AVAR

2024

The Battle for Cyber Supremacy

4th – 6th December 2024

Hotel Feathers, Chennai, India

27th ANNUAL CYBER SECURITY CONFERENCE

PARTNERS

Gold Sponsor

eset

Digital Security
Progress. Protected.

Silver Sponsors

CYBER THREAT ALLIANCE

ManageEngine

kaspersky

Bronze Sponsors

AV comparatives

ANKERCLOUD

Axidian

T Shirt Sponsor

SE LABS

Lanyard Sponsor

K7 SECURITY

Supporting Sponsors

CSA
CLEAN SOFTWARE ALLIANCE

Gen™

FLASHM

赛可达实验室
skd labs

Community & Media Partners

cxo cywayz

women in cybersecurity WiCyS

ACNNEWSWIRE

TECH OUTLOOK CIO

CYBER DEFENSE MAGAZINE

THE CYBER EXPRESS

CONTENTS

Abstracts

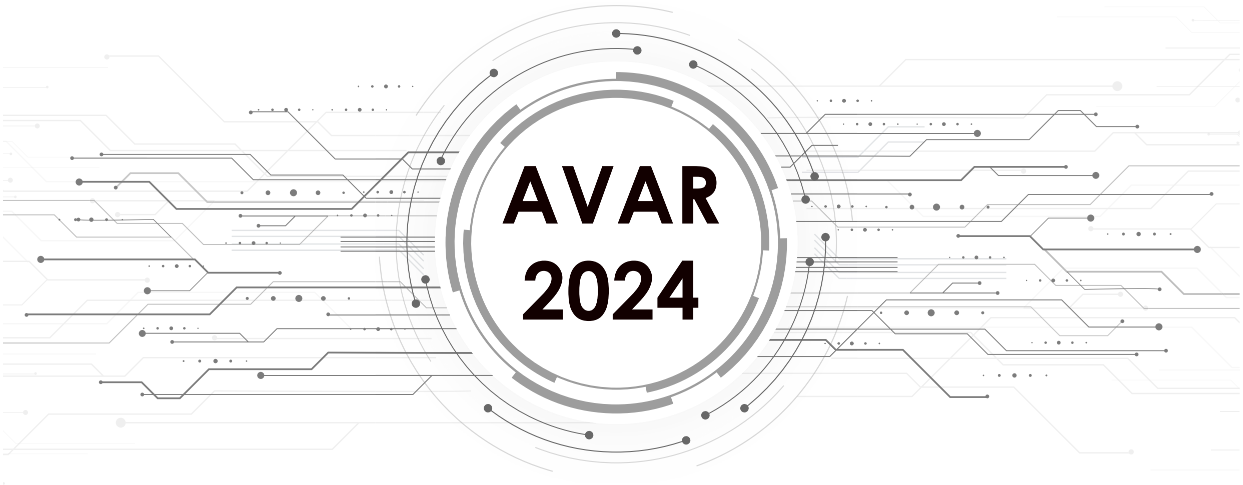
CONTENTS

Panel Discussions

CONTENTS

CISO Connect

Panel Discussion



CEO MESSAGE

International cyber security practitioners again gather for an AVAR event, and I warmly welcome the community to AVAR 2024!

AVAR's conferences set the standard for cyber security knowledge sharing and networking, and AVAR 2024 is no exception: the 27th edition of AVAR's annual conferences will once again feature the world's leading experts and organizations, cutting-edge research, and actionable insight. Any cyber security stakeholder, including leaders, researchers, regulators, and law enforcement, will find value in the discussions at AVAR 2024.

Our theme for the conference this year is 'The Battle for Cyber Supremacy' which has been chosen as cyber security is now a battlefield literally, as nations wage war in the digital sphere, and metaphorically, as cyber security teams feel that they are fighting a battle against relentless adversaries with constant escalation in conflict.

Generative AI is the latest weapon in this battle and, similar to other security technology, it is a weapon that both sides possess. When both sides are evenly matched in terms of capabilities, supremacy will be achieved by the side that makes the best use of available resources which requires knowledge sharing and collaboration – which are the goals of AVAR 2024!

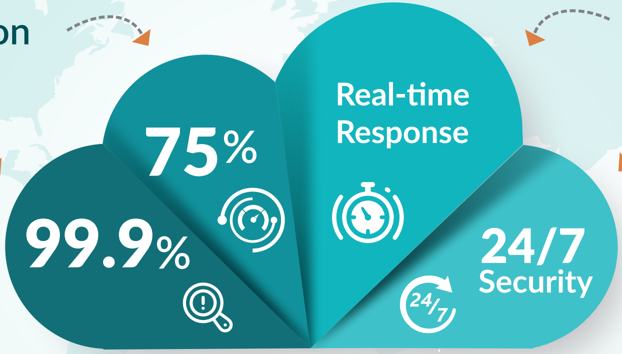
AVAR 2024 includes more than 50 speakers chosen for their unrivalled expertise, with presentations on the latest advancements in threat research and 5 panel discussions featuring distinguished cyber security leaders sharing their experiences from the frontlines of the digital battlefield. Wars also essentially require alliances and AVAR 2024 creates opportunities to identify areas of mutual interest through networking sessions designed to promote relationship building.

Every battle has outstanding generals, and AVAR's CISO Awards recognize exceptional CISOs whose leadership has transformed their organisation's cyber security strategy and results.

Battles are won when everyone contributes to victory, and I am delighted that so many cyber security stakeholders are joining us at AVAR 2024. I thank all the speakers, delegates, partners, and sponsors for their participation in this conference.

I again welcome you to AVAR 2024 and thank you for being warriors in the battle to create a cyber safe world.

Kesavardhanan J
CEO of AVAR



75%
Real-time Response
99.9%
24/7 Security

AGENDA

DAY 1 Wednesday, 4th December, 2024

Time	Activity
16:30 – 18:00	Registration
19:00 Onwards	Welcome drinks reception and dinner

DAY 2 Thursday, 5th December, 2024

Time	Track 1
9:00 – 9:25	Registration
9:25 - 10:40	Conference opening **Welcome Address: Kesavardhanan J** *CEO, AVAR* **Inaugural Address: Dr. Palanivel Thiaga Rajan,** *Minister for Information Technology and Digital Services, Government of Tamil Nadu* **Keynote Address: Artificial Intelligence in Cyber Security** **Lt General (Dr) Rajesh Pant** *Chairman – Cyber Security Association of India* **Keynote Address: Mr. Kumar Jayant, IAS** *Additional Chief Secretary to Government, Information Technology and Digital Services, Government of Tamil Nadu* **Keynote Address: Manickam Kanniah** *Sr. Director, Verizon*
10:40 – 11:00	Refreshment Break

DAY 2 Thursday, 5th December, 2024

Time	Track 1	Time	Track 2	Time	CISO Connect
11:00 – 11:30	**NGate: Novel Android malware for unauthorized ATM withdrawals via NFC relay** Lukas Štefanko, Jakub Osmani, *ESET*	11:00 – 11:30	**Sweet and Spicy Recipes for Government Agencies by SneakyChef** Chetan Raghuprasad, *Cisco*	11:00 – 11:10	**Introduction to CISO workshop** Vaidyanathan Chandramouli, *Apayapadh Advisory*
11:30 – 12:00	**Leveraging Generative AI for Revolutionizing Malware Analysis: A Gemini-Powered Approach** Marvin Castillo, Lovely Jovellee Lyn B Antonio, *G-Data*	11:30 – 12:00	**Exploitation of 0-day vulnerability in Yandex.Browser for persistence** Ivan Korolev, Igor Zdobnov, *Doctor Web*	11:10 – 11:40	**Adversarial Use of GenAI** Michael Daniel, *CTA*
12:00 – 12:30	**The Dark Evolution: MuddyWater's New Tactics and the Manticore Alliance** Lomada Suresh Reddy, Uma Madasamy, *K7 Computing*	12:00 – 12:30	**Exploiting JSON Injection in Microsoft 365 Admin Portal for Email Security Evasion in Spear-Phishing Operations** Reegun Richard Jayapaul, *Trustwave*	11:40 – 12:10	**The Invisible Line: Securing Endpoints in a World Without Boundaries** Romanus Raymond Prabhu, *Zoho Corporation (ManageEngine)*
12:30 – 12:50	**Behind Enemy Lines: Discovering Initial Phases of Cyber Attacks in Asia** Jose Luis Sanchez, *VirusTotal - Google*	12:30 – 12:50	**EastWind Campaign: Defending Against the Latest APT31 Attacks (Sponsor Presentation)** Georgy Kucherin, *Kaspersky*	12:10 – 12:40	**The Future of Cybercrime – Fact or Fiction?** Peter Stelzhammer, *AV-Comparatives*
				12:40 – 12:50	
12:50 – 14:00	Lunch Break				
14:00 – 14:30	**Double check your Zabbix agents: The mystery of GoblinRAT** Vladimir Nestor, *Solar*			14:00 – 14:20	**Defend your cloud infrastructure from Identity Threats** Chandresh Rajkumar, Himani Kambale, *Unosecur*
14:30 – 15:00	**Rise of Synergistic threats: Deception, face swap, GenAI, and obscure Crypto DEX, following the trail of evasive iOS and Android apps** Jagadeesh Chandraiah, *Sophos*	14:30 – 14:50	**Harnessing Language Models for Detection of Evasive Malicious Email Attachments** Abhishek Singh, Kalpesh Mantri, *InceptionCyber.ai*	14:20 – 15:00	**Third Party Vendor Risk Management (Panel Discussion)** Akkaiah Janagaraj, *LTIMindtree* Ashok Kumar Jeyachandran, *G3 Cyberspace* Subramanian Vaithi, *Nium* Sarita Padmini, *Protiviti* Peter Stelzhammer, *AV-Comparatives*
15:00 – 15:30	**SAETI: State-Actor Empowered Threat Intelligence… A Good or a Bad thing?** Righard Zwienenberg, Eddy Willems, *ESET, WAVCi*	14:50 – 15:10	**Beyond the Radar: Analysing the Linux Variant of RedTail Malware** Prashant Tilekar, *Forescout Technologies*	15:00 – 15:20	**Axidian Shield – Identity Threat Detection and Response (ITDR)** Kirill Bondarenko, *Axidian*
		15:10 – 15:30	**Reimagining a robust supply chain security architecture** Pradeep Sekar, *Optiv Security*	15:20 – 15:30	**Interactive Q&A session** Vaidyanathan Chandramouli, *Apayapadh Advisory*
15:30 – 15:50	Refreshment Break				

Day 2 Thursday, 5th December, 2024

Time	Track 1	Time	Track 2
15:50 - 16:20	**GPT vs Malware Analysis: Pitfalls and Mitigations** Ben Herzog, *Check Point*	15:50 - 16:40	**Supply Chain Integrity: Cyber Defense Strategies in the Digital Era (Panel Discussion)** Balakrishnan Kanniah, *VA Tech Wabag* Debasish Das, *One Tata Operating Network* Kannan Srinivasan, *GAVS Technologies* Manickam Kanniah, *Verizon* Vimalaasree Anandhan, *Poshmark*
16:20 - 16:50	**Hunting for Operation FlightNight: Attack Targeted towards Indian Government and Energy sectors** Amey Gat, *Fortinet*		
19:00 - 19:30	Pre-dinner Drinks		
19:30 - 22:00	Gala Dinner		

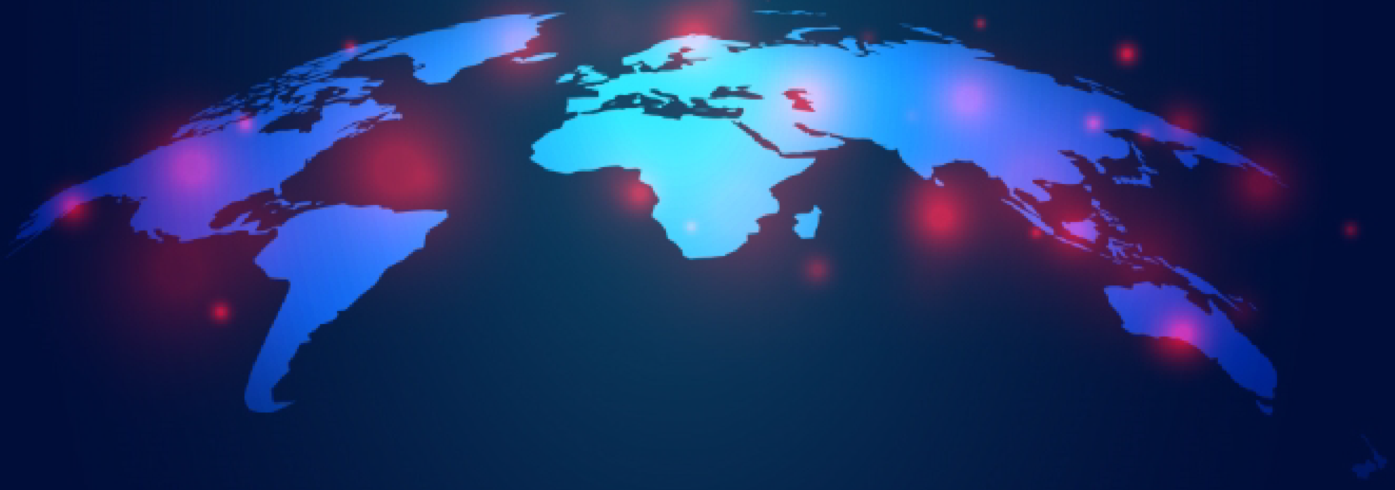
DAY 3 Friday, 6th December, 2024

Time	Track 1
10:00 - 10:20	**Keynote Address: Akkaiah Janagaraj,** *Global Head of Cybersecurity Practice, LTIMindtree*
10:20 - 10:40	**Keynote Address: Threat Intelligence from the Frontlines: A Global Perspective on Evolving Cyber Threats** *Igor Kuznetsov, Director, Global Research and Analysis Team – Kaspersky*

Time	Track 1	Time	Track 2
10:40 - 11:10	**From Code to Crime: Exploring Threats in GitHub Codespaces** Jaromir Horejsi, *Trend Micro*	10:40 - 11:10	**Cloudy With a Chance of RATs: Unveiling APT36 and The Evolution of ElizaRAT** Itan Delshad, *Check Point*
11:10 - 11:40	**Exploring vulnerable Windows drivers** Vanja Svajcer, *Cisco*	11:10 - 11:40	**Navigating Cybersecurity Challenges and Adversaries in Smart Power Meter Technologies** Vikas Karunakaran*, Sectrio*
11:40 - 12:00	Refreshment Break		
12:00 - 12:30	**Charming Viper, Vanishing Crypto** Dhanush, Arun Kumar, *K7 Computing*	12:00 - 12:40	**The Human Element in Cyber Security (Panel Discussion)** Chethan S. Iyengar, *Standard Chartered* Jeannette Jarvis, *Cyber Threat Alliance* Lalit Gupta, *Al Gihaz Holding* Righard Zwienenberg, *ESET* Vimalaasree Anandhan, *Poshmark*
12:30 - 13:00	**Beyond the Package: The New Frontier of MSIX Attack** Prakash Galande, Nitin Shekokar, *Symantec – Broadcom*	12:40 - 13:00	**Challenges in Reverse Engineering Rust-based Malware** Nguyen Tien Cong, Bui Huy Anh, *CMC Cyber Security*
13:00 - 14:10	Lunch Break		

DAY 3 Friday, 6th December, 2024

Time	Track 1	Time	Track 2
14:10 - 14:40	**Should Your EDR Be Based in User-mode? You Might Want to Reconsider** Omri Misgav, *Independent Security Researcher*	14:40 - 15:00	**RATs in the sewers: diving into the BitTorrent cesspool (Sponsor Presentation)** Martin Jirkal, Roman Šíma, *ESET*
14:40 - 15:10	**Deep into the evolution of the SteganoAmor campaign: how the TA558 attacked companies around the world** Aleksandr Badaev, Kseniia Naumova, *Positive Technologies*		
15:10 - 15:30	**With Great Research Comes Great Responsibility (Sponsor Presentation)** Michael Daniel, *Cyber Threat Alliance*	15:00 - 15:30	**Bypassing evasive binaries with Dynamic Binary Instrumentation** Dr. Vlad Constantin Craciun, Andrei Catalin Mogage, *Bitdefender*
15:30 - 15:50	Refreshment Break		
15:50 - 16:30	**Securing your Cloud Infrastructure: Navigating the Dangers (Panel Discussion)** Chandresh Rajkumar, *Unosecur* Dr. Anshu Premchand, *Tech Mahindra* Karthikeyan K, *Logitech* Michael Daniel, *Cyber Threat Alliance* Srinivasan Balraj, *Muthoot Fincorp*	15:50 - 16:30	**Healthcare Cyber Attacks: Managing the Domino Effect (Panel Discussion)** Diptesh Saha, *Accel Limited* Gowdhaman Jothilingam, *LatentView Analytics* Kannan Srinivasan, *GAVS Technologies* Romanus Raymond Prabhu, *Zoho Corporation (ManageEngine)* Senthil Subramaniam ESR, *Infinite Computer Solutions* Smith Gonsalves, *CyberSmithSECURE*
16:30 - 16:50	**The Rise And Fall Of Golang Malware** Subhajeet Singha, *Quick Heal*	16:30 - 16:50	**Lazarus targets freelance developers with DeceptiveDevelopment** Matěj Havránek, *ESET*
16:50 - 17:00	Closing Address		
17:00 - 17:45	EGM and Members’ meeting		



AVAR 2024

SPEAKERS/AUTHORS AND ABSTRACTS

NGATE: NOVEL ANDROID MALWARE FOR UNAUTHORIZED ATM WITHDRAWALS VIA NFC RELAY

Abstract:

While theoretical NFC relay attacks have been discussed for years, real-world attacks remain rare – especially successful ones. Dive with us into NGate, the first publicly known, in-the-wild, Android malware that used an NFC relay attack to facilitate remote ATM withdrawals, and successfully stole thousands from victims in Czechia early in 2024 – with a little help from social engineering and phishing.

These attacks started in Czechia in November 2023. Initially, the attackers took advantage of progressive web apps (PWAs), which are essentially websites that function like mobile apps. They then advanced their tactics by using a more complex form of PWAs called WebAPKs. This progression led to the final step of their attack: distribution of the NGate malware.

To spice things up, we'll delve into NFCGate, the legitimate, open-source, NFC research toolkit that the NGate malware is based on, and explain two additional attack scenarios that can be achieved using the same tooling. During our presentation, we will demonstrate NFC attacks against contactless payments, and NFC token cloning. We will show how attackers can use a smartphone to scan contactless cards in public places, enabling them to make payments simultaneously at a remote terminal. Additionally, we will demonstrate how an attacker can clone the UID of MIFARE Classic 1k NFC contactless smartcards to gain access to restricted areas.

Lukas Štefanko
ESET

Bio:

Lukas Štefanko is an experienced malware researcher with a strong engineering background and a well-demonstrated focus on Android malware research and security. With more than 13 years' experience with malware, he has been focusing on improving detection mechanisms of Android malware and in the past couple of years has made major strides towards heightening public awareness around mobile threats and app vulnerabilities. He has presented at several security conferences such as RSA, Virus Bulletin, Confidence, DefCamp, BountyCon, AVAR, CARO Workshop, Infoshare, Ekoparty, and Copenhagen CyberCrime.

SWEET AND SPICY RECIPES FOR GOVERNMENT AGENCIES BY SNEAKYCHEF

Abstract:

This presentation is about a malicious campaign operated by a Chinese-speaking threat actor, SneakyChef, targeting government agencies, likely the Ministry of External/ Foreign Affairs or Embassies of various countries since as early as 2023, using SugarGh0st RAT and SpiceRAT.

Talos assesses with high confidence that SneakyChef operators are likely Chinese-speaking based on their language preferences, usage of the variants of Chinese's popular malware of choice, Gh0st RAT, and the specific targets, which include the Ministry of External Affairs of various countries and other government entities with the motive of Espionage and data theft. Their notable TTPs include Spear-Phishing campaigns, DLL Side-Loading, custom c2 communication protocol, and abusing legitimate applications.

SneakyChef has used various techniques in this campaign with multi-staged attack chains to deliver the payload SugarGh0st and SpiceRAT. Throughout this presentation, I will discuss various attach-chains and the techniques the threat actor has employed to establish persistence, evade the detections, and implant the RATs successfully.

SugarGh0st RAT infection chains:

We discovered and analyzed three different attack chains in this campaign that delivered the SugarGh0st RAT.

The first infection chain starts with a malicious RAR file containing a Windows Shortcut file with a double extension. When a victim opens the shortcut file, it runs a command to drop and execute an embedded JavaScript file. The JavaScript eventually drops a decoy, an encrypted SugarGh0st payload, a DLL loader, and a batch script. Then, the JavaScript executes the batch script to run the dropped DLL loader by sideloading it with a copied rundll32. The DLL loader will decrypt the encrypted SugarGh0st payload in memory and run it reflectively.

Like the first infection chain, the second attack starts with a RAR archive file containing a malicious Windows Shortcut file forged as the decoy document. The Windows shortcut file, by executing the embedded commands, drops the JavaScript dropper file into the %TEMP% location and executes it with cscript. The JavaScript drops a decoy document, a legitimate DynamicWrapperX DLL, and the encrypted SugarGh0st in this attack. The JavaScript uses the legitimate DLL to enable the embedded shellcode to run the SugarGh0st payload.

The third attack chain is slightly different than the two. Here, the threat actor uses an SFX RAR as the initial vector for this attack. When a victim runs the executable, the SFX script executes to drop a decoy document, DLL loader, encrypted SugarGh0st, and a malicious VB script into the victim's user profile temporary folder and executes the malicious VB script. The malicious VB script establishes persistence by writing the command to the registry key "UserInitMprLogonScript," which executes when a local workgroup or domain user logs into the system. When a user logs into the system, the command runs and launches the loader DLL using regsvr32.exe. The loader reads the encrypted SugarGg0st RAT, decrypts it and injects it into a process.

SpiceRAT infection chains:

In another set of attacks of this campaign, we discovered two other types of attack chains where the actor SneakyChef was implanting a new RAT we dubbed SpiceRAT. The infection chain involves multiple stages launched by an HTA or the LNK file.

The LNK-based infection chain begins with a malicious RAR file containing a Windows shortcut (LNK) and a hidden folder. This folder contains multiple components: a malicious executable launcher, a legitimate executable, a malicious DLL loader, an encrypted SpiceRAT masquerading as a legitimate help file (.HLP), and a decoy PDF document. When the victim extracts the RAR file, the LNK, and a hidden folder are dropped from their machine. Upon a victim opening the shortcut file, which masqueraded as a PDF document, it executes an embedded command to run the malicious launcher executable from the dropped hidden folder. This malicious launcher executable is a 32-bit binary compiled on Jan 2nd, 2024. When launched by the shortcut file, it reads the victim machine's environment variable, the execution

SWEET AND SPICY RECIPES FOR GOVERNMENT AGENCIES BY SNEAKYCHEF

path of the legitimate executable, and the path of the decoy PDF document and runs them using the API ShellExecuteW. The legitimate file is one of the components of the SpiceRAT infection, which will side-load the malicious DLL loader to decrypt and launch the SpiceRAT payload.

The HTA-based infection chain begins with an RAR archive delivered via spear-phishing email. The RAR file contains a malicious HTA file. When the victim runs the malicious HTA file, the embedded malicious Visual Basic script runs and executes and drops the embedded base64 encoded downloader binary and a malicious batch script into the victim machine's applications temporary folder. The batch script decodes and runs a malicious downloader that downloads and unpacks the components of the SpiceRAT, including a legitimate executable, malicious DLL, and an encrypted file. The batch script configures a Windows task that runs the legitimate executable, which side-loads the malicious DLL. The malicious DLL decrypts and runs the SpiceRAT reflectively. The SpiceRAT further downloads the plugin and implants it on the victim's machine as a further-on-payload.

After explaining the attack chains, I will discuss the SugarGh0st RAT and the SpiceRAT functionalities. I will also share insights about our discovery of the RAT's unique command and control communication patterns.

Finally, I will share the indications of SneakyChef's origin as a Chinese-speaking actor and the attribution of the SugarGh0st and SpiceRAT attacks to them.

Chetan Raghuprasad
Cisco Talos

Bio:

Chetan Raghuprasad is a Security researcher with the Cisco Talos, focusing on hunting and researching the latest threats in the cyber threat landscape generating actionable intelligence. He seeks to uncover threat actors' tactics, techniques, and procedures by reversing and analysing the threats to identify the actors' TTPs, motives, and origins. Chetan also publicly represents Cisco Talos by writing the Talos blogs and talking at cybersecurity conferences worldwide.

Chetan Raghuprasad has 16 years of experience in the Information Security sector, having worked within Threat Intelligence, Cyber incident response, and digital forensic analysis teams in technology companies, consulting and financial institutions. Chetan has assisted legal cyber security and Insider threat investigation cases as digital forensic expert.

LEVERAGING GENERATIVE AI FOR REVOLUTIONIZING MALWARE ANALYSIS: A GEMINI-POWERED APPROACH

Abstract:

Generative AI (Gen AI) has emerged as a transformative technology with potential applications across various domains. In the realm of cybersecurity, Gen AI's ability to analyze vast amounts of data and generate insights has sparked interest in its potential. This research explores the efficacy of Gemini, a cutting-edge Gen AI model, as an assistant in the analysis of malware.

The research will showcase the step-by-step process of utilizing Gemini for malware analysis. We will outline the specific techniques and all prompts used to identify Indicators of Compromise (IOCs), such as network signatures, registry modifications, and file system artifacts. The results obtained from Gemini's analysis are compared with the findings of human analysts[1][2] to assess the model's accuracy and effectiveness. Additionally, the research highlights the challenges and limitations encountered when utilizing Gen AI for malware analysis.

This research focuses on Gemini's capability in analyzing different types of malware, with a particular emphasis on Stealer and Remote Access Trojan (RAT). Other malware types, such as Loader, Dropper, Downloader, and Ransomware, are also explored. The analysis involves decompiling malware samples using Ghidra and IDA Pro on various high-level programming languages, primarily focusing on C/C++, but also encompassing malware written in different scripting languages like Javascript, PowerShell, and HTML. By feeding the decompiled code into Gemini, we will utilize its vast knowledgebase and contextual understanding to dissect the intricacies of these threats.

While acknowledging the challenges associated with AI integration, such as the risk of overreliance and the false positives, this research underscores the potential of generative AI to revolutionize malware analysis. We aim to provide practical insights for cybersecurity community, demonstrating the value of combining Gen AI's analytical capabilities with the expertise of human analysts to effectively combat the ever-evolving landscape of cyber threats.

Marvin Castillo
G Data AV Lab. Inc.

Bio:

Marvin started his career in cybersecurity in 2018. Currently working as a Virus Analyst at G Data AV LAB Inc, he specializes in malware analysis, reverse engineering, and threat detection. With a deep passion for threat research, he is constantly engaged in exploring the latest trends and technological advancements.

Lovely Jovellee Lyn B Antonio
G Data AV Lab. Inc.

Bio:

Lovely has over 11 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 traveling together.

EXPLOITATION OF 0-DAY VULNERABILITY IN YANDEX.BROWSER FOR PERSISTENCE

Abstract:

The Russian cybersecurity landscape is now characterized by an ever-growing number of APT attacks on Russian companies. Intruders try to disrupt production processes, stop business operations and exfiltrate information. All of these results in downtime, audits, infrastructure overhauls, etc., which translates into lost profits. Moreover, criminals can be very resourceful in achieving their goals, exploiting all kinds of previously unknown vulnerabilities. Doctor Web has uncovered an APT attack that stands out among others for its rather unusual way to achieve persistence.

In this attack, the criminals attempted to exploit the previously unknown DLL Search Order Hijacking vulnerability in popular Russian browser Yandex.Browser to gain a long-term persistence on the compromised system. The hijacking of the browser would allow attackers to bypass firewalls, create processes from the context of Yandex.Browser, execute commands, etc. The DLL itself is designed to download a previously unseen modular trojan.

In our presentation, we will cover the following aspects of the attack: initial access, execution, persistence, C&C, and evasion. We will also examine the malware involved.

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.

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.

THE DARK EVOLUTION: MUDDYWATER'S NEW TACTICS AND THE MANTICORE ALLIANCE

Abstract:

MuddyWater, the Iranian state-sponsored APT group also known as MERCURY, Mango Sandstorm, Seedworm, and Static Kitten, has been making waves since 2017, primarily targeting Middle Eastern nations but now expanding to India and the USA. Under the same Iranian Ministry of Intelligence and Security (MOIS) umbrella, two more APT groups, Scarred Manticore and Void Manticore, emerged in 2023. Scarred Manticore specializes in espionage, gaining initial access through the Liontail malware framework, while Void Manticore focuses on destructive campaigns, utilizing manual file deletion and custom wipers like BiBi.

MuddyWater's modus operandi involves spear-phishing to deploy backdoors like PowGoop, POWERSTATS, and Mori, often using legitimate file-sharing services for distribution. In 2023, it shifted towards Remote Monitoring and Management (RMM) tools for interactive sessions and increased its focus on Israeli companies. Its evolving C2 infrastructure, from leaked frameworks to the new muddyc2Go and DarkBeatC2, demonstrates adaptability.

Mid-2024 saw another shift with the introduction of the custom "bugsleep" backdoor, injected into browsers or applications like OneDrive for covert control and data exfiltration. This backdoor employs EDR evasion techniques by manipulating process signature and dynamic code policies.

The recent alliance between Scarred Manticore and Void Manticore, combining espionage and destructive capabilities, raises concerns about the potential for shorter, more impactful campaigns.

In this presentation we will scrutinize the upgraded "bugsleep" backdoor, its EDR evasion mechanisms, and the evolution of MuddyWater's C2 frameworks, whilst also shedding light on the TTPs and effective collaborations of the deadly Manticore duo. Given MuddyWater's effectiveness in espionage and its existing interest in Israeli targets, we will also explore whether it might collaborate with or share tools with the other MOIS APT groups to enhance their combined destructive potential.

THE DARK EVOLUTION: MUDDYWATER'S NEW TACTICS AND THE MANTICORE ALLIANCE

Lomada Suresh Reddy
K7 Computing

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.

Uma Madasamy
K7 Computing

Bio:

Uma completed her Master's degree in Computer Science and Engineering from Anna University in 2021. She started her career as Threat Researcher at K7 Labs, her main role involves detecting and reversing different types of malware at various layers, in addition to staying informed about the latest industry trends. She has a strong passion for cybersecurity and safeguarding the digital realm. Also, she has written and published various technical blogs on K7 Labs technical blog page.

EXPLOITING JSON INJECTION IN MICROSOFT 365 ADMIN PORTAL FOR EMAIL SECURITY EVASION IN SPEAR-PHISHING OPERATIONS

Abstract:

Utilizing Microsoft M365 services enables the circumvention of email security measures, allowing for the successful delivery of spear-phishing emails with malicious JSON injection content to targeted users. This method has been demonstrated effectively in an environment featuring Microsoft SafeLinks. Notably, the attacker does not require hosting the payload externally. The lack of sanitization of the 'displayname' and 'Password' input allows for the inclusion of special characters and links that can bypass Safe Links and other email security detections.

Note : This is the continuity of first part which I shared in Avar 2022, This is the findings and study of another new vector which I found latest

Refer: https://aavar.org/avar2022/index.php/spoofing-microsoft-m365-service-to-send-phishing-emails-that-will-bypass-email-security-protections/

This scenario is indicative of JSON injection, effectively circumventing security mechanisms like Safe Links. While CWE-91 is traditionally referred to as 'XML Injection', it broadly encompasses the manipulation of structured data formats, including JSON.

Research Status

These vulnerabilities were responsibly reported to Microsoft. Microsoft validated the findings but has not fixed them as of now, marking them for future review.

Reegun Richard Jayapaul
Trustwave

Bio:

As a Principal Threat Hunter at Trustwave, I work the SpiderLabs team to conduct threat hunting and research, simulate, and discover new attacks, and develop enhanced detection and prevention mechanisms. With over 13 years of experience in security research, malware analysis, reverse engineering, incident response, security training, and offensive security, I have served clients across diverse sectors and technologies. I am a contributor to the LOLBAS (Living Off the Land Binaries and Scripts) project, documenting binaries and scripts that attackers use to circumvent security controls. My discoveries and reporting of multiple vulnerabilities, including a Microsoft Teams RCE and privacy issues. My mission is to bolster the defensive capabilities of the cybersecurity community by sharing my offensive methodologies and findings. I possess extensive experience in addressing various security threats and malware, particularly exploit kits, and APT groups from DPRK, Russia, PRC, and TA505. Notably, I have been a principal contributor to the investigation of the GoldenSpy and GoldenHelper threat groups, further showcasing my expertise in the field of cybersecurity.

BEHIND ENEMY LINES: DISCOVERING INITIAL PHASES OF CYBER ATTACKS IN ASIA

Abstract:

In an era where cyber threats are increasingly sophisticated and pervasive, understanding the early stages of cyber attacks is crucial for effective defense. This talk is a practical talk designed to illuminate the covert operations of threat actors targeting Asia, sometimes by threat actors based in Asia as well. This presentation will delve into the methodologies and tactics employed by cybercriminals and advanced persistent threats (APTs) during the initial phases of their attacks, providing actionable insights and strategies for improve the detection/hunting capabilities.

We will explore real case studies of operations in Asia we observed, dissecting the early indicators. Attendees will gain practical insights into the very early phases behaviors commonly used by threat actors. By examining these stages, we will identify patterns and techniques that can be directly applied for early detection and mitigation.

Jose Luis Sanchez
VirusTotal – Google

Bio:

Joseliyo Sanchez is a security engineer at VirusTotal - Google. Member of the ENISA Working Group on Cyber Threat Landscapes. Previously worked at McAfee and BlackBerry as a threat researcher. His main objectives are threat hunting that leads to detection engineering and analysis of APTs and Crime groups.

EASTWIND CAMPAIGN: DEFENDING AGAINST THE LATEST APT31 ATTACKS

Abstract:

APT31 is an advanced Chinese-speaking threat actor that has been consistently targeting high-profile organizations all around the world, including those located in Europe. While tracking this actor, we have discovered its latest activities that were conducted at the end of July 2024. So, what tactics did APT31 use in these attacks, and most importantly, how can we defend against them?

To answer these questions, we will first discuss how APT31 was initially infecting networks of target organizations. Following that, we will speak about tools that we found used to gather information about compromised machines. Afterwards, we will describe what information from infected computers attackers were interested in, as well as what unique malware was used to exfiltrate it. While discussing the malware, we will demonstrate various analysis techniques useful to reverse engineers that allow to efficiently deobfuscate the discovered implants. Additionally, we will pay particular attention to techniques that APT31 leveraged to make its activities less noticeable to security solutions.

We will then use all the presented information to compare recent attacks of APT31 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 APT31 attacks.

Georgy Kucherin
Kaspersky

Bio:

Alongside his dedication to his academic pursuits as a student at Moscow State University, Georgy demonstrates an unwavering passion for unraveling the intricacies of complex malware and employing reverse engineering techniques to analyze and understand its inner workings. With a strong background in cybersecurity research, Georgy has contributed significantly to the field through his comprehensive investigations into advanced persistent threats (APTs) such as FinFisher, APT41, and Lazarus. Georgy actively shares his research findings at prominent conferences, including VirusBulletin, AVAR, Security Analyst Summit, and other renowned gatherings, where his presentations captivate audiences and contribute to the collective knowledge of the cybersecurity community. Driven by a relentless pursuit of knowledge and a commitment to securing the digital landscape, Georgy Kucherin is an emerging force in the field of cybersecurity research, poised to make lasting contributions in the fight against cyber threats.

DOUBLE CHECK YOUR ZABBIX AGENTS: THE MYSTERY OF GOBLINRAT

Abstract:

Sometime ago, our team spotted how something in the network of a critical infrastructure organization was deleting system logs. We didn’t find anything suspicious during the initial analysis of the affected machine; however, at some point we spotted a malicious service that looked like a Zabbix agent on a neighboring host. Further investigation revealed that the agent turned out to be a malicious program that we called GoblinRAT.

One of the most interesting things about it is how hard it tries to be invisible to security engineers:

- it has lots of code features aimed at evading detection (self-destruction, processes masquerading, port-knocking, etc.);
- it used hacked websites of legitimate businesses for C2-communications;
- as we’ve been unraveling incidents involving GoblinRAT, we haven’t seen samples of this malware using the same persistence technique twice.

The RAT was used in one of the stealthiest and most mysterious attacks we have ever investigated. We saw it on a very limited number of targets, and nowhere else. We tried to search on our own; we shared our samples with industry colleagues, but the result was nothing. We managed to follow the malware evolution from 2020 to 2022. In our talk we will conduct a deep dive into how GoblinRAT works, and perhaps, with the help of our colleagues from different parts of the world, we will manage to solve the riddle of GoblinRAT: shed light on its origin and activities outside of those we saw in our investigations.

Vladimir Nestor
Solar

Bio:

Vladimir started his career in cyber security as a digital forensic engineer during his university studies in UTMN in 2018. At the same time he also participated in a large number of CTF challenges, which helped him to develop his reverse engineering skills. Vladimir used this invaluable experience to fight against modern cyber threats when he joined Solar in 2021 and later got promoted to head of reverse engineering in the 4RAYS research team. He is also working on his PhD degree and currently he is a PhD candidate at Cryptology and Cybersecurity department in MePHI, Moscow.

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

BRANDEFENSE
CHECK POINT
CISCO
CUJOAI
CyberCX
FORTINET
Gen
Hitachi Systems
JUNIPer NETWORKS
K7 COMPUTING
LevelBlue/Labs
maltiverse
McAfee
minsait An Indra company
NEC
NOZOMI NETWORKS
NTT
OneFirewall
Outpost24
paloalto NETWORKS
panda a WatchGuard brand
Penta SECURITY
RAPID7
Red Piranha
REVERSING LABS
SANDS Lab
Scitum
SecurityScorecard
SK shieldus
SOCRadar Your Eyes Beyond
SONICWALL
SOPHOS
Symantec A Division of Broadcom
TEHTRIS FACE THE UNPREDICTABLE
Telefónica Tech
TINEXTA CYBER

JOIN US!

https://www.cyberthreatalliance.org

CYBER THREAT ALLIANCE

RISE OF SYNERGISTIC THREATS: DECEPTION, FACE SWAP, GENAI, AND OBSCURE CRYPTO DEX, FOLLOWING THE TRAIL OF EVASIVE IOS AND ANDROID APPS

Abstract:

Synergistic refers to the idea that combined elements or efforts produce a greater effect together than the sum of their individual effects. Synergetic threats refer to how the interaction or cooperation of multiple individual innocuous looking elements results in an outcome that would be classified as a threat when you combine those elements. Generative AI (GenAI) into the mix, the threat becomes more potent and dangerous.

We have noticed that in the last few years, with the advance of technology, there has been a rise of threats that only look malicious when you combine elements together. These could be fake reward-based e-shopping apps, fraud apps, and fake romance and investment scam apps.

A relatively new shopping app or investment or cryptocurrency app wouldn't look malicious until you check the source, how it was distributed and made to install using social engineering, and finally know that they lost money.

There are several stages to these apps, starting from choosing victims to deceiving app store reviews, social engineering, and finally using multiple wallets, obscure decentralised exchanges, and money mules to extract money.

With the advance and availability of GenAI, we have noticed and read about increased use of face swapping using AI generated images, using auto-generated text and voice for communication, and script generation.

In this presentation, we will –

- Discuss what are Synergistic mobile threats and why we think it's increasingly difficult to identify them.
- Discuss different types and stages of Synergistic threats.
- How they appear innocuous and change to evade App store reviews
- Gen AI use, discuss freely available tools, share screenshots sent by victims, and adverts of Gen AI tools used by threat actors
- Discuss the money trail use of threat actors including use of obscure Cryptocurrency DEX.

RISE OF SYNERGISTIC THREATS: DECEPTION, FACE SWAP, GENAI, AND OBSCURE CRYPTO DEX, FOLLOWING THE TRAIL OF EVASIVE IOS AND ANDROID APPS

Jagadeesh Chandraiah
SophosLabs

Bio:

Jagadeesh Chandraiah is a senior malware researcher at SophosLabs, specializing in mobile malware analysis. He has been working at SophosLabs for over 10 years. He started working on Windows malware analysis and is currently focusing on mobile and Mac malware analysis. He has a master's degree in computer systems security from the University of South Wales.

Jagadeesh likes to track malware, research and find novel ways to detect and remediate them. He is a frequent contributor to the Sophos X-Ops blog and has written blog posts on several malware topics. He also regularly presents his research at international security conferences and, in the past, has presented his research at DeepSec, AVAR, CARO, and Virus Bulletin. Outside of work, Jagadeesh enjoys playing badminton."

HARNESSING LANGUAGE MODELS FOR DETECTION OF EVASIVE MALICIOUS EMAIL ATTACHMENTS

Abstract:

The HP Q3 2023 Threat Report highlights that 80% of malware is delivered via email, with 12% bypassing detection technologies to reach endpoints. The 2023 Verizon Data Breach Report also indicates that 35% of ransomware infections originated from email. Two primary factors contribute to evasion: the volume and cost challenges of sandbox scanning, which lead to selective scanning and inadvertent bypasses, and the limitations of detection technologies like signature-based methods, sandbox and machine learning, which rely on the final malicious payload for decision-making. However, evasive multi-stage malware and phishing URLs often lack malicious payload when analyzed by these technologies. Additionally, generative AI tools like FraudGPT and WormGPT facilitate the creation of new malicious payloads and phishing pages, further enabling malware to evade defenses and reach endpoints.

To address the challenge of detecting evasive malware and malicious URLs without requiring the final malicious payload, we will share the detailed design of an Interpretative Processor Engine (IPE) specifically designed to detect malicious attachments, URLs, and identity-based attacks by understanding the semantics of the email and leveraging them as features instead of relying on the final malicious payload for its decision making. The IPE harnesses a layered approach employing supervised and unsupervised AI-based models leveraging transformer-based architecture to derive deeper meaning embedded within the email's body, text in the attachment, and subject.

We will first dive into the details of the semantics commonly used by threat actors to deliver malicious attachments, which lays the foundation of our approach. These details were derived from the analysis of a dataset of malicious emails. The text from the body of the email was extracted to create embeddings. UMAP aided in dimensionality reduction, and clusters were generated based on their density in the high-dimensional embedding space. These clusters represent different types of semantics employed by threat actors to deliver malicious attachments.

In the presentation we will share the details of our approach in which every incoming email undergoes zero-shot semantic analysis using Llama-3 to determine if it contains semantics typically used by the threat actors to deliver malicious attachments. Additionally, email's body is further analyzed for secondary semantics, including tone, sentiment, and other nuanced elements. Once semantics are identified, hierarchical topic modeling is then applied to uncover the relationships between various topics.

Primary and secondary semantics from the email, along with hierarchical topic modeling, deep file parsing results of attachments, and email headers, are sent to the expert system. This system combines the information using rules to determine if the email (with attachments or URLs) is malicious or benign.

This comprehensive approach identifies malicious content without depending on the final payload, which is crucial for any detection technology.

Our presentation will show how LLM models can effectively detect evasive malicious attachments without depending on the analysis of the malicious payload, which typically occurs in the later stages of attachment analysis. Our approach is exemplified by our success in defending against real-world threats, including HTML smuggling campaigns, Microsoft credential phishing scams, MS Office remote template injection attacks and even new APT attack targeting a defense-related organization.

Using insights from our case studies, our presentation will detail an APT attack on a defense-related organization and explain how leveraging semantic analysis as a feature set successfully detects such attacks. The presentation will conclude with results observed from the production traffic.

HARNESSING LANGUAGE MODELS FOR DETECTION OF EVASIVE MALICIOUS EMAIL ATTACHMENTS

Abhishek Singh
InceptionCyber.ai

Bio:

Abhishek Singh is the Founder and CTO of InceptionCyber.ai. He is a security R&D leader with 15+ years of experience, passion, and a proven track record of driving AI and Cyber Security Research and Engineering, which solves complex problems, resulting in a winning technology leading to revenue gains at Cisco, FireEye, and Microsoft. He holds 39 patents, has authored 17 research papers, seven technical white papers, contributed to three books and presented his research at Virus Bulletin 2023, 2020, 2019, Black Hat 2022, 2013, RSA 2016, CansecWest 2009, AVAR 2023, ACSA.

Patents and papers detail work in algorithms, generative and predictive AI-based approaches to detect advanced threats, and architecture of technologies such as the virtual machine-based approach for threat analysis, EDR, RASP, DAST, Active Defense (Deception), email, web, and IPS.

Many algorithms and preventive features Abhishek has designed are key concepts in technologies like RASP and Active Defense (Deception). His notable recognitions include the following:

2019 Reboot Leadership Award (Innovators Category): SC Media

Shortlisted for Virus Bulletin's 2018 Péter Szőr Award

Cyber Security Professional of the Year - North America (Silver Winner) Cyber Security Excellence Awards 2020

He holds a Double Master of Science in Computer Science and Information Security from the prestigious College of Computing, Georgia Tech, and a B.Tech in Electrical Engineering from the prestigious Indian Institute of Technology, IIT-BHU. He has also completed a Master of Engineering Leadership (ELPP++) from UC Berkeley and Postgraduate AI and Deep Learning Courses from the Indian Institute of Technology, IIT-Guwahati.

HARNESSING LANGUAGE MODELS FOR DETECTION OF EVASIVE MALICIOUS EMAIL ATTACHMENTS

Kalpesh Mantri
InceptionCyber.ai

Bio:

Kalpesh Mantri is the Founding Principal Research Engineer at InceptionCyber.ai, bringing over 12 years of expertise in Cybersecurity Research and Development. He spearheads pioneering research initiatives and develops innovative, patented solutions with a focus on investigating email threats, particularly within the phishing and malspam landscape.

Before joining InceptionCyber.ai, Kalpesh held the position of Senior Security Engineer, where he specialized in malware reverse engineering, threat hunting, and advanced detection techniques. He played a pivotal role in investigating APT (Advanced Persistent Threat) attacks, notably contributing to the exposure of critical operations such as 'Operation SideCopy' and 'Operation HoneyTrap,' which targeted defense sectors.

Kalpesh is an active member of the cybersecurity community and a regular speaker at prominent security conferences. His presentations have been featured at Virus Bulletin (2020), AVAR (2023, 2016, 2015), and CARO Workshop (2020, 2017).

He holds both Bachelor's and Master's degrees in Computer Science and has completed a Professional Certificate Programme in Applied Data Science and Machine Learning from the Indian Institute of Management Kozhikode (IIM Kozhikode).

SAETI: STATE-ACTOR EMPOWERED THREAT INTELLIGENCE... A GOOD OR A BAD THING?

Abstract:

State-Actor Empowered Threat Intelligence (SAETI) represents a potent blend of government resources and cybersecurity expertise aimed at identifying, assessing, and mitigating threats in cyberspace. On the positive side, SAETI can significantly enhance national security by providing comprehensive insights into potential cyberthreats from hostile states, criminal organizations, and terrorist groups. Governments can leverage their vast resources, including advanced technologies and intelligence networks, to gather and analyze data more effectively than private entities can. This level of threat intelligence can lead to more robust defense mechanisms, better-prepared responses to cyber incidents, and a more secure digital infrastructure for both public and private sectors.

But the empowerment of state actors in threat intelligence also raises several concerns. One major issue is the potential for abuse of power and overreach. State actors with extensive surveillance capabilities might infringe on citizens' privacy and civil liberties under the guise of national security. The "centralized" control over threat intelligence might lead to a lack of transparency and accountability, making it difficult to ensure that such powers are not misused. There is a risk that the focus on national security could lead to the suppression of dissent and the targeting of political opponents, thereby undermining democratic values. And it can also cause private organizations to lose visibility as they will lose telemetry possibilities, such as with the EU regulated "electronic IDentification, Authentication and trust Services", or short: eIDAS.

A significant drawback is the international implications of SAETI. When state actors engage in cyberoperations, it can escalate tensions between nations and contribute to an ongoing cyberarms race. Countries might feel compelled to enhance their own cybercapabilities in response, leading to an environment of mutual distrust and increased cyberconflict. This can also complicate diplomatic relations and international cooperation on cybersecurity issues; Instead of fostering a collaborative approach to securing cyberspace, the involvement of state actors may lead to a fragmented and adversarial global landscape. Information professionals in the public sector have the Code of Ethics, established by the International Federation for Information Processing (IFIP) in 2020. Almost all affiliated organizations for information professionals endorse this code as a basis and guideline for methods, best practices, standards, and frameworks. The question is whether state-affiliated actors can and will use a code similar to the one that provides confidence in the private sector.

Join us while we take a tour having a look at all the good and bad things of SAETI, where of course a flashback to ancient and historical intelligence services is not forgotten, as we always must learn from past mistakes, right?

SAETI: STATE-ACTOR EMPOWERED THREAT INTELLIGENCE… A GOOD OR A BAD THING?

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 on 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.

Eddy Willems
WAVCi

Bio:

Eddy Willems is a worldwide known cyber security expert from Belgium. He is a board member of 3 security industry organizations, EICAR, AVAR and LSEC, and is independent Security Evangelist at WAVCi, his own company. 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 over 3 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 recent Dutch SF cyberthriller 'Het Virus' (English version coming soon). Eddy is a known inspiring speaker and is giving lectures and presentations (including TEDx) worldwide for a very diverse audience from children to experts.

BEYOND THE RADAR: ANALYSING THE LINUX VARIANT OF REDTAIL MALWARE

Abstract:

In the current cybersecurity landscape, Linux systems are increasingly targeted by sophisticated threats and malware, with RedTail serving as a prime example. While the Windows variant of this malware has received considerable attention, its Linux counterpart has largely gone unnoticed. This presentation aims to comprehensively examine this lesser-known Linux variant.

RedTail is a sophisticated malware designed for unauthorized cryptocurrency mining, specifically targeting Monero. First identified in January 2024, it has been active since at least December 2023. Recent iterations demonstrate enhanced evasion and persistence mechanisms, highlighting the significant expertise and resources behind its development.

Previously, RedTail was delivered by exploiting several vulnerabilities, including those affecting ThinkPHP (CVE-2018-20062), Log4j (CVE-2021-44228), VMWare Workspace ONE (CVE-2022-22954), TP-Link routers (CVE-2023-1389), Ivanti Connect Secure (CVE-2023-46805 and CVE-2024-21887), and PAN-OS (CVE-2024-3400).

This presentation will analyse a recent campaign that delivered newer versions of RedTail via exploits of CVE-2024-4577, a critical security vulnerability in PHP servers.

Through a detailed analysis and structured workflow, we will explore RedTail's inner workings. This deep dive will include an overview of RedTail's behaviour, persistence mechanisms, interactions with miner pools, encrypted communication methods, monitoring and concealment capabilities, and the development of a Command and Control (C2) environment. By understanding these aspects, we aim to shed light on this sophisticated threat and enhance our defense strategies against it.

Prashant Tilekar
Forescout Technologies

Bio:

Prashant Tilekar is a senior threat detection engineer at Forescout Technologies, he has over 9 years of experience in the cyber security domains. He specializes in threat detection, threat hunting, deep malware analysis, reverse engineering, APT campaign tracking and threat intelligence analysis. Additionally, he is committed to spreading his knowledge through writing blogs, white papers and participating in international conferences. Prashant has been a speaker at many top security conferences, including VB2023, AVAR2023, AVAR2021 and ThreatCon.

REIMAGINING A ROBUST SUPPLY CHAIN SECURITY ARCHITECTURE

Abstract:

Global supply chains are undergoing massive strains in 2024 due to geopolitical conflicts, rapid technological evolution and regulatory changes that pose challenges to organizations irrespective of the industries they operate in. The extended supply chain for hardware suppliers and service providers spans several countries and continents while the sprawl of software components and open-source projects further increase the sophisticated nature of supply chain attacks. Another internal challenge for organizations is the governance and ownership of supply chain security which is usually shared amongst security, procurement and legal teams. Securing the supply chain and ensuring uninterrupted business operations have become top of mind for business and security leaders in their day-to-day job responsibilities.

So how can global organizations protect their supply chains from cyber criminals targeting them, suppliers and third-party vendors with whom they have dependencies, counterfeit products from being introduced and software supply chain vulnerabilities from impacting downstream organizations. This talk will focus on a step-by-step approach to build a supply chain security architecture and focus on three key components: hardware supply chain, software supply chain and service provider supply chain. An evaluation of the current state of each of these layers and the components needed to make them more robust will be presented so audience members can apply it within their own organizations.

In this interactive session, we will discuss a real-life case study of a Canadian multinational financial services company where the challenge was to securely manage the organization's supply chain across the 36 countries it was operating in. For this organization, we leveraged and applied architectural principles to build in traceability from the key business objectives of the executive stakeholders to the specific security services, mechanisms, and components that every security and procurement teams needed to incorporate to secure their supply chain. These security components were utilized to build a supply chain architecture that weaved in governance for the security and procurement teams involved. The result is an adaptable security architecture that is used by security teams as well as business objectives that matter to the CEO and Board.

REIMAGINING A ROBUST SUPPLY CHAIN SECURITY ARCHITECTURE

Pradeep Sekar
Optiv Security Inc.

Bio:

Pradeep Sekar is a seasoned cyber security leader who has worked closely with and guided Fortune 100 and Fortune 500 Chief Information Security Officers (CISO), Chief Information Officers (CIO) and their teams across various industries on developing and sustaining a secure, adaptive and robust cyber security program. His unique expertise includes the delivery of innovative cyber strategy solutions and benchmarking insights for global organizations as they look to transform their cyber programs.

He is currently a Managing Director with Optiv Security Inc. where he leads the Strategy & Risk Management Services. He is also the leader for the 'Security in Mergers & Acquisitions' offering which advises and supports clients with conducting security due-diligence efforts and enhancing the security posture of the combined entity in the merger or acquisition transaction.

He is a member of the Economic Times India Leadership Council, which is an exclusive peer group forum of Heads of Businesses from Corporations representing all Indian industries and aims to work towards the end goal of transforming India's business ecosystem through deliberations and candid exchange of ideas, setting macro agenda for scaling up businesses and driving change that would have a positive impact on business and the overall economy.

He has published thought leadership around security governance, threat profile and risk assessments in industry publications such as ISACA journal as well as on Optiv website (www.optiv.com). He has presented at the IIA/ISACA 9th Annual Hacker conference in Chicago, US; ISACA Annual Karnataka conference in Bangalore, India; and ISC2 Bangalore chapter conference.

GPT VS MALWARE ANALYSIS: PITFALLS AND MITIGATIONS

Abstract:

For what fundamental reasons does The Big Promise of AI fail in domains that require deep expertise such as malware analysis, and what can we do to mitigate that failure? What do we do when GPT-4 casually suggests an analyst should take a course of action that multiplies the project's time cost by a factor of three thousand? In this talk we will probe, characterize, name and give examples of the limiting principles that together constitute the 'hard ceiling' we encountered trying to apply GPT-4 to malware analysis, and other problem domains that require expertise. We will then show a variety of techniques that we used to break free of these limitations.

Ben Herzog
Check Point Software

Bio:

Ben is a security researcher. His technical work includes reverse engineering of Rust PL features and cryptanalysis of targeted ransomware. He has also published technical profiles of various malware strains, as well as many introductory texts and detailed reviews on the subjects of malware, cryptography and vulnerability research.

HUNTING FOR OPERATION FLIGHTNIGHT: ATTACK TARGETED TOWARDS INDIAN GOVERNMENT AND ENERGY SECTORS

Abstract:

We were analyzing binaries from targeted attack towards Indian Government entities and energy sector entities in a operation coined as Operation FlightNight. It was interesting to do research and check the activities done by malware used by these threat actors. The targeted Phishing campaign spread a customized malware which was stealing information from multiple browsers of the victims.

This presentation will cover various aspects about Operation FlightNight binary Analysis & Threat Hunting:

- Threat Hunting for this custom malware
- Tactics and Delivery mechanism used by Actors to infect the victims. (Targeted Spear Phishing)
- Malware Payloads analysis
- Data stealing methods
- Behavioral indicators
- Threat Hunting for this custom malware

Amey Gat
Fortinet

Bio:

Currently working as a Principal Threat Researcher at Fortinet. Working from 19+ years in industry, previously worked as Threat Intelligence Researcher, Information Security consultant, Developer of Firewall/IDS/IPS devices. Worked in various aspects of Threat Intelligence like Darknet coverage, OSINT, Building & deploying Honeypots, Automation of Darknet data collection. Moderator and Core Team member of hackers group Garage4hackers one of the leet hacker groups of India. Python programmer, official programmer in the past and Now for automation and fun and the love of python. Lock picking enthusiastic, done lock picking workshop at Garage4Hackers meet. Also conducted the first Lock picking workshop in India at NullCon 2015. Hardware and Electronics enthusiast, works with AVR and other embedded devices as a hobby. Created first ever hardware badge of Nullcon conference in 2014.

FROM CODE TO CRIME: EXPLORING THREATS IN GITHUB CODESPACES

Abstract:

Cloud-based remote development environments allow developers to virtually code from anywhere and start right from any device with a browser and an internet connection. GitHub Codespaces, initially in preview for specific users, became widely available for free in November 2022 during the GitHub Universe online event. This cloud-based IDE allows developers and organizations to customize projects by using configuration-as-code features, easing some previous pain points in project development. Since any GitHub user could create Codespaces, it did not take long for attackers to find ways of abusing this service. Since June 2023, we have noticed in-the-wild campaigns spreading infostealer malware. We found that GitHub Codespaces was being abused to develop, host, and exfiltrate stolen information via webhooks.

This is the first time GitHub Codespaces has been abused by cybercriminals to develop infostealing malware.

In this presentation, we will introduce Github Codespaces and go through the different features of this service. We then have a look at the malicious campaigns and malware families observed in-the-wild. One interesting and discussed piece of malware is called DeltaStealer, a family of credential stealers implemented in Rustlang or frameworks like Electron. The stealer's source code seems to be a rinse-and-repeat of similar projects shared on GitHub and hence, several variants of the malware exist. Some variants of the stealer possess quite unique features - in addition to implementing anti-debug features, credential stealing capabilities for Chromium-based web browsers, cryptocurrency wallets and applications like Discord, Steam, they achieve persistence using a well-known technique of patching ASAR files of Discord. The patch lowers the security of authentication process in Discord, and exfiltrates sensitive user information to a cloud-based webhook.

The infostealers have been developed using cloud-based IDEs and contain interesting artifacts like debug symbols which in turn reveal information about the developer(s) of the infostealer. The developer(s) behind this family of stealers are also quite active on various social media platforms, where they boast the capabilities of their infostealers. In the presentation, we will include some of the screenshots shared on social media proving the usage of cloud-based IDEs.

We will conclude the presentation with insights on how to hunt for similar threats and recommendations on the measures one can take against such evolving threats where malware authors leverage cloud services to rapidly develop infostealers.

Jaromir Horejsi
Trend Micro

Bio:

Jaromir Horejsi is a Senior Threat Researcher for Trend Micro Research. He specializes in tracking and reverse-engineering threats such as APTs, DDoS botnets, banking Trojans, click fraud, and ransomware that target both Windows and Linux. His work has been presented at RSAC, SAS, Virus Bulletin, HITB, FIRST, AVAR, Botconf, and CARO.

CLOUDY WITH A CHANCE OF RATS: UNVEILING APT36 AND THE EVOLUTION OF ELIZARAT

Abstract:

APT36, also known as Transparent Tribe, is a Pakistan-based threat actor which became notorious for persistently targeting Indian government organizations, diplomatic personnel and military facilities. APT36 has executed numerous cyber-espionage campaigns against Windows, Linux, and Android systems.

In a recent campaign, the actor utilized a particularly insidious Windows RAT known as ElizaRAT. First discovered in 2023, ElizaRAT has undergone significant evolution, enhancing its capabilities to evade detection and maintain reliability with its command and control (C&C) communication, a key aspect of its development.

This presentation will focus on the evolution of ElizaRAT, examining the various payloads and infrastructures employed by APT36. We will detail the advantages and limitations of their campaigns and offer a fresh perspective on tracking this threat actor.

Itan Delshad
Check Point Software

Bio:

Itan is a seasoned threat researcher currently working at Check Point's Research Group (CPR). With 5 years of military experience as a malware researcher and SOC analyst, Itan has a strong foundation in cybersecurity. After transitioning from the military, Itan spent two years in the government sector, where he developed a deep passion for threat intelligence. This journey ultimately led him to his current role at Check Point, where he continues to leverage his extensive expertise in the field.

EXPLORING VULNERABLE WINDOWS DRIVERS

Abstract:

Drivers have long been of interest to threat actors, whether they are exploiting vulnerable drivers or creating malicious ones. Vulnerable drivers, LOLDrivers, are difficult to detect and successfully leveraging one can give an attacker full access to a system.

Windows drivers and the kernel can be overwhelming to learn about, as these topics are vast and highly complex. The documentation available on these subjects is daunting and difficult to navigate for newcomers, even for those with programming experience.

This initial hurdle and steep learning curve create a high barrier of entry into the subject. To many, the kernel space seems to be an arcane and hidden part of the operating system.

With the existence of vulnerable drivers, there is a need for those who can analyze them to identify and understand vulnerabilities. This analysis requires specific knowledge of the Windows operating system, which can be difficult to acquire.

This presentation will explore vulnerable Windows drivers and their recent usage by malicious actors. The attendees will leave with understanding of vulnerabilities in Windows drivers as well as the operating system mitigations designed to prevent a successful exploitation.

Vanja Svajcer
Cisco

Bio:

Vanja Svajcer works as a Technical Leader at Cisco Talos. He is a security researcher with more than 20 years of experience in malware research, cyber threat intelligence and detection development.

Vanja enjoys tinkering with automated analysis systems, reversing binaries and analysing mobile malware. He thinks all the time spent hunting in telemetry data to find new attacks is well worth the effort. He presented his work at conferences such as Virus Bulletin, RSA, CARO, AVAR, BalCCon and others.

NAVIGATING CYBERSECURITY CHALLENGES AND ADVERSARIES IN SMART POWER METER TECHNOLOGIES

Abstract:

In this presentation, titled "Navigating Cybersecurity Challenges and Adversaries in Smart Power Meter Technologies," we will explore the growing landscape of cyber threats targeting the energy industry, with a particular emphasis on smart power meter technologies. The session will begin with a detailed analysis of recent cyber incidents that have disrupted the sector, focusing on high-profile attacks that have exposed vulnerabilities in the smart grid infrastructure. We will identify and profile the key threat actors involved, including nation-state actors, organized crime groups, and independent hackers. By delving into their motives and objectives, we will provide insights into the diverse array of adversaries targeting these critical systems.

The core of the presentation will cover the tactics, techniques, and procedures (TTPs) employed by these malicious entities. We will dissect specific attack vectors, such as malware deployment, remote access exploits, and advanced persistent threats (APTs), to illustrate how these adversaries infiltrate and manipulate smart meter networks. In addition to discussing the technical aspects of these attacks, we will highlight the real-world consequences, including financial losses, compromised data integrity, and potential impacts on energy distribution and consumer trust.

A key feature of the presentation will be a recorded demonstration of a live attack on a smart meter. This demonstration will showcase the methods used by attackers to manipulate meter readings, providing a tangible example of the threats posed by insufficient cybersecurity measures. Through this live demonstration, attendees will gain a deeper understanding of the technical intricacies involved in such attacks and the potential for widespread disruption. The session will conclude with recommendations for enhancing security protocols and strategies to mitigate these risks, ensuring a more resilient and secure energy infrastructure.

Vikas Karunakaran
Sectrio

Bio:

I head the Threat Research team at Sectrio, where I specialize in OT Security and honeypot technologies. I joined Sectrio seven years ago as a Lead Threat Researcher, starting with IoT malware analysis before moving into the world of OT security. My main focus is on OT threat intelligence, and I've been deeply involved in developing and implementing OT honeypot and deception technologies. My background includes extensive work in malware analysis, threat hunting, risk assessments, and signature writing, and I enjoy sharing my insights through blogging and thought leadership in the cybersecurity space.

CHARMING VIPER, VANISHING CRYPTO

Abstract:

Have you heard of Vipersotfx, the Info-Stealer which stole more than $2.5 million worth of cryptocurrency? Vipersotfx has updated its TTPs in its recent campaign, and the changes warrant exploration. This Info-Stealer emerged in early 2020 as a javascript-based RAT dubbed as Vipersoftx, and has been updating its TTPs on a regular basis to steal cryptocurrency and credentials, whilst also connecting back to its C2 to download additional payloads.

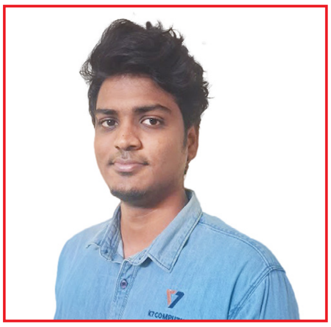
Vipersoftx has evolved from being a clipboard hijacker to a user-credential stealer, also swiping cryptocurrency, and has upgraded its C2 communication methods as part of its arsenal. Over the years, Vipersoftx has typically spread via pirated software to install malicious browser extensions named Venomsoftx for Chromium-based browsers. This swaps the cryptocurrency wallet addresses by tampering with the API request whenever a user interacts with a cryptocurrency website.

Last year it abused DLL-search-order to side-load a malicious DLL that decrypts a shellcode using byte-mapping to get to the next stage. This done, along with a few anti-VM and anti-monitoring checks, it then downloads and executes a PowerShell script to get the final payload of Vipersoftx. This time, however, in addition to browser hijacking it also tries to extract passwords from a couple of password managers and uses a C2 server protected by being hidden behind a DGA.

Vipersotfx's recent campaign has been via ebooks as a front. Whilst the ebooks load, in the background an AutoIt script invokes functions from the .net CLR library to execute a base64-encoded AES-encrypted PowerShell payload. Before executing the scripts, it deploys AMSI-bypass procedures. Finally, it siphons off cryptocurrency and system info as a base64-encoded string dispatched to its C2, and proceeds to download additional payloads.

In this presentation, we will conduct an in-depth analysis of the TTPs employed by VipersoftX to deceive users, bypass security products, and steal cryptocurrency and user credentials. We will also explain in detail the evolution in its C2 communication infrastructure to send data and to receive additional payloads.

CHARMING VIPER, VANISHING CRYPTO



Dhanush
K7 Computing

Bio:

Dhanush completed his Bachelor's degree in Computer Science from Thiruvalluvar University 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. Dhanush is passionate about malware analysis and reverse engineering, and his research findings are published on the K7 Labs technical blog page. During his leisure time, he enjoys playing chess and travelling with his friends.

Arun Kumar
K7 Computing

Bio:

Arunkumar completed his Bachelor's degree in Mechanical Engineering from Anna University in 2021. Although he initially pursued a career in the mechanical field, he later transitioned into the IT sector and began working as a Threat Researcher at K7 Labs, his main job responsibilities include analysing and identifying various types of malware at different levels, as well as keeping current with the latest trends in the field. Arun is passionate about malware analysis and reverse engineering, and his research findings are published on the K7 Labs technical blog page.

Digital Security
Progress. Protected.

Protect your organisations against cyberthreats with **award-winning, AI-native, cybersecurity solutions.**

ESET PROTECT TIERS

		ESET PROTECT ENTRY	ESET PROTECT ADVANCED	ESET PROTECT COMPLETE	ESET PROTECT ENTERPRISE	ESET PROTECT ELITE
Platform modules	CONSOLE (CLOUD/ON-PREM)	●	●	●	●	●
	MODERN ENDPOINT PROTECTION (WITH NGAV)	●	●	●	●	●
	SERVER SECURITY	●	●	●	●	●
	MOBILE THREAT DEFENSE	○	●	●	●	●
	FULL DISK ENCRYPTION		●	●	●	●
	ADVANCED THREAT DEFENSE		●	●	●	●
	VULNERABILITY & PATCH MANAGEMENT			●		●
	MAIL SERVER SECURITY	○	○	●	○	●
	CLOUD APP PROTECTION	○	○	●	○	●
	EXTENDED DETECTION AND RESPONSE				●	●
	MULTI-FACTOR AUTHENTICATION	○	○	○	○	●
Add-ons & Extras	THREAT INTELLIGENCE	○	○	○	○	○
	SHAREPOINT SECURITY	○	○	○	○	○
	ENDPOINT ENCRYPTION	○	○	○	○	○

● Included
○ Optional

eset.com

Digital Security
Progress. Protected.

SUCCESS STORY

Canon Marketing Japan Inc. adopts ESET MDR solution

"The implementation of ESET's security solutions has been seamless across our approximately 23,000 computers and devices, with no concerns or complaints reported by any of the thousands of employees who utilize the system."

Mr. Taro Tanaka
General Manager, IT Architect Division,
Canon Marketing Japan Inc.

Canon Marketing Japan Inc.

Website
https://canon.jp/

COUNTRY
Japan

The Challenge
Canon Marketing Japan, a longtime ESET user, decided to strenghten its security posture due to rising malware threats and remote work trends. It anticipated a year-long implementation and tuning due to its large operation.

The Solution
ESET PROTECT MDR Ultimate provided Canon Marketing Japan with confidence in monitoring alerts and identifying suspicious behaviors post-implementation. The company successfully deployed EDR/XDR on 23,000 devices in just four months, thanks to the strategic use of ESET MDR services, enabling a rapid enhancement of its security operations.

ESET KEY BENEFITS

- World-class XDR technology
- Full MDR with round-the-clock premium support
- Ease of management
- Cost and resource efficiency

BEYOND THE PACKAGE: THE NEW FRONTIER OF MSIX ATTACK

Abstract:

From late 2023, we are observing various threat actors using spurious MSIX Windows app package files to distribute a wide range of malware payloads. MSIX is a Windows application package installation format that enables enterprises to stay updated. IT teams and developers use it to deliver various applications within enterprises.

The threat actors behind it have been employing various tactics such as malvertising and search engine optimization poisoning to lure users into downloading Windows installers for popular web browsers, extensions and various well known software brands such as Notion, Trello, Braavos or OneNote. We have observed various financially motivated threat actors like FIN7 are misusing MSIX files as initial access vector. These threat actors are found delivering malware payloads like **DarkGate, NetSupport RAT, Fakebat, Batloader, etc.** Further some of these infections also lead to **ransomware distributions.**

Presentation will cover following points:

- Deep dive on **MSIX package** structure and it's working.
  - Types of files inside package and processes involved in its working.
  - Package support framework
- Techniques used by threat actors to abuse **MSIX**
- **Case Study:** Provide an analysis on some of attack cases observed abusing MSIX files.
  - It will include analysis of various malware components used in subsequent stages in the infection chain such as PowerShell scripts, PEEXE/PEDLL files, ZIP/GPG/7Z files, etc.
- **Actions:** Detection possibilities
- Key takeaway

This MSIX abusing techniques are not discussed widely so this presentation will help cybersecurity community to defend against MSIX attack campaigns.

BEYOND THE PACKAGE: THE NEW FRONTIER OF MSIX ATTACK

Prakash Galande
Symantec - Broadcom

Bio:

Prakash Galande is a senior security researcher at Symantec, division of Broadcom with more than 12 years of experience. He is passionate about malware analysis and reverse engineering.

He likes to research and find innovative ways to detect malware behavior and technique. Occasionally he likes to write blogs.

He has written blog posts on several malware topics and also presented his research findings at AVAR.

Nitin Shekokar
Symantec - Broadcom

Bio:

Nitin N Shekokar is a seasoned cybersecurity professional with 17 years of experience in threat research and operations.

Currently serving as the Global Efficacy Lead at Symantec, division of Broadcom. He ensures robust protection against emerging threats across all Symantec security product stacks.

Nitin holds three patents in the cybersecurity domain and has presented his research at prominent international conferences, including Virus Bulletin and AVAR.

CHALLENGES IN REVERSE ENGINEERING RUST-BASED MALWARE

Abstract:

The rise of Rust as a programming language has led to its adoption in various domains, including malware development. This paper delves into the specific challenges encountered in reverse engineering Rust-based malware, an emerging threat in the cybersecurity landscape. Unlike traditional malware written in languages such as C or C++, Rust's unique features—memory safety guarantees, zero-cost abstractions, and efficient concurrency—complicate the reverse engineering process. The analysis begins with an overview of Rust's architecture and its implications for malware development. Key challenges discussed include the complexity of Rust's binary structure, the obfuscation resulting from its monomorphization and inlining during compilation, and the difficulties in decompiling and disassembling Rust executables. The paper further explores the limitations of existing reverse engineering tools and techniques when applied to Rust binaries, highlighting the need for advanced methodologies and specialized tools to effectively analyze and mitigate Rust-based malware threats. Through case studies and practical examples, this research aims to provide insights and propose potential solutions to enhance the reverse engineering capabilities for cybersecurity professionals dealing with Rust-based malware.

Nguyen Tien Cong
CMC Cyber Security

Bio:

Nguyen Tien Cong is a young security researcher with a strong interest in reverse engineering and finding vulnerabilities. He graduated with a degree in Cyber Security from the University of Science and Technology of Hanoi. Now, he works at CMC Cyber Security as a Software Developer and Malware Analyst/Digital Forensics expert. He is also the main developer of the real-time engine for CMC Antivirus, playing a key role in improving the software's ability to detect threats.

Bui Huy Anh
CMC Cyber Security

Bio:

Bui Huy Anh is a Digital Forensics and Threat Hunting Engineer with a strong background in cybersecurity. He began his career early, starting as a malware research intern during his second year at the Posts and Telecommunications Institute of Technology (PTIT). After earning his engineering degree, he pursued a professional path in malware research. His work focuses on malware analysis, developing cutting-edge detection and remediation technologies, and hunting advanced persistent threats (APT). Huy Anh's expertise and dedication drive him to develop innovative solutions to safeguard against evolving cyber threats.

SHOULD YOUR EDR BE BASED IN USER-MODE? YOU MIGHT WANT TO RECONSIDER

Abstract:

Following the largest global IT outage in history this past July, which disrupted numerous services and industries, many took to the public stage to advocate against having endpoint security vendors design and develop agents that are kernel-based.

Unlike legacy signature-based detection, the strength of next gen security solutions, particularly Endpoint Detection and Response (EDR) systems, lies in the visibility and context they provide. Over the years, these capabilities have actually been implemented through monitoring operations in user-mode.

To beat EDRs, attackers and malware developers either try to break execution chains to obscure context or to disrupt visibility by blinding them to the operations executed by a process. Unfortunately, disrupting visibility is relatively straightforward due to a fundamental flaw: the reliance on the same execution environment that is intended to be protected.

The talk will first touch on limitations of purely user-mode EDRs such as lack of boot-time protection and inaccessible processes. It will then explore the main approach used by adversaries in the wild: bypass and evade hooks. The research presented will map all known techniques along with a proposed detection scheme focusing on runtime and forensics indicators, based on reverse engineering and in-depth analysis of each method, to benefit all researchers. Lastly, the talk will cover a less popular tactic used by adversaries which is to completely disarm the protection engine entirely in-process.

By the end of the session, hopefully we'll successfully debunk the myth that user-mode only EDRs are adequate for comprehensive security.

Omri Misgav
Independent Security Researcher

Bio:

Omri is an independent security researcher with over a decade of experience in the field. Previously, he headed a security research group in Fortinet's FortiGuard Labs, focused on OS internals, malware and vulnerabilities. Omri joined Fortinet following enSilo's acquisition, where he was the security research team leader and spearheaded the development of new offensive and defensive techniques. Before that, he led the R&D of unique network and endpoint security products for large-scale enterprise environments and was part of an incident response team, conducting investigations and hunting for nation-state threat actors. Omri is a past speaker in various conferences such as DEF CON, AVAR, BSideLV, BSidesTLV, FIRST TC, and others.

DEEP INTO THE EVOLUTION OF THE STEGANOAMOR CAMPAIGN: HOW THE TA558 ATTACKED COMPANIES AROUND THE WORLD

Abstract:

In our talk, we will cover the activities of the TA558 group, which we have been monitoring over the past year. Originally targeting Latin America, the group has expanded its presence to other regions and is targeting a range of sectors including government, manufacturing, electricity, construction, transportation, information technology, education, financial, and pharmaceutical, among others.

The TA558 group uses compromised legitimate FTP and SMTP servers as infrastructure for C2 servers and to store stolen data, and compromised legitimate SMTP servers to send malicious emails. An important feature of the group's activities is the use of steganography, where useful files are hidden within images and text files.

During the talk, we will demonstrate the evolution of the group's attacks, as well as the most popular kill chains using different malware.

Our presentation will be based on information we have published previously, but will also include additional details, including attacks we have seen since our report was published: *https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/*

DEEP INTO THE EVOLUTION OF THE STEGANOAMOR CAMPAIGN: HOW THE TA558 ATTACKED COMPANIES AROUND THE WORLD

Aleksandr Badaev
Positive Technologies

Bio:

Alexander is a threat intelligence specialist and his work includes OSINT, tracking APT, cybercrime groups and hacktivist activity. He also provides expertise in various formats, including indicator data for Positive Technologies products.

In 2023, he graduated from the Moscow Technical University of Communications and Informatics with a degree in "Infocommunication technologies and communication systems."

Previously, he worked at Group IB as a Threat Intelligence Analyst in the Complex Threat Research Department (APT). He joined Positive Technologies in 2023 as a specialist of threat intelligence department, PT ESC.

Kseniia Naumova
Positive Technologies

Bio:

Kseniia is a threat researcher at Positive Technologies, where she focuses on researching malware in the network, improving network traffic analysis tools, and searching for new approaches to detect network threats. She shares her research with other malware analysts on the X platform - https://x.com/naumovax. Kseniia also devoted time to exploring web-related threats, conducting osint research, and developing a system for countering and detecting social engineering attacks in her master's degree in cybersecurity.

In 2022, she graduated from the National Research University «Moscow Power Engineering Institute» with a bachelor's degree in computer system security. In 2024, she graduated from the National Research Nuclear University «Moscow Engineering Physics Institute» with a master's degree in information security in financial monitoring. Her career started in 2020 researching web threats at Kaspersky Lab for two years before joining Positive Technologies in 2022.

Kseniia organized cybersecurity events for students at multiple educational programs. She's been playing CTF with the team since 2018. Her international team participated in the 2022 and 2023 BlackHat MEA final CTF.

RATS IN THE SEWERS: DIVING INTO THE BITTORRENT CESSPOOL

Abstract:

From APT attacks to lowly cybercrime, the BitTorrent protocol is often used as a method to gain illegally obtained files and, as such, is the perfect gateway to content-wanting victims. BitTorrent websites have long been used as the primary distribution vector of XtremeRAT and Filesponger stealer but was also misused in 2022 when Mandiant reported a supply-chain attack targeting the Ukrainian government, where a modified Windows 10 installer was distributed via a local torrent-sharing site. To detect such bad actors at the source, ideally before they compromise users, we researched and developed Torrent Crawler, a project to scan and monitor suspicious BitTorrent sites to better understand this popular P2P protocol as a compromise vector, and to discover new malware.

In this presentation, we study one of the cases we discovered using our crawler: a cluster of 20+ remote access trojans (RATs) stemming from the common AsyncRAT codebase, including the well-known forks like DCRat and VenomRAT but also previously unknown variants developed by various malware authors. We dissect the unique monetization plugins used by these variants but also look at the connections between the various malware developers and provide insights into how their RATs are sold in this competitive low-cost RAT segment.

As for Torrent Crawler, we show specific interesting problems of monitoring the sites – like establishing a system that does not help with illegal torrent propagation – along with statistics, a landscape overview, and some tips if you decide to tackle a similar project. For a start, we are scanning over half a dozen carefully selected torrent websites, including some of the biggest. We will share our insights into malicious actors we have found as well as tactics and techniques encountered.

Martin Jirkal
ESET

Bio:

Martin Jirkal is a seasoned malware researcher with over a decade of experience in the security industry, specializing in malware analysis and detection. He co-developed reverse engineering courses at the Czech Technical University, and continues to occasionally instruct students on deconstructing computer applications. Currently, he leads a team dedicated to tracing crimeware and addressing forensic challenges. Martin has also presented at conferences such as Virus Bulletin and CARO. In addition to his professional pursuits, he is a passionate gamer and enjoys tinkering with everything from IKEA furniture to smart home automations.

Roman Šíma
ESET

Bio:

Roman Šíma is a dedicated malware analyst at ESET, with over five years of specialized experience in malware analysis and threat hunting. His professional interests include reverse engineering, adversary tactics, and forensic investigations. Outside of work, Roman is passionate about sports, enjoys playing retro video games, and is an avid reader.

WITH GREAT RESEARCH COMES GREAT RESPONSIBILITY

Abstract:

For years, the cybersecurity community argued about how researchers should disclose newly discovered vulnerabilities in information technology products. After considerable debate and not a little rancor, the industry settled on a set of principles for that process, known as responsible or coordinated vulnerability disclosure. As the disclosure process has become regularized, another problem has become prominent: post-disclosure communications about disclosed vulnerabilities in a cybersecurity product. As an industry, we need to talk about such vulnerabilities in order to disseminate protections and prompt appropriate action. On the other hand, using disclosed vulnerabilities for marketing purposes is tempting but ultimately counterproductive. Since we currently lack principles for such post-disclosure communications, uncertainty about acceptable behavior runs rampant. This talk will propose that the cybersecurity industry develop a "responsible vulnerability communication" code of conduct, and it will outline what some of the components of such a code could be.

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.

BYPASSING EVASIVE BINARIES WITH DYNAMIC BINARY INSTRUMENTATION

Abstract:

Binary analysis is an important step during the reverse engineering of malicious threats. While for various reasons, some of these threats are easy to decompile and understand, others implement a lot of evasive techniques, allowing them to reach a sense of awareness for analysis environments like debuggers, sandboxes, emulators, etc. If any of these checks detect the presence of an analysis environment, the application may refuse to continue execution or it can just change the behavior to anything that might look benign. To automate the reverse engineering of such binaries, we developed COBAI (Complex Orchestrator for Binary Analysis and Instrumentation) a DBI (Dynamic Binary Analysis) framework which allows us to profile malicious binaries and create rich execution traces. Compared to existing DBIs, COBAI is capable to stack multiple plugins, fix a significant amount of evasive techniques, and only follow the application code and payloads. In this presentation we discuss the side effects of having or not such a technology, as well as presenting a short comparative evaluation to understand its power, its limits and the effort to make it better. In our evaluation we include ransomware binaries (for Windows operating system), public tests for DBIs, as well as public benign binaries implementing hundreds of tests for various analysis environments. Among all these tests, COBAI is capable to pass short below 100% of them, where others bearly reach 30%. Our work was also published on arXiv (https://arxiv.org/abs/2306.13529), but was never presented in public.

Vlad Constantin Craciun
Bitdefender

Bio:

Vlad Craciun is an Assistant Professor at the "Alexandru Ioan Cuza" University of Iasi, Faculty of Computer Science (Romania), studying the field of automated binary analysis. He joined Bitdefender Laboratories in early 2009, being involved in projects like file-infector disinfection, post-incident response, forensics, building of ransomware decryption tools and automating the reverse-engineering of binaries. His current research interests include automated binary analysis, cryptography, symbolic execution, behaviour and Control Flow Graph analysis.

THE RISE AND FALL OF GOLANG MALWARE

Abstract:

In the last half of a decade, there has been an advent and huge influx in usage of Golang based malware In-The-Wild (ITW). The ease of writing malware-oriented code with the advent of new libraries mimicking 'software-development' projects by various developers around the globe, has helped in Golang Malware development and customization. Starting from very basic information stealers, campaign-oriented implants to ransomware and wipers, the advent of Golang has been very welcomed.

In this talk, we will delve deep into the statistics of Golang based malware AKA the rise of it from a geographical angle, which made various anti-malware products and researchers to opt for a different route to deal with it. We will see why it caused problems and havoc by looking into some well-known state sponsored campaigns, ransomware groups and various wide spread malware campaigns which utilized Golang. We will also look into various "mistakes" made by these operators which helped malware researchers to develop proactive measures against such malicious implants.

Then, we will collectively look into some unique artefacts present in Golang based malware, which has now led to early detections of Golang Malware AKA the fall of Golang malware. We shall discuss how few open-source code repositories which are heavily abused by Golang malware is aiding malware researchers to deal with it making them a step ahead. Finally, this talk will delve deep into the 'Final Pillars' aka Go-Obfuscator & Garble and how they are heavily abused giving Golang Malware developers a sense of pseudo-rise and reasons to why will it be again the sole reason of fall of it in near future.

We, will also release a tool 'Go-Peep' which aims on aiding researchers to extract the artefacts discussed in the talk, that aims to helping defenders to triage and deal with Golang-based malware.

Subhajeet Singha
Quick Heal Technologies Limited

Bio:

Subhajeet is working as a Security Researcher in Security Labs at Quick Heal. His areas of focus are threat intelligence, research along with reverse engineering to improve detection capabilities and to aid in further research.

LAZARUS TARGETS FREELANCE DEVELOPERS WITH DECEPTIVEDEVELOPMENT

Abstract:

Lazarus is one of the most active APT groups and has a long history of innovation in the field of cyberthreats, always looking for new ways to achieve its goals. Aside from politically and strategically motivated activities such as espionage, Lazarus has also been known to focus on financial gain. It started by stealing money from banks and financial institutions in some of the largest known cyberheists, but nowadays has reoriented towards cryptocurrency theft, targeting cryptocurrency exchanges and other related entities.

Lazarus's DeceptiveDevelopment operation, also known as ContagiousInterview, has been going on since 2023 and shares some notable similarities with previous Lazarus campaigns, namely the use of social engineering, faux recruiter profiles on social media, and delivering malware disguised as job offers or job challenges. What makes DeceptiveDevelopment unique is its targeting of individual freelance developers throughout the entire world, primarily those associated with cryptocurrency projects. The intention behind this is twofold – theft of the cryptocurrency wallets belonging to these individuals and gaining access to larger projects and institutions these developers may be a part of, for potential further intrusion.

In this presentation, we focus on the origin of the DeceptiveDevelopment campaign and its progression over time. We also provide insight into the infrastructure used, including an overview of new, recently discovered malware versions. With the permission of the victims, we present actual conversations between the attackers and their targets; these provide useful insight into how the actor operates. We aim to "connect the dots" and provide a comprehensive overview of this operation, providing a basis for further threat research and hunting.

Matěj Havránek
ESET

Bio:

Matěj Havránek is a malware researcher at ESET with 10 years of experience in the fields of malware analysis and threat hunting. In addition to malware research, he focuses on APT activity tracking and developing analytic tools. He is a fan of ciphers and cryptography, and enjoys challenges.

AVAR 2024

PANEL MEMBERS

SUPPLY CHAIN INTEGRITY: CYBER DEFENSE STRATEGIES IN THE DIGITAL ERA (PANEL DISCUSSION)

Balakrishnan Kanniah
VA Tech Wabag

Bio:

Dynamic and results-oriented IT Leader with 28 years of experience in managing digital transformation, Cybersecurity, IT&ITES transformation, product development/implementation programs and business initiatives.

Adept at Program management, defining processes, controlling risk, and optimizing resources to drive efficiency and success. Experienced in leading multi-million-dollar IT Services development and cyber security programs, ensuring timely, budget-conscious, and quality delivery across global markets.

Competencies

Program & Delivery Management: Expertise in driving large-scale SDLC and IT Services, digital transformation programs, with a strong focus on Cloud, IT Security and SaaS product development and deployment.

Strategic Leadership: Skilled in aligning IT with business strategy, crafting roadmaps, driving programs to deliver complex business requirements through innovative technology solutions.

Team Leadership: Experience in leading cross-functional large teams (400+), fostering collaboration and achieving program goals.

Agile Transformation: Proven success in leading agile transformation, fostering a culture of continual improvement across business, product, and technology.

Stakeholder Management: Exceptional ability to interface with C-level executives, driving strategic vision, change, and performance improvement.

Talent Acquisition & Development: Effective in attracting, developing, and leading high-quality talent, maximizing productivity and exceeding customer expectations.

SUPPLY CHAIN INTEGRITY: CYBER DEFENSE STRATEGIES IN THE DIGITAL ERA (PANEL DISCUSSION)

Debasish Das
One Tata Operating Network

Bio:

- CISO – One Tata Operating Network (OTON) for the Tata Group.
- Global Delivery Head – Cloud Security Services , TCS.
- Program Director – For Large Global Bank, HQ in Singapore
- Technology Head – For World's largest LNG based in UK, US & AUS.
- Enterprise Architect – Global Manufacturing, Oil & Gas, Automobile, Telcos.
- CoE Head – Large Wall Street based Global Investment Bank, US.
- 19 years in Technology & Business Leadership Roles.
- Member of IEEE, IEI & DSCI. Certified Data Privacy Lead Assessor – DCPLA.
- Alumnus of BITS Pilani & IIM Calcutta. PhD Scholar @ IIM Ranchi (Strategic Management)
- Executive Management Programs from INSEAD & Fisher College of Business (The Ohio State University).
- Graduate from Tata Management Training Centre (TMTC) & TCS LEAD Academy.
- Cybersecurity Advisor & Strategist for Tata Business Excellence Group (TBExG), Tata Sons Group Digital Innovation Office & 16 Tata Group Companies.
- Consulting, Advisory & Audits for Global Clients – CIS Assessments, Tata Cyber Excellence Assessment, SOC 2 Type 2, ISO 27001, RBI Audit Support, Internal/External Audits

SUPPLY CHAIN INTEGRITY: CYBER DEFENSE STRATEGIES IN THE DIGITAL ERA (PANEL DISCUSSION)

Bio:

- Business Unit Head for Tata Group Cybersecurity (16 Clients ; Rev INR 200 Cr ; 200 FTEs).
- Global Delivery Head for TCS Cloud Security Services across (50+ clients ; Rev INR 160 Cr ; 250+ FTEs).
- Global Delivery Head for 2 Large Banking & Oil & Gas Clients (Rev $ INR 400 Cr ; 300+ FTEs).
- Conceptualized & Setup from scratch -"Tata Cyber Defense Center" (Rev INR 100 Cr, INR 560 CR savings)
- Incubated INR 200 Cr TCS Video Assurance & Analytics Service Line. Launched Video Assurance & Analytics Platform & acquired 10 new clients in US, UK, AUS & Asia.
- Intellectual Property : 4 Patent Filings, 2 Patent Grants, 10+ Publications in IEEE, IEI & Springer.
- Author of Book "Mobile Application Development …" published by Springer in 2022.
- Invited Speaker/Key Industry Contributions – Businessworld CISO Roundtable, Tata Business Excellence Leadership Conclave, ProMfg CIO Thinkturf , OpenText Innovation Forum & IEEE Conference.
- Guest Lecture for Texas A&M University (US), Kingston Business School (UK), IIM Sambalpur, NIT Rourkela, NIT Warangal, KIIT University, IIT Bhubaneswar & BIT Mesra.

Key Awards/Recognition:

- TCS Best Implemented Cybersecurity Program (2024)
- Tata Group Chairman's Award for Significant Contribution to Tata Group Cybersecurity (2023)
- Best Cyber Excellence Assessor Award for Tata Group (2023)
- TCS Innovista Winner for APAC (2021); Top Seed in Piloted Technologies @ TCS Innovista (2017)
- TCS Best Managed Program (2009, 2010), Best Manufacturing Supplier Award 2008
- Honeywell International – Best Implemented Pilot Program (2005)

SUPPLY CHAIN INTEGRITY: CYBER DEFENSE STRATEGIES IN THE DIGITAL ERA (PANEL DISCUSSION)

Kannan Srinivasan
GAVS Technologies

Bio:

A proven award-winning leader and strategist having 24 years of experience recognized for translating business imperatives into actionable deliverables using a range of influencing skills to obtain stakeholder buy-in at all levels. A very active member to build and support the cybersecurity community by giving keynote address, webinars and conduct sessions to SMB organizations.

Subject matter expert in the areas of MSSP, Managed SOC, Cloud security, Vulnerability Management, GRC, Identity and Access Management

Manickam Kanniah
Verizon

Bio:

A seasoned Cyber Security Professional having close to two decade of industry experience in Information & Cyber Security. Holds MBA in IT & System in ICFAI University and Diploma Holder in Electronics & Communication Engineering. Along with academic, holding many professional certifications in Security, Network and system. Started the IT career as Customer support Engineer, specialized in System and Networking then moved to Cyber Security. Currently Heading the Cyber Security team delivering Cyber Services in global scale. Trained many working professionals on CISSP and CEH.

SUPPLY CHAIN INTEGRITY: CYBER DEFENSE STRATEGIES IN THE DIGITAL ERA (PANEL DISCUSSION)

Vimalaasree Anandhan
Poshmark

Bio:

Vimalaasree is a Cybersecurity Leader with 20 years of experience in application and cloud security, DevSecOps, and risk management. She currently Heads the Cybersecurity Department at Poshmark India, 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.

With a Master's in Science and a Bachelor's in Engineering, she is focused on securing applications and fostering cybersecurity talent. Vimalaasree is also the President of Nex Gen Cyber Women, a community supporting women in cybersecurity.

THE HUMAN ELEMENT IN CYBER SECURITY (PANEL DISCUSSION)

Chethan S. Iyengar
Standard Chartered

Bio:

For over 22 years, Chethan S. Iyengar has been at the forefront of cybersecurity, transforming how global enterprises protect their most valuable assets. From safeguarding sensitive data of millions of customers to streamlining security for organizations with over 100,000 employees, Chethan has consistently delivered results that matter. Known for blending innovation with execution, he has built a legacy of driving impact where it counts—at the intersection of security, business growth, and sustainability.

Jeannette Jarvis
Cyber Threat Alliance

Bio:

I am responsible for Cyber Threat Alliance's partnerships, branding, and communications efforts. I have worked in cybersecurity for 25 years, previously holding various senior leadership positions, including Director of Product Marketing at Fortinet and Director of Product Management at McAfee and Intel Security. I also served in leadership roles at Microsoft and Boeing. I am on the advisory board for Virus Bulletin, an international organization covering the global threat landscape.

THE HUMAN ELEMENT IN CYBER SECURITY (PANEL DISCUSSION)

Lalit Gupta
Al Gihaz Holding

Bio:

Dr. Lalit Gupta, widely recognized as the "Cyber Doctor," is a distinguished cybersecurity leader with over 25 years of experience. He serves as the President of the Cyber Security Council of India and is the Group Head of IT GRC & Cybersecurity at Al Gihaz Holding. Dr. Gupta is an Honorary Doctorate awardee in Cybersecurity for exceptional R&D contributions and has been honored with several accolades, including the Pillars of India Award and the Bharat Gaurav Samman.

As a global thought leader, Dr. Gupta has expertise in IT governance, risk management, cloud security, compliance, and privacy. He is a sought-after speaker and mentor, renowned for his innovative strategies in AI-driven cybersecurity, incident response, and business continuity. Dr. Gupta's contributions to national cybersecurity initiatives, such as the establishment of CERT-In, reflect his commitment to advancing cybersecurity globally.

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.

THE HUMAN ELEMENT IN CYBER SECURITY (PANEL DISCUSSION)

Vimalaasree Anandhan
Poshmark

Bio:

Vimalaasree is a Cybersecurity Leader with 20 years of experience in application and cloud security, DevSecOps, and risk management. She currently Heads the Cybersecurity Department at Poshmark India, 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.

With a Master's in Science and a Bachelor's in Engineering, she is focused on securing applications and fostering cybersecurity talent. Vimalaasree is also the President of Nex Gen Cyber Women, a community supporting women in cybersecurity.

SECURING YOUR CLOUD INFRASTRUCTURE: NAVIGATING THE DANGERS (PANEL DISCUSSION)

Chandresh Rajkumar
Unosecur

Bio:

Chandresh is a seasoned engineer with experience across various product verticals in the software industry, focusing on cloud-based solutions and scalable systems. He has worked in leadership and technical roles, showcasing solid skills in system architecture, cloud security technologies and general engineering perspectives. He has extensive experience building product lines from ground zero to go-to-market with agility, whether regarding scalability, sustenance, or reliability. He is heading the Unosecur engineering work group to detect, predict and remediate identity security threats in near real-time across cloud providers.

Dr. Anshu Premchand
Tech Mahindra

Bio:

Dr. Anshu is a persuasive thought leader with 24+ years of experience in digital & cloud services, technical solution architecture, IT modernization, research & innovation, agility & devSecOps. She heads multi-cloud & digital services at Hitech, Media & Entertainment unit of TechM. In her last role she was Global Head of Solutions & Architecture of Google Business Unit of Tata Consultancy Services where she was responsible for data modernization, application & infrastructure modernization, automation, security and AI programs. She has extensive experience in designing large scale cloud transformation initiatives and advising customers across domains in areas of breakthrough innovation. Anshu holds a PhD in Computer Science. She has special interest in simplification programs and has published several papers in international journals like IEEE, Springer & ACM.

SECURING YOUR CLOUD INFRASTRUCTURE: NAVIGATING THE DANGERS (PANEL DISCUSSION)

Karthikeyan K
Logitech

Bio:

Karthikeyan K is a results-driven cybersecurity leader with 14 years of expertise in application security, cloud and cloud-native security, offensive security, and DevSecOps. As a Principal Security Architect/Senior Engineering Manager at Logitech, Karthikeyan K is dedicated to safeguarding organizations from evolving digital threats while fostering a culture of security awareness and innovation.

Certified in CISSP, CISA, and AWS Security, Karthikeyan K brings a wealth of knowledge in data privacy and secure product development. They have previously held key roles at Freshworks and are deeply committed to the global cybersecurity community, serving as the OWASP Chapter Lead and Defcon Lead in Chennai.

Throughout their career, Karthikeyan K has partnered with leading organizations to fortify security postures through secure development methodologies, impactful cloud security initiatives, and pioneering offensive security strategies. They are passionate about helping startups and businesses develop secure products, ensuring resilience against cyber threats.

Beyond technical expertise, Karthikeyan excels in leadership, having built high-performing cybersecurity teams and cultivated continuous learning environments. They remain at the forefront of industry trends, empowering organizations to thrive in an increasingly digital world. Driven by a passion for making a tangible impact, they are committed to enhancing cybersecurity practices and fostering innovation in the field.

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.

SECURING YOUR CLOUD INFRASTRUCTURE: NAVIGATING THE DANGERS (PANEL DISCUSSION)

Srinivasan Balraj
Muthoot Fincorp

Bio:

I'm Srinivasan, an information security professional with 18+yrs of experience, currently working for Muthoot FinCorp as Vice president-Head of information security, audit, and compliance. Expertise in Information Security internal and external audit, Third Party risk management, Operational risk, Compliance and Regulatory management, Security training and awareness. Have worked with multinational banks such as Citibank, Standard Chartered bank & UK based Fintech bank Revolut, also with US SaaS based company Zuora on various capacities. I'm based out of Chennai. Have travelled to 6 countries and am a foodie.

Apart from work, I'm a passionate Toastmaster wherein I nurture young generation in their communication and leadership skills. Have served as Area Director in handling 100+ professionals and students. My motto "If you stop learning, you stop growing."

HEALTHCARE CYBER ATTACKS: MANAGING THE DOMINO EFFECT (PANEL DISCUSSION)

Diptesh Saha
Accel Limited

Bio:

- An Enterprise leader, mentor , a CISSP, CISM with around 2 decades of experience in IT Industry handling Security Consulting & Managed Services.
- He has been the Architect of setting up multiple Global SOC (Security Operation Centre) for Enterprises.
- He is a Cyber Security strategic advisor to multiple Global companies and startups.
- He has been featured and awarded As "10 most Promising Enterprise Biz Security Architect of the year, 2019" by CIO Review Group and awarded as CISO of the Year 2023 at Digital transformation summit, by Transformance media group
- Presently he is responsible as a CISO & Practice Head, Cyber Security for ACCEL Group.
- He has delivered 200+ sessions to Corporates & Colleges out of his interest in learning & sharing knowledge.
- He is an active member of ISACA, ISC2 Chennai Chapter, and Cyber peace foundation.

Gowdhaman Jothilingam
LatentView Analytics

Bio:

- 22+ Yrs of experience in IT and Cyber security Domain and successfully implemented many IT Solutions.
- Implemented some of the Key Cyber Security solutions Security Incidents Events Management (SIEM), Cyber Risk Quantification (Safe Security), Attack Surface Management (ASM), End Point Detection and Response (EDR), Mobile Device Management (MDM), Data Leakage Prevention (DLP), Cloud Identity Premium (CIP) and Data classifications to safeguard the data.
- Managed the ISO 27001:2013, ISO 27701, PCI DSS, HIPAA, TISAX, CCPA and GDPR compliance programs.
- Implemented various IT solutions across organizations - ERP solutions, Knowledge Management Solutions, CRM Platforms and Collaboration solutions.
- Handled Partnership Portfolio, and Enterprise Risk Management and helped the organisations in building the ODC and setting up client environments based on their requirements.
- Expert at launching technology programs that safeguard data, streamline operations, drive innovation, and advance business strategy.
- Spearheaded IT security community chapters and helped the IT leaders to share their knowledge.

HEALTHCARE CYBER ATTACKS: MANAGING THE DOMINO EFFECT (PANEL DISCUSSION)

Kannan Srinivasan
GAVS Technologies

Bio:

A proven award-winning leader and strategist having 24 years of experience recognized for translating business imperatives into actionable deliverables using a range of influencing skills to obtain stakeholder buy-in at all levels. A very active member to build and support the cybersecurity community by giving keynote address, webinars and conduct sessions to SMB organizations.

Subject matter expert in the areas of MSSP, Managed SOC, Cloud security, Vulnerability Management, GRC, Identity and Access Management

Romanus Raymond Prabhu
Zoho Corporation (ManageEngine)

Bio:

As the Director of product support, he is responsible for ensuring that ManageEngine's UEMS (Unified Endpoint Management & Security) customers across the globe are happy. He oversees the seamless onboarding, product training and implementation, and support experience for all customers. He also heads the product evangelists, professional services, partner certification, and customer success teams to nurture long-term relationships with each client, and in turn nurtures community champions for ManageEngine. He is passionate about customer and employee success, solving complex challenges with teamwork and innovative thinking. He is recognised as a corporate IT leader for his entrepreneurial spirit, curiosity, and thought leadership. He has a strong passion for endpoint security and championing security solutions as a security evangelist. His role also demands evaluating technologies and applying industry leading trends and tools to achieve delivery, quality, and business objectives that drive the business forward.

HEALTHCARE CYBER ATTACKS: MANAGING THE DOMINO EFFECT (PANEL DISCUSSION)

Senthil Subramaniam ESR
Infinite Computer Solutions

Bio:

I am Senthil Subramaniam ESR, a Security professional & leader with 20+ years of experience, working as Global CISO for Infinite Computer Solutions, with extensive expertise and experience in Security Governance, strategy, security operations, IT Audits, Privacy, Cloud security, BCP/DR, Risk Management and Compliance. Currently I am based out of Chennai.

Smith Gonsalves
CyberSmithSECURE

Bio:

Smith Gonsalves developed an obsession with computers at the age of 3, which evolved into a hunger to master the art of cybersecurity by the time he turned 15. Since then, he has dedicated over a decade to building security strategies for some of the world's leading companies—ranging from hundred-million-dollar MNCs to billion-dollar unicorns.

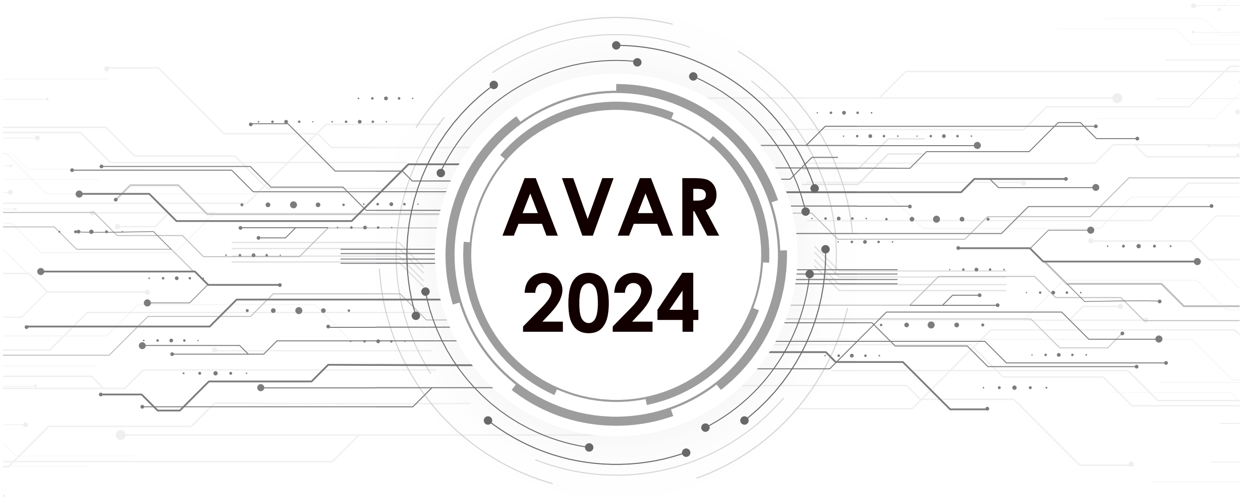
Over the years, Smith has served as a Virtual Chief Information Security Officer (vCISO) and Security Advisor to industry board members across diverse verticals such as SaaS-based product companies and sectors like Logistics, Automobile, EdTech, Pharma, BPOs, Metal & Steel, and Oil & Gas. His expertise spans the entire spectrum of cybersecurity, including cloud security, applications, APIs, and containerized environments.

As the founder of CyberSmithSECURE, Smith has helped corporates and MNCs secure their assets, manage compliance, and mitigate threats that could impede growth. In the last three years, CyberSmithSECURE has provided cybersecurity solutions to over 200 companies, delivering transformative results.

Having devoted his life to information security, Smith actively collaborates with other cybersecurity professionals to share insights and advance the field. For organizations seeking complete security and compliance for their most valuable assets, Smith Gonsalves and CyberSmithSECURE provide the expertise and solutions to meet those needs.

AVAR 2024

CISO CONNECT



AVAR recognizes that CISOs are the frontline leaders in the battle against cyber attacks. CISOs are more than just technology leaders, and are responsible to the Board and the broader community of enterprise stakeholders for preventing operational disruption, with associated erosion of business value, through the proactive and successful deployment of cyber defenses.

CISOs, therefore, require a broad gamut of knowledge and skills to meet the expectations of diverse stakeholders. AVAR facilitates such development by including a CISO Workshop in AVAR 2024. Conducted exclusively for CISOs, the CISO Workshop includes a panel discussion and sessions from cyber security organizations that will focus on leadership concerns and advances in cyber defense technology.

ADVERSARIAL USE OF GENAI

Abstract:

Since Generative AI tools emerged into the public domain, speculation has run rampant about how adversaries might make use of these tools. However, adoption of GenAI tools by malicious actors has been slower than expected nor has it fundamentally altered the cybersecurity landscape. The Cyber Threat Alliance has developed a Joint Analytic Report exploring this issue. This talk will highlight the findings from the [draft] report, the evidence we have for adversarial use of GenAI tools to date, and what we might expect to change over the near term. The talk will conclude by discussing the mitigations CTA's members recommend to deal with the evolving use of AI tools by malicious actors.

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.

THE INVISIBLE LINE: SECURING ENDPOINTS IN A WORLD WITHOUT BOUNDARIES

Abstract:

Endpoints are no longer just devices like laptops and smartphones; the lines keep moving and endpoints are suddenly everywhere and nowhere at once. AI is redefining endpoint security by predicting threats and adapting in real-time. But as defenses strengthen, so do attackers. This session explores how AI redraws the security landscape, with real-world examples and strategies for staying ahead.

We once saw endpoints as predictable: laptops, desktops, smartphones—each a contained node we could secure. But those days are over. The lines we drew around devices have dissolved into something invisible—if they ever existed at all. Security now feels like trying to grasp air.

Enter Large Language Models (LLMs), which are rewriting endpoint security. LLMs are doing more than spotting anomalies—they're predicting them. By processing vast amounts of global threat intelligence (CVE, CWE, NVD) and local organizational knowledge, these models adapt to specific conditions, ensuring defenses aren't just reactive but contextualized and proactive.

Imagine a new malware variant appears. Instead of waiting for patches or relying on static defenses, LLMs pull from global and local knowledge to generate real-time, customized responses. These models learn and anticipate threats, enabling defenses to evolve dynamically. AI-driven security moves beyond traditional detection methods, offering near-autonomous protection that adapts in real-time.

Yet, as AI strengthens defenses, it also strengthens attackers. AI-generated malware morphs at speeds traditional patching can't match, blending into legitimate behavior so seamlessly even the best models can struggle to differentiate. This new reality requires security that thinks and acts in tandem.

Through reasoning and action frameworks, AI-driven models break down threats step by step, recalibrating defenses dynamically. This ensures that as attackers adapt, defenses can respond in real-time, reducing vulnerabilities before they're exploited.

This talk isn't about quick fixes. It's about understanding that endpoints—whether IoT devices, cloud APIs, or containerized apps—are no longer static. They're shape-shifters, and securing them requires defenses that can shift just as fast. We'll explore real-world examples of AI-driven security and confront the hard questions: How do we stay ahead when the lines between legitimate use and attack blur? How do we evolve security models fast enough to counter AI-driven threats?

By the end, you'll see the endpoint as a moving target. You'll leave with a deeper understanding of how LLMs can help secure it—not with static solutions but with AIdriven adaptability in a world where the endpoint is everywhere, and nowhere, at once.

THE INVISIBLE LINE: SECURING ENDPOINTS IN A WORLD WITHOUT BOUNDARIES

Romanus Raymond Prabhu
Zoho Corporation (ManageEngine)

Bio:

As the Director of product support, he is responsible for ensuring that ManageEngine's UEMS (Unified Endpoint Management & Security) customers across the globe are happy. He oversees the seamless onboarding, product training and implementation, and support experience for all customers. He also heads the product evangelists, professional services, partner certification, and customer success teams to nurture long-term relationships with each client, and in turn nurtures community champions for ManageEngine. He is passionate about customer and employee success, solving complex challenges with teamwork and innovative thinking. He is recognised as a corporate IT leader for his entrepreneurial spirit, curiosity, and thought leadership. He has a strong passion for endpoint security and championing security solutions as a security evangelist. His role also demands evaluating technologies and applying industry leading trends and tools to achieve delivery, quality, and business objectives that drive the business forward.

THE FUTURE OF CYBERCRIME – FACT OR FICTION?

Abstract:

Advanced Threats, Deepfakes and Cybercrime as a Service!

The presentation "The Future of Cybercrime – Fact or Fiction?" explores the emerging trends reshaping the digital threat landscape. It delves into advanced threats, the rise of deepfakes as tools of deception, and the proliferation of Cybercrime-as-a-Service (CaaS). Attendees will gain insights into how these developments challenge traditional defences and the evolving strategies needed to mitigate them. Drawing from real-world examples and expert analysis, this session separates hype from reality to equip organisations with actionable intelligence for future-proofing their cybersecurity.

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.

DEFEND YOUR CLOUD INFRASTRUCTURE FROM IDENTITY THREATS

Chandresh Rajkumar M
Unosecur

Bio:

Chandresh is a seasoned engineer with experience across various product verticals in the software industry, focusing on cloud-based solutions and scalable systems. He has worked in leadership and technical roles, showcasing solid skills in system architecture, cloud security technologies and general engineering perspectives. He has extensive experience building product lines from ground zero to go-to-market with agility, whether regarding scalability, sustenance, or reliability. He is heading the Unosecur engineering work group to detect, predict and remediate identity security threats in near real-time across cloud providers.

Himani Kambale
Unosecur

Bio:

Himani Kambale is a seasoned cybersecurity professional specializing in identity threat defense and cloud security. Currently serving as a key member of Unosecur, Himani contributes to the development of AI-powered solutions that safeguard cloud infrastructures from identity threats. Himani's career is marked by a commitment to enhancing cloud security through advanced technologies. By focusing on breach prevention and automated remediation, Himani ensures that security and business teams can collaborate seamlessