28th ANNUAL CYBER SECURITY CONFERENCE

AVAR 2025

SHIFTING POWER IN CYBER DEFENSE

3RD TO 5TH DECEMBER 2025

KUALA LUMPUR, MALAYSIA

SPONSORS & PARTNERS

Silver Sponsors

Bronze Sponsor

T Shirt Sponsor

Delegate Bag Sponsor

Lanyard Sponsor

Supporting Sponsors

Supported by

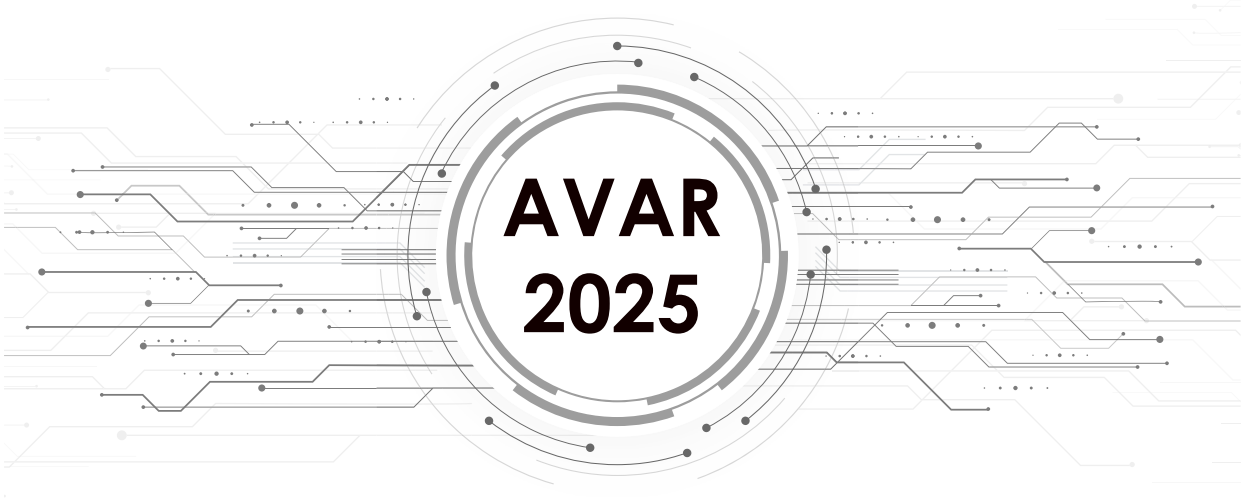
Supporting Partners

Media Partners

CONTENTS

CONTENTS

CONTENTS



CEO MESSAGE

Every year, cyber security practitioners and stakeholders from around the world gather at AVAR's conferences to discuss how we can stem the rising tide of cyber attacks. We gather again in 2025 – but this year is unlike previous years.

We have chosen the theme Shifting Power In Cyber Defense because of a significant change in cyber security: with this year, defense is on the offense. Law enforcement and cyber security organizations have increased meaningful collaboration, resulting in more arrests, more takedowns, and more disruption of criminal ecosystems. We are not just defending against cyber attacks; we are making life more difficult for threat actors before they can launch an assault.

Winning a few battles does not mean the war is won. We face new challenges in our mission to protect the world. The most obvious and tangible threat is dynamic, AI-driven malware generation. We don't yet have working compiled binaries from AI but research clearly indicates that threat actors are harnessing LLMs for harm. They are resourceful and adapt quickly – which we must match.

Another challenge that is currently over the horizon but may soon become a present threat is quantum computing. Today's encryption may be no match for tomorrow's decryption capabilities, which has seen the emergence of "harvest now, decrypt later" strategies where adversaries gather encrypted data to be unlocked by tomorrow's quantum machines. The world must move towards quantum-safe algorithms and we must prepare to defend today's data against tomorrow's quantum-powered threats.

AVAR 2025 addresses these challenges with two approaches: through the conventional route of presentations and discussions around these topics and, launching this year, training sessions that enable cyber security practitioners to take the lead against these threats through coaching that provides practical countermeasures that deliver immediate real-world benefits.

The common thread that binds these initiatives, and all of us, together is that we are a community. We share what we know, we help and inspire each other, and we stand stronger together. We will prevail as long as this spirit endures. I thank all the speakers, delegates, partners, and sponsors for your enthusiastic participation in AVAR 2025 and welcome everyone to Kuala Lumpur where we will lay the technical and personal foundations for the future of cyber security.

Kesavardhanan J
CEO of AVAR

CISCO TALOS

OUR JOB IS YOUR DEFENSE

LEARN MORE ABOUT HOW TALOS SUPPORTS CISCO CUSTOMERS AT

talosintelligence.com

AGENDA

DAY 1 Wednesday, 3rd December, 2025

Time	Activity
14:00 – 16:30	MARC I (Malware Analysis Report Competition) Lena Yu, *Malware Village*
16:30 – 18:00	Registration
19:00	Welcome drinks reception and dinner

DAY 2 Thursday, 4th December, 2025

Time	Track 1
09:00 – 09:30	Registration
9:30 - 10:40	**Welcome Address: Kesavardhanan J** CEO, *AVAR* **Conference Opening: Righard Zwienenberg** Chairman, *AVAR* **Keynote Address: Dato' Dr Amirudin Abdul Wahab** CEO, *Cyber Security Malaysia* **Keynote Address: Tanvinder Singh** Director Cyber Security & Privacy, *PWC* **Keynote Address: Michael Daniel** President & CEO, *Cyber Threat Alliance*
10:40 – 11:00	Refreshment Break

DAY 2 Thursday, 4th December, 2025

Time	Track 1	Time	Track 2	Time	CISO Connect
11:00 – 11:30	**Sniffing Around: Unmasking the LongNosedGoblin operation in Southeast Asia and Japan** Anton Cherepanov, Peter Strýček, *ESET*	11:00 – 11:30	**High Stakes, Hidden Threats: Unmasking the Vault Viper Network with DNS** Maël Le Touz, John Wojcik, *Infoblox*	11:00 – 11:05	**Introduction to CISO workshop** Dr. Peter Leong
11:30 – 12:00	**Inside the Shadows: APT Tactics Using MSC Files, Grim Resource Injection, and AppDomain Hijacking** Hossein Jazi, Douglas Santos, *Fortinet*	11:30 – 12:00	**Lotus in Perpetual Bloom: Sustained Espionage in Southeast Asia with Evolving Sagerunex Backdoors** Joey Chen, *Cisco*	11:05 – 11:25	**Quantum Reckoning: Cyber Security At A Tipping Point** Felissa Mariz Marasigan, Mark Gabriel Rizare, *EY GDS (CS) Philippines, Inc.*
12:00 – 12:30	**Shadows in Native Code: The Rise of AOT Compilation in Modern .NET Malware** Sarang Popat Sonawane, *Crowdstrike*	12:00 – 12:30	**NTLM Exploit Redux!** Anurag Shandilya, Arnab Mandal, Satyam Yadav, *K7 Computing*	11:25 – 11:45	**Countering the Unthinkable: Disrupting Advanced Threats with Unconventional Defenses** Ken Soh, *Athena Dynamics*
12:30 – 13:00	**No Payload For You: Inside Sidewinder's Selective Exploitation Strategy** Eliad Kimhy, Santiago Pontiroli, *Acronis*	12:30 – 13:00	**SESE: Social Engineering Second Edition** Righard Zwienenberg, Eddy Willems, *ESET, WAVCi*	11:45 – 12:25	**Leading with Risk – How CISOs Can Drive Business Decisions (Panel Discussion)** Ridzwan Mahdi, *Maxis* Dr. Peter Leong, *MY CIO Service* Vikneswaran Kunasegaran, *CREST* Arivindran Saidoo, *KPMG Malaysia* Malini Kanesamoorthy, *AmBank Group* Dharshan Shanthamurthy, *SISA*
				12:25 – 13:00	**Training Session: Building a Secure Malware Analysis Environment** Lena Yu, *Malware Village*
13:00 – 14:00	**Lunch Break**				
14:00 – 14:30	**ConnectUnwise: How Threat Actors Abuse ConnectWise Installer as Builder for Signed Malware** Lance Jansen Caoile Go, Karsten Hahn, *G Data AV Lab Inc / G Data Cyberdefense AG*	14:00 – 14:30	**ValleyRAT Unleashed: A Deep Dive into its Modern Arsenal and Tactics** Hiromu Kubiura, Shota Nakajima, Ryonosuke Kawakami, *LY Corporation/ Cyber Defense Institute, Inc.*	14:00 – 14:40	**Disaster Recovery – What Works, and Doesn't, in the Real World (Panel Discussion)** Wisnu Tejasukmana, *SLB* Ridzwan Mahdi, *Maxis* Ashok Kumar J, *G3 Cyberspace* Shah Mijanur Rahman, *Inmagine Group* Dinesh Barathy, *Collectius Group*

DAY 2 Thursday, 4th December, 2025

Time	Track 1	Time	Track 2	Time	CISO Connect
14:30 – 15:00	**Yet Another Cyberespionage Operation In Vietnam** Tran Duy Nam, Dat Nguyen The, *VNPT Cyber Immunity*	14:30 – 15:00	**Modern Fileless RAT Tactics: Node.js Abuse : Technical Analysis and Threat Attribution** Reegun Richard Jayapaul	14:40 – 15:20	**Compliance & AI – Governing the New Technology On The Block (Panel Discussion)** Vikneswaran Kunasegaran, *CREST* Syarifah Bahiyah Rahayu, *Universiti Pertahanan Nasional Malaysia* Ruban Bala, *Banking Industry* Cameron Camp, *SecureIQLabs* Yusfarizal Yusoff, *PETRONAS Digital*
15:00 – 15:30	**An Analysis of Cloud Infrastructure Utilization in Malware Command and Control** Tran Thi Hieu Ngan, Bui Huy Anh, *CMC Cyber Security*	15:00 – 15:30	**Generative AI, Retrieval-Augmented Generation (RAG) and Agentic AI in Offensive Cyber Operations** Aaron Aubrey Ng, *Stanford University*		
15:30 – 15:50	Refreshment Break				
15:50 – 16:10	**The Silent Invaders: Understanding and Combating macOS Infostealers** Srinivasan Govindarajan, Pranjal Gupta, *Microsoft*	15:50 – 16:50	**Shared Vision: Advancing Cybersecurity Through Collective Innovation (Panel Discussion)** Vanja Svajcer, *Cisco* Erik Heyland, *AV-Test* Xavier P. Capilitan Jr., *G Data AV Lab Inc* Santeri Kangas, *F-Secure* James Thang, *Help Group* Ken Soh, *Athena Dynamics* Jacky AW, *Kenanga Group*	15:50 – 16:50	**Training Session: AI Management Systems for CISOs – Navigating Governance, Risk, and Compliance** S Kumar Subramania, *K7 Cyber Security*
16:10 – 16:30	**Using Linguistics and Psychological Profiling in Threat Actor Attribution** Rishika Desai, *BforeAI*				
16:30 – 16:50	**Booking a Threat: Inside LummaStealer's Fake reCAPTCHA** Arvin Lauren L. Tan, John Rey B. Dador, Arvin Jay S. Bandong, *G DATA AV Lab Inc.*	16:50 – 17:10	**Beyond Pen Tests & Red Teams: A New Approach to Measuring Enterprise Cybersecurity Effectiveness** Bijay Limbu Senihang, *SecureIQLab*	16:50 – 16:55	**Closing Remarks** Dr. Peter Leong
19:00 – 22:00	**Pre-dinner Drinks & Gala Dinner**				

DAY 3 Friday, 5th December, 2025

Time	Track 1
10:00 – 10:20	**The (Un)Natural Science of Malware,** Lena Yu, *Malmons World Ltd & World Cyber Health – Malware Village*

Time	Track 1	Time	Track 2
10:20 – 10:50	**Unmasking AI-Themed Malvertising Targeting Social Media Users** Jaromír Hořejší, *Check Point*	10:20 – 10:50	**Simplicity as a Weapon for Stealth and Persistence** Chetan Raghuprasad, *Cisco*
10:50 – 11:20	**AI Voice Honeypots – Turning Scam Calls into Real-Time Threat Intelligence** Claudiu Laurentiu Tirisi, Alexandru Paul Marinescu, *Bitdefender*	10:50 – 11:20	**Ghost Math: Syscall-Only Injection, Deterministic Shellcode & QUIC C2 – A Modern EDR Bypass Monograph** Ananda Krishna, Anand Sreekumar, *UST*
11:20 – 11:40	Refreshment Break		
11:40 – 12:10	**IDFKA Backdoor: The Hidden Threat of Rust Implants in Modern APT Campaigns** Vladimir Stepanov, Anna Mazurkiewicz, *Rostelecom-Solar*	11:40 – 12:20	**Transparency Wars: Exposing Hidden Biases in Testing (Panel Discussion)** Luis Corrons, *Gen* Simon Edwards, *SE Labs* Righard Zwienenberg, *ESET* Samir Mody, *K7 Computing*
12:10 – 12:40	**The Open doorX : From Directory Listing to Attribution** Shogo Hayashi, Nobuyuki Amakasu, *NTT Security Holdings*	12:20 – 12:50	**No Impregnable Fortress: How Team46 Carries Out Successful Attacks on Russian Companies** Vladislav Lunin, *Positive Technologies*
12:40 – 13:10	**Meet VenomSEO: New Threat Targeting Malaysian Websites for Black SEO** Igor Zdobnov, Ivan Korolev, *Doctor Web*	12:50 – 13:10	**Hidden Malice: Inside Tiny FUD's Mac Backdoor** Suresh Reddy Lomada, *K7 Computing*
13:10 – 14:10	Lunch Break		
14:10 – 14:40	**From Code to Clues: Leveraging LLMs to RAT out Android SpyMax** Baran Kumar, *K7 Computing*	14:10 – 14:40	**Cracking the Vault: Real-World Crypto Wallet Exploits and Defense Strategies** Rijul Chauhan, Mansi Aggarwal, *Mastercard*
14:40 – 15:10	**When Firewalls Go Blind: Custom Tools, AI Agents, and the Fall of Traditional Network Inspection** Sangay Lama, Cameron Camp, *SecureIQLab*	14:40 – 15:10	**Leveraging Generative AI for dynamic file honeypots in Windows Kernel** Vladimir Strogov, Sergey Ulasen, *Acronis*
15:10 – 15:30	**Windows threats and COM interfaces (Sponsor Presentation)** Vanja Svajcer, *Cisco*	15:10 – 15:30	**Tracing the Origin: Fingerprints in MSC File for Clustering and Attribution** Kazuya Nomura, Rintaro Koike, *NTT Security Holdings*
15:30 – 15:50	Refreshment Break		

DAY 3 Friday, 5th December, 2025

Time	Track 1	Time	Track 2
15:50 – 16:20	**Emmenhtal Loader: The Silent Enabler of Modern Malware Campaigns** Lovely Jovellee Lyn Antonio, Ricardo Pineda Jr, Louis Victor Sorita Jr, *G Data AV Lab Inc*	15:50 – 16:30	**Data Without Borders? Sovereignty, Trust, and the Cloud Dilemma (Panel Discussion)** Michael Daniel, *Cyber Threat Alliance* Selvakumar Manickam, *Universiti Sains Malaysia* Murugason R. Thangaratnam, *Novem CS* Syahril Aziz, *Secure InSight Sdn Bhd* Vimalaasree Anandhan, *Poshmark*
16:20 – 17:00	**Internal Threats – Strategies for Partner-Dependent Organizations (Panel Discussion)** Peter Stelzhammer, *AV-Comparatives* Jairam Ramesh, *AIA Digital+* Tanvinder Singh, *PwC* Jonathan Tam, *Schneider Electric* *Ekneswaran Matandor*	16:30 – 17:00	**Operation DRAGONCLONE: Chinese Telecommunication industry targeted via VELETRIX & VShell malware** Sathwik Ram Prakki, Subhajeet Singha, *Quick Heal*
17:00 – 17:10	Closing Address		

WE ARE CTA

WE ARE STRONGER TOGETHER

CTA is a non-profit organization that is working to improve the cybersecurity of our digital ecosystem by enabling real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field.

CTA's mission is to improve the overall cybersecurity of the global digital ecosystem. We seek to:

PROTECT ENDUSERS
DISRUPT MALICIOUS ACTORS
ELEVATE OVERALL SECURITY

JOIN US!

https://www.cyberthreatalliance.org

CYBER THREAT ALLIANCE

SNIFFING AROUND: UNMASKING THE LONGNOSEDGOBLIN OPERATION IN SOUTHEAST ASIA AND JAPAN

Abstract:

In this talk, we will present a detailed case study of a cyberespionage campaign that we uncovered targeting organizations in Southeast Asia and Japan. We attribute this campaign to the LongNosedGoblin threat actor, which has been active since at least 2023.

Our research reveals how LongNosedGoblin leverages Active Directory Group Policy to deliver custom malware across numerous workstations within compromised environments. One such payload, dubbed NosyHistorian, is a lightweight infostealer, designed to collect browser history, likely to help identify high-value targets within the affected organizations. Following this reconnaissance phase, the attackers deployed more advanced backdoors and data exfiltration tools. For instance, they used a full-featured backdoor we named NosyDoor, which leverages the Microsoft OneDrive service for command-and-control (C&C) communications and includes functionality to bypass the Antimalware Scan Interface (AMSI).

During our presentation, we will deliver an in-depth analysis of the custom malware arsenal and the TTPs (tactics, techniques, and procedures) employed by this APT group. We will also detail our attribution process and explore potential links and overlaps with other threat actors operating in the region.

Anton Cherepanov
ESET

Bio:

Anton Cherepanov is a Senior Malware Researcher at ESET, responsible for analyzing and hunting the most complex cyber threats. He has conducted extensive research on the Sandworm APT group. Anton has presented his findings at numerous international conferences, including Black Hat USA, Virus Bulletin, and CYBERWARCON. His professional interests include reverse engineering and hunting for previously unknown threats.

Peter Strýček
ESET

Bio:

Peter Strýček is a Malware Researcher at ESET who enjoys reverse engineering and analyzing complex threats. He has a particular interest in analyzing malware targeting platforms such as Linux and macOS.

INSIDE THE SHADOWS: APT TACTICS USING MSC FILES, GRIM RESOURCE INJECTION, AND APPDOMAIN HIJACKING

Abstract:

As the cyber threat landscape evolves, so do the tactics employed by advanced persistent threats (APTs). With the increasing disablement of macros in Microsoft Office, threat actors have adapted, turning to new methods for malware delivery over recent years. Since early 2022, there has been a noticeable shift away from traditional macro-based attacks toward techniques involving ISO files, HTML smuggling, LNK files, and CHM files. Among these methods, the use of Microsoft Common Console (MSC) files remains underexplored yet has emerged as a powerful tool for malware delivery and persistence in Windows environments. Although initially limited in use, MSC files began gaining significant traction among threat actors in early 2024. Kimsuky was one of the first groups to incorporate MSC files into its campaigns, leveraging various techniques to target victims. Recently, Kimsuky expanded its MSC-based attacks by using Zoom-themed lures, incorporating the legitimate Zoom application to add credibility and increase engagement. Following Kimsuky's example, other APT groups- including Mustang Panda, Earth Baxia, APT32 and APT Bitter- have adopted MSC files as part of their initial infection strategies. Some of these APTs combine novel methods like Grim Resource Injection and AppDomain Manager Hijacking to enhance the efficacy and stealth of their attacks.

These attacks, which use legitimate Windows subsystems and tools to deliver malicious payloads, pose significant challenges for detection. Traditional enterprise security solutions often focus on identifying the aftermath of these techniques- such as the loading of malicious code into legitimate Windows processes- rather than the techniques themselves.

Current EDR tools generally provide limited visibility into the full attack chain and tend to rely on known malicious payload signatures or newer detection methods, such as stack-based similarity hashing, to detect frameworks like Sliver, Cobalt Strike, and Metasploit. This technical deep dive will explore how APT groups are exploiting the hidden capabilities of MSC files to conduct stealthy, sophisticated attacks.

We'll provide a timeline of MSC file adoption by various threat actors and examine the structure of weaponized MSC files, focusing on advanced techniques like Grim Resource Injection and AppDomain Manager Hijacking, which enable malicious code execution in .NET environments. Recent campaigns demonstrate how APTs are increasingly using these novel techniques to expand their toolsets and evade modern security controls. We'll also discuss detection challenges, showcase a demo of these methods in action, and highlight their implications for current detection mechanisms.

INSIDE THE SHADOWS: APT TACTICS USING MSC FILES, GRIM RESOURCE INJECTION, AND APPDOMAIN HIJACKING

Hossein Jazi
Fortinet

Bio:

Hossein Jazi is a Senior Threat Intelligence Specialist at Fortinet, where he plays a key role as an active researcher with expertise in APT tracking, malware analysis, cyber threat intelligence, and AI security. His work focuses on identifying and monitoring APT activities, as well as publishing in-depth analyses of their operations.

Hossein was the first to identify and name the Evasive Panda and Lazy Scripter threat actors, and he has authored more than 50 blogs profiling various cyber adversaries. His current initiatives include developing proactive techniques to track threat actors, collaborating with partners to create advanced research tools, and leading efforts to disrupt and dismantle cybercriminal operations.

With a master's degree in computer science and over 15 years of experience specializing in cybersecurity and APT analysis, Hossein continues to push the boundaries of threat research to make the digital world more secure.

Douglas Santos
Fortinet

Bio:

With more than two decades of experience in the cybersecurity field, I possess a unique blend of sales soft skills and deep technical acumen, making me a well-rounded individual who is at ease working in both technical and non-technical environments. My keen understanding of the cyber threat landscape allows me to communicate potential threats and vulnerabilities, as well as complex security issues and possible countermeasures, to any audience with ease.

Currently, my focus is on developing innovative ways to advance the state of the art in cyber threat intelligence, while managing a team of researchers and engineers. Our goal is to identify new attack vectors and develop proactive intelligence to protect against them. To help me achieve this mission, I am driving our partnership with MITRE CTID and participating in projects that are augmenting the state of the art when it comes to threat intelligence standards, tools, and response. We are also deploying these tools and standards across Fortinet's products and systems.

My vast experience, technical expertise, and communication skills have enabled me to excel in the cybersecurity industry, and I look forward to continuing to drive innovation and progress in this field.

SHADOWS IN NATIVE CODE: THE RISE OF AOT COMPILATION IN MODERN .NET MALWARE

Abstract:

The landscape of malware development is experiencing a significant shift as threat actors increasingly leverage Ahead of Time (AOT) compilation in .NET frameworks. Traditionally, .NET applications have been relatively straightforward to reverse engineer due to their intermediate language representation, which preserves substantial program structure and metadata. However, the growing adoption of AOT compilation—which transforms .NET code directly into native machine code—presents formidable new challenges for security researchers and malware analysts.

Our preliminary research indicates that approximately 75% of .NET AOT samples identified in the wild demonstrate malicious intent, suggesting this technique has been rapidly embraced by threat actors. AOT compilation effectively eliminates the Microsoft Intermediate Language (MSIL) layer, forcing analysts to work directly with assembly code and significantly complicating the reverse engineering process. This technique serves as an emerging obfuscation strategy that requires minimal effort from malware authors while providing substantial protection against analysis.

This paper examines the technical characteristics of AOT-compiled malware, presents methodologies for identification and analysis of these samples, and explores the development of specialized tools to recover function signatures and type information. We demonstrate how traditional .NET analysis techniques fail against AOT-compiled binaries and propose new approaches combining static and dynamic analysis to overcome these limitations. Furthermore, we discuss the security implications of Microsoft's continued enhancement of AOT capabilities in newer .NET versions, which inadvertently provides malware authors with increasingly sophisticated evasion techniques.

As AOT compilation becomes more accessible with each .NET release, understanding its security implications becomes critical for maintaining effective malware detection and analysis capabilities in the evolving threat landscape.

Sarang Popat Sonawane
CrowdStrike

Bio:

Sarang Sonawane currently holds the role of Security Researcher within CrowdStrike's Malware Research Team, boasting 9+ years of experience with a primary focus on reverse engineering.

In recognition of his expertise, he has presented at security conferences, including BlackHat MEA and AVAR. He also loves playing CTF challenges and has successfully completed the Flare-On 9 and 11 security challenges.

Beyond his dedication to cybersecurity, Sarang thrives on intellectual challenges in the malware analysis domain. When not dissecting malicious code, he passionately engages in cricket matches and eagerly explores new destinations, satisfying his adventurous spirit.

NO PAYLOAD FOR YOU: INSIDE SIDEWINDER'S SELECTIVE EXPLOITATION STRATEGY

Abstract:

Active since at least 2012, Sidewinder has carried out sustained and highly targeted espionage campaigns across Southeast Asia. Often labeled as unsophisticated, the group instead demonstrates strong operational discipline and a clear focus on precision targeting. In this presentation, we share new research into Sidewinder's tooling, infrastructure, and delivery methods, based on recent campaigns targeting government ministries, military entities, public institutions, and financial organizations.

Through multi-stage spear-phishing, geofenced payload distribution, and sandbox evasion, Sidewinder ensures that only its intended victims receive the actual malware while analysts are left with nothing to work with. The group's infrastructure fingerprints each request and generates unique payloads per victim, leaving minimal evidence behind.

Our investigation reveals highly customized intrusion chains, obfuscated shellcode, and staged malware deployed via trusted executables and DLL sideloading. We also explore potential overlaps with other regional APTs such as SideCopy and related clusters, highlighting shared techniques, tactics, and procedures.

Attendees will gain insights into Sidewinder's evolving playbook, practical detection strategies, and a broader understanding of its place within the regional APT landscape.

Santiago Pontiroli
Acronis

Bio:

Santiago Pontiroli is a cybersecurity expert focusing on threat intelligence efforts at Acronis as Lead Scurity Researcher of the Acronis Threat Research Unit (TRU). He specializes in analyzing nation-state actors, criminal organizations, and financially motivated threat groups, focusing on malware analysis, reverse engineering, and creating advanced detection capabilities.

Beyond his work at Acronis, Santiago is an active contributor to the cybersecurity community. He has authored articles and whitepapers and presented his research at renowned global conferences, including Virus Bulletin, CARO, Nuit du Hack, MITRE ATT&CK, BlueHat, 8.8, and ekoParty.

CONNECTUNWISE: HOW THREAT ACTORS ABUSE CONNECTWISE INSTALLER AS BUILDER FOR SIGNED MALWARE

Abstract:

In March 2025, we noticed and started tracking an unusually high number of ConnectWise-based malware. ConnectWise is a remote desktop application usually used by tech support to provide remote assistance. This new malware campaign weaponized trust in an unexpected way: by delivering validly signed ConnectWise ScreenConnect installers repurposed as remote access malware. These binaries were distributed via phishing emails, cloud platforms or AI related websites. These samples managed to pass traditional AV detection signature checks and appear benign – all while handing attackers control of the victim's desktop without visible warnings such as tray icons or prompts or with fake Windows update messages and application icons.

A technique known as Authenticode stuffing made this campaign possible. Custom configuration data of ConnectWise such as command-and-control server addresses, user messages, background images or UI suppression flags are embedded into the installer's certificate table – a section not covered by Authenticode's hashing. This allows threat actors to build their own remote access malware while retaining ConnectWise's valid authenticode signature.

Our analysis compared different variations of ConnectWise samples which revealed that only differences between the binaries were found within the certificate data. Using tools such as PortexAnalyzer and Authenticode Lint, we extracted this data, reverse engineered its structure and wrote a config extractor. To detect abused ConnectWise installers, we created YARA rules which search for suspicious configurations strings (such as those controlling UI elements).

While the Certificate Authority has revoked the abused certificate as of June 2025, numerous variations of the malware remain in circulation using similar techniques. In line with this, we'll be presenting how we have managed to detect this unusual form of malware with the hopes of shifting the balance of power between cyber threats and defense.

CONNECTUNWISE: HOW THREAT ACTORS ABUSE CONNECTWISE INSTALLER AS BUILDER FOR SIGNED MALWARE

Lance Jansen Caoile Go
GData AV Lab Inc

Bio:

Lance Go is a cybersecurity professional with 3 years of experience in the field. He mainly focuses on malware research and is always on the lookout for new and interesting threats. Throughout his career, he has sought out opportunities to learn from more experienced professionals to continuously refine and improve his own workflow. He is currently pursuing a Master's Degree in Computer Science at the University of the Philippines Diliman, where his thesis focuses on image-based malware analysis. Outside of academics and work, Lance enjoys a variety of hobbies including freediving, flying drones, playing badminton, and building automations. His friendly and inquisitive nature allows him to meet people from diverse backgrounds and learn skills across a wide range of fields.

Karsten Hahn
GData Cyberdefense AG

Bio:

Karsten Hahn has a Master's Degree in Computer Science from HTWK Leipzig. His master thesis about static Portable Executable analysis won the FBTI Award in 2015, which is doted at 1000 Euro. Since 2015 he works for GDATA CyberDefense AG. At the time he started as Malware Analyst, moved to a Lead Engineer position in 2022, where he was responsible for protection engineering of GDATA's new MEDR product. He became Principal Malware Researcher in 2024 and is now responsible for threat research, blog article writing and internal trainings.

YET ANOTHER CYBERESPIONAGE OPERATION IN VIETNAM

Abstract:

This presentation examines a cyber-espionage campaign conducted by a Chinese threat actor targeting Vietnamese organizations in early 2024. The attackers deployed a variant of the FinalDraft (SquidDoor) malware via a layered infection chain leveraging LOLBins and COM-based scheduled tasks to evade detection. C2 communication was stealthily handled through Outlook drafts using the Microsoft Graph API.

The malware was heavily obfuscated with junk instructions and nested garbage function calls. To analyze it effectively, we applied symbolic execution with state tracking, enabling the removal of over 30,000 junk instructions and reconstruction of the real execution flow. The final payload included modules for LSASS credential theft, PowerShell execution without powershell.exe, and screen capture.

This talk provides a technical walkthrough of the infection chain, deobfuscation methodology, and post-exploitation modules, highlighting advanced techniques used to maintain persistence and evade defenses.

Tran Duy Nam
VNPT Cyber Immunity

Bio:

Tran Duy Nam is a Threat Analyst at VNPT Cyber Immunity, specializing in advanced persistent threat (APT) tracking, malware behavior analysis, and threat intelligence research. With a deep focus on dissecting malware techniques and understanding adversarial tactics, techniques, and procedures (TTPs), he contributes to proactive cyber defense by identifying emerging threats and providing actionable intelligence. His work bridges technical analysis and strategic threat profiling, helping organizations anticipate and mitigate sophisticated cyber attacks. Passionate about cybersecurity, he continuously develops methodologies to enhance threat detection and incident response capabilities.

AN ANALYSIS OF CLOUD INFRASTRUCTURE UTILIZATION IN MALWARE COMMAND AND CONTROL

Abstract:

In recent years, malware authors have increasingly favored using legitimate cloud platforms such as Telegram, Discord, Google Drive, and Dropbox as Command and Control (C2) channels. This tactic allows malware to evade traditional detection mechanisms and hide in normal user traffic.

In this paper, we analyze real-world malware campaigns that use cloud infrastructure as a control channel, focusing on how cloud APIs are used to steal data, download payloads, and send remote commands. We will present techniques for masking and evading detection, as well as why many current security products fail to detect this method.

In addition, we will present practical methods for detecting and mitigating these threats, including behavioral monitoring, anomaly detection, and threat hunting via cloud telemetry.

This article aims to raise awareness among users and enterprises of this growing trend and provide specific strategies to defend against malware that exploits cloud infrastructure.

Tran Thi Hieu Ngan
CMC Cyber Security

Bio:

Tran Thi Hieu Ngan is a Malware Researcher who began her career as a malware research intern in her third year at university. After earning her bachelor's degree, she pursued a professional path in malware research. Her work focuses on malware analysis, developing advanced detection and remediation technologies, and hunting advanced persistent threats (APT). She is committed to continuous professional development, building the expertise required to proactively safeguard against emerging cyber risks.

Bui Huy Anh
CMC Cyber Security

Bio:

As Head of Anti-Malware Solutions Department, a senior cybersecurity expert with extensive experience in malware research and analysis, Bui Huy Anh plays a key role in researching cyber security threat, designing and implementing advanced security solutions for enterprises, aiming to develop CMC's comprehensive cybersecurity ecosystem, aligned with international standards and capable of responding to sophisticated threats.

THE SILENT INVADERS: UNDERSTANDING AND COMBATING MACOS INFOSTEALERS

Abstract:

macOS infostealers have rapidly evolved into a major cybersecurity threat, with their prevalence doubling in the past year. These threats, often distributed as malware-as-a-service, are increasingly targeting macOS users across industries and geographies. The latest wave of infostealers particularly variants like Atomic Stealer which demonstrate enhanced stealth, persistence, and backdoor capabilities.

This paper investigates how macOS infostealers leverage emerging initial access vectors, including malvertising and the impersonation of trusted applications such as Slack, Homebrew, and more recently, ClickFix – a new method that further expands their reach and deception capabilities. Once inside, they leverage payload encryption, advanced obfuscation, and token regeneration to maintain access and exfiltrate sensitive data, including credentials, browser artifacts, and crypto wallets.

We will analyze infection chains, shared codebases, MITRE ATT&CK mappings, and the broader impact of these threats. The session will also highlight proactive defense strategies, including dynamic detection, user awareness, and endpoint hardening, to counter this growing menace.

Srinivasan Govindarajan
Microsoft

Bio:

Srinivasan Govindarajan is a Senior Security Researcher at Microsoft India, specializing in macOS threat detection and malware analysis. With over 13 years of experience in the cybersecurity domain, he brings deep expertise in reverse engineering, stealthy payload detection, and advanced infostealer campaigns. His work focuses on uncovering sophisticated macOS threats and developing robust detection strategies.

Pranjal Gupta
Microsoft

Bio:

Pranjal Gupta – Security Researcher 2 at Microsoft with 9 years of experience in the cybersecurity domain. Working in the MacOS security research team and has expertise in reverse engineering and malware analysis and security product development.

USING LINGUISTICS AND PSYCHOLOGICAL PROFILING IN THREAT ACTOR ATTRIBUTION

Abstract:

Traditional threat actor attribution primarily focuses on TTPs (Tactics, Techniques, and Procedures), but this method is increasingly ineffective when adversaries employ similar strategies or attempt to mask their identities. This paper introduces an advanced attribution methodology that combines cyber linguistics, behavioral profiling, and Natural Language Processing (NLP). By analyzing linguistic markers such as vocabulary, syntax, tone, intent, and prominent words, alongside sentiment analysis, we identify distinct patterns that differentiate threat actor groups. This approach reveals not only behavioral traits but also the psychological drivers behind attack campaigns. By integrating NLP techniques for tone and intent detection, we provide more nuanced insights into the actors' motivations. This advanced model enhances attribution accuracy, enabling threat intelligence teams to refine defensive strategies and proactively counter emerging threats. This work represents a step forward in making attribution more precise, dynamic, and actionable for the cybersecurity community.

Rishika Desai
BforeAI

Bio:

Rishika Desai is a leading threat intelligence and cybercrime researcher with a strong focus on OSINT and dark web investigations. Featured in Forbes and Dark Reading as a subject matter expert, she was also awarded as Rising Star of the Year 2025 by BSides Bangalore. Rishika regularly shares her insights at global conferences and is known for her engaging, real-world approach to cybersecurity education. As a mentor and founder of a thriving cyber community, she is dedicated to shaping the next generation of cyber defenders.

About SecureIQLab

Independent Cybersecurity Validation for APAC

SecureIQLab is an independent analyst firm specializing in cloud cybersecurity validation that empowers organizations to make confident technology choices through rigorous, transparent testing.

By combining analyst-grade market intelligence with our new SecureIQLab Nepal PVT Ltd., APAC operations, we deliver globally recognized validation services tailored to the region's unique threat landscape, including local attack scenarios.

Core Validation Focus Areas

Our expertise covers critical technologies:

- **Cloud WAAP (Web Application &API Protection)**
- **Advanced Cloud Firewalls (ACFW) / NGFW**
- **Gen AI Security**
- **Enterprise Browsers**
- **Advanced Cloud Firewalls (ACFW) / NGFW**
- **Security Service Edge (SSE) & SASE**

- **NEUTRAL & VENDOR-AGNOSTIC:** 100% independent testing, free from vendor influence.
- **AI-POWERED VALIDATION:** Our SocX® platform evaluates the resilience of modern, ML- driven security tools.
- **STANDARDS ALIGNMENT WITH HOLISTIC VALIDATION:** We measure threat blocking alongside operational impact, including efficiency and usability aligning with global standards like NIST(CSF), OWASP and CISA.

SecureIQLab

Independent, outcome-driven validation

SecureIQLab Nepal PVT, will deliver globally

+977 1-4541540

info@secureiqlab.com

148 Thirbam Sadak, Kathmandu, Nepal

Scan to Contact

BOOKING A THREAT: INSIDE LUMMASTEALER'S FAKE RECAPTCHA

Abstract:

In February 2025, G DATA Malware Analysts observed and closely monitored the occurrence of a threat campaign employing ClickFix, an emerging social engineering technique that manipulates users into executing malicious commands under the guise of resolving a system error or verification. It evades traditional signature-based detections by requiring human interaction, complicating automatic scanning procedures. Since its emergence in 2024, ClickFix has been adopted in multiple malicious campaigns as an initial vector for delivering malicious payloads. Through our internal sourcing, we found out that there are numerous malware families such as VidarStealer, XWormRAT and DonutLoader were actively using ClickFix as their primary vector.

The campaign we investigated leveraged a malware distribution site disguised as booking confirmation pages from well-known travel platforms, which directed users through fake CAPTCHA processes to initiate the ClickFix mechanism. Further analysis confirmed that the final payload delivered through this method was LummaStealer, a widely distributed information-stealing malware commonly sold under the Malware-as-a-Service (MaaS) model.

The research revealed targeted victims in various countries, including the Philippines and Germany. During the investigation, we uncovered two booking itinerary documents showing information details modeled after legitimate platforms such as Booking.com and HR.com. Initially, these documents were addressed to a hotel in the Philippines but were later modified to reference a hotel in Germany, suggesting a potential shift in target or an attempt to evade detection by altering geographical indicators. Unknown to the target victim, malicious scripts are executed that invoke commands to external sources, which ultimately download LummaStealer samples. We also observed how the downloaded LummaStealer samples evolved, from downloading the payload directly to employing advanced obfuscation methods such as Binary Padding and Indirect Control Flow to further evade detection.

This research further explores the unique infection process by which the LummaStealer samples reach the victim's system, as well as other related telemetry observed during this sophisticated campaign. Notably, the samples gathered during the investigation were unique as they cannot be sourced from any public threat sourcing sites.

BOOKING A THREAT: INSIDE LUMMASTEALER'S FAKE RECAPTCHA

Arvin Lauren Tan
G DATA AV Lab Inc.

Bio:

Arvin Lauren Tan is a cybersecurity professional with over 7 years of experience in the industry, specializing in threat research, analysis, and product detection. Throughout his career, he has developed deep expertise in reverse engineering, malware analysis, and threat hunting, protecting individuals and organizations against emerging cyber threats. Outside of work, Arvin maintains an active lifestyle through jogging and biking. He also enjoys both casual and competitive computer gaming as a way to relax, sharpen his strategic thinking, and stay connected to the tech community.

John Rey Dador
G DATA AV Lab Inc.

Bio:

John Rey Dador is an aspiring cybersecurity professional with a strong interest in malware analysis, threat intelligence, and ethical hacking. Although he has only three years of experience in the field, he actively builds his skills through self-study and hands-on practice, always seeking ways to improve and grow. This is his first time attending AVAR or any conference but he is excited and motivated to participate in more as he continues to strengthen his cybersecurity skills. Despite working in tech, he has always dreamed of becoming a professional athlete. He enjoys all physical sports, especially boxing and MMA. More than greatness or glory, what motivates him more is his love for God, his family and his long-time girlfriend.

Arvin Jay Bandong
G DATA AV Lab Inc.

Bio:

Arvin Jay Bandong is a cybersecurity professional with a strong background in software engineering. After spending 3 years as a software engineer, he transitioned into cybersecurity and has since gained 3 years of experience specializing in malware analysis, threat intelligence, and signature creation. Joining a cybersecurity conference for the first time as both a speaker and participant, he looks forward to connecting with professionals in the field and learning new things from them.

HIGH STAKES, HIDDEN THREATS: UNMASKING THE VAULT VIPER NETWORK WITH DNS

Abstract:

Southeast Asia's cyber threat landscape is evolving faster than ever before. This transformation has been marked by the proliferation of industrial scale scam centres and cyber-enabled fraud operations, driven by sophisticated transnational criminal syndicates and interconnected networks of money launderers, human traffickers, data brokers, and other specialist service providers – particularly those involved in casinos and online gambling.

Against this backdrop, in February 2025, Infoblox Threat Intel, in collaboration with the United Nations Office on Drugs and Crime Regional Office for Southeast Asia and Pacific (UNODC ROSEAP), set out to examine a cluster of illegal online gambling platforms. In what followed, Infoblox researchers uncovered one of Asia's leading iGaming software suppliers or 'white labels' distributing a custom browser with significant security implications. Advertised as "privacy-friendly' and able to bypass censorship where online gambling is strictly prohibited. The browser proceeds to route all connections through servers in China and installs several persistent, involuntary programs that run silently in the background – features consistent with remote access trojans (RATs) and other malware.

Through DNS analysis, reverse engineering and threat hunting, as well as more conventional investigative work, Infoblox Threat Intel has been able to end a decade's long mystery, ultimately unmasking the broader criminal network behind this operation and its direct link to the infamous Suncity Group and convicted Triad boss, Alvin Chau. This abstract offers a glimpse into the first public release of what has been dubbed Vault Viper, marking the second in a series of previously unreported threat actors and criminal service providers operating at the intersection of illicit online gambling, cyber-enabled fraud, high-tech money laundering and human trafficking. Building on Infoblox's past Vigorish Viper research, the investigation traces tens of thousands of associated domains – with several still currently in use by documented criminal networks – detailing Vault Viper's vast DNS footprint, command-and-control (C2) infrastructure, unique tooling, and ownership structure concealed through a tangled web of companies registered in dozens of countries.

The presentation will conclude with a discussion around various challenges in investigating, classifying, and disrupting this unique category of threat actor. Attendees will also gain a new perspective on the implications of growing criminal sophistication and professionalism within the regional cyber threat landscape, as well as the value of a DNS-based approach in identifying and disrupting sprawling criminal networks.

HIGH STAKES, HIDDEN THREATS: UNMASKING THE VAULT VIPER NETWORK WITH DNS

Maël Le Touz
Infoblox

Bio:

Maël Le Touz is a Staff Threat Researcher at Infoblox where he specializes in the detection of threats as they manifest in the domain name system (DNS).
His background is in financial fraud investigation and he has strong experience in reverse engineering. He reverse engineered critical components of the Decoy Dog malware that confirmed the DNS C2 was distinct from the open source Pupy project.

He recently focused his research on the Chinese speaking landscape, contributing to the discovery of VIgorish VIper and a number of other criminal syndicates dealing in gambling, malware,scams and trafficking. He was a speaker at a number of cyber security conferences including Black Hat, Infosecurity and Les Assises.

John Wojcik
Infoblox

Bio:

John Wojcik is a Senior Threat Researcher at Infoblox where he specializes in DNS threat intelligence and cyber and cyber-enabled crimes in East and Southeast Asia. As part of Infoblox's Threat Intel, he works with governments and enterprises in the region to strengthen resilience against evolving and accelerating cyber risks through DNS.

John joins Infoblox as a former Senior Analyst with UNODC's Regional Office for Southeast Asia and the Pacific in Bangkok, Thailand, where he led the agency's open-source and criminal intelligence portfolios, specializing in cyber-enabled fraud, high-tech money laundering, and virtual assets.

At Infoblox, he focuses on DNS threat intelligence and supporting Protective DNS adoption, where his research aims to demonstrate how visibility and intelligence at the DNS layer can serve as key line of defense against modern-day threats. He continues to share his expertise to strengthen resilience and support the broader security community.

LOTUS IN PERPETUAL BLOOM: SUSTAINED ESPIONAGE IN SOUTHEAST ASIA WITH EVOLVING SAGERUNEX BACKDOORS

Abstract:

Lotus Blossom is an advanced Chinese-speaking threat actor that has been consistently targeting critical sectors, including government, manufacturing, telecommunications, and media in Philippines, Vietnam, Hong Kong, and Taiwan. While tracking this actor, we have discovered its latest activities that were conducted between 2018 to the end of 2024 and we believe they are still active now. So, what tactics did Lotus Blossom use in these attacks, and most importantly, how can we defend against them?

To answer these questions, we will first discuss how Lotus Blossom was initially infecting networks of target organizations. Following that, we will discuss the advanced persistence methods employed by Lotus Blossom, including installing the Sagerunex backdoor in system registries, the WMI commands that how they do lateral movement, leverage several hacking and open-source tools and operating multiple stages in every campaign. Each stage is carefully executed, indicating a well-planned strategy aimed at achieving long-term objectives. Furthermore, we identified two new Sagerunex variants that mark a significant evolution in their operations. These variants no longer rely on traditional Virtual Private Server (VPS) infrastructure for command-and-control (C2) communications. Instead, they utilize legitimate third-party cloud services such as Dropbox, Twitter, and the Zimbra open-source webmail platform as C2 tunnels, demonstrating enhanced stealth and detection evasion capabilities.

We will then use all the presented information to compare recent attacks of Lotus Blossom with the ones conducted a few years ago and identify common flaws in the actor's offensive strategy. In turn, finding these flaws will allow us to discuss how to build an efficient defense strategy against further Lotus Blossom attacks.

Joey Chen
Cisco

Bio:

Joey Chen is working as a cyber threat researcher for Cisco Talos in Taiwan. His major areas of research include incident response, APT/cybercrime investigation, malware analysis, and cryptography analysis. He has been a speaker at Botconf, HITB, Virus Bulletin, CODEBLUE, and HITCON. Now he is focusing on the security issues of targeted attacks, emerging threats and IOT systems. He also develops an automation intelligence platform to help his team get more sleep at night.

NTLM EXPLOIT REDUX!

Abstract:

Amidst endemic cyber warfare, 2025 has been witnessing a resurgence of credential relay attacks targeting Windows environments to infiltrate government, organisation and individual infrastructure. CISA has reported that the NTLM relay technique is being actively exploited by APT groups such as Fancy Bear (aka APT28), Cozy Bear (aka APT29), Blind Eagle (aka APT-C-36), and UAC-0194.

In March 2025, two closely-linked vulnerabilities, CVE-2025-24054, an SMB hash disclosure spoofing vulnerability, and CVE-2025-24071, a file explorer spoofing vulnerability, were patched by Microsoft. Minimal interaction, like clicking on a file or extracting an archive, could lead to a successful exploitation of these vulnerabilities, resulting in dispatching NTLM hashes over the network into hostile hands. The vulnerabilities' root cause can be traced to the flawed implementation of Windows' handling of URL values present in library files (extension .library-ms), thus triggering an SMB request for any UNC paths encountered. The in-the-wild exploitation of CVE-2025-24054 was attributed to Fancy Bear, targeting governments in Poland and Romania. Working exploit code has been reportedly available for sale on the Dark Web.

CVE-2025-33073, an SMB client Elevation of Privilege (EoP) vulnerability, patched in June 2025, is an NTLM reflection attack, wherein the victim's machine is tricked into performing a local NTLM authentication over SMB giving SYSTEM level access to the attacker. This happens as a result of bypassing security checks when processing a request involving a DNS record that contains a marshalled string (i.e. a server name appended with a magic string generated by encoding server information used for Kerberos authentication) as the domain name. Even though the exploit PoC for the vulnerability was available as soon as the vulnerability was patched, there are no reports of its active in-the-wild exploitation at the time of writing this abstract.

Our previous research on NTLM disclosure vulnerabilities such as CVE-2021-36942 in Windows Local Security Authority (LSA) and CVE-2023-23397 in Outlook, both of which were exploited in-the-wild, provides us with key insights on today's exploitation mechanisms. Credential relay attacks are clearly far from over, and understanding the low-level kinetics behind these attacks will help defend against such exploitations.

In this presentation, we will detail the root causes leading to the relay attacks based on the exploitation of CVE-2025-24071 and CVE-2025-33073, aided by live demos for both. We will also analyse diffed code that reveals Microsoft's patches to prevent exploitation of these vulnerabilities. Finally, we will highlight some best practices to defend against these attacks.

NTLM EXPLOIT REDUX!

Anurag Shandilya
K7 Computing Pvt Ltd

Bio:

Anurag Shandilya is the Vulnerability Research Manager at K7 Labs. His areas of research include Windows and IoT vulnerabilities. He has 9+ years of experience in Vulnerability Research and Vulnerability Assessment & Penetration Testing (VAPT). He has presented at AVAR (2018, 2020, 2021 and 2022), VB (2019, 2023) and CARO (2020) and actively contributes to the K7 Labs blog.

Arnab Mandal
K7 Computing Pvt Ltd

Bio:

Arnab Mandal is a Vulnerability Researcher in K7 Labs specializing in Windows Exploitation Techniques. His analyses of various Windows vulnerabilities are detailed on K7 Labs' technical blog page. He also specializes in identifying, and mitigating vulnerabilities across web and mobile applications, network infrastructure, and APIs.

Satyam Yadav
K7 Computing Pvt Ltd

Bio:

Satyam Yadav is a Vulnerability Researcher for K7 Computing, specializing in n-day vulnerability analysis in Windows systems. He also brings expertise in identifying and mitigating security risks across web applications, network infrastructure, and APIs. He writes technical blogs that are published on the K7 Labs technical blog page. Additionally, he also authors IDS detection signatures for K7 products.

SESE: SOCIAL ENGINEERING SECOND EDITION

Abstract:

The Second Edition (SE) of Social Engineering looks at how social engineering has changed—and gotten more dangerous—with the rise of tools like large language models (LLMs), artificial intelligence (AI), and deepfakes. What used to be a hands-on process of tricking people with emails or phone calls has evolved into automated, highly convincing attacks. Now, AI can write messages that sound exactly like a real person, carry on believable conversations, and target victims with scary accuracy, all at scale. These tools have made it easier than ever for attackers to fool people quickly and effectively.

Deepfakes and AI-driven profiling have taken things even further. Scammers can now create fake videos and voice clips that look and sound just like someone you know—bosses, coworkers, family members. With so much personal data online, AI can tailor scams specifically to each target's behavior, interests, and fears. That means the attacks feel more real and are harder to detect. And no one's safe: younger people get flooded with slick scams and misinformation, working professionals face AI-powered impersonation in their inboxes, and older adults are hit with new tricks that go way beyond what they've seen before.

In the presentation, we'll show a mix of classic and newer, more advanced social engineering attacks—and take a look at what's coming next. The future of this space is moving fast, and with AI getting smarter and quantum computing on the horizon, we're already imagining what a Third Edition might look like. One thing's clear: staying ahead of these threats means rethinking how we protect ourselves and building awareness across all ages and industries.

Righard Zwienenberg
ESET

Bio:

Zwienenberg began his work with computer viruses in 1988 after encountering his first virus issues at the Technical University of Delft. This experience sparked his interest in virus behavior, leading him to study and present solutions and detection methods ever since. Over nearly four decades, he has worked for various companies, including CSE Ltd., ThunderBYTE, Norman, and ESET. He has also held or continues to hold positions in several industry organizations, such as AMTSO, AVAR, the WildList, IEEE ICSG, and serves on the Advisory Board for Europol's European Cyber Crime Center (EC3) and Virus Bulletin. He also runs his own computer security consultancy company (RIZSC).

Zwienenberg has been a member of CARO since late 1991. He is a frequent speaker at conferences, including Virus Bulletin, EICAR, AVAR, FIRST, APWG, RSA, InfoSec, SANS, CFET, ISOI, SANS Security Summits, IP Expo, government symposia, SCADA seminars, and other general security events. Beyond his professional work in security, his hobbies include playing drums, performing magic, modeling balloons, restoring ancient computers, and much more.

SESE: SOCIAL ENGINEERING SECOND EDITION

Eddy Willems
WAVCi

Bio:

Eddy Willems is a worldwide known cyber security expert from Belgium. He is a board member of 2 security industry organizations, EICAR and LSEC, and is independent Security Evangelist at WAVCi, his own company. In 1989, Eddy was introduced to the early cyber security industry due to an incident with the very first ransomware, the AIDS information trojan. Willems still owns the last remaining physical copy worldwide. Since 1989, he is Belgian's internationally most quoted cyber security expert. He became a founding member of EICAR in 1991, one of the world's first security IT organizations. Eddy has been working for nearly 4 decades as cyber security expert for several security companies like G DATA, Kaspersky and Westcon. He is also COO of CSA (Clean Software Alliance) since 2024. In 2013 he published his first book 'Cyberdanger' in English, German and Dutch. He is also co-author of the SF cyberthriller 'The Virus' (Dutch 2022, English 2025). Eddy is a known inspiring speaker and is giving lectures and presentations (including TEDx) worldwide for a very diverse audience from children to experts.

VALLEYRAT UNLEASHED: A DEEP DIVE INTO ITS MODERN ARSENAL AND TACTICS

Abstract:

Reported cases increased sharply from late 2024 to 2025. We observed attacks by SilverFox primarily targeting Chinese-speaking individuals in Southeast Asia and East Asia, abusing multiple legitimate software programs, including fake LINE installers, to spread ValleyRAT. Further investigation revealed that the attacks were not limited to LINE and that a variety of software programs were being exploited.

ValleyRAT was thought to be original malware exclusive to SilverFox, but source code and a builder are in circulation, and the builder was released at least as early as February 2023. As a result, as of July 2025, attacks using various execution chains are being carried out using this malware.

ValleyRAT's attack chain is often distributed as a fake software installer using SEO poisoning or phishing emails. However, espionage-like attacks have also been reported, such as spear-phishing emails targeting businesses, such as government agency communications or invoices.

ValleyRAT uses a wide variety of tools and techniques. In this presentation, we will organize attacks using ValleyRAT observed since 2025 by the following execution chain:

- DLL side-load fake installer

- Payload embedded in the image (a.k.a. PNGPlug)

- Go-Lang

- APT-like Masquerading Loader

- Donuts

During our investigation, we discovered new patterns using WinRAR SFX and Go language loaders. We also found cases where the same export name as MustangPanda was used in DLL side-loading in ValleyRAT's execution chain.

For each execution chain, we will analyze the targets, TTPs, and C2 infrastructure, and propose a classification of ValleyRAT's attack campaigns. Finally, we will share hunting techniques for ValleyRAT (Winos 4.0).

VALLEYRAT UNLEASHED: A DEEP DIVE INTO ITS MODERN ARSENAL AND TACTICS

Hiromu Kubiura
LY Corporation

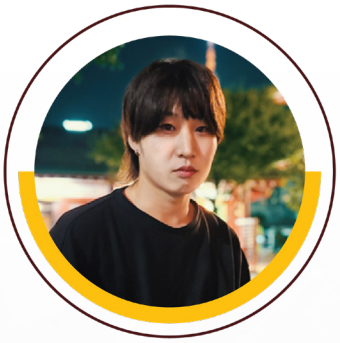
Bio:

At LY Corporation, I conduct threat intelligence focused on malware analysis and phishing countermeasures. I have presented at Black Hat USA Arsenal and BSides Tokyo.

Ryonosuke Kawakami
Cyber Defense Institute, Inc

Bio:

Ryonosuke Kawakami is a threat researcher at Cyber Defense Institute with deep expertise in malware analysis and reverse engineering. His work focuses on tracking APT campaigns, reverse engineering malware, and conducting memory forensics. He turns low-level findings into action—deobfuscating code, profiling C2, and informing APT attribution.



Shota Nakajima
Cyber Defense Institute, Inc

Bio:

Shota Nakajima is a Tech Lead of Threat Intelligence at the Cyber Defense Institute, Inc. He specializes in malware analysis, with deep expertise in reverse engineering. In the field of threat intelligence, he actively tracks the latest Advanced Persistent Threats (APTs) and has presented his extensive research at numerous international conferences, including JSAC, VB, HITCON, AVAR, CODE BLUE and Black Hat Arsenal. Leveraging his specialized knowledge, he is also dedicated to developing practical and effective threat intelligence products.

MODERN FILELESS RAT TACTICS: NODE.JS ABUSE : TECHNICAL ANALYSIS AND THREAT ATTRIBUTION

Abstract:

This presentation explores a modern threat that leverages Node.js to operate entirely in memory, bypassing traditional endpoint protections. The malware analyzed is a fileless remote access trojan written in JavaScript, designed to evade detection and provide persistent control over compromised systems. Delivered through socially engineered lures, such as fake job interview processes and CAPTCHA forms, this malware reflects tradecraft frequently linked to North Korean state-sponsored groups.

Once deployed, the RAT establishes communication with a command-and-control server using XOR-obfuscated and compressed HTTP traffic. It supports advanced features such as SOCKS5 proxy tunneling and is equipped with anti-analysis mechanisms, including virtual machine detection to avoid sandbox environments. These characteristics allow it to remain hidden in enterprise environments while enabling adversaries to maintain long-term access.

To fully understand its behavior and control mechanisms, we reconstructed and operated a replica of the command-and-control infrastructure. This reverse engineering effort revealed the malware's operational commands, communication patterns, and the level of control it grants to attackers. Our findings indicate a broader trend in the adoption of Node.js for malware development, due to its flexibility, cross-platform capabilities, and lower detection footprint.

This session will detail the technical architecture of the malware, walk through the infection chain, and share behavioral patterns useful for detection. We will also map the observed tactics to threat actor activity, presenting strong links to campaigns attributed to the Lazarus group. The talk includes detection strategies, YARA rules, and endpoint artifacts for defenders to use in their environments.

Attendees will leave with a deeper understanding of emerging JavaScript-based threats, attacker tooling evolution, and practical insights for threat hunting and incident response in enterprise networks.

Reegun Richard Jayapaul

Bio:

Director of Threat Research at Cyderes with over 14 years of experience in threat research, malware analysis, reverse engineering, incident response, and offensive security. I build solutions to help organizations defend against evolving cyber threats.

My team regularly publishes new research and contributes to the broader security community. I'm an active contributor to the LOLBAS project, documenting how attackers abuse legitimate binaries to bypass security controls.

I've reported critical vulnerabilities, including a remote code execution flaw in Microsoft Teams, and led investigations into major malware campaigns such as GoldenSpy and GoldenHelper. I use threat intelligence to shape proactive defense strategies and improve detection capabilities.

GENERATIVE AI, RETRIEVAL-AUGMENTED GENERATION (RAG) AND AGENTIC AI IN OFFENSIVE CYBER OPERATIONS

Abstract:

In this talk, we begin with taking stock of how Generative AI (GenAI) has influenced the conduct of offensive cyber operations, primarily improving the adversary's operational effectiveness. With Aquatic Panda (aka Charcoal Typhoon), a prolific China-nexus adversary as the frame of reference, we will discuss how the current state of GenAI can improve the adversary's tactics, techniques, and procedures (TTPs).

Following then, we will look into how Retrieval-Augmented Generation (RAG) can be applied to generate novel TTPs that would materially enhance an adversary's offensive capabilities. We will conclude the discourse with a brief prognosis of the impact that Agentic AI could have on offensive cyber operations, particularly in the areas of autonomous operations, agent specialisation, and false flag operations.

Aaron Aubrey Ng
Stanford University

Bio:

Aaron is a Senior Systems Engineer at CrowdStrike where he advises customers on their security needs and solutions. He is based in Dubai and supports the CrowdStrike business across the Middle East, Turkey, and Africa (META) region. As a security and intelligence evangelist. Aaron speaks at various security conferences including BlackHat MEA, DeepINTEL, MENA ISC, GovWare, RootCon, AVAR, BSides, SINCON, and StandCon.

Prior to joining industry, Aaron served 12 years of Active Duty in the Singapore Armed Forces as a Military Intelligence Officer. He served in multiple command appointments in classified Intelligence units, and garnered staff experience in the areas of strategic planning and policy development. In his penultimate tour of duty, Aaron was instrumental in developing the masterplan for the Digital and Intelligence Service (DIS), the digital service branch of the SAF.

Outside of work, Aaron contributes to cybersecurity research and education. He collaborates with the Stanford Gordian Knot Center for National Security Innovation on research covering China's cyber capabilities. Aaron is also serving as an Adjunct Faculty member at the Faculty of Computer Information Science at the Higher Colleges of Technology (HCT) in the UAE, and is currently undergoing the Instructor Development Program with the SANS Institute.

BEYOND PEN TESTS & RED TEAMS: A NEW APPROACH TO MEASURING ENTERPRISE CYBERSECURITY EFFECTIVENESS

Abstract:

Enterprises are investing heavily in next-generation security technologies—WAAP, XDR, EDR, SASE, and AI-based detection systems—yet successful breaches continue to outpace these defenses. Despite impressive claims, many cloud and hybrid security stacks fail against similar core weaknesses: poor API hardening, weak path traversal protections, and incomplete input sanitization.

This presentation explores real-world case studies and controlled red-team assessments that reveal how even top-tier security platforms can collapse under modest, targeted attacks. We examine why architectural complexity, vendor abstraction, and misplaced confidence in "intelligent" automation often create exploitable blind spots that traditional testing fails to uncover.

AI-driven defenses promise smarter detection, but bolting on machine learning for marketing appeal rarely translates to measurable resilience. We demonstrate which AI security implementations show genuine effectiveness in practice—and which remain superficial bolt-ons that satisfy compliance rather than defense.

Finally, we introduce a practical framework for evaluating your own security stack: how to test it neutrally, quantify real defensive performance, and separate genuine protection from expensive illusion. Attendees will gain a clear, evidence-based understanding of why cloud defenses often underperform, how to measure their effectiveness in realistic conditions, and what practical changes actually close the gap between investment and security.

Bijay Limbu Senihang
SecureIQLab

Bio:

Bijay Limbu Senihang is the Country Director (APAC) at SecureIQLab, leading regional strategy, enterprise engagement, and advanced security validation programs. He brings 14 years of cybersecurity experience spanning penetration testing, security auditing, cyber defense, and independent product validation.

At SecureIQLab, Bijay plays a key role in expanding the adoption of scientific, evidence-driven validation methodologies for modern security technologies, including WAAP, XDR, ACFW, SASE, and AI-driven security platforms. He works closely with cybersecurity researchers, security engineering teams, and global vendors to strengthen and elevate the capabilities of security products worldwide.

He began his career as a penetration testing engineer before becoming an Information Security Auditor, completing more than 200 audits for financial institutions across Asia. He later built Nepal's first Security Operations Center and, for the past five years, has focused on independent cybersecurity product validation to help enterprises understand the real-world effectiveness of their security technologies.

Bijay is also the author of *The Vulnerability Paradox: Unraveling Why We Keep Building Insecure Software.*

Independent Tests of Cybersecurity Solutions

AV comparatives

Analyst firms who rely on AV-Comparatives Test data

IDC

FROST & SULLIVAN

FORRESTER®

Gartner®

kuppingercole ANALYSTS

Omdia by informa techtarget

Where Security Meets Trust

UNBIASED. TRANSPARENT. TRUSTED.

www.av-comparatives.org

UNMASKING AI-THEMED MALVERTISING TARGETING SOCIAL MEDIA USERS

Abstract:

Social media platforms provide cybercriminals with significant opportunities to launch malicious attacks against unsuspecting users. One prevalent infection vector is malvertising, where threat actors craft compelling posts tied to trending topics, such as generative AI or major global events, and exploit ad networks to maximize their reach. These deceptive posts often include links to fraudulent domains impersonating legitimate AI tools, enticing users to download and install malicious payloads. These payloads typically contain info-stealers capable of exfiltrating sensitive personal data, such as login credentials or financial details, which can be used to gain unauthorized access or hijack victims' social media accounts.

In this presentation, we examine the current landscape of malvertising on social media platforms and analyze the most common techniques employed by cybercriminals to deceive users. We will focus on a prolific AI-themed malvertising campaign, dissecting its entire infection chain from initial engagement to payload delivery. Examples of fake and hijacked Facebook pages, boosted malicious posts, and distributed malicious packages will be presented. We will demonstrate our approach to analyzing these often multi-layered, obfuscated packages and extracting critical artifacts, such as campaign IDs and command-and-control (C&C) servers, from the samples.

Additionally, we will analyze several notable malware families observed in the wild, including:

Remote Access Trojans (RATs) like XWorm, PureHVNC with advanced data-stealing capabilities

Information stealers, such as Noodlophile, written in .NET or Python

Finally, we will share our threat-hunting techniques and discuss the primary targets of these campaigns, providing insights into mitigating such threats.

Jaromír Hořejší
Check Point

Bio:

Jaromír Hořejší is a Security Researcher at Check Point Research, specializing in tracking and reverse-engineering threats, including APTs, DDoS botnets, banking trojans, click fraud, and ransomware targeting Windows and Linux systems. His work has been presented at leading conferences such as RSAC, SAS, Virus Bulletin, HITB, FIRST, AVAR, Botconf, and CARO.

AI VOICE HONEYPOTS – TURNING SCAM CALLS INTO REAL-TIME THREAT INTELLIGENCE

Abstract:

AI-powered voice scams are exploding. Voice cloning and scripted dialogues have made it nearly impossible to distinguish legitimate phone calls from fraudulent ones. So, we decided to fight fire with fire.

The AI Voice Honeypot is a system designed to engage scam callers and transform those conversations into real-time threat intelligence. Using synthetic personas tailored for specific scam scenarios, the system responds like a real victim, detects manipulation tactics, and extracts Indicators of Compromise (IoCs): phishing URLs, mule account probes, and other attack vectors. We perform real-time classification and assessment of scam calls, enriching each interaction with contextual insights and extracted signals.

This presentation will cover:

- How speech-to-text, large language models, and threat intelligence are chained to analyze scam behavior mid-call
- How IoCs are harvested and enriched automatically, feeding detection pipelines and user-facing protections
- How synthetic personas are leaked into attacker ecosystems to attract scam calls
- How leaks and conversations are linked via RAG systems, augmenting LLM understanding and enabling traceability
- How ethical and legal guardrails are enforced around synthetic voice interactions, including challenges like staying in character, avoiding deception that crosses legal lines, managing angry callers, and responding to sensitive prompts such as confirming fake purchases

Attendees will gain insights into the design considerations, system behavior, and challenges of using conversational AI in adversarial settings and how voice interaction itself can become a powerful source of threat intelligence.

AI VOICE HONEYPOTS – TURNING SCAM CALLS INTO REAL-TIME THREAT INTELLIGENCE

Claudiu Laurentiu TIRISI
Bitdefender

Bio:

Claudiu is a security researcher at Bitdefender, specializing in building Honeypot systems to fight against voice scams using the power of generative AI and some human inspiration. He completed his Computer Science degree in 2024 with a thesis on Image Generation Techniques and is currently studying for a Machine Learning Master's. You can usually find him bobbing his head to music.

Alexandru Paul MARINESCU
Bitdefender

Bio:

Alexandru Marinescu is a Technical Manager at Bitdefender, with over ten years of experience in Mobile Security and Forensics. He has contributed to advanced cybersecurity technologies, particularly in threat detection, anomaly analysis, and threat intelligence. Outside the professional realm, he enjoys skiing, hiking, and trail running.

IDFKA BACKDOOR: THE HIDDEN THREAT OF RUST IMPLANTS IN MODERN APT CAMPAIGNS

Abstract:

In the spring of 2025, we investigated an incident in which attackers exploited a PostgreSQL vulnerability to achieve remote code execution and deploy TinyShell. The adversaries demonstrated exceptional tradecraft: nearly all traces were wiped, malicious processes masqueraded as legitimate ones (e.g., "postgres: reader process"), and the implant existed solely in memory. SIEM analysis revealed C2 servers with domains spoofing the victim's infrastructure and its ISP, including an address belonging to a third-party contractor. Further investigation within the contractor's environment uncovered a custom Rust-based implant that the threat group had operated for over a year while remaining undetected. Subsequent analysis confirmed that other major organizations had also been compromised by this sophisticated APT campaign.

The identified implant supports a broad range of operational modes: from passive and active TCP to ICMP, implemented via raw sockets or the libpcap library with ICMP packet filtering. It also features so-called "magic" modes — spootftcp, magictcp, active and passive knock (port knocking), as well as a mode called future. The implant can conceal its own process and persist its last received configuration.

In this talk, we will:

- Dive deep into its operational modes, protocol implementation details, network infrastructure, and the full capabilities of the embedded backdoor.
- Share our experience — and the pain — of reverse engineering Rust malware, a language that, in the hands of attackers, turns into a true nightmare for analysts.
- Attempt to answer one lingering question: is its name somehow tied to the legendary DOOM?

This implant is unlike anything previously observed in the wild and undoubtedly deserves the attention of the community.

IDFKA BACKDOOR: THE HIDDEN THREAT OF RUST IMPLANTS IN MODERN APT CAMPAIGNS

Vladimir Stepanov
Rostelecom-Solar

Bio:

Vladimir Stepanov began his career as a malware analyst in 2021.

Since 2024, he has been working at the Solar 4RAYS Cyber Threat Research Center, specializing in reverse engineering APT malware and public reporting. Vladimir has public speaking experience at multiple private and public events, including OffZone Cybersecurity Conference and others. His threat research articles are regularly published in Solar 4RAYS blog.

Anna Mazurkiewicz
Rostelecom-Solar

Bio:

Anna Mazurkiewicz is Incident Response Engineer at Solar 4RAYS Cyber Threat Research Center. Having moved from a Linux system administrator position more than 2 years ago, she possesses a versatile outlook on large IT systems and communication between a customer and a cybersecurity provider. She participates in large-scale cybersecurity incidents as DFIR Engineer and contributes to public Solar 4RAYS research.

THE OPEN DOORX : FROM DIRECTORY LISTING TO ATTRIBUTION

Abstract:

In July 2024, during the course of our threat research, we identified an interesting web server with directory listing enabled. Among the available files, we discovered an ELF binary named “doorX”, which became the subject of our investigation. This sample was later recognised as part of a malware family that came to be widely known as “Auto-Color”.

In this presentation, we will begin by analyzing the doorX malware, outlining its functions and key characteristics. Particular emphasis will be placed on its techniques for evading detection and hindering analysis – including its implementation of covert communications and encrypted traffic.

We will then share our findings about the web server where doorX was discovered, focusing on the files hosted there. Of particular interest was the presence of ShadowPad, a well-known modular backdoor. We will provide a brief overview of both the loader and main component of ShadowPad that we identified on the server. Finally, we will examine advanced attack groups that use doorX, including various elements such as ShadowPad. We believe this is the first time that publicly available information has mentioned APT actors related to doorX.

By the end of this talk, attendees will gain a detailed understanding of doorX’s behaviour and operational context, and will be better informed about the actor using it. This knowledge will help SOC, IR, and CSIRT professionals to develop effective countermeasures against malware campaigns involving doorX.

Shogo Hayashi
NTT Security Holdings

Bio:

Shogo Hayashi is a security analyst at NTT Security Holdings. His main specialization is responding to EDR detections, creating detection rules, analyzing malware and research cyber threat. He is a cofounder of SOCYETI, an organization for sharing threat information and analysis technique to SOC analysts in Japan. He has spoken at AVAR, JSAC, VB, SAS, CODE BLUE and has written several white papers and blogs.

Nobuyuki Amakasu
NTT Security Holdings

Bio:

Nobuyuki Amakasu is a security analyst at NTT Security Holdings, mainly engaged in EDR log analysis, malware analysis and research cyber threat. He previously worked as an SE, responsible for system construction (amongst other things), and has been in his current position since 2018.

MEET VENOMSEO: NEW THREAT TARGETING MALAYSIAN WEBSITES FOR BLACK SEO

Abstract:

In this presentation, we will talk about VenomSEO, a newly identified advanced persistent threat (APT) group targeting governmental and corporate websites running on Linux platforms in Malaysia with the aim of facilitating Black SEO operations.

The group's primary objective appears to be the compromise of web servers for traffic redirection and monetized search engine manipulation.

We will delve into a recent case study involving a targeted attack on a Malaysian company, shedding light on VenomSEO's infiltration strategies and post-exploitation activities.

Further investigation has revealed that similar compromises have occurred across multiple countries, including Brazil, India, and Thailand.

VenomSEO employs a sophisticated arsenal of attack techniques, including zero-day exploits, web shells, privilege escalation, backdoors, rootkits, and credential harvesting tools. We will analyze their tactics, techniques, and procedures (TTPs), offering insights into detection, mitigation, and defense strategies against this emerging threat.

Igor Zdobnov
Doctor Web, Ltd.

Bio:

Igor Zdobnov joined Doctor Web in 2002 as a malware analyst and since 2009 has been working as a chief malware analyst. He is leading different security projects inside the company, threat intelligence, threat detection and prevention. He is passionate in malware analysis, reverse engineering and building machine learning malware detection systems.

Ivan Korolev
Doctor Web, Ltd.

Bio:

Ivan Korolev joined Doctor Web in 2014 as a malware analyst and since 2019 has been working as a team leader for botnet research team. He is focused on analyzing targeted attacks, botnets and emerging threats. He likes to find vulnerabilities and participate in bug bounties in spare time.

FROM CODE TO CLUES: LEVERAGING LLMS TO RAT OUT ANDROID SPYMAX

Abstract:

SpyMax, a.k.a. SpyNote, has been one of the most prevalent Android Remote Access Trojan (RAT) families since the initial strains seen in 2020, and has proven quite arduous to reverse engineer till date.

The difficulty is primarily due to challenging techniques employed by the threat actors like multistage dynamic deobfuscation and loading, and encrypted/G-Zip compressed network traffic with non-standard or custom protocols.

SpyMax has wide-ranging adversarial capabilities, viz. GPS tracking, ability to record and send videos to C2, extraction of Google Authenticator codes, simulation of user gestures, exfiltration of sensitive information. In short, it has the ability to take over complete control of the compromised device by abusing accessibility permissions.

Notably, we have seen a recent surge in the number of SpyMax infections in the Asian region, with prominence in India, following the source code leak of CypherRat (a variant of SpyMax) in 2022. Victims have had significant financial losses, typically in the range of ₹15,000-25,000 (US$ 170-280) per victim, but this is just the tip of an iceberg, based on incidents wherein we have first hand information. The total corpus of losses is likely huge given the prevalence and reach of this RAT.

Enter AI and LLMs, technologies that have been transforming reverse engineering and malware analysis. Employing AI-aided frameworks like LLM-MalDetect and Llama, with well-crafted, optimized prompt engineering, helped us decode SpyMax's dynamic loading and encrypted network traffic techniques efficiently and effectively. These tools managed partial de-obfuscation of the Java class files, revealing certain aspects of the original code's intent. Undoubtedly, the results proved far superior to the output from traditional Android reversing methods and tools.

In this talk, we will delve into SpyMax's internal architecture, analysing its obfuscation mechanism, payload delivery strategies and C2 infrastructure, based on our deep analyses of two damaging, insidious real-world incidents involving malware distribution via Telegram and WhatsApp. Further, we intend to play Devil's Advocate vis-a-vis the leveraging of LLMs for Android malware analysis, showcasing their efficacy in reversing difficult samples, yet highlighting some of the potential pitfalls to watch out for.

Baran Kumar S
K7 Computing Pvt Ltd

Bio:

Baran Kumar S, a Senior Threat Researcher at K7 Labs, plays a crucial role in identifying, analyzing, and mitigating emerging cyber threats. With a Master's degree in Computer Applications earned in 2002, Baran has over two decades of experience and expertise in the cybersecurity domain.

He began his professional journey as a Technical Support Engineer at K7, gaining valuable hands-on exposure to customer issues and real-world security challenges. Over the years, he transitioned into threat research, developing deep knowledge of malware analysis, reverse engineering, and threat intelligence across both Windows and Android platforms.

His work involves dissecting malicious software, understanding attacker techniques, and crafting detection strategies to protect users worldwide. Passionate about cybersecurity, Baran regularly shares his findings on the K7 Labs technical blog. His articles often explore the latest trends in mobile threats, offering readers valuable insights into emerging risks and best practices for digital safety.

WHEN FIREWALLS GO BLIND: CUSTOM TOOLS, AI AGENTS, AND THE FALL OF TRADITIONAL NETWORK INSPECTION

Abstract:

As TLS adoption surpasses 90% of global web traffic, the visibility once provided by deep packet inspection (DPI) is rapidly fading. Full SSL/TLS decryption—once a pillar of network threat detection—has fallen out of favor due to performance degradation, operational complexity, legal concerns, and evolving protocols like HTTP/3, QUIC, and encrypted DNS. As organizations move toward zero trust and adopt cloud-native security like SASE (Secure Access Service Edge), the practicality of full-payload inspection continues to decline.

Here, we explore how this reduced visibility affects threat detection, particularly as attackers leverage generative AI to craft exploits, obfuscate payloads, automate reconnaissance, and scale phishing attacks with unprecedented precision. AI agents and LLMs have significantly lowered the barrier to entry for complex attack campaigns, which now blend seamlessly into encrypted traffic flows.

We compare how traditional NGFWs and SASE platforms handle SSL decryption today, analyze their limitations in modern encrypted environments, and evaluate how security features like HSTS, certificate pinning, and DNS-over-HTTPS break legacy inspection methods. The paper also examines how attackers increasingly craft “signatureless” payloads, rendering DPI ineffective without access to decrypted traffic. As payload access becomes rare, defenders must shift toward metadata inspection, behavior-based analytics, and AI-driven anomaly detection.

This work highlights the pressing need to rethink network security visibility in an encryption-first, AI-assisted threat landscape. It calls for new strategies that balance privacy, performance, and detection fidelity, and maps a path forward for enterprises caught between compliance limitations and escalating adversarial capabilities.

WHEN FIREWALLS GO BLIND: CUSTOM TOOLS, AI AGENTS, AND THE FALL OF TRADITIONAL NETWORK INSPECTION

Sangay Lama
SecureIQLab

Bio:

Sangay Tamang is a Security Researcher and Team Manager at SecureIQLab LLC, where he leads the Security Research and Validation division. He specializes in evaluating cloud-native security platforms, including Web Application Firewalls, API protection, and next-generation cloud firewalls, against real-world threats. Sangay has led multiple validation projects with industry-leading vendors, producing widely recognized comparative reports. Alongside his research, he has contributed to academia as a tutor and project supervisor, mentoring students in networking, robotics, and IoT. His passion lies in applied cybersecurity research, developing custom tools, and advancing strategies for resilience in an encryption-first world.

Cameron Camp
SecureIQLab

Bio:

Cameron Camp, CISSP, is a Senior Security Researcher at SecureIQLab with extensive security background all the way up the stack from embedded hardware, firmware and IoT hacking, to medical devices and industrial control systems, with a specific focus on Linux-powered platforms. He's now focusing on cloud security, with an emphasis on understanding how to secure the connective tissue holding all the pieces together in an adversarial environment.

EMMENHTAL LOADER: THE SILENT ENABLER OF MODERN MALWARE CAMPAIGNS

Abstract:

Modern malware distribution is evolving, with commodity loaders transforming into sophisticated Malware-as-a-Service (MaaS) platforms. One such loader, Emmenhtal, has emerged as a key player in financially motivated cybercrime, initially used to distribute infostealers like CryptBot and Lumma. However, recent campaigns indicate a strategic pivot, integrating Emmenhtal with SmokeLoader, a well-established modular malware known for code injection, persistence, and stealthy payload execution. The discovery of this new method remains largely unknown to the public.

This research dissects Emmenhtal's evasive execution flow, its strategic abuse of Living Off the Land Binaries and Scripts (LOLBAS) like Mshta and PowerShell for covert operation, and its growing significance in the Malware-as-a-Service (MaaS) landscape.

The primary focus of our research is on the observed recent attack on First Ukrainian International Bank (pumb.ua), Emmenhtal facilitated a multi-stage infection chain designed to bypass traditional security controls. The campaign began with a phishing email attached with a 7z archive containing a bait PDF and a downloader shortcut, leading to the retrieval of a malicious .lnk file. This .lnk leveraged Mshta to execute a hidden HTA script embedded inside a trojanized DCCW.exe binary, maintaining a stealthy footprint. The HTA script will then interpret the embedded JavaScript, which then launches an encoded PowerShell script. This PowerShell script is responsible for downloading and executing the SmokeLoader payload.

By understanding its evolution and operational techniques, we will present how modern loaders are reshaping the threat landscape and tackling how we can refine detection and mitigation strategies.

EMMENHTAL LOADER: THE SILENT ENABLER OF MODERN MALWARE CAMPAIGNS

Lovely Jovellee Lyn Antonio
G Data AV Lab Inc

Bio:

Lovely has over 12 years of experience in the information security industry, specializing in threat research, analysis, and creating detection signatures. Recently, she has focused on curating training curriculums and career programs for employee upskilling. She has participated in malware research projects and previously presented at AVAR conferences. She is happily married to a fellow researcher, and they enjoy exploring foods and travelling together.

Ricardo Pineda Jr
G Data AV Lab Inc

Bio:

Ricardo has over 20 years of experience in the cybersecurity industry, specializing in threat research, analysis, and creating detection signatures. Throughout his career, he has contributed to developing advanced security measures, helping organizations stay ahead of emerging threats. In recent years, he has also focused on mentoring and knowledge-sharing, ensuring the next generation of cybersecurity professionals is well equipped to tackle evolving challenges.

Happily married for 12 years, Ricardo enjoys spending time with his family, including his two children. Outside of work, he is an avid RPG gamer, finding relaxation and creativity in immersive story-driven worlds.

Louis Victor Sorita Jr
G Data AV Lab Inc

Bio:

Louis is a seasoned cybersecurity professional with 12 years of experience in the field. As a senior virus analyst, he specializes in threat research and detection, proactive threat hunting, and delivering internal cybersecurity training to enhance organizational resilience. Recently entering married life, Louis also enjoys playing video games, particularly soulslike titles that challenge his strategic thinking and perseverance.

SIMPLICITY AS A WEAPON FOR STEALTH AND PERSISTENCE

Abstract:

In recent years, cyber threat actors have increasingly shifted away from the development of complex, custom-built malware, opting instead for a more subtle and strategic approach that leverages legitimate tools already present within target environments. This significant change reflects a growing preference for "living off the land" tactics—techniques that exploit built-in features of operating systems and widely available offensive security frameworks to maintain access, escalate privileges, and exfiltrate sensitive data while leaving a minimal footprint. Such methods present numerous advantages: they effectively bypass many traditional defenses, substantially reduce the risk of detection, and enhance the operational longevity of intrusions.

The persistent attacks uncovered by Cisco Talos that specifically target organizations in Japan serve as a prime example of this evolution in tactics. In this presentation, we will delve into the discovered campaign and examine the techniques employed by the attackers to effectively mask their presence and evade conventional detection methods. Alongside the disclosure of the attackers' campaign, we will also discuss our discovery of a pre-configured installer script located on the command and control (C2) server. This script is designed to deploy a comprehensive suite of adversarial tools and frameworks, including Blue-Lotus, BeEF, and Viper C2, all hosted on an Alibaba cloud container Registry. This finding highlights the alarming potential for the misuse of such tools for malicious purposes by the attackers.

Talos observed the attackers' attempts to steal the victim's machine credentials during this campaign. However, we assess with moderate confidence that the attackers' motives extend beyond mere credential harvesting, based on our observations of other post-exploitation activities. These activities include establishing persistence, escalating privileges to SYSTEM level, and gaining potential access to adversarial frameworks, all of which indicate a strong likelihood of future attacks.

We conclude the presentation with a few suggestions to the audience. As adversaries are increasingly favoring simplicity over complexity in their approaches, it is more crucial than ever for organizations to adhere to fundamental security practices—such as regular patching, vigilant monitoring, and effective segmentation—which are vital defenses. Additionally, maintaining continuous readiness for the rapid exploitation of public CVEs is essential in combating these evolving threats.

Chetan Raghuprasad
Cisco Talos

Bio:

Chetan Raghuprasad is a Cyber Threat Research Engineering Technical Leader with Cisco Talos, where he focuses on investigating the latest developments in the global cyber threat landscape. In his role, Chetan analyses emerging threats to uncover adversary tactics, techniques, and procedures, identifying their motives and origins to produce actionable intelligence. He is deeply involved in disseminating this strategic, operational, and tactical intelligence to counter modern cyber risks. As a recognized subject matter expert, Chetan also publicly represents Cisco Talos by authoring official blogs and speaking at major cybersecurity conferences worldwide. With 17 years of dedicated experience in the information security sector, Chetan has cultivated deep expertise in Threat Intelligence, Digital Forensics, and Cyber Incident Response. His extensive background includes key roles in financial institutions, forensic consulting firm, and leading technology companies.

GHOST MATH: SYSCALL-ONLY INJECTION, DETERMINISTIC SHELLCODE & QUIC C2 — A MODERN EDR BYPASS MONOGRAPH

Abstract:

This monograph presents a 72-hour red-team campaign engineered to subvert two leading Endpoint Detection & Response (EDR) platforms—CrowdStrike Falcon (sensor v5.66) and Microsoft Defender for Endpoint (MDE, build 2309)—plus a Zeek 6 + Suricata 7 network inspection stack.

The operation hinged on three research pillars:

1. Thread-less, syscall-only process injection, eliminating the canonical handle → RW → CreateThread → DLL Load heuristic.

2. Deterministic "mathematical" shellcode that reconstructs itself on the victim in 38 ms from trigonometric constants, erasing static payload artefacts.

3. QUIC/HTTP-3 command-and-control that mimics Chrome 121 JA3 fingerprints and rides inside Google CDN domain fronting.

We document the full attacker workflow, enumerate every EDR alert generated (with timestamps, rule IDs and severity), and analyse exactly why each detection triggered or failed, mapping countermeasures to MITRE ATT&CK v14. Defender-ready Sigma, Splunk SPL and Osquery artefacts are appended.

Ananda Krishna
UST

Bio:

Ananda Krishna is a Senior Offensive Security Engineer (Red Team) at CyberProof, a UST company. His work centers on adversary simulation and emulation, evasion methodologies, and building custom C2 frameworks. He has responsibly reported vulnerabilities to NASA and multiple Fortune 500 organizations and is an active member of the OWASP Kerala Chapter.His work is grounded in repeatable tests and measured results from real-world operations.

NO IMPREGNABLE FORTRESS: HOW TEAM46 CARRIES OUT SUCCESSFUL ATTACKS ON RUSSIAN COMPANIES

Abstract:

In my presentation, I will talk about how we discovered the advanced Team46 group, which carries out successful attacks on Russian companies. The group uses a wide range of techniques to gain initial access, from classic phishing to one-click exploit chains for Google Chrome (CVE-2025-2783). The group uses exploits not only to penetrate the network, but also to maintain persistence, for example, through the CVE-2024-6473 vulnerability for Yandex Browser. In addition to using well-known tools such as CobaltStrike and Donut, Team46 creates and actively develops its own tools, such as the Dante and Trinper backdoors, and also has an extensive/complex of network infrastructure.

Vladislav Lunin
Positive Technologies

Bio:

Vladislav Lunin, Senior Threat Intelligence Specialist of the Positive Technologies Expert Security Center Sophisticated Threat Research Group

Previously, worked at Dr.Web as a virus analyst.
Speaker at relevant conferences – OFFZONE, PHDays.

I am also a former “CTF” player, an active “Flare-On” player, and a contributor to “XAKEP” Journal.

HIDDEN MALICE: INSIDE TINY FUD'S MAC BACKDOOR

Abstract:

Tiny FUD is a dangerous Backdoor, first seen in early 2025, that targets macOS devices. It allows cybercriminals to secretly access the device, steal passwords, banking information, and take screenshots.

What makes Tiny FUD hard to detect are its clever hiding techniques. It uses DYLD injection to sneak malicious code into trusted system programs. It also changes its process name to mimic common apps such as Safari, making it difficult to spot in system monitors. The malware hides its files from the Mac Finder view, making it harder to find by a user once it burrows into the system.

To avoid macOS's security checks, Tiny FUD uses self-signing tricks that help it appear safe. It also delays its execution slightly to evade anomaly detection and cleans up all its system traces before it exits execution. It also randomizes User Agent Strings to masquerade as regular browser HTTP traffic to remain under the radar of firewalls, and communicates with its C2 servers using stealthy encoded messaging.

In this presentation we unmask Tiny FUD's core functionality, analysing the rare DYLD injection technique. We'll look at how it targets the dynamic linker to ensure its covert execution and persistence, bypassing many security tools. Its relatively low prevalence indicates that threat actors are testing stealthier methods. As DYLD injection grows more sophisticated or widespread, it could pose significant detection challenges. Early understanding of this technique is crucial for future macOS defenses. The rise of such malware underscores the need for deep research and proactive security measures.

Suresh Reddy Lomada
K7 Computing Pvt Ltd

Bio:

Suresh Reddy completed his Bachelor's degree in Computer Science and Engineering from Vignan Institute of Technology and Science In 2022. He began his professional journey as a Threat Researcher at K7 Labs, his primary job responsibilities involve reversing and detecting various types of malware at multiple layers and as well as staying up-to-date with the latest trends. Suresh Reddy is passionate about malware analysis and reverse engineering on Windows and MacOS files, and his research findings are published on the K7 Labs technical blog page. During his leisure time, he enjoys playing cricket, writing stories and travelling with his friends.

CRACKING THE VAULT: REAL-WORLD CRYPTO WALLET EXPLOITS AND DEFENSE STRATEGIES

Abstract:

As blockchain ecosystems continue to scale and crypto wallets evolve into high-value digital vaults, threat actors are adapting with increasing sophistication. In February 2025, the Lazarus Group executed one of the most consequential cyberattacks in the crypto industry, siphoning over $1.4 billion in ETH from Bybit via its external wallet infrastructure. This breach exposed critical architectural vulnerabilities in multisignature logic, key management protocols, and internal operational controls.

This paper presents a comprehensive exploration of crypto wallet security, beginning with foundational concepts in blockchain architecture and wallet classifications—custodial vs. non-custodial, hot vs. cold—and progressing into the mechanics of smart contracts and multisignature (multisig) wallets. It highlights common implementation pitfalls that often go unnoticed during wallet development.

The threat landscape is examined through the lens of advanced persistent threats (APTs), with a focus on the Lazarus Group's evolving tactics. These include phishing, social engineering, and supply chain compromise, which enable attackers to escalate from endpoint intrusion to smart contract exploitation. A detailed narrative reconstruction of the Bybit 2025 breach reveals how gaps in multisig authorization, backend misconfigurations, and key custody failures enabled a full compromise.

To ground the analysis in practice, the paper includes a live simulation of a vulnerable multisig wallet. `This simulation demonstrates unauthorized owner injection, fund exfiltration, and laundering techniques—mirroring real-world attacker behavior as observed during the 2025 Lazarus Group cyberattack on Bybit.

Rijul Chauhan
Mastercard

Bio:

Rijul Chauhan is a Security Consultant focused on making cybersecurity practical and accessible. At Mastercard, he helps organizations strengthen their defenses by translating complex risks into clear, actionable strategies, with experience spanning cybersecurity strategy, product security, and financial system resilience. Beyond security, Rijul enjoys exploring new music and coffee culture—a balance that fuels his curiosity inside and outside of tech.

LEVERAGING GENERATIVE AI FOR DYNAMIC FILE HONEYPOTS IN WINDOWS KERNEL

Abstract:

In the field of cyber security, dynamic file honeypots serve as critical tools for detecting and analysing malicious activities, especially zero-day ransomware attacks. This paper explores the integration of generative AI (GenAI) with file honeypots to enhance their effectiveness. By dynamically generating virtual decoy content, these advanced honeypots deceive attackers and protect real data. The discussion includes technical aspects of implementing file honeypots, focusing on two primary cases: dynamically inserted virtual honeypot files and honeypot files wrapped around real protected files. The paper also outlines the benefits of using GenAI for realistic content generation, continuous adaptation and enhanced threat intelligence. This approach not only bolsters security measures but also reduces storage footprints and improves overall cyber security resilience. operating in the region.

Vladimir Strogov
Acronis

Bio:

Vladimir Strogov has 30+ years of experience in kernel level development in both storage and security areas (file systems, virtualization, data protection, reverse engineering, anti-malware solutions). He has worked on multiple Veritas and Symantec projects for nearly a decade. Additionally, he has worked at Kaspersky Lab in Core Drivers Group in roles of technical expert and team leads. Strogov is currently the Director of Development, Kernel Team at Acronis, having joined the team in 2016.

Sergey Ulasen
Acronis

Bio:

Sergey Ulasen is Senior Director of AI Development at Constructor Technology, leading AI/ML/NLP research and development areas. He is the developer of the “Eugene Goostman” bot, the first ever bot to pass the Turing test. Ulasen is an expert in artificial intelligence computer systems with emphasis in natural language processing, speech recognition, image processing, and complex system modelling and research. He has 20+ years of experience in developing robust, scalable, and configurable commercial software for scientific and business applications. Ulasen developed the award-winning Natural Language Processing software.

TRACING THE ORIGIN: FINGERPRINTS IN MSC FILE FOR CLUSTERING AND ATTRIBUTION

Abstract:

Since March 2024, numerous APT groups have conducted attacks that exploit MSC files. Several methods for abusing MSC files have already been publicly documented, including Taskpad, GrimResource, Kamikaze and EvilTwin. We have been collecting and analysing over 100 malicious MSC files since early 2024, closely tracking their development. Through this research, we discovered that MSC files often retain artefacts depending on their creation environments. These artefacts can reveal how a given MSC file was created, highlight similarities with other files, and support the attribution or classification of the threat actors behind them.

In this presentation, we will begin by outlining the fundamentals of MSC files, followed by a detailed overview of known exploitation techniques. We will then share concrete cases showing how various APT groups have leveraged MSC files in real-world attacks. Furthermore, we will present our findings on the unique fingerprints found in malicious MSC files and demonstrate how they can be used for clustering and analysis. Finally, we will explore whether our methodology can also be applied to other file types beyond MSC.

Attendees will gain an in-depth understanding of malicious MSC files and learn how to apply clustering techniques based on file characteristics. This knowledge will enable SOC analysts, incident responders and CSIRT teams to conduct more advanced investigations and threat research involving MSC-based attacks.

Kazuya Nomura
NTT Security Holdings

Bio:

Kazuya Nomura is a SOC analyst at NTT Security Holdings. Currently, his main duty is responding to IDS/IPS/EDR log detection, but he also interested in malware analysis and data visualization. He posted articles about both in NTT Security. He has spoken at CODE BLUE, JSAC, HITCON in the past.

Rintaro Koike
NTT Security Holdings

Bio:

Rintaro Koike is a security researcher at NTT Security Holdings. He is engaged in threat research and malware analysis. In addition, he is the founder of “nao_sec” and is in charge of threat research. He focuses on APT attacks targeting East Asia and web-based attacks. He has been a speaker at VB, SAS, Botconf, AVAR and others.

OPERATION DRAGONCLONE: CHINESE TELECOMMUNICATION INDUSTRY TARGETED VIA VELETRIX & VSHELL MALWARE

Abstract:

In June 2025, Seqrite Labs uncovered Operation DRAGONCLONE, a sophisticated cyber- espionage campaign targeting China Mobile Tietong, a major telecom provider in mainland China. The attack chain began with a ZIP archive (附件.zip) containing a trojanized executable mimicking internal training tools. This executable sideloaded a malicious DLL via a legitimate Wondershare Repairit binary, resulting in-memory execution of a stealthy 64-bit loader named VELETRIX. The loader exhibited advanced evasion through Sleep-Beep anti- sandbox timing, API hashing, and "IPFuscation" technique—embedding encrypted shellcode as IPv4 string patterns, decoding and executing it via the EnumCalendarInfoA callback mechanism.

The decoded payload instantiated the VShell backdoor, a Golang-based, cross-platform remote shell delivered as tcp_windows_amd64.dll. This implant communicated over WinSock APIs with command-and-control (C2) servers across Hong Kong, the U.S., and Singapore. Forensic analysis identified 44 variants sharing a hardcoded configuration salt (qwe123qwe), with some binaries digitally signed, potentially via compromised certificates—one linked to Shenzhen Thunder Networking Technologies Ltd. The infrastructure bore strong overlaps with known Chinese APTs such as UNC5174 (Uteus) and Earth Lamia, previously observed exploiting vulnerabilities like CVE-2024-1709 (ScreenConnect) and CVE- 2025-31324 (SAP NetWeaver).

Additional servers hosted tools like Cobalt Strike, SuperShell, and reconnaissance dashboards (e.g., Asset Lighthouse System), indicating a well-resourced and modular campaign infrastructure. Operation DRAGONCLONE exemplifies an evolution in China-nexus cyber operations—combining DLL sideloading, cross-platform loaders, certificate abuse, and obfuscation via shellcode-IP encoding. The campaign underscores the growing complexity of APT tooling targeting critical national infrastructure, demanding deeper memory inspection, behavioral analytics, and cross-platform visibility.

OPERATION DRAGONCLONE: CHINESE TELECOMMUNICATION INDUSTRY TARGETED VIA VELETRIX & VSHELL MALWARE

Sathwik Ram Prakki
Quick Heal

Bio:

Sathwik Ram Prakki works as Senior Security Researcher at Seqrite Labs, Quick Heal. His areas of research are threat intelligence, APT hunting, delving into dark web and malware analysis. With a background in offensive security and knowledge of OS internals, he is keen on enhancing detections and infrastructure for threat hunting and CTI. Starting his cybersecurity career at C-DAC, under the Ministry of Electronics & IT in India, Sathwik has shared insights on APTs, ransomware and malware ecosystems at conferences such as AVAR, BlueHat, Botconf, c0c0n, FIRSTCON and Virus Bulletin.

Subhajeet Singha
Quick Heal

Bio:

Subhajeet Singha is a security researcher at Quick Heal's Seqrite Labs, specializing in threat intelligence, malware research, and reverse engineering. His work focuses on analysing emerging cyber threats, uncovering sophisticated attack campaigns, and enhancing detection mechanisms to strengthen cybersecurity defences. With a deep understanding of malware behaviour and threat actor tactics, Subhajeet actively investigates advanced persistent threats (APTs), reverse-engineers complex malware strains, and contributes to research initiatives that improve industry-wide threat detection. His expertise spans multiple domains, including cyber threat hunting, and the development of proactive defence strategies.

PIVOT
FOR ENDPOINT
2026

SE LABS ®

https://selabs.uk/pivot

AVAR 2025

PANEL MEMBERS

SHARED VISION: ADVANCING CYBERSECURITY THROUGH COLLECTIVE INNOVATION (PANEL DISCUSSION)

Vanja Svajcer
Cisco

Bio:

Vanja Svajcer works as a Threat Researcher at Cisco Talos. Vanja enjoys tinkering with automated analysis systems, reversing binaries and analysing mobile malware. He thinks time spent scraping telemetry data to find indicators of new attacks is well worth the effort. He presented his work at conferences such as AVAR, Virus Bulletin, RSA, CARO, FSec, Bsides, BalcCon and others.

Xavier P. Capilitan Jr.
G Data AV Lab Inc

Bio:

Xavier Jr. Capilitan is the Chief Operating Officer at G DATA AV Lab, Inc., based in Metro Manila, Philippines, with over two decades of leadership experience across cybersecurity operations, enterprise delivery, and organizational transformation. He has spent more than 11 years at G DATA driving strategic execution, governance, and large-scale operational programs alongside boards and senior executives to deliver sustainable growth and service excellence. Prior to this, Xavier built a 12-year career at Trend Micro, progressing through technical and leadership roles in malware analysis, threat-response automation, training and development, and global operations.

His work focused on designing high-volume incident response systems, leading international teams, and improving detection turnaround times worldwide. Known for combining technical depth with people centric leadership, Xavier brings strong expertise in Agile delivery, automation, and workforce development.

He holds a Master's in Entrepreneurship and a Master's in Computer Science from Ateneo de Manila University, along with undergraduate degrees in Computer Engineering and Physics reflecting a career anchored in resilience, operational excellence, and building high-performing global teams.

SHARED VISION: ADVANCING CYBERSECURITY THROUGH COLLECTIVE INNOVATION (PANEL DISCUSSION)

Santeri Kangas
F-Secure

Bio:

Santeri Kangas is Chief Technology Officer at F-Secure Oyj, a cybersecurity pioneer with 30 years of experience spanning from the early days of the anti-virus industry to today's AI-driven threat landscape. Throughout his career, Santeri has led global cybersecurity labs and driven breakthrough advances in AI-powered threat detection, vulnerability research, and router security. He has launched award-winning enterprise and endpoint security solutions and is currently leading F-Secure's development of next-generation scam protection technologies. His work has shaped the security landscape for consumers, enterprises, and service providers worldwide.

James Thang
Help Group

Bio:

James Thang is an award-winning technology strategist and digital transformation leader with more than 27 years of experience in software development, IT project management, and enterprise innovation. He currently serves as the Group CIO at HELP Education Group, where he drives large-scale digital transformation initiatives across the organization.

His career has spanned Asia Pacific, China, and Europe, holding senior leadership roles including CEO, Group CIO, CTO, and COO at leading organizations such as Daimler Chrysler TSS, Time dotCom, Microsoft, and UCSI Group. James has presented to boards and shareholders of multinational corporations and public-listed companies and is a sought-after keynote and panel speaker across Southeast Asia.

James has received multiple international recognitions, including Outstanding CIO of the Year 2025, CIO of the Year 2025 for Innovation in EdTech, and the ETCIO Transformative CIO Award (2022–2024). He is also a Global CIO Forum Global Champion 2024, three-time World CIO 200 Legend Category (2023-2025), Country Ambassador and Vice President for Malaysia, as well as a three-time IDC ASEAN CIO100 Award recipient (2023-2025).

Beyond his professional work, James is a passionate Arowana fish enthusiast and a certified Professional Judge for AquaFair Malaysia, reflecting his dedication to excellence both in and outside the technology sphere

SHARED VISION: ADVANCING CYBERSECURITY THROUGH COLLECTIVE INNOVATION (PANEL DISCUSSION)

Ken Soh
Athena Dynamics

Bio:

Ken Soh is the Group CIO of BH Global and CEO of Athena Dynamics, a cybersecurity subsidiary he co-founded in 2014. With over 35 years in ICT, he has led major digital transformation initiatives and built Athena into a trusted service provider serving 350+ public and private entities, including those in defense, maritime and critical infrastructure. He chairs SGTech's Cyber Security Chapter (Sep 2022-Sep 2025) and co-chairs with CSA the Cyber Security Assurance Alliance. Ken has been an avid speaker/writer and has received multiple leadership awards, including AiSP Cyber Security Leaders, Dun & Bradstreet Singapore Business Eminence, CIO100, ASEAN CIO accolades. He holds an Executive MBA from the NTU-UC Berkeley Programme and a MSc in Computer Studies (AI) with distinction from the University of Essex.

Jacky AW
Kenanga Group

Bio:

Strategic and forward-thinking technology risk and cybersecurity leader with over 15 years of experience across global financial institutions and regulated industries. I specialize in building robust governance frameworks, simplifying control taxonomies, and aligning policy with emerging technologies and regulatory landscapes.

Currently serving as Head of Tech Risk, BCM, and Chief Information Security Officer (CISO) at Kenanga Investment Bank, I lead enterprise-wide risk strategy and oversee cybersecurity policies aligned with standards like ISO 27001, NIST, GDPR, and BNM RMiT. My work bridges first- and second-line functions, enabling better resilience, compliance, and risk culture.

Erik Heyland
AV-Test

Bio:

Erik Heyland, Head of Testing Labs, has been with AV-Test for over 17 years and brings extensive operational insight into anti-malware testing and standardization. He is committed to advancing global testing practices and strengthening collaboration across the security ecosystem.

TRANSPARENCY WARS: EXPOSING HIDDEN BIASES IN TESTING (PANEL DISCUSSION)

Luis Corrons
Gen

Bio:

Luis Corrons is a cybersecurity expert with more than 25 years of experience analyzing threats and helping people protect their digital lives. He works at Gen, the global company behind Norton, Avast, AVG, and Avira, where he serves as Security Evangelist and is one of the company's main spokespersons on threat-related topics.

Throughout his career, Luis has specialized in tracking malware and scam trends, building awareness of emerging threats, and explaining complex issues in a way that connects with both technical and non-technical audiences. He has been an active voice in the cybersecurity community since 1999, regularly speaking at international conferences such as Virus Bulletin, CARO Workshop, AVAR, APWG, and more.

Beyond his role at Gen, Luis serves as Chairman of the Board at the Anti-Malware Testing Standards Organization (AMTSO) and sits on the board of MUTE, contributing to industry-wide collaboration on testing, standards, and transparency. He is a frequent media contributor on TV, radio, and major news outlets, where he helps raise public awareness about online security and cybercrime.

Simon Edwards
SE Labs

Bio:

Simon Edwards is the founder and CEO of SE LABS, a London-based company that specialises in advanced security testing. He provides tailored security advice to large businesses and more general technical advice to small businesses and individuals.

Simon focuses on cyber security and develops ways to test computer security products and services. He built and ran the world's first real-world anti-virus test and continues to innovate in testing that involves computer hacking.

A founder member of the Anti-Malware Testing Standards Organization (AMTSO), Simon held a Chair position on its Board of Directors for over a decade.

Simon features on the Cyber Security DE:CODED podcast, which provides security advice for businesses and individuals, recognising that people need security in both their work and personal lives.

TRANSPARENCY WARS: EXPOSING HIDDEN BIASES IN TESTING (PANEL DISCUSSION)

Samir Mody
K7 Computing

Bio:

Samir Mody graduated from the University of Oxford in 2000 with a First-Class Masters degree in Chemical Engineering, Economics and Management. He spent over 9 years at Sophos UK, the final 3 as Threat Operations Manager of SophosLabs. Since August 2010 he has been running K7 Labs in Chennai, India. Samir has actively contributed to the IEEE Taggant System project and other industry collaborations such as AMTSO and CTA. He has co-authored and/or presented papers and participated in panel discussions at various international security conferences (EICAR, VB, AVAR). Samir's interests include reading (philosophy, politics, history, literature, and economics), sport and classical music.

Righard Zwienenberg
ESET

Bio:

Zwienenberg began his work with computer viruses in 1988 after encountering his first virus issues at the Technical University of Delft. This experience sparked his interest in virus behavior, leading him to study and present solutions and detection methods ever since. Over nearly four decades, he has worked for various companies, including CSE Ltd., ThunderBYTE, Norman, and ESET. He has also held or continues to hold positions in several industry organizations, such as AMTSO, AVAR, the WildList, IEEE ICSG, and serves on the Advisory Board for Europol's European Cyber Crime Center (EC3) and Virus Bulletin. He also runs his own computer security consultancy company (RIZSC).

Zwienenberg has been a member of CARO since late 1991. He is a frequent speaker at conferences, including Virus Bulletin, EICAR, AVAR, FIRST, APWG, RSA, InfoSec, SANS, CFET, ISOI, SANS Security Summits, IP Expo, government symposia, SCADA seminars, and other general security events. Beyond his professional work in security, his hobbies include playing drums, performing magic, modeling balloons, restoring ancient computers, and much more.

DATA WITHOUT BORDERS? SOVEREIGNTY, TRUST, AND THE CLOUD DILEMMA (PANEL DISCUSSION)

Michael Daniel
Cyber Threat Alliance

Bio:

Michael Daniel serves as the President & CEO of the Cyber Threat Alliance (CTA), a not-for-profit membership association that enables cyber threat information sharing among cybersecurity organizations. Prior to CTA, Michael served as US Cybersecurity Coordinator from 2012 to 2017, leading US cybersecurity policy development both domestically and internationally, facilitating US government partnerships with the private sector, and coordinating significant incident response activities. From 1995 to 2012, Michael worked for the Office of Management and Budget, overseeing funding for the U.S. Intelligence Community. Michael also works with the private sector Ransomware Task Force, Aspen Cybersecurity Group, the World Economic Forum's Global Future Council on Cybersecurity and the Partnership Against Cybercrime, and other organizations improving cybersecurity in the digital ecosystem. In his spare time, he enjoys running and martial arts.

Selvakumar Manickam
Universiti Sains Malaysia

Bio:

Dr. Selvakumar Manickam is a leading authority in cybersecurity and AI. As a professor and the director of the Cybersecurity Research Center, he has been instrumental in advancing security and privacy research. His contributions have significantly shaped algorithms and models that address complex challenges in cybersecurity. Dr. Manickam's passion lies in forging connections between theory and practice, often by integrating cybersecurity and AI technologies. Equipped with decades of software development expertise, he also spearheads cutting-edge projects in AI-driven automation, optimizing efficiency and safety across diverse sectors, including manufacturing and agriculture. His work has catalyzed significant improvements in productivity and security, showcasing the transformative potential of AI in real-world applications. A prolific researcher and author, Dr. Manickam consistently publishes in top-tier journals and presents at prestigious conferences. He has cultivated a new generation of experts in the hybrid field of AI and cybersecurity. His insights are highly valued by journalists and industry leaders, solidifying his reputation as a thought leader in cybersecurity and AI. Dr. Manickam's dedication to pushing the boundaries of knowledge makes him an influential figure in shaping the future of these critical fields

DATA WITHOUT BORDERS? SOVEREIGNTY, TRUST, AND THE CLOUD DILEMMA (PANEL DISCUSSION)

Murugason R. Thangaratnam
Novem CS

Bio:

Murugason R. Thangaratnam is a visionary cybersecurity leader with over 26 years of senior management and entrepreneurial experience, and currently serves as the CEO and Co-Founder of an award-winning cybersecurity company. He has also served on several influential national working committees, including the Protem Committee on Data Governance reporting to the Minister of Digital, the National Digitalisation Committee, and a joint working group with a key industry regulator that culminated in the recently announced guidelines for the stockbroking sector. He has been invited to speak or serve as a panelist at more than 50 conferences across Malaysia, the region, and the global stage.

He is a trusted advisor to key digital and regulatory stakeholders, including the Minister of Digital Malaysia and the Malaysian Digital Economy Corporation (MDEC). His high-impact cybersecurity workshops have equipped leaders from the Malaysian Parliament, major telecommunications providers, legal institutions, credit bureaus, and National Critical Information Infrastructure (NCII) organisations under the Cyber Security Act 2024. He serves as Lead Facilitator at the Institute of Corporate Directors Malaysia, Cyber Intelligence Lead with the US-based Equanimity Group, Adjunct Practice Professor at the University Malaysia of Computer Science and Engineering (UNIMY), and Honorary Advisor to LTT Global in EdTech innovation. His global recognition includes the Outstanding Leadership Award at the Internet 2.0 Conference 2023 in Dubai and the Cyber Security Appreciation Award 2025 in Malaysia.

Syahril Aziz
Secure InSight Sdn Bhd

Bio:

Datuk Syahril Aziz is a cyber security amd resiliency expert with twenty seven (27) years of experience in Information Systems, Security and Continuity Technology covering technical aspects, assurance services and advisory to government and private firms. He is a PMP C|CISO CiSA CiSM LPT (M) CBCP GPEN and CTAL-TM certified professional that has in-depth experience in critical systems and security application management. Has helped numerous organizations from diverse vertical markets within South East region countries and Saudi Arabia to enhance their security posture and resiliency.

DATA WITHOUT BORDERS? SOVEREIGNTY, TRUST, AND THE CLOUD DILEMMA (PANEL DISCUSSION)

Vimalaasree Anandhan
Poshmark

Bio:

Vimalaasree is a Cybersecurity Leader with nearly two decades of expertise in application and cloud security, as well as DevSecOps practices. She oversees security operations, governance, risk management, and compliance, ensuring a robust security posture for the organisation. Her focus includes securing applications, mitigating vulnerabilities, and building resilient systems.

She has previously held key positions at Ernst & Young (EY), Tata Communications, Cognizant, and BNY Mellon, where she significantly advanced cybersecurity measures.

She holds a Master's in Science and a Bachelor's in Engineering, along with several industry-recognized certifications in cybersecurity and risk management.

She is a member of many vibrant cybersecurity communities like ISACA, ISC2, WiCyS and serves as the President of Nex Gen Cyber Women, a community dedicated to empowering women in cybersecurity.

INTERNAL THREATS – STRATEGIES FOR PARTNER-DEPENDENT ORGANIZATIONS (PANEL DISCUSSION)

Peter Stelzhammer
AV-Comparatives

Bio:

Peter Stelzhammer is the Co-Founder of AV-Comparatives, a globally recognised leader in independent cybersecurity testing. With over two decades of experience, Peter has pioneered rigorous, scientific methodologies for evaluating cybersecurity solutions. His research forms the basis for results widely used by major publications, industry analysts, and security vendors to inform their recommendations.

In addition to his role at AV-Comparatives, Peter serves as the IT Security Experts Group speaker at the Chamber of Commerce Austria. He also supports cybersecurity research at the University of Innsbruck and the Management Center Innsbruck, where he mentors and shapes the next generation of cybersecurity professionals through his expertise.

Jairam Ramesh
AIA Digital+

Bio:

Jairam Ramesh is a globally recognized cyber security leader with two decades of experience protecting enterprises, governments, and critical infrastructure. As the Director of Cyber Security for AIA Group, he has built world-class SOCs, pioneered AI-driven defense strategies, and shaped security adoption across 18 markets. He has been a trusted advisor to regulators, law enforcement, and Fortune 500s. Known for transforming cyber resilience at scale, he brings deep expertise in threat intelligence, digital forensics, and crisis management right from the battle field to board room meetings.

INTERNAL THREATS – STRATEGIES FOR PARTNER-DEPENDENT ORGANIZATIONS (PANEL DISCUSSION)

Tanvinder Singh
PwC

Bio:

Tanvinder is a Director within the Cyber Security practice of PwC Malaysia. He has 18 + years of cross industry experience in defining, developing, and executing change and cybersecurity strategies in large organisations. He has a proven track record as a thought-leader with broad subject matter knowledge in information security domains and success in developing and implementing cybersecurity technologies for large institutions. Tanvinder is adept at managing both projects and people, as seen through his experience in formulating technology strategy and platform architecture while leading large change initiatives across cybersecurity.

Jonathan Tam
Schneider Electric

Bio:

Jonathan Tam is the Senior Cybersecurity Officer for East Asia Zone. He is responsible in leading Cybersecurity Governance, Risk and Compliance. He supports the Cybersecurity IT/OT governance across the region and assist in technical advisory and consultancy.

Jonathan has over 24 years of Cybersecurity Industry experience certified experience in the Cybersecurity domain and multiple operating systems & network platforms. He has an expert IT & OT technology grasp within plant architectures on various control systems technology platforms. He also has cybersecurity engagement experience across multiple industry verticals, including Oil & Gas, the financial sector and government authorities.

Areas of expertise include cybersecurity assessment, audit, consultancy & advisory, enterprise-class information technology, architecture design, compliance and risk analysis and solutions design/implementation.

INTERNAL THREATS – STRATEGIES FOR PARTNER-DEPENDENT ORGANIZATIONS (PANEL DISCUSSION)

Ekneswaran Matandor

Bio:

Ekneswaran Matandor (Ekkey) is an accomplished technology leader with over 15 years of experience across cybersecurity, enterprise infrastructure, blockchain, and AI-driven innovation. He has held senior roles at HP and IBM, where he specialized in cybersecurity strategy, digital infrastructure, and enterprise-scale technology integration.

In the blockchain and crypto sector, Ekkey has provided consulting expertise to Era Swap Technologies and Coin Governance System, advising on token economics, security frameworks, and the governance of decentralized ecosystems.

A recognized voice in the regional tech community, he has been invited as a speaker and panelist at major technology summits, including:

- ASEAN Blockchain Summit – Malaysian representative on Cybersecurity and Web3
- Boracay Blockchain Summit – Keynote on Tokens vs Coins
- Bali Blockchain Summit – Panelist on blockchain adoption and future regulation
- Guest Speaker, University of Nottingham Malaysia – Addressed final-year Computer Science students on AI, cybersecurity, and career pathways
- World Ai Show - Moderator , Ai on Adaptive defense
- Moderator , Data Infrastructure and pipeline Architecture
- Fire chat session , Ai for Healthcare

Ekkey is Previously is the Chief Technology Officer of OC Global Technology Sdn Bhd, leading the Otalk platform and digital ecosystem. He combines strategic vision with technical expertise to drive innovation in AI, blockchain, and digital engagement, while ensuring world-class cybersecurity and scalability.

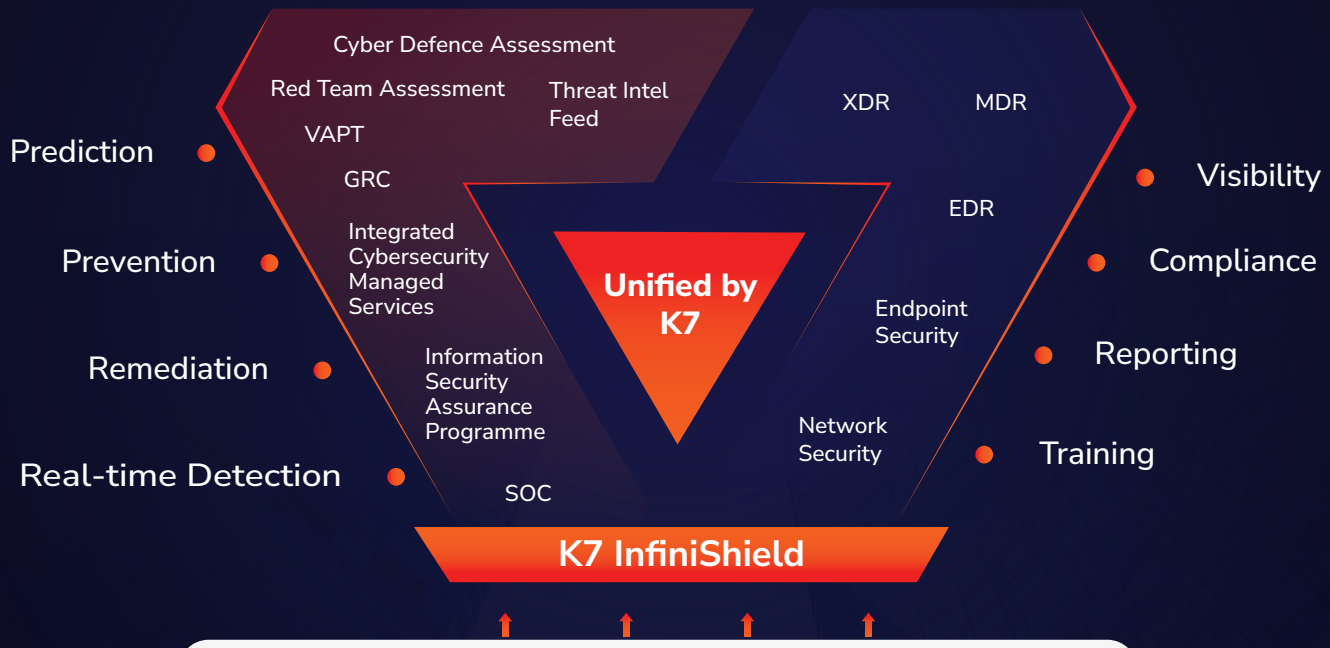
K7 SECURITY

The Global Cybersecurity Pioneer

India | Singapore | UAE | USA

360° ENTERPRISE CYBERSECURITY

FOR ASSURED COMPLIANCE AND THREAT DEFENCE



Endpoints | Servers | Networks | Cloud | Wireless Systems

IoT | Thick Clients | Embedded Systems | POS | SCADA

Active Directory | Web Applications | Mobile Applications

APIs | Blockchain | AI | Social Media

App Stores | Dark Web

www.k7cybersecurity.com

AVAR 2025

CISO CONNECT

INTRODUCTION TO CISO WORKSHOP

Dr. Peter Leong

Bio:

Peter has been in Information Technology since 1992, in various industries namely Financial Services Industry (FSI), Global Shared Services Centre (GSSC), Manufacturing, Oil & Gas (O&G), Automotive, Retail & Consulting. Currently, he's performing C-Level's Consultative Advisory as a Service (CaaS), business transformation, project management services, speakers & trainings on request's basis.

- He is from rank & file and has been in IT towers of Data Center & IT Operations, Infrastructure & Applications Management, Project/Program Management, People/Resource Management, Financial Management, Pre-Sales, Business Technologies, Service Delivery Management, Advisory & Consulting, Technology Risks Management, Roadmap & Strategy, CyberSecurity& Strategic Workforce Planning (SWP).
- He is providing CISO/CDPO advisory services, overseeing ISMS of the Group, Policies & Standards, Governance & Compliance's, Audit, Processes & Standards, Risks Management, Info/ CyberSecurity & Data Protection.

QUANTUM RECKONING: CYBER SECURITY AT A TIPPING POINT

Abstract:

As quantum computing technology rapidly advances, its potential to disrupt cybersecurity is starting to pose a real danger in information technology. By utilizing Shor's algorithm, quantum computers could compromise widely used public key cryptographic systems such as RSA, DSA, and ECC, while Grover's algorithm threatens to undermine symmetric encryption. Although large-scale quantum computers are still years away, the security implications are already clear. Threat actors are increasingly employing "Harvest Now, Decrypt Later" (HNDL) techniques to exfiltrate encrypted data with the intention of decrypting it once quantum capabilities mature. This poses a substantial threat to long-term data security, trust in contracts, and regulatory stability, especially in critical industries like healthcare, defense, banking, finance, and vital infrastructure.

This presentation emphasizes the early indicators of quantum disruption for organizations and addresses the critical necessity for proactive strategies. It explores the initiatives of the National Institute of Standards and Technology (NIST) in standardizing post-quantum cryptography (PQC) and highlights the significance of cryptographic agility in assessing vendors. We will also divulge key strategies for quantum computing precautions such as developing cryptographic asset inventories, transitioning to hybrid cryptographic systems, and deploying post-quantum algorithms are becoming essential components of a robust enterprise security strategy.

As adversaries deploy quantum weapons, executive management and security professionals must shift from reactive defense to proactive cryptographic resilience. Companies that delay quantum readiness expose their most sensitive data to significant risks, both now and in the future. The advantage in cybersecurity will belong to those who adapt swiftly in this evolving frontier, transforming cryptography from a passive defense into a powerful tool for foresight and resilience.

QUANTUM RECKONING: CYBER SECURITY AT A TIPPING POINT

Felissa Mariz Marasigan
EY GDS (CS) Philippines, Inc.

Bio:

Felissa Mariz Marasigan is a Cybersecurity Consultant with 7 years of professional experience across multiple domains, including reverse engineering, malware analysis, and cybersecurity incident response. Beginning her career in technical malware analysis, she developed a strong foundation in understanding and dissecting malicious code, which later expanded into broader roles within incident response and digital forensics.

Having worked closely with Cyber Security Incident Response Teams (CSIRTs), Felissa has been actively involved in investigating advanced threats, mitigating enterprise-scale security incidents, and strengthening organizational defenses. Currently serving as a SOC Analyst, she focuses on proactive monitoring, threat hunting, and building resilient security operations to adapt to today's fast-evolving cyber landscape.

Mark Gabriel Rizare
EY GDS (CS) Philippines, Inc.

Bio:

Mark Gabriel Rizare is a cybersecurity professional with 2 years of experience as a SOC Analyst, specializing in monitoring security alerts, analyzing potential threats, and responding to incidents in real time. In this role, he has developed strong expertise in handling security events under pressure, investigating malicious activity, and improving incident response processes. With a solid technical foundation in Electronics and Communication Engineering, Mark brings an analytical and detail-oriented approach to cybersecurity operations. He is passionate about advancing his skills in threat detection and defense strategies.

COUNTERING THE UNTHINKABLE: DISRUPTING ADVANCED THREATS WITH UNCONVENTIONAL DEFENSES

Abstract:

As cyber adversaries evolve, so must our defenses. Traditional cybersecurity measures, while essential, often fall short against advanced threats that exploit not just technical gaps but also cognitive and procedural blind spots. To outpace these sophisticated attackers, we must embrace disruptive thinking and unconventional defense strategies that challenge the status quo.

In this session, we will explore with examples how disruptive technologies can shift the advantage back to defenders. More importantly, we will discuss how breaking the attacker's thought process and disrupting the root causes of vulnerabilities (and stop focusing on the effect) are critical to reshaping the cyber battleground.

Key takeaways include:

- Understanding why conventional defenses is not longer effective against advanced threats
- How disruptive technologies can effectively protect against attack vectors
- Practical strategies for organizations to innovate their defensive posture in an age of evolving threats
- Join us to discover how outthinking the attacker and disrupting the playbook can redefine your cybersecurity resilience

Ken Soh
Athena Dynamics
(A BH Global Company)

Bio:

Ken Soh is the Group CIO of BH Global and CEO of Athena Dynamics, a cybersecurity subsidiary he co-founded in 2014. With over 35 years in ICT, he has led major digital transformation initiatives and built Athena into a trusted service provider serving 350+ public and private entities, including those in defense, maritime and critical infrastructure. He chairs SGTech's Cyber Security Chapter (Sep 2022-Sep 2025) and co-chairs with CSA the Cyber Security Assurance Alliance. Ken has been an avid speaker/writer and has received multiple leadership awards, including AiSP Cyber Security Leaders, Dun & Bradstreet Singapore Business Eminence, CIO100, ASEAN CIO accolades. He holds an Executive MBA from the NTU-UC Berkeley Programme and a MSc in Computer Studies (AI) with distinction from the University of Essex.

TEAM CYMRU™
THE POWER OF PURE SIGNAL™

PURE SIGNAL™ SCOUT

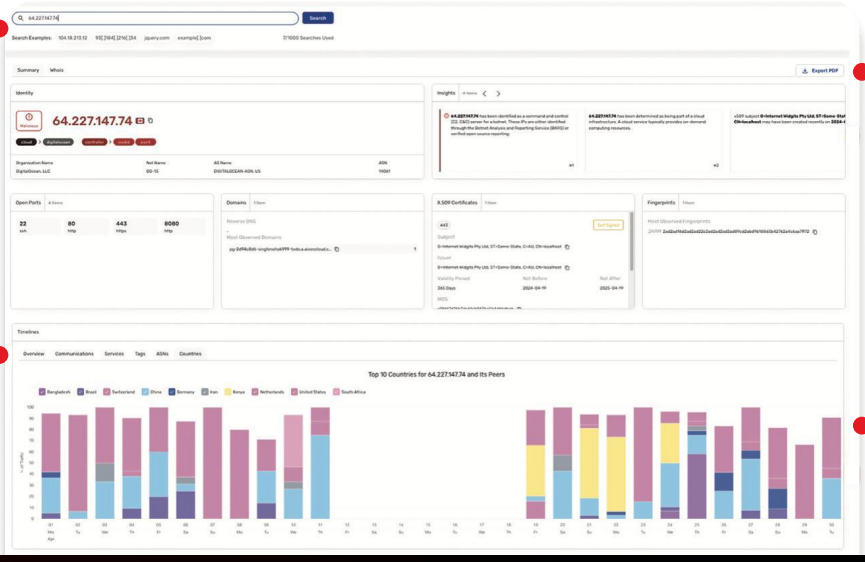
Transform your Security team with the World's Fastest Threat Hunting tool

Respond to alerts and assess risk faster with real-time IP intelligence

Pure Signal™ Scout is a powerful cyber threat hunting and network intelligence tool that provides real-time visibility of external threats, at speeds others can't match.

Simple IP Lookup with summarized whois and tags for added context

Visualize data across timelines



Lightning fast insights to assess risk

Intuitive Graphical Results display IP activity

Eliminate Noise of False Positives: Focus on critical threats

Avoid alert overload with high-fidelity intelligence and accurate data.

Gain Immediate Context

Get real-time context needed to defend against the APT's and adversaries targeting your organization now.

Detect Supply Chain Compromises

Monitor third-third party infrastructures to reduce risks from third-party compromises.

Level up your SOC

Gain unmatched insight into malicious infrastructure in real-time to create your own threat intelligence.

Consolidate multiple feeds and tools

Streamline your SOC by consolidating data from multiple sources to a single comprehensive source, reducing the cost, complexity, and burden of managing multiple data feeds.

Preemptive Network Defenses

Gain proactive intelligence to harden your network defenses and controls.

Scan the QR Code or visit https://www.team-cymru.com/threat-intelligence-platform

LEADING WITH RISK – HOW CISOS CAN DRIVE BUSINESS DECISIONS (PANEL DISCUSSION)

Ridzwan Mahdi
Maxis

Bio:

Cybersecurity and Data Protection leader specialising in GRC for highly regulated industries — telecommunications and financial services. I design and implement control environments that satisfy regulators and auditors while enabling business agility.

What I do

- Lead enterprise GRC and Data Protection strategy: policies, risk frameworks, audit readiness, and regulatory engagement (MCMC INS, NACSA, JPDP/PDPA, MAS TRM).
- Embed security and privacy into transformation: cloud migrations, identity modernisation, DLP/SASE, third-party risk.
- Translate cyber and privacy risk into business language for boards and executive committees.

Highlights

- Built and scaled GRC and Data Protection functions across telco and fintech, aligning to ISO 27001, ISO 27017 & ISO 27018, PCI DSS, NIST CSF.
- Delivered Cloud SIEM, DLP via SASE & M365, centralised IAM & MDM, and KRIs/KPIs for board reporting.
- Blended finance expertise (CA ANZ) with CISSP & CISA to drive risk-based decisions.

LEADING WITH RISK – HOW CISOS CAN DRIVE BUSINESS DECISIONS (PANEL DISCUSSION)

Dr. Peter Leong
MY CIO Service

Bio:

Peter has been in Information Technology since 1992, in various industries namely Financial Services Industry (FSI), Global Shared Services Centre (GSSC), Manufacturing, Oil & Gas (O&G), Automotive, Retail & Consulting. Currently, he's performing C-Level's Consultative Advisory as a Service (CaaS), business transformation, project management services, speakers & trainings on request's basis.

- He is from rank & file and has been in IT towers of Data Center & IT Operations, Infrastructure & Applications Management, Project/ Program Management, People/Resource Management, Financial Management, Pre-Sales, Business Technologies, Service Delivery Management, Advisory & Consulting, Technology Risks Management, Roadmap & Strategy, CyberSecurity& Strategic Workforce Planning (SWP).
- He is providing CISO/CDPO advisory services, overseeing ISMS of the Group, Policies & Standards, Governance & Compliance's, Audit, Processes & Standards, Risks Management, Info/CyberSecurity & Data Protection.

Vikneswaran Kunasegaran
CREST

Bio:

Vikneswaran is a GIAC certified Penetration Tester who obtained his Bachelor's Degree in Computing specializing in Computer Security from APIIT (now known as APU). He has been in the industry for nearly a decade, possessing expertise in vulnerability assessment, penetration testing, compromise assessment, red teaming, and more. On top of that, he is a cyber security awareness speaker with over a dozen talks held with various groups, including Board Members of certain organizations. He is currently managing a team of 20 security consultants and ethical hackers who provide security testing services for various clients across Malaysia and its neighbouring countries. He is also building a team for Incident Response and Endpoint Recovery Services at FIRMUS by becoming familiar with various EDR technologies and getting certified in them. His main objective from the start has been to provide quality cyber security services to clients without compromising on quality or the client's experience.

LEADING WITH RISK – HOW CISOS CAN DRIVE BUSINESS DECISIONS (PANEL DISCUSSION)

Arivindran Saidoo
KPMG Malaysia

Bio:

Arivindran Saidoo (Ari) is a seasoned cybersecurity leader with over two decades of experience in guiding clients through the transformation of their security programs across diverse industries such as Oil & Gas, Utilities, Telecommunications, and Financial Services. Previously serving as the Cybersecurity Country Head and SEA OT Security Lead for a prominent Fortune 500 consulting company, he also held leadership roles as the Head of OT Security Practice at a leading Big 4 firm in Malaysia. Known for his role as a trusted cybersecurity advisor to major conglomerates during his consulting engagements, Ari has been instrumental in helping clients in their successful IT-OT convergence journey and in establishing resilient CISO functions for his clients. Currently, he holds the esteemed position for ISA Connect APAC region.

Malini Kanesamoorthy
AmBank Group

Bio:

Malini is currently the Group Chief Information Security Officer at AmBank Group, a position she has held since February 2021. Prior to joining AmBank, she was the Regional Head of the Data Protection and Security Advisory function for AIA Group. She's an innovative and forward-thinking professional with a pioneering career with over two decades of experience working in multinational companies and financial services industry.

With a strong background in Information Technology, Advisory, Technology and Cyber Risk Management, Governance, Outsourcing Risk, Compliance and Strategy formulation, she has demonstrated leadership and vision in transforming the organization's cybersecurity posture through a strategic effective security program which combines maturity-based and risk-based programs towards a proactive (predictive) cyber security model.

She's been commended for being a change catalyst to foster information security culture with the objective of enforcing a pragmatic approach to managing IT risk and security as a key business enabler in the current corporate landscape. Malini leads by example and with her strong passion for the industry, the people and the business, she is often consulted and invited to share valuable information to the audience and the industry peers, in an easily digestible and engaging format without jargons.

LEADING WITH RISK – HOW CISOS CAN DRIVE BUSINESS DECISIONS (PANEL DISCUSSION)

Dharshan Shanthamurthy
SISA

Bio:

Dharshan Shanthamurthy is the Founder and CEO of SISA, a rapidly growing deep tech company that plays a critical role in safeguarding the world's digital payment infrastructure. Originally a Chartered Accountant, Dharshan made a bold transition into cybersecurity over 22 years ago and is now widely recognized as a trailblazer in the industry.

He holds over 10 global cybersecurity certifications and was among the first Indians trained at the prestigious US-CERT Coordination Centre. As one of India's earliest cyber security assessors and digital forensic investigators, Dharshan brings a rare combination of business acumen and deep technical expertise to the table.

Under his leadership, SISA has led several pioneering efforts—including India's Digital Threat Report and the Quantum Cyber Readiness Whitepaper in collaboration with CERT-In, the Government of India's nodal cybersecurity agency.

A sought-after global speaker, Dharshan has delivered keynotes at more than 250 platforms across 21 countries. He is also the force behind Cybersmart Bharat, a flagship CSR initiative aimed at equipping underprivileged youth in India with cybersecurity skills. His vision is simple yet ambitious: to establish India as a global powerhouse in cybersecurity innovation.

Let's talk at AVAR 2025!

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST INSTITUTE - THE INDEPENDENT SUPPLIER OF SERVICES IN THE FIELDS OF:

- ✅ IT SECURITY & ANTIVIRUS RESEARCH
- ✅ DETECTION & ANALYSIS OF THE LATEST MALICIOUS SOFTWARE
- ✅ COMPREHENSIVE AND COMPARATIVE TESTING OF SECURITY PRODUCTS
- ✅ CERTIFICATION IOT, EDR, NTP

AV-TEST av-test.org 2025
AWARD
BEST PROTECTION

ERIK HEYLAND
MEMBER OF THE BOARD
AT AV-TEST

G3 CYBER SPACE | G3 SEC.AI™

G3 Cyberspace powers Trusted Digital Growth, delivering intelligent cybersecurity and compliance solutions for organizations at every stage of digital transformation.

G3 Sec.ai is our all-in-one cybersecurity and compliance platform, blending automation, insight, and expert support for every organization.
Our **TRACS** module delivers next-level assurance for Third party risk automated, reliable, and ready to help your business grow securely.

From smart solutions to tailored services, we turn cybersecurity into your strategic advantage.

To learn more at www.g3cyberspace.com

DISASTER RECOVERY – WHAT WORKS, AND DOESN'T, IN THE REAL WORLD (PANEL DISCUSSION)

Wisnu Tejasukmana
SLB

Bio:

Wisnu is a cloud security architect at SLB corporation. Wisnu holds a Bachelor Degree in Chemical Engineering and is currently certified in CCSK, CCSP and CEH, amongst others. He has 26+ years in SLB organization, with experiences ranging from IT delivery in service desk and onsite IT, distributed servers and to now in cyber security for the past nine years. His primary activities now is architecting secure gen AI, threat modeling and cloud security for SLB.

Ridzwan Mahdi
Maxis

Bio:

Cybersecurity and Data Protection leader specialising in GRC for highly regulated industries — telecommunications and financial services. I design and implement control environments that satisfy regulators and auditors while enabling business agility.

What I do

- Lead enterprise GRC and Data Protection strategy: policies, risk frameworks, audit readiness, and regulatory engagement (MCMC INS, NACSA, JPDP/PDPA, MAS TRM).
- Embed security and privacy into transformation: cloud migrations, identity modernisation, DLP/SASE, third-party risk.
- Translate cyber and privacy risk into business language for boards and executive committees.

Highlights

- Built and scaled GRC and Data Protection functions across telco and fintech, aligning to ISO 27001, ISO 27017 & ISO 27018, PCI DSS, NIST CSF.
- Delivered Cloud SIEM, DLP via SASE & M365, centralised IAM & MDM, and KRIs/KPIs for board reporting.
- Blended finance expertise (CA ANZ) with CISSP & CISA to drive risk-based decisions.

DISASTER RECOVERY – WHAT WORKS, AND DOESN'T, IN THE REAL WORLD (PANEL DISCUSSION)

Ashok Kumar J
G3 Cyberspace

Bio:

I am Ashok Kumar J., a seasoned expert with over 20 years of experience in Data Privacy, Cybersecurity, Governance, Risk & Compliance (GRC), Enterprise Risk Management, Business Continuity Management (BCM), Audit, and Vendor Risk Assessment.

I am currently the Founder of G3 Cyberspace, a product-based cybersecurity and compliance company building next-generation solutions for third-party risk, data privacy, and governance automation.

I specialize in cybersecurity and global data privacy implementation, helping organizations navigate complex regulatory landscapes, including GDPR, CCPA, and other international frameworks. My work extends to cybersecurity in strategic decision-making, where I have advised leadership teams on aligning security with business priorities. I have also served as a Global Data Protection Officer (DPO), leading privacy strategies across multiple jurisdictions, and as a fractional CISO for M&A initiatives and complex enterprise transitions, ensuring risk and compliance integration at the board level.

Throughout my career, I have held leadership roles such as:

- Global Head of Compliance and Data Protection Officer at BCT
- Senior Manager of Third-Party Risk Management at Standard Chartered Bank and Capgemini
- Lead Consultant in Cybersecurity at Wipro
- Lead in Information Security, BCM, and GDPR at Equiniti

With extensive expertise in cyber threats, risk assessment, and vulnerability management, I have driven enterprise-wide compliance initiatives, combining strategic insight with operational execution.

DISASTER RECOVERY – WHAT WORKS, AND DOESN'T, IN THE REAL WORLD (PANEL DISCUSSION)

Shah Mijanur Rahman
Inmagine Group

Bio:

Shah Mijanur is a distinguished Cybersecurity Leader, CISO, and Head of Security, recognized as a security maven with over 10 years of experience driving excellence in global security strategy. He excels in SecOps, Incident Response, Cloud Security, Threat Modeling, and securing GenAI workloads, defining and implementing innovative security strategies that align with business goals and enhance threat detection.

Currently serving as the Head of Security at Inmagine Group, Mijanur defines and communicates multi-year security strategies, aligning them with board-level risk appetite and business objectives. He leads, inspires, and develops multidisciplinary security teams, including AppSec, CloudSec, Red Team, and SOC, fostering collaboration and innovation while mentoring team members to excel.

A recognized thought leader, Mijanur regularly briefs executive leadership on security posture and has shared his insights at major international events, including the BlackHat Asia Executive Summit in Singapore and the AWS ASEAN ExecLeaders Summit.

He is actively dedicated to fostering growth in the cybersecurity community as the AWS Malaysia Security Usergroup Leader. In this role, he leads a vibrant community of AWS Security Enthusiasts.

DISASTER RECOVERY – WHAT WORKS, AND DOESN'T, IN THE REAL WORLD (PANEL DISCUSSION)

Dinesh Barathy
Collectius Group

Bio:

Dinesh Barathy is a highly accomplished and multi-skilled IT professional with a wealth of experience working with mid to large-size multinational corporations (MNCs) across the globe. With a strong foundation in technology management, Dinesh has played a pivotal role in designing, implementing, customizing, upgrading, and migrating IT solutions throughout his career. Throughout his professional journey, Dinesh has had the privilege of working alongside industry leaders in various sectors, gaining invaluable expertise and developing a diverse range of technical skills. His extensive experience spans across multiple countries, allowing him to cultivate a global perspective on IT practices and strategies.

Not only has Dinesh excelled in his technical expertise, but he has also demonstrated exceptional leadership capabilities in developing high-performing teams. With a keen focus on delivering exceptional services, Dinesh has nurtured teams that consistently surpass expectations while promoting a culture of continuous improvement through innovation and technology.

Dinesh pursued his academic aspirations and earned a master's degree in technology management from the esteemed University of Malaysia Sarawak. This academic achievement served as a solid foundation for his professional growth and enabled him to excel in his career.

Currently, Dinesh holds the esteemed position of Regional Head of Information Technology in Collectius Group, a leading restructuring and servicing partner to financial institutions and commercial companies in Asia. In this influential role, he oversees technology operations across seven countries, demonstrating his ability to manage complex IT infrastructures on a regional scale.

"Success is no accident. It is hard work, perseverance, learning, studying, sacrifice, and most of all, love of what you are doing or learning to do."
- Pele

COMPLIANCE & AI – GOVERNING THE NEW TECHNOLOGY ON THE BLOCK (PANEL DISCUSSION)

Vikneswaran Kunasegaran
CREST

Bio:

Vikneswaran is a GIAC certified Penetration Tester who obtained his Bachelor's Degree in Computing specializing in Computer Security from APIIT (now known as APU). He has been in the industry for nearly a decade, possessing expertise in vulnerability assessment, penetration testing, compromise assessment, red teaming, and more. On top of that, he is a cyber security awareness speaker with over a dozen talks held with various groups, including Board Members of certain organizations. He is currently managing a team of 20 security consultants and ethical hackers who provide security testing services for various clients across Malaysia and its neighbouring countries. He is also building a team for Incident Response and Endpoint Recovery Services at FIRMUS by becoming familiar with various EDR technologies and getting certified in them. His main objective from the start has been to provide quality cyber security services to clients without compromising on quality or the client's experience.

Syarifah Bahiyah Rahayu
Universiti Pertahanan Nasional Malaysia

Bio:

Dr. Syarifah Bahiyah Rahayu binti Syed Mansoor is a Malaysian academic and researcher specializing in cybersecurity, digital forensics, and semantic technologies. She currently serves as the Director of the Cyber Security & Digital Industrial Revolution Centre at the National Defence University of Malaysia (UPNM).

Dr. Syarifah holds a Ph.D. and has contributed significantly to the field through various publications. Her research interests encompass blockchain security, hybrid consensus algorithms, and machine learning techniques. She has also been involved in developing digital forensic process models tailored for the defense and security sectors.

In addition to her academic roles, Dr. Syarifah has participated in international research collaborations, including a visiting position at EURECOM's Digital Security department in France. She is also a member of the editorial team for the International Journal of Electrical and Computer Engineering Systems.

Dr. Syarifah's work continues to influence advancements in cybersecurity and digital technologies, particularly within the context of Malaysia's defense and security sectors.

COMPLIANCE & AI – GOVERNING THE NEW TECHNOLOGY ON THE BLOCK (PANEL DISCUSSION)

Ruban Bala
Banking Industry

Bio:

Ruban was previous Head of Infrastructure and Application Security Risk & Head of Cyber Risk at Ryt Bank, one of Malaysia leading financial services company working to empower Malaysian financially.
In this role as Risk management on the following domain technology risk, cloud risk, application security risk and cyber risk, he helps protect the company from Cyber Threats.
Having spent 22 years across all layers of technology and industries, Ruban has focused his time and effort on perfecting an approach to delivery business results by using technology to its full capability and safest potential. Prior to RYT Bank, Ruban was a part of the initial team members who started up Digital Nasional Berhad (a MYR 16.5B, 10-year Malaysian initiative to enable rapid digitisation for the economy by using 5G enablement), Ruban was tasked to help kickstart and run an approach to define enterprise security architecture and adequate cyber security controls are in place for Cyber threat detection, protection and monitoring of the nation's single 5G wholesale network that is meant to service all 5 Telco operations and enterprise. His responsibilities include developing and governing Enterprise Security Architecture, overseeing the implementation of advanced security technologies and ensuring compliance with global cyber security standards and regulations. Ruban was the Malaysia 1st (5G security) telco security architect, helping build and secure the enterprise security architecture for Digital Nasional Berhad 5G network that consist of 5G RAN, Transport and Core network.

Cameron Camp
SecureIQLabs

Bio:

Cameron Camp, CISSP, is a Senior Security Researcher at SecureIQLab with extensive security background all the way up the stack from embedded hardware, firmware and IoT hacking, to medical devices and industrial control systems, with a specific focus on Linux-powered platforms. He's now focusing on cloud security, with an emphasis on understanding how to secure the connective tissue holding all the pieces together in an adversarial environment.

COMPLIANCE & AI – GOVERNING THE NEW TECHNOLOGY ON THE BLOCK (PANEL DISCUSSION)

Yusfarizal Yusoff
PETRONAS Digital

Bio:

Ts. Yusfarizal is a seasoned cybersecurity leader with over 24 years of experience in information security, systems, and network architecture across multiple industries including telecommunications, finance, government, certificate authority, oil and gas, and enterprise IT services. His extensive background in both enterprise and service provider environments provides him with a holistic perspective on complex security challenges and the strategic solutions needed to address them.

Combining deep technical expertise with strong leadership acumen, Yusfarizal has successfully driven cybersecurity transformation programs, led the development of security architectures, and implemented enterprise-wide security frameworks that align with regulatory standards and business objectives. His leadership is defined by a results-driven approach, strategic foresight, and a commitment to building cyber-resilient organizations.

Throughout his career, Yusfarizal has built and mentored high-performing teams, managed critical security initiatives, and advised senior executives on security governance, risk management, and compliance. His portfolio includes developing and enforcing enterprise security policies, overseeing incident response and threat mitigation, and architecting secure solutions tailored to highly regulated and dynamic environments.

Accredited by MBOT as Professional Technologist and an active contributor to the cybersecurity community, he frequently shares insights as a speaker and panellist at industry conferences, schools, and universities—advocating for stronger cyber awareness and talent development across sectors.

Gen | norton Avast LifeLock by norton MoneyLion

Sponsor of AVAR 2025

Gen is a global company dedicated to powering Digital Freedom, helping people live their digital lives safely, privately, and confidently. Behind our vision for a safer digital world is Gen Threat Labs, the research team uncovering and analyzing emerging threats and scams worldwide. Their insights and technical expertise power the technologies that protect millions every day.

Learn more at **GenDigital.com**

SECURITY INSIGHTS 101

Knowledge Series

Share Your Expertise at AVAR's Webinars

Write to rgdwivedy@aavar.org

TRAINING SESSION: BUILDING A SECURE MALWARE ANALYSIS ENVIRONMENT

Lena Yu
Malware Village

Bio:

Lena Yu, also known as LambdaMamba, is the founder of World Cyber Health and Malware Village. She created the Malmons aka Malware Monsters, has authored research papers for numerous conferences including CARO and Virus Bulletin, taught at top universities, is the author of the upcoming book "The (Un)Natural History of Malware", and is an international keynote speaker.

Lena founded Malware Village at DEF CON and various conferences worldwide to give malware analysts a home. Before founding Malware Village, Lena was a malware researcher at ANY.RUN, and before specializing in malware, she worked in computer architecture, compiler research, and chip design.

TRAINING SESSION: AI MANAGEMENT SYSTEMS FOR CISOS – NAVIGATING GOVERNANCE, RISK, AND COMPLIANCE

S Kumar Subramania
K7 Cyber Security

Bio:

32 years rich experience including 8+ years of Process Audits, Compliance Audits, IT audits, Risk assessments, Info-Sec assessments and 15+ years of Management Consulting in leadership role with comprehensive expertise on sustainable business modelling and IT Infrastructure modernization. Management consulting expertise on ICT Solution Design (DC-DR, Cloud Migration, Information. Security, IT Infrastructure, BCP, Digital transformation). Worked on multiple flagship transformation projects with various clients.

In long 32 Years of journey worked and delivered most of the industry and verticals. Core expertise in the Real Estate, FMCG, BSFI, Manufacturing, Oil and Gas, Government, Telecom. With deep understanding of business functions and its infrastructure earned reputation and been trusted by top executives. Alignment of the IT with the business objective is the core expertise.

AVAR

Association of anti Virus Asia Researchers

AVAR exists to prevent the spread of cyber threats by fostering international cyber security collaboration

The AVAR Platform

Knowledge Center

Professional Development

Networking & Partnering

Conferences & Presentations

Product Launches

Join AVAR Today!

Individual & Corporate Memberships Are Available

www.aavar.org

28th ANNUAL CYBER SECURITY CONFERENCE

AVAR 2025

SHIFTING POWER IN CYBER DEFENSE

3RD TO 5TH DECEMBER 2025

KUALA LUMPUR, MALAYSIA