openness and interoperability in the identity, public key infrastructure (PKI), cryptography space, this integration enables IT admins using Sectigo certificates to confidently automate the entire certificate lifecycle from a secure, central platform.

"With work environments going perimeter-less and integrity issues at play in increasingly complex and



untrusted IT environments, organisations are looking to step up their certificate lifecycle management (CLM) programs," said Rajesh Ganesan, president of ManageEngine. "The integration of Key Manager Plus with Sectigo is an important step in helping security teams protect applications and infrastructures, improve their overall CLM maturity, and reduce risks to their reputation."

IMPORTANCE OF FACE-TO-FACE MEETINGS POST COVID

TOUFIC DERBASS, MEA MANAGING DIRECTOR, MICRO FOCUS



he COVID-19 pandemic got all of us used to the idea of working from home. The transition from the physical to the virtual provided a welcome break and we all warmed to the idea of blurring professional and personal lives and the flexibility that remote work gave us. During the lockdown, in particular, there was a need for technology to step in and connect people, and so businesses managed to hold on and witness growth despite everyone being at home. However, now that the worst of the pandemic is behind us, businesses continue to grapple with what the future of work should be likewhether to continue with the remote work/online trend, or revert to physical meetings as they were before.

Undoubtedly, digital meeting platforms such as Zoom and Teams brought in greater efficiency and reduced costs incurred for physical meets, such as for commuting and arranging physical meeting venues. However, as we re-examine the conversation around business outcomes, it becomes increasingly clear the absence of the 'thrill' of meeting and connecting with



people in a physical scenario has hit companies hard. The emotional void created by a lack of human interaction has definitely impacted customer-facing organisations and it has become amply clear that a return to face-to-face meetings is the need of the hour.

For most of us, a physical return to the office is for 'social' reasons-the chance to connect with friends, interact with customers and get feedback real-time. It's also about a definite structure to everyday activities-a clear demarcation between home and office life. However, there are other definite advantages to business outcomes if face-to-face meetings are encouraged, especially those that involve direct interaction with customers.

To begin with, businesses are built on relationships, and there's no better way to develop a strong rapport with clients and connect with them on a deeper level, than physical meetings. Although digital communication has taken huge strides and evolved significantly in recent years, the power of face-to-face interactions can never be discounted.

This is where the importance of non-verbal communication comes in-the

physiological changes, body language, feelings, facial expressions and sitting postures of people that provide instant cues about what a customer is thinking. Emotions are expressed through body language and also through the expressions, tone and volume of what is said. These provide valuable feedback that can be suitably responded to.

Imagine a meeting where two people disagree strongly on an issue. In a physical, face-to-face setting, this disagreement can be kept to the minimum by timely inventions by the rest of the attendees and the meeting concluded amicably, with the final deal concluded successfully. In an online meeting, however, the intervention will be minimum, where both sides will probably be allowed to present their views and then be shut down abruptly, so as to move on to the next item on the agenda. The meeting could end in stalemate. as timely interventions may not be possible and so the argument may not be favourably resolved. This will perhaps result in an opportunity lost, to perhaps, seal a deal.

In the sales field, in particular,

THE EMOTIONAL VOID CREATED BY A LACK OF HUMAN INTERACTION HAS DEFINITELY IMPACTED CUSTOMER-FACING ORGANISATIONS.

face-to-face meetings help to remove any miscommunication between the salesperson and their prospects. The physical presence of both sides means there is undivided attention, the direct opportunity to see the product or experience the service and receive instant feedback, as opposed to online meetings where the 'actual feel' is missed.

This doesn't mean that we should disregard online meetings altogether; it just means we should work out a balance between the two forms. Face-to-face meetings are all about building long term relationships; its all about strategy; it's all about opening our eyes to what's happening in the country, in the region, and staying alert and aware of the public pulse-all of which is difficult to achieve in virtual meetings.

BEYONDTRUST INTRODUCES NEW INTELLIGENT IDENTITY AND ACCESS SECURITY PLATFORM

RAJ CHERUKURI, CHIEF PRODUCT OFFICER, BEYONDTRUST

eyondTrust, the leader in intelligent identity and access security, has announced the BeyondTrust Platform, featuring a modern architecture that delivers unprecedented visibility of identities and access across an organisation's entire digital estate. from on-premises to cloud, hybrid and operational technology environments. The BeyondTrust Platform delivers the most powerful intelligent identity and access security through an elegant, unified platform and interface that removes friction and drives unparalleled insights for organisations of all sizes.

Today, organisations are being asked to do more with less, while facing an expanding threat landscape. They know they cannot solve emerging security problems with a disjointed patchwork of solutions or a poorly integrated ecosystem.

"Our customers have told us they want a single platform that removes complexity and the risk created by fragmented infrastructure," said Raj Cherukuri, Chief Product Officer at BeyondTrust. "They need solutions that accelerate time to value with easy deployments and deliver a robust set of common capabilities to reduce security risk, while accelerating their digital transformation initiatives."

The BeyondTrust Platform leverages a single interface to discover, manage, and protect identities, control access, as well as proactively detect anomalous activity. This new solution reduces complexity and management burden through a revolutionary single agent approach and unified management console across

all BeyondTrust apps. Along with the platform, BeyondTrust also announced:

- BeyondTrust's new Endpoint
 Security App, a modern privilege
 management solution that enables
 better policy management, access
 control, aggregated application
 monitoring, and threat detection;
 these integrated capabilities prevent
 attackers from elevating privileges,
 mitigating cyberattacks.
- The initial release of BeyondTrust's new Cloud Privilege Manager
 App, which provides visibility and management of entitlements across multicloud environments from a single pane of glass. Together, with the Endpoint Security App, it enables broad visibility of identities across an organisation's onpremises and cloud footprint.

By adopting a natively integrated and unified solution for identity and access security, organisations can better tackle existing use cases and expand to emerging ones, further reducing their attack surface. The BeyondTrust Platform provides a unified view of an organisation's identity landscape. This visibility helps organisations:

- Better manage, control, and protect their identity landscape
- More effectively control access to critical resources
- Easily meet security and compliance tarnets

Key features and benefits include:

 Breakthrough User Experience

 Unprecedented ease of use by leveraging natively integrated common capabilities, which can be

- activated as needed with a new trial and self-service approach
- Unified Management A single console and unified dashboard deliver navigation, management, and reporting across all apps
- A Universal Agent Streamlined deployment and straightforward maintenance with automatic installs and upgrades with no reboot required
- Asset Discovery Gain unified cross domain visibility with scanning across the entire environment
- Unified Policy Management Proactively manage drift with a
 policy advisor, a common policy
 framework, out-of-the-box policy
 templates and version control
- Centralised Reporting Leverage information holistically across apps to support better decision-making, with easy customisation options
- Holistic Visibility Gain insight into privileges in use across the entire IT environment – on-premises, cloud, bybrid
- Identity Security Insights Use identitycentric and cross app analytics for better decision making and prevent problems before they happen
- Health Monitoring Keep track of the health and status of your endpoints and assets with proactive analytics
- Multitenant Deployment –
 Create multiple tenants within a
 deployment with complete isolation
 to match the organisation's
 structure

Pricing and Availability

The BeyondTrust Platform and its initial apps will be available globally in Q1 2023.

GLOBAL
DEV
SLAM
10-13 OCT 2022

DUBAI WORLD TRADE CENTRE

× GITEX

Supported by

مقر المبرمجيـــــن coders (hq)

Featuring the inaugural





POWERING CODING INGENUITY

THE WORLD'S LARGEST MEET UP FOR

THE DEVELOPER & CODING COMMUNITY

TECH PIONEERS ON STAGE



Travis Oliphant
Creator of NumbPy
& Co-Founder





UNION USA

A



Sebastian Ramirez Montano Creator





Pablo Galindo Salgado Physicist & Software Engineer - R&D Python Infrastructurea

Bloomberg UK

DON'T MISS OUT, GET YOUR DELEGATE PASS



For delegate group booking, call Fahad Khalife at: +971 4 308 6805 | globaldevslammarketing@dwtc.com

G L O B A L D E V S L A M . C O M # G L O B A L D E V S L A M

Founding Partners















SECURITY FIRST



SASCHA GIESE OF SOLARWINDS TELLS ANITA JOSEPH ABOUT SECURE BY DESIGN. THE IT TRENDS REPORT. AND THE HYBRID CLOUD OBSERVABILITY PLATFORM

achieve it. Secure by Design is a response to the SUNBURST incident in December 2020. We used this incident to turn each stone in our environment and spent much thought on the software design process. Until then, we followed what was considered industry best practice, like every other software company. But the incident showed such best practices could no longer deal with the

changing threat landscape and state-sponsored

attacks. We significantly improved the security of

our software design process in many details.

ell us about Secure by Design

and how SolarWinds hopes to

To give you an idea, we no longer use static resources. For instance, in IT, we are quick in spinning up a VM for a test, but once the trial finishes, we tend to keep the VM running. We forget about it and move on. There is an attack point here. Attackers who gained access to such an unmonitored VM have all the time in the world to discover the environment. To counter this, we

moved away from static solutions and switched to a highly dynamic Kubernetes-based system. Each time a developer finishes a task or stops working at the end of the day, the resources will automatically destroy themselves.

Also, previously we had one build pipeline, which means developers ship code to a compiler that converts the hand-written code into machine readable executables. The next step is forwarding the executables to download platforms for end users. Now we have multiple independent development pipelines. The first team creates code and documents every single step, the second team rebuilds the code from the documentation, and the third team checks the integrity and authenticity of both code versions. That way, we can bypass many security problems. These changes improved our security, and we also shared it with other software vendors because what happened at SolarWinds happened elsewhere a few months later. We want to help the software community prevent such situations from happening again.



SolarWinds has always maintained that it has been on a journey towards becoming Secure by Design, but how has the long-term goal and objective then accelerated mainly post the pandemic?

Everything happened during the pandemic or before. I don't think there were any significant changes post the pandemic. For us internally, for the engineers, it wasn't easy initially because so many things changed. But eventually, everyone got used to it. So, it's working exactly the way we expected; we're very proud of the system.

It's an industry first to come up with measures to improve the security of software design. It's something exceptional. And it is not something that's finished and done. We can't say everything planned is sorted and set in stone because it is a dynamic process.

Whenever we discover something designed to be improved, we improve it. And we use minor incidents to test our strategies. For example, imagine a user doesn't log out of a workstation. It's usually not a big deal, but we use instances like these to test our security policies. Even if it's a tiny incident, we go the whole way and evaluate our processes with notifications, alerts, etc. It's like a fire drill that helps us prepare and keeps us on our toes.

Let's come to hybrid cloud. The
SolarWinds IT Trends report 2022
indicates that the shift to hybrid cloud
has only resulted in increasing IT
management complexity which has
created doubt and a lack of confidence
among tech professionals as to how
best to manage their IT environments.
What advice would you give them?

Unfortunately, there's no easy solution that works for all situations. Increased complexity is a huge problem, and if you look for the root cause of the complexity, you have to look back - it's a chain that starts with the human attention span.

We, as humans, no longer want to wait. So, businesses must adapt and

IT'S AN INDUSTRY
FIRST TO COME UP
WITH MEASURES
TO IMPROVE THE
SECURITY OF
SOFTWARE DESIGN.
IT'S SOMETHING
EXCEPTIONAL.

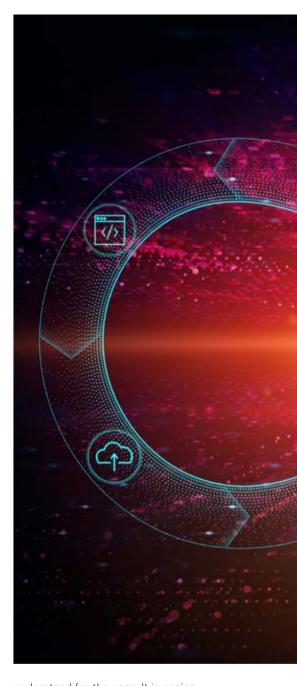
change their requirements, leading to significant IT changes. Today, IT is no longer just supporting the company; it is running it, and correctly implementing new technology is a great way to gain a competitive advantage. This is how increased complexity starts. You could probably say it's a homemade problem, but businesses must evolve to stay alive and competitive.

How to fight complexity? It would help if you had the expertise and various ways to gain it. It requires giving your IT teams enough time to learn and develop new skills, or you increase headcount and hire additional IT professionals with the necessary expertise. But that's not always possible, given the global shortage of IT professionals.

Another way would be to get third parties into the business for a while, maybe a contractor who sets up a multicloud environment, for instance. There are solutions to every complexity, but there is no one-size-fits-all solution.

In this context, can you tell us more about the SolarWinds Hybrid Cloud Observability platform?

The Hybrid Cloud Observability platform is an evolution of what was previously known as the Orion Platform. The Orion Platform has been in the market for 15 years. It's a modular system that grew with customers' demands. However, in the last couple of years, we noticed that the market is changing, so we came up with the new platform, Hybrid Cloud Observability, which is easier to



understand for the user. It is easier to understand the licensing, and the deployment is more straightforward. Customers get more features for the same price. The software can be deployed in any scenario, whatever the customer needs, on-prem, in a private cloud, public cloud, or hybrid. It can manage/observe any IT environment. So, the platform allows users to get different layers of information into one system, enabling them to perform a



faster root cause analysis. Keep in mind, when something breaks in IT, the first question is not how to fix it but who has to fix it.

With Hybrid Cloud Observability, we allow different groups - the network team, server admins, and cloud architects- to use the same tool and access the same data. The solution has some features that help users identify the root cause of problems. That, in a nutshell, is the new platform.

Today, the focus is on business resilience, continuity, and growth. How does multi-cloud observability help organisations with all of these?

Multi-cloud isn't new, but it's still a complex construct. There are many variables and moving parts, and it's crucial to understand workloads, application delivery, and connectivity. However, the connectivity between different clouds isn't that basic and can be pretty complicated. What is not

understood can't be observed, and what is not observed can't be managed. Multi clouds are complex, and a platform like Hybrid Cloud Observability is more than beneficial to know how things work. Most customers mix AWS and Azure globally. And those are supported out of the box by our product. It's a question of attaching a security token, and then we retrieve all the information straight from the cloud provider. It's pretty easy to use.

With security being a huge concern and priority today, where does the security aspect come into play in this observability scenario?

Our annual IT Trends Report discovered complexity as the biggest problem, and it's the same for security. I'd probably say that security and IT operations have one least common denominator: lack of visibility.

If you don't see or understand a performance problem, you can't fix it.

And if you don't see or understand a risk, you can't mitigate it.

Security teams and security professionals use different tools than

operational teams. Still, it would be beneficial for them to understand data flow and how applications talk to each other, and observability allows them to gain complete insight into the environment. So yes, it is helpful for security teams, too.

Do you believe that the Hybrid Cloud Observability platform could remedy many of the issues facing IT teams today in terms of managing complexity and security as the shift to hybrid IT continues to accelerate?

The short answer is yes. I briefly touched on this example: in IT, multiple teams,

WITH HYBRID CLOUD
OBSERVABILITY, WE
ALLOW DIFFERENT
GROUPS - THE
NETWORK TEAM,
SERVER ADMINS,
AND CLOUD
ARCHITECTS- TO USE
THE SAME TOOL AND
ACCESS THE SAME
DATA.



like networks, and applications, work in silos and use their toolset. If you have a unified platform that brings the groups together, brings humans together, that's a huge advantage. It's probably something that an individual in IT doesn't see as a crucial topic. But the IT Director or the CIO, someone with the big picture in mind, will instantly understand the benefits for the whole IT department and what it means to the business. But sometimes, it's also about the simple fact that such a tool gives people more time during their workday.

An IT professional spends more than half of the day fixing broken things. We



IF YOU DON'T SEE OR UNDERSTAND A PERFORMANCE PROBLEM, YOU CAN'T FIX IT. AND IF YOU DON'T SEE OR UNDERSTAND A RISK, YOU CAN'T MITIGATE IT.

call this firefighting, and it's usually a waste of time because that is time that can't be spent on improving IT, can't be spent on gaining a competitive advantage, and can't be spent on learning how to deal with new technology. So, firefighting is a waste of time, but unfortunately, as we know, things break, and things misbehave in IT. The need for firefighting remains, but if a tool could automate steps and even work autonomously in the background, it would be highly beneficial for each organization. It doesn't have to be a global player. Even smaller businesses see how easy Hybrid Cloud Observability is and understand that it can help with consolidating tools and lowering stress on individuals, reducing costs significantly.

What's next for SolarWinds?

There are a few things in the background that we are working on. For quite some time, we've been focusing on Artificial Intelligence. And we've built our own; we didn't go the way of purchasing an already existing framework. Our data has been training the system for the last eight months. We also reached out to a few customers who were okay with providing us with insights. Our AI will make it into

THE HYBRID CLOUD
OBSERVABILITY
PLATFORM IS AN
EVOLUTION OF WHAT
WAS PREVIOUSLY
KNOWN AS THE
ORION PLATFORM.

the product and lower IT professionals' workload.

There's a multi-layered approach. The first thing we want to do is reduce unnecessary alerts; that's important because if we receive text messages or emails all day about stuff that's not relevant, we tend to ignore it. And when something serious happens, we don't respond because we missed it. We use Al to look into a situation, discover whatever caused an alert, and relate it to all previously collected information.

Let's say, for instance, we manage a hypervisor like VMware, and the hypervisor runs with 90% CPU or 90% memory. Traditional systems will probably see 90% as a lot and instantly send an alert. However, if this condition is active for a longer timeframe and everything else is working fine, there's no real reason to alert. A notification will do.

Now, let's say CPU utilisation increases from 90 to 95%. That's an anomaly so that the AI will look into the reasons. And if the system sees that, for example, 20 virtual machines were running previously and now it's 22, that's a valid reason the CPU would go up. We wouldn't send an alert but instead deliver a notification to an ITSM solution for change management.

If, however, we see that the increase in the CPU is coming from a single machine, maybe a database, we'll look deep into the database, collect all information and send it to the resolver group only, which would be the DBAs in this example.

This is the first step. There are a couple of other things in the pipeline, but they're further ahead. We have many plans here at SolarWinds; one could say we're on a mission!

RE-ASSESSING SECURITY



WERNO GEVERS, REGIONAL DIRECTOR AT MIMECAST MIDDLE EAST, TELLS ANITA JOSEPH ALL ABOUT FMAIL SECURITY AND THE IMPACT OF CYBER THREATS ON THE BUSINESS LANDSCAPE.

imecast's latest
research has revealed
the impact of cyber
threats on digital
transformation in the

Middle East. Tell us more.

We conducted this survey across 400 IT individuals across the UAE and Saudi, specifically focusing on IT decision makers. We did this survey to understand three things: the impact digital transformation had on the threat environment, how decision makers are responding to this. And then of course, how they work with third parties to combat these threats.

What is quite interesting to see is that digital transformation has really increased the attack surface, which has, of course, changed the security posture of companies as well. If you think of the old-world way, we might have been an on premise or in a hybrid world. We had our own risk and security posture. When we move into a new digital world, we taking on these new big collaboration platforms like Office 365 or Google and we're taking on a completely new risk profile. And what we've seen is that there's a direct relationship between adoption and risk. A good example of this would be if you think of the early days of the pandemic, when we adopted Zoom

DIGITAL TRANSFORMATION HAS INCREASED THE ATTACK SURFACE, WHICH HAS, OF COURSE, CHANGED THE SECURITY POSTURE OF COMPANIES AS WELL.

working from home, we very quickly saw a whole new list of vulnerabilities that came out on Zoom specifically. Even after the meetings got password protected, you still would have received phishing links to join meetings or random people joining your meetings as well. So that's what we've seen in terms of the relationship between adoption and risk. But also, the research found and more than two-thirds of organisations in the region had to postpone a digital transformation initiative due to cyber security concerns, with more than 65% reporting that they've cancelled such initiatives outright. So it just goes to show that organisations are still taking this very seriously and they are taking the fact that they have to bake security into their digital transformation journey, which is really, really positive to see as well.

What we also found is that organisations face constantly evolving fake profiles, and more than 40% of organisations reported an increase in

cross site scripting. We've also seen more than 40% report an increase in typical phishing attacks and insider threats as well.

The biggest challenge for IT decision makers to combat this is the lack of capacity, the resources as well as the budget. So what IT decision makers typically do to overcome these challenges is that they look at best of breed vendors that can support them with this.

Automation has another key role. As part of the survey, we found that automation is expected to free up considerable hours per month at an entry level specialist and the CISO levels, which is creating valuable capacity for IT teams to work on more high value activities.

How important is cybersecurity among business leaders and decision makers today?

Cyber security has always been important, but I think we've seen this in Gartner's



research as well that it's becoming more and more prevalent at a board level. More than 80% of companies at a board level have cybersecurity as one of the top five priorities. It's always been really important, but I think the pandemic just sort of accelerated the whole process and fast tracked everything, and we see a lot more importance on cybersecurity.

We know that the pandemic has stretched companies' networks, accelerated digital transformation growth and exposed them to the growing volume of increasingly sophisticated cyber threats. We've also seen a sharp increase in things like ransomware attacks, and the rise of ransomware as a service is putting businesses under immense pressure. I also think that now security leaders understand that cybersecurity

can play an integral part in the disruption or success of any organisation.

Also, more and more companies also have employees working remotely. They're using their company assets to access things like online shopping, etc, so they're exposing new risks to the organisation.

And I think IT decision makers and CISOs and CIOs are playing a more and more important role in creating awareness at a board level and making sure that organisations understand the impact of these attacks and what the long-term effect could be on the reputation and the brand of any organisation.

Absolutely. Coming to email security, can you give us an overview of the pattern of email-based threats in the region?

I think globally there's quite a pattern- I

think the evolution of email and threats within email is guite interesting. I think in the early 2000s we dealt with spam and then after that, in 2010, we saw some phishing emails coming out of dangerous links embedded into a documents or emails itself. And then it evolved into things like business email compromise, where we've seen somebody impersonating somebody within the organisation that is involved into supply chain attacks down the line. All of a sudden, your suppliers and customers are at risk at the same time. And then this has gone beyond your perimeter as well. This has gone all the way to your brand-you need to protect your brand and outside world and your customers and suppliers expect you to protect them against things like fake websites. So I think it's a multifaceted faceted approach in order to combat this. But I think if we just look at emails specifically, and within the rounds of some of the research we've done, we've seen that more than 90% of the companies that we've surveyed, have seen an increase in phishing attacks where the majority reporting these are occurring more frequently. So I think what has happened is with the shift to working from home, more and more organisations are relying on these collaboration tools. Our work surface is really comprised of email and things like Slack Teams, Zoom, etc. So there's a wealth of data and information residing within these platforms, hence, it's an attractive target for attackers today.

I think also most according to the survey, most companies are bracing for an email-based attack that could cause considerable harm. More than eight out of 10 said that they will experience some sort of email borne attack that would perhaps significantly impact on organisations as well.

According to our latest state of email security report, more than two thirds of companies reported an increase in email base threats as well. So we've done multiple surveys, where this data has revealed itself, and it clearly shows that email is definitely something that should be taken very seriously.

he Trellix Threat Labs

Vulnerability Research team

has released research detailing
an unauthenticated remote
code execution vulnerability,
filed under CVE-2022-32548, affecting
multiple routers from DrayTek, a Taiwanese
company that manufactures Small Office
and Home Office (SOHO) routers.

The attack can be performed without user interaction if the management interface of the device has been configured to be internet facing. A one-click attack can also be performed from within the LAN in the default device configuration. The attack can lead to a full compromise of the device and may lead to a network breach and unauthorized access to internal resources. All the affected models have a patched firmware available for download on the vendor's website.

"With many businesses implementing work from home policies over the last two years, these affordable devices offer an easy way for Small and Medium Sized Businesses (SMBs) to provide VPN access to their employees. For this reason, we decided to look into the security of one of their flagship products, the Vigor 3910. We uncovered over 200k devices which have the vulnerable service currently exposed on the internet and would require no user interaction to be exploited," said Philippe Laulheret, Senior Security Researcher at Trellix.

The compromise of a network appliance such as the Vigor 3910 can lead to a host of undesirable outcomes including leak of sensitive data stored on the router: access to the internal resources located on the LAN that would normally require VPN-access or be present "on the same network"; man-inthe-middle of the network traffic; spying on DNS requests and other unencrypted traffic directed to the internet from the LAN through the router; packet capture of the data going through any port of the router or Botnet activity. Furthermore, failed exploitation attempts can lead to reboot of the device, denial of service of affected devices and other possible abnormal behavior.



TRELLIX FINDS UNAUTHENTICATED REMOTE CODE EXECUTION IN DRAYTEK VIGOR ROUTERS



PHILIPPE LAULHERET, SENIOR SECURITY RESEARCHER, TRELLIX

For those organizations that use DrayTek routers, Trellix recommends:

- Make sure the latest firmware is deployed to the device. The latest firmware can be found on the website of the manufacturer.
- In the management interface of the device, verify that port mirroring, DNS settings, authorized VPN access and any other relevant settings have not been tampered with.
- Do not expose the management interface to the Internet unless absolutely required. If you do, make sure you enable 2FA and IP restriction to minimize the risk of an attack.
- Change the password of affected devices and revoke any secret stored on the router that may have been leaked.

"Edge devices, such as the Vigor 3910 router, live on the boundary between internal and external networks. As such they are a prime target for cybercriminals and threat actors alike. Remotely breaching edge devices can lead to a full compromise of the businesses' internal network. This is why it is critical to ensure these devices remain secure and updated and that vendors producing edge devices have processes in place for quick and efficient response following vulnerability disclosure, just as DrayTek did," added Laulheret. "We applaud the great responsiveness and the release of a patch less than 30 days after we disclosed the vulnerability to their security team. This type of responsiveness and relationship shows true organisation maturity and drive to improve security across the entire industry." 1







THE WORLD'S LARGEST AND MOST INFLUENTIAL TECH + STARTUP EVENT

10-14 OCT 2022 DUBAI WORLD TRADE CENTRE



EVENT PASS



Believe the hype, it's here.

ENTER THE NEXT

DIGITAL UNIVERSE

#GITEXGLOBAL gitex.com

170+
COUNTRIES

700+ STARTUPS

4000+ COMPANIES

DIAMOND SPONSOR



GOLD SPONSORS

PLATINUM & LANYARD SPONSO

_

LVER SPONSOR









_____ ATTENDEES BADGE
SPONSOR

CONNEXIONS

MAJLIS LOUNGE SPONSOR

INNOVATION PARTNER -











CYBERSECURITY MYTHS THAT ARE HARMING YOUR BUSINESS

DAN WOODS, GLOBAL HEAD OF INTELLIGENCE AT F5

n the past two years, the world has been shocked economically, politically, and technologically.

Technology advancement has shifted into overdrive from its already dizzying pace.

Against this backdrop, a series of cybersecurity myths have gained traction, often prompting well-meaning security teams to focus on the wrong things. Here are seven of them to keep a watchful eye on:

Myth #1: Only a small number of social media accounts are fake.

A lot of enterprises know they have bots, but the reality is social media companies often don't know and don't want to know how many bots they really have.

We did a proof of concept with a social networking site some years ago that showed 98% of their logins were automated bots. This company was very proud of their rapid growth and excited for the future, but it turns out they only had a tenth of the subscribers they thought they had.

The significance of this knowledge and why it is important has been playing out in a very public way with the acquisition of Twitter. The value of the company is largely based on its number of users. Elon Musk's challenge to the company to demonstrate that spam bots and fake accounts are less than 5% is a fair expectation for any investor, advertiser, potential business partner, and even its users.

I predict that Twitter's bot number is closer to 50% or more. Companies should be required to validate users are human and effectively manage and mitigate their bot traffic.

Simply stated, the success of malicious bots indicates a security failure. Bot prevention is critical to ensuring the integrity of the information flowing through these sites, but also having accurate data for companies to make important business decisions and for others doing business with them.

Myth #2: Bot prevention is an in-house DIY project.

We've seen good companies with big budgets and brilliant technical

staff doing battle with bots for years. Yet when we analyse the bot traffic in these organisations, expecting to see sophisticated bots that had evolved to overcome their defences, it just isn't the case.

Companies have been fighting bots by blocking IPs, regions, and autonomous systems, and here is where we see the evolution of malicious bot traffic—attacks are now coming from hundreds of thousands, even millions of IP addresses. Those network layer defences only take you so far.

My mantra is that client-side signals are king. You must have behavioral biometrics. You must interrogate the browser and interrogate the device. All of those signals taken in the aggregate are how you identify not just bots but malicious humans as well.

Companies also think they can hire their way out of this situation, but there is no way to hire enough IT people to fix a problem this vast. The only way to really fight automation is with automation.

Myth #3: Focus should always be on a mysterious new threat on the horizon.

Those of us in security, the tech press, and corporate PR share a common fear of those threat actors who are constantly innovating and staying ahead of us. But in many ways, attacks are still the same with only slight tweaks along the way.

Most of the bots we see today show the same level of sophistication that we saw five years ago. They just come from different places. Credential stuffing still works in spite of two-factor authentication and/or CAPTCHA. Attackers won't innovate new attack vectors as long as the original vector remains successful. All they need to do is come up with a way to dodge new defences.

Companies do need to consider emerging

threats and try to prepare for them, but the industry also needs to continue to mitigate last year's threats.

Myth #4: Managing multiple clouds is a hard challenge that requires unobtainable talent

The multiple cloud world is a reality that many, if not most, companies are living in today. Whether it's because of an acquisition, integration with a partner, or just capturing best-of-breed features, multicloud is here to stay.

Yet when I ask companies if they're in multiple clouds, one answer I hear repeatedly is some version of, "Yes, unfortunately." Companies who operate across multiple clouds sometimes do so begrudgingly and don't embrace the opportunity to get the best of all worlds.

Today there's no reason that managing and securing your IT estate across multiple clouds should be arduous. Cloud vendors have built interoperability into their strategies, and there are many other providers whose solutions are designed to remove the burden of integration, abstract their functionality across clouds, and deliver it through a simple, unified interface.

Myth #5: Securing the enterprise's architecture and devices is enough.

Security teams are focused on the enterprise's infrastructure, their servers, their computers, their desktops—everything inside the organisation. What they largely are not focused on is the home networks of all the organisation's employees.

An attacker might want to target the CEO to access mergers and acquisitions insights or other strategic information, but monetizing that isn't as easy as targeting an accounts payable clerk or an IT administrator. At a time when working from home is more common than ever, home

networks are an emerging loophole for bad actors.

Myth #6: You can trust your employees.

Insider threats have an enormous advantage simply because it's human nature to assume the best of those around us. But the fact is you can't hire 50 or 100 employees without the very real risk of introducing a bad apple or two to the barrel.

Disgruntled employees don't just leave bad reviews on Glassdoor. They can throw sensitive files onto a thumb drive and walk right out the door. There's even a growing concern that they might leave malicious software in the system.

I've long had a theory that insiders are probably behind a lot of ransomware attacks. An IT administrator can easily create a persona on the dark web, give that persona access to the system to install malware, and then issue a demand for ransom—and in turn advocate that the company just pay the ransom. It's important to note that I've not yet seen evidence of this, but the incentive is certainly there.

Myth #7: Our biggest cyber threats come from nation state actors targeting infrastructure.

When the Colonial Pipeline was attacked a year ago, causing long lines at gas stations that inconvenienced consumers on the East Coast, it was major international news.

Yet, there is little to no conversation about the millions of Americans who are defrauded every year online, many of whom are elderly and living on their retirement savings. This is a tremendous threat to our social safety net that can have devastating effects on people and their families—much more so than having to wait in line and pay more for gas.

I spent years in law enforcement investigating cybercrime, more often than not with frustrating results, and this issue is a passion of mine. Attacks on our infrastructure are important and very real, but when you listen to the stories of these victims it's clear that widespread cyber fraud should be getting more attention than it is.

THOSE OF US IN SECURITY, THE TECH PRESS, AND CORPORATE PR SHARE A COMMON FEAR OF THOSE THREAT ACTORS WHO ARE CONSTANTLY INNOVATING AND STAYING AHEAD OF US.

WIPERS & IOT BOTNETS DOMINATE THREAT LANDSCAPE: NOZOMI REPORT

ROYA GORDON, OT/IOT SECURITY RESEARCH EVANGELIST, NOZOMI NETWORKS



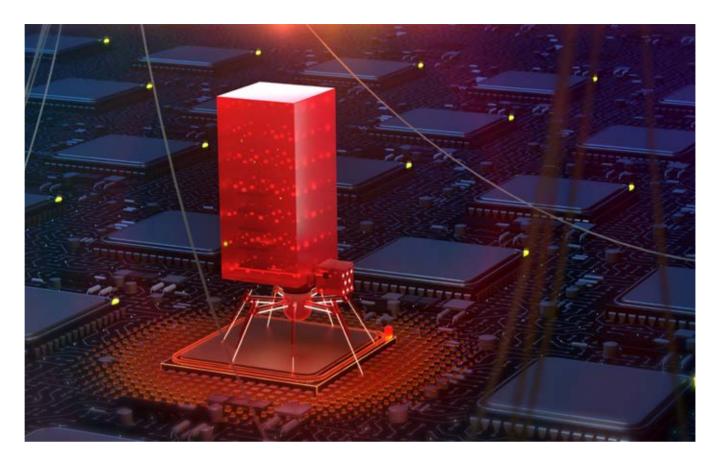
he latest OT/IoT security
report from Nozomi Networks
Labs finds wiper malware,
IoT botnet activity, and the
Russia/Ukraine war impacted
the threat landscape in the first half of

Since Russia began its invasion of Ukraine in February 2022, Nozomi Networks Labs researchers saw activity from several types of threat actors, including hacktivists, nation-state APTs, and cyber criminals. They also observed the robust usage of wiper malware, and witnessed the emergence of an Industroyer variant, dubbed Industroyer2, developed to misuse the IEC-104 protocol, which is commonly used in industrial environments.

Additionally, in the first half of 2022, malicious IoT botnet activity was on the rise and growing in sophistication.

Nozomi Networks Labs set up a series of honeypots to attract these malicious botnets and capture their activity in order to provide additional insights into how threat actors target IoT. In this research, Nozomi Networks Labs analysts uncovered growing security concerns for both hard-coded passwords and internet interfaces for end-user credentials. From January to June 2022, Nozomi Networks honeypots found:

March was the most active month



with close to 5,000 unique attacker IP addresses collected.

- The top attacker IP addresses were associated with China and the United States.
- "root" and "admin" credentials were most often targeted and used in multiple variations as a way for threat actors to access all system commands and user accounts.

On the vulnerability front, manufacturing and energy continue to be the most vulnerable industries followed by healthcare and commercial facilities. In the first six months of 2022:

- CISA released 560 Common
 Vulnerabilities and Exposures (CVEs)
 down 14% from the second half of 2021
- The number of impacted vendors went up 27%
- Affected products were also up 19% from the second half of 2021

"This year's cyber threat landscape is complex," said Roya Gordon, Nozomi Networks OT/IoT Security Research Evangelist. "Many factors including increasing numbers of connected devices, the sophistication of malicious actors, and shifts in attack motivations are increasing

the risk for a breach or cyber-physical attack. Fortunately, security defenses are evolving too. Solutions are available now to give critical infrastructure organisations the network visibility, dynamic threat detection, and actionable intelligence they need to minimise risk and maximise resilience."

Nozomi Networks' "OT/IoT Security Report" provides security professionals with the latest insights needed to reevaluate risk models and security initiatives, along with actionable recommendations for securing critical infrastructure. This latest report includes:

- A review of the current state of cybersecurity
- Trends in the threat landscape, and solutions for addressing them
- A recap of the Russia/Ukraine crisis, highlighting new related malicious tools and malware
- Insights into IoT botnets, corresponding IoCs and threat actor TTPs
- Recommendations and forecasting analysis.

NOZOMI NETWORKS LABS SET UP A SERIES OF HONEYPOTS TO ATTRACT THESE MALICIOUS BOTNETS AND CAPTURE THEIR ACTIVITY IN ORDER TO PROVIDE ADDITIONAL INSIGHTS INTO HOW THREAT ACTORS TARGET IOT.



consulting business, and as a business we help organisations and government entities to develop more effective and efficient cyber security programs and instill confidence in their readiness to defend against and respond to cyber threats.

What are some of the leading cyberattacks that businesses are grappling with today, especially in the context of accelerated digital transformation?

The modern threat landscape is vast. In today's environment, consumers have learned to work, shop, entertain themselves, stay in touch with friends and family and even improve their health and wellbeing using online platforms. With consumers and businesses continuing to drive more operations online, the pressure on digital security will continue to rise.

One thing we can always count on is the level of uncertainty in the cyber realm. Attackers regularly change their approach to evade detection, leaving defenders struggling to keep up.

The ransomware threat has grown significantly throughout the past decade, and it will continue in this upward trend. We're seeing cyber criminals conducting sophisticated multi-faceted extortion operations at a rising tempo, using new ways to deploy ransomware rapidly and efficiently throughout business environments.

Additionally, with the increase in reliance on cloud technology, errors in misconfiguration plus increased attack surface and interconnectivity are other ways in for attackers that are anticipated to grow in tandem with enterprise cloud adoption.

Today's Threat Intelligence focuses primarily on inputs. How is Mandiant's Threat Intelligence offering different?

Our incident response consultants discover adversarial techniques, tools, malware and indicators of compromise

OUR INCIDENT RESPONSE CONSULTANTS DISCOVER ADVERSARIAL TECHNIQUES, TOOLS, MALWARE AND INDICATORS OF COMPROMISE WELL BEFORE THEY ARE WIDELY KNOWN OR CATEGORISED – AND CONTINUE TO TRACK THEM AS THEY EVOLVE.

(IOCs) well before they are widely known or categorised – and continue to track them as they evolve. This early knowledge data is continually added to our Intel Grid, automatically updating customers' Mandiant Advantage products and dramatically reducing the time to leverage this information from weeks to minutes.

What is a digital risk protection solution and why is it important?

We launched our Digital Risk Protection Solution a couple of months ago. It's all about helping organisations to build up an intelligence-led picture of their attack surface plus looking at what could impact them on the deep and dark web. This allows security leaders to proactively mitigate threats before they disrupt business operations. The solution itself is a combination of our Mandiant Advantage Digital Threat Monitoring, Attack Surface Management and Threat Intelligence products, and is available as either a selfmanaged solution or as a service.

Security leaders are able to gain:

- Visibility into external exposure and targeting: Identify vulnerabilities and gain insight on risk factors impacting the extended enterprise and supply chain through attack surface mapping and deep and dark web activity monitoring.
- Threat analysis and risk identification: Proactively protect against eminent threats by understanding which threat actors

- are targeting the organisation, what they are after (financial gain, espionage or other) and how they are planning to attack.
- Cyber threat intelligence driven prioritisation: Confidently prioritise defensive measures and investments by leveraging threat intelligence derived from Mandiant's frontline investigations, expertise and in-depth analysis.

What is Mandiant's plan for the ME region, going forward?

Digitalisation is on the rise in the Middle East region and although it holds immense potential for huge rewards, it also brings with it significant risks that organisations need to ensure they're well-prepared to tackle.

Mandiant's latest M-Trends 2022 report confirms that professional and financial services, healthcare, retail, high tech and government were the most frequent targets of cyber attackers throughout 2021, but no matter what the industry or size, every organisation should be working to strengthen and test their defences.

We will continue to initiate more dialogue with executive management in the region around cyber risk and the impacts proactive and reactive measures have on an organisation's risk profile. Our approach, derived from numerous program transformations aims to help organisations build a better approach to identifying, mapping and driving down risks in a meaningful and methodical way.

HIVE, LOCKBIT **& BLACKCAT RANSOMWARE GANGS** CONSECUTIVELY **ATTACK SAME NETWORK:** SOPHOS REPORT

JOHN SHIER. SENIOR SECURITY ADVISOR, SOPHOS

ophos, a global leader in next-generation cybersecurity, has announced in the Sophos X-Ops Active Adversary whitepaper, "Multiple Attackers: A Clear and Present Danger," that Hive, LockBit and BlackCat, three prominent ransomware gangs, consecutively attacked the same network. The first

two attacks took place within two hours, and the third attack took place two weeks later. Each ransomware gang left its own ransom demand, and some of the files were triple encrypted.

"It's bad enough to get one ransomware note, let alone three," said John Shier, senior security advisor at Sophos. "Multiple attackers create a whole new level of complexity for recovery, particularly when network files are triple encrypted. Cybersecurity that includes prevention, detection and response is critical for organizations of any size and type—no business is immune."

The whitepaper further outlines additional cases of overlapping cyberattacks, including cryptominers, remote access trojans (RATs) and



bots. In the past, when multiple attackers have targeted the same system, the attacks usually occurred across many months or multiple years. The attacks described in Sophos' whitepaper took place within days or weeks of each other—and, in one case, simultaneously—often with the different attackers accessing a target's network through the same vulnerable entry point.

Typically, criminal groups compete for resources, making it more difficult for multiple attackers to operate simultaneously. Cryptominers normally kill their competitors on the same system, and today's RATs often highlight bot killing as a feature on criminal forums. However, in the attack involving the three ransomware

groups, for example, BlackCat—
the last ransomware group on the
system—not only deleted traces of
its own activity, but also deleted
the activity of LockBit and Hive. In
another case, a system was infected
by LockBit ransomware. Then,
about three months later, members
of Karakurt Team, a group with
reported ties to Conti, was able



to leverage the backdoor LockBit created to steal data and hold it for ransom

"On the whole, ransomware groups don't appear openly antagonistic towards one another. In fact, LockBit explicitly doesn't forbid affiliates from working with competitors, as indicated in Sophos' whitepaper," said Shier. "We don't have evidence of collaboration, but it's possible this is due to attackers recognizing that there are a finite number of 'resources' in an increasingly competitive market. Or, perhaps they believe the more pressure placed on a target—i.e. multiple attacks—the more likely the victims are to pay. Perhaps they're having discussions at a high level, agreeing to mutually beneficial agreements, for example, where one group encrypts the data and the other exfiltrates. At some point, these groups will have to decide how they feel about cooperation whether to further embrace it or become more competitive-but, for

TARGETED ORGANISATION RECEIVED THREE DIFFERENT RANSOMWARE NOTES FOR TRIPLE ENCRYPTED FILES.

now, the playing field is open for multiple attacks by different groups."

Most of the initial infections for the attacks highlighted in the whitepaper occurred through either an unpatched vulnerability, with some of the most notable being Log4Shell, ProxyLogon, and ProxyShell, or poorly configured, unsecured Remote Desktop Protocol (RDP) servers. In most of the cases involving multiple attackers, the victims failed to remediate the initial attack effectively, leaving the door open for future cybercriminal activity. In those instances, the same RDP misconfigurations, as well as applications like RDWeb or AnyDesk, became an easily exploitable pathway for follow-up attacks. In fact, exposed RDP and VPN servers are some of the most popular

listings sold on the dark web.

"As noted in the latest Active
Adversary Playbook, in 2021
Sophos began seeing organisations
falling victim to multiple attacks
simultaneously and indicated that this
may be a growing trend," said Shier.
"While the rise in multiple attackers is
still based on anecdotal evidence, the
availability of exploitable systems gives
cybercriminals ample opportunity to
continue heading in this direction."

To learn more about multiple cyberattacks, including a closer look at the criminal underground and actionable advice on safeguarding systems against such attacks, read the full whitepaper, "Multiple Attackers: A Clear and Present Danger," on Sophos.com. 1

CLOUD BOX TECHNOLOGIES

ONE OF THE PREMIERE IT INFRASTRUCTURE SOLUTION PROVIDERS IN THE MIDDLE EAST

WHO WE ARE

Empowering our clients

We are proud to be a UAE based ISO 9001 & 27001 certified organization headquartered in Dubai Sheikh Zayed Road with a passion for technology & Smart Solutions

Our values are derived from the Emirati culture with a vision to participate in the growth and development of the UAE

We have a highly experienced, innovative technical team with many years of experience in delivering projects ranging from simple to very complex.

Our experience has been gained through working with some of the largest global organizations in both the public and private sectors



TALK TO US

(04) 344 5022 +971 50 852 8022 info@cbt.ae



HOW TO BROWSE THE WEB SECURELY

PHIL MUNCASTER, GUEST WRITER AT ESET

eb browsers are our gateway to the digital world. We spend hours on them each day, which makes them not only a vital tool for legitimate users, but a valuable target for threat actors. Over the years they've become a repository of credentials, cookies, web searches, and other juicy information that could be targeted by cybercriminals.

They may even use attacks to control your computer remotely and access the network it's connected to.

Threats go beyond malicious third parties. Many users may also feel slightly queasy at the thought of third-party advertisers and others accessing and tracking their personal information via the browser. Fortunately, there's plenty you can do to manage these risks.

Top browser threats

There are plenty of threats out there: some targeting browsers more directly than others. Here are a few of the top ones:

Exploitation of vulnerabilities in

browsers or any plugins/extensions you may have installed. This tactic could be used to steal sensitive data or download additional malware. Attacks often start

with a phishing email/message, or by visiting a site that has been compromised or is controlled by the attacker (drive-by-download).

Malicious plug-ins: There are thousands of plugins on the market, which users can download to enhance the browsing experience. However, many have privileged browser access. That means malicious plugins spoofed to appear legitimate could be used to steal data, download additional malware and much

DNS poisoning: DNS is the address book of the internet, converting the domain names we type into IP addresses, so that our browsers display the sites we want to visit. However, attacks on the DNS entries stored by your computer, or on DNS servers themselves, could allow attackers to redirect browsers to malicious domains like phishing sites.

Session hijacking: Session IDs are issued by websites and app servers when users log in. But if attackers manage to brute force these IDs or intercept them (if they aren't encrypted), then they could log in to the same sites/apps masquerading as the user. From there, it's a short hop to stealing sensitive data and potentially financial details.

Man in the middle/browser attack: If the attackers manage to insert themselves between your browser and the websites you're viewing, they might be able to modify traffic – for example, redirecting you to a phishing page, delivering ransomware, or stealing logins. This is especially true when using public Wi-Fi networks.

Web app exploitation: Attacks like crosssite scripting can still target apps on your machine rather than the browser, but the latter is used to deliver or execute the malicious payload.

The privacy angle

These scenarios all involve malicious third parties. But let's not forget the large amounts of data that internet providers, websites, and advertisers collect on visitors every day as they browse the web.

Cookies are small bits of code generated by web servers and stored by your browser for a certain amount of time. On the one hand, they save information that can help to make the browsing experience more personalized—for example, showing relevant ads or ensuring you don't have to log in multiple times to the same site. But on the other hand, they represent a privacy concern and a potential security risk, if hackers get hold of them to access user sessions.

In the EU and some US states, the use of these is regulated. However, when presented with a pop-up of options, many users simply click to accept the default cookie settings.

How to browse the web more securely

There's plenty that users can do to mitigate security and privacy risks when browsing the web. Some involve the browser directly; others are best practices that can have a positive knockon impact. Here are some key best practices:

- Keep your browser and plugins updated, to mitigate the risk of vulnerability exploitation. Uninstall any out-of-date plugins to reduce the attack surface further
- Only visit HTTPS sites (ones with

CONSIDER USING A
PRIVACY-CENTRIC
BROWSER/SEARCH
ENGINE TO MINIMISE
COVERT DATA SHARING.

- a padlock in the browser address bar), meaning hackers can't snoop on traffic between your browser and the web server
- Be "phishing aware" to reduce the risk of browser threats that travel via email and online messages.
 Never reply to or click through on an unsolicited email without checking the sender's details.
 And don't hand over any sensitive information
- Think before downloading any apps or files. Always go through official sites
- Use a multi-factor authentication (MFA) app to reduce the impact of credential theft
- Use a VPN from a reputable provider, and not a free version.
 This will create an encrypted tunnel for your internet traffic to keep it safe and hide it from third-party trackers
- Invest in multi-layered security software from a reputable vendor
- Enable automatic updates on your
 OS and device/machine software
- Update browser settings to prevent tracking and block third-party cookies and pop-ups
- Switch off password auto-save in the browser, although this will impact the user experience when logging in

Consider using a privacy-centric browser/search engine to minimise covert data sharing

Use private browsing options (i.e., Chrome Incognito mode) to prevent cookie tracking

Many of the above tips are optional and will depend on how strong your privacy concerns are. Some users are prepared to accept a certain amount of tracking in return for a smoother browsing experience. However, the security tips (like HTTPS, automatic updates, security software) are essential to reduce your exposure to cyberthreats. Happy browsing.

EXPLOIT DETECTIONS IN MIDDLE EAST RISE 8% IN Q2 2022



DR. AMIN HASBINI, HEAD OF GLOBAL RESEARCH AND ANALYSIS TEAM (GREAT), META REGION, KASPERSKY

xploits are programs or pieces of code written by cybercriminals that are designed to take advantage of a bug or vulnerability in an application or operating system running on a local or remote system (PC, server, mobile device, IoT device, etc.). Using an exploit, attackers gain unauthorised access to the applications or operating systems on these systems.

Zero-day exploits – those relying on vulnerabilities that were previously unknown to the software vendor – are often used for cyberespionage on different organisations and are particularly dangerous for large businesses, government agencies, individuals with access to valuable data. Zero-day exploits were at the heart of some of the most infamous cyberattacks around the world, such as the Sony Pictures attack, Stuxnet, MysterySnail, PuzzleMaker and others.

In 2021, Kaspersky found 4 zero-day vulnerabilities in Microsoft products that cybercriminals could exploit – CVE-2021-28310, CVE-2021-31955, CVE-2021-31956, and CVE-2021-40449. They were discovered with Kaspersky's Exploit prevention technology, which detects not only known exploits, but suspicious anomalies in programs' behavior as well – and therefore helps cybersecurity practitioners reveal new vulnerabilities.

Bahrain saw the most significant increase in exploit detections in Q2 compared to Q1 among the Middle East

countries – by 137% to 22,186 cases, with the share of affected users rising by 36%. It was followed by Saudi Arabia – exploit detection saw an increase of 57% to 523,367, while the share of affected users decreased by 9%. Oman saw a 12% rise in exploit detection cases to 16,871, with the share of affected users decreasing by 9%. In the United Arab Emirates, the number of detections remained almost unchanged in Q2 at 192,959 (1% increase from Q1), and the share of users affected by exploits decreased by 10%.

On the contrary, the most significant decrease in exploit detections in Q2 compared to Q1 in the Middle East countries happened in Egypt – by 19% to 450,828 cases, with the share of users affected by exploits decreasing by 11%. Qatar saw a decrease in exploit detections by 12% to 38,140 (7% decrease in the share of affected users). Kuwait saw a decrease of 8% in exploit detections to 13,932 cases, however, the share of users affected rose by 12%.

"Over the last years we have seen the attackers' firm interest towards zeroday exploits – vulnerabilities previously unknown to vendors that pose a serious threat to all users, home and corporate. These exploits give attackers an easy access to victims. That's why it is important not only to constantly update your systems, but also to install security solutions that proactively discover unknown threats. Of equal importance is providing your cybersecurity team with access to the latest

threat intelligence and regular professional trainings," said Dr. Amin Hasbini, Head of Global Research and Analysis Team (GReAT), Middle East, Turkey and Africa region at Kaspersky. "Kaspersky's Exploit Prevention technology was designed to add an additional layer of protection for the most frequently targeted programs and technologies. It provides an efficient and non-intrusive way for blocking and detecting both known and unknown exploits. EP is an integral part of Kaspersky's behavior-based detection capabilities."

To protect your organisation from exploits, Kaspersky experts recommend:

- Update your device's OS and other third-party software as soon as possible and do so regularly
- Use a reliable endpoint security solution such as Kaspersky Endpoint Security for Business that is powered by exploit prevention, behavior detection and a remediation engine that is able to roll back malicious actions.
- Provide your SOC team with access to the latest threat intelligence and regularly upskill them with professional training.
- Along with proper endpoint protection, dedicated services can help against high-profile attacks. The Kaspersky Managed Detection and Response service can help identify and stop attacks at the early stages before attackers achieve their goals.











FUTURE BLOCKCHAIN SUMMIT فمة مستقبل البلوك تشين

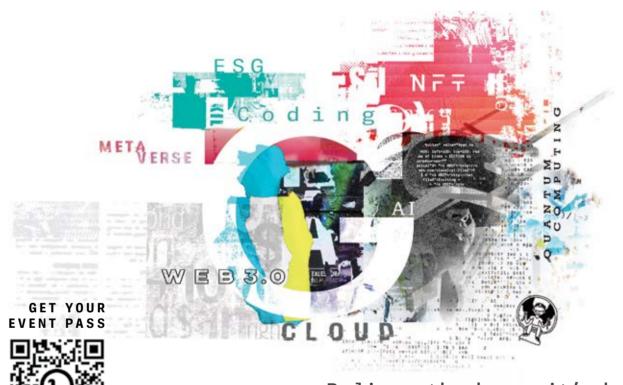




10-14 OCT 2022 DUBAI WORLD TRADE CENTRE

SHOW TIMINGS: 10 Oct - 11am to 5pm | 11 - 14 Oct - 10am to 5pm

THE WORLD'S LARGEST & MOST INFLUENTIAL TECH + STARTUP EVENT



Believe the hype, it's here. ENTER THE NEXT DIGITAL UNIVERSE



GOLD SPONSOR -

GOLD SPONSOR -

TECH & DIGITAL

TIII Technole Innovati Institute ERICSSON.



SILVER SPONSOR INNOVATION PARTNER

CONNEXIONS

MAJLIS LOUNGE SPONSOR

ADGE SPONSOR











NEXT WAVE OF RANSOMWARE

EDWIN WEIJDEMA. GLOBAL TECHNOLOGIST. VEEAM SOFTWARE



ansomware as a trend will continue to affect businesses across the world – with attack types and tactics from cybercriminals evolving all the time. As attacks get more sophisticated, so do the consequences of falling victim to ransomware and the complexity of the clean-up.

The stakes are therefore higher than ever for businesses when it comes to protecting against ransomware attacks. Organisations need to understand the emerging trends that we will see gather speed, and prepare their defences for the ransomware onslaught.

Make your business insurable: The tension between insurers and businesses affected by ransomware is mounting. In EMEA we have already seen global insurance giant AXA announced that it will stop writing cyber-insurance policies in France that reimburse customers for extortion payments made to ransomware criminals. Furthermore, the Dutch government has considered banning

insurers from covering the cost of ransom payments made by businesses operating in the Netherlands. With insurers overwhelmed and frustrated by ransomware claims, underwriters will tighten up their policies to ensure clients are meeting predetermined conditions such as investing in appropriate cybersecurity and employee training before paying out.

Watch out for triple extortion: This technique designed to make businesses pay more and pay faster involves extending the attack to the victim's customers and partners. Traditionally, ransomware attacks involve cybercriminals locking down and encrypting systems then demanding a ransom payment to regain access. In 2019 ransomware strains such as DoppelPaymer gave cybercriminals the ability to lock down systems and exfiltrate data simultaneously. Not only can attackers demand ransom money for regranting access to key IT systems. but they can also threaten to publish exfiltrated data online if the victim didn't pay up. Triple extortion involves a third element - directing the attack beyond its initial target, using multi-layered extortion techniques to harm the victim's customers and partners.

Minimise the threat within: Various studies suggest that over 60% of data breaches and cybersecurity incidents are caused by insider threats. Disgruntled employees understand the power they have in terms of opening the doors to the outside. Equally, perfectly satisfied employees who do not grasp the importance of practising good digital hygiene can be equally dangerous. Digital hygiene is the first line of defence for an organisation. Using two-factor authentication and restricting file access to only those who need it are ways of limiting the amount of damage a single user can do if security is compromised intentionally or unintentionally. Furthermore, training and education are vital to making sure employees

A 'HUMAN FIREWALL' COMBINED WITH THE RIGHT TECHNOLOGY CAN HELP ORGANISATIONS PREPARE FOR THE RANSOMWARE ATTACKS THAT WILL INEVITABLY COME THEIR WAY THIS YEAR AND BEYOND.

are confident identifying and reporting potential attacks.

Beware of the slow burn: Advanced Persistent Threat (APT) attacks involve unauthorised users gaining access to a system or network and remaining there for an extended period of time without being detected - waiting for the right opportunity to steal valuable data. Cyberattackers are clever about choosing the right time to strike and maximising their chances of getting an easy payday by compromising a company when they are at their most vulnerable or when the stakes are highest. For example. an attacker may be ready to take your systems down and exfiltrate data but know that your company is due to IPO in a few months. It, therefore, makes sense to wait it out and take you down at the moment you need the operational and reputational damage least and will be most willing to payout to end the attack.

Enforce the law: Law enforcers are trying to bridge the imbalance between risk and reward for cybercriminals. Cybercriminals can make huge sums of money with little or no threat of prosecution. This will and has to change. However, given the borderless nature of cybercrime, governments must agree on an international legal framework for punishing cybercrime. Until then legal action will mainly be directed towards the victims rather than the criminals. Many governments are debating whether they should make ransomware payments illegal, so businesses resist the temptation to pay ransoms - cutting off cybercriminals' income supply.

Moreover, cryptocurrencies like Bitcoin, commonly viewed as a hacker's dream, actually have the potential to help law enforcers bring criminals to justice.

Digital ledgers like Blockchain make it easier to 'follow the money' as records cannot be altered or deleted. Therefore, once criminals turn their cryptocurrency into 'real money', the digital ledger can theoretically unmask them.

Protect your data: Everything from the advancing threat landscape to changes in the way the legal and insurance sectors view ransomware payouts puts the onus on data protection and cybersecurity. Organisations must consult with their technology partners about deploying Modern Data Protection solutions that can detect, mitigate and remediate ransomware attacks. Data must be backed up and recoverable across physical, virtual, cloud, SaaS and Kubernetes so that in the event of a ransomware attack, businesses can remediate and recover quickly rather than being forced into paying the ransom.

As well as implementing Modern Data Protection solutions, businesses must prioritise improving digital hygiene levels across their entire employee base. Employee education and awareness training can help to create a more digitally secure culture across the organisation. A 'human firewall' combined with the right technology can help organisations prepare themselves for the ransomware attacks that will inevitably come their way this year and beyond. \$\mathbb{1}\$

IT'S TIME TO BRING IN CYBERSECURITY EXPERTS

CALLSIGN STUDY SHOWS BUILDING DIGITAL TRUST CAN BOOST GLOBAL ECONOMY BY US \$3000 GDP PER CAPITA.



new global study has identified significant economic value in building digital trust. A 5% increase in digital trust results in an average increase in GDP per capita of US \$3,000. The Digital Trust Index: the value of digital trust is seminal research, conducted by Callsign, the digital trust pioneer, and the Centre for Economics and Business Research (Cebr), into the attitudes and drivers of digital trust across modern economies. The findings come at a critical time for the global economy with economic slowdowns occurring, building digital trust has the potential to unleash

trillions of dollars in economic growth.

In the MEA region 56.3% of respondents say that online and digital services can be trusted. But in terms of the factors that negatively impact digital trust, 21.1% of MEA consumers said their experience with online fraud led to their distrust in online services. Other factors negatively impacting trust in online services include experience of data breaches, cited by 12.8% of MEA respondents. Further, 15% of MEA consumers believe that there is a lack of transparency in online and digital services, and 16.1% voiced concern that they do not always know how to use online and digital services safely leading to mistrust.

CONSUMERS IN MEA WANT A SECURE DIGITAL WORLD AND GOVERNMENTS WANT TO CONTINUE TO GROW THE DIGITAL ECONOMY IN THE REGION.

Saeed Ahmad, MD Callsign MENA said, "This research is ground-breaking because for the first time we are able to quantify the value of trust in our digital world both in economic terms and in societal terms. The results of this research should be a call to action for businesses and governments to work together to build a secure, ethical digital identity framework so that citizens can live digitally, safely, and to boost economic growth at this critical time."

54% of consumers expect governments to create a more secure digital world. To achieve this, three quarters (77%) of respondents reported support for the creation of a digital identity system covering technology, process and data policies overseen by an independent body. Consumers would trust banks and financial services firms the most to create and maintain the system. 47% of those surveyed expect a digital identity system to be part of their everyday lives the next 12 months.

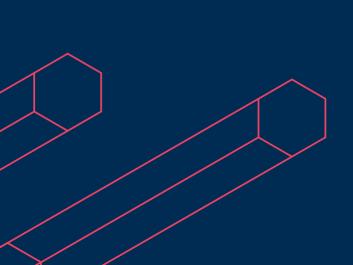
Ahmad continued, "The foundation of digital trust is our digital identities. We need to know who we are interacting with online to be able to trust in brands, transactions and people. Consumers in MEA want a secure digital world and governments want to continue to grow the digital economy in the region, they need to work with businesses to reap the benefits of the GDP per capita that building digital trust could bring. Our research demonstrates we have a trillion-dollar opportunity and given the global economic challenges today, we can't afford to ignore it anymore." 1



Be data ready.

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

commvault.com



The future of cybersecurity is cybersecurity as a service.



Sophos Managed Detection and Response

24/7 analyst-led threat hunting, detection and response delivered as a fully managed service for any security environment.

For more information visit sophos.com/mdr or contact: salesmea@sophos.com

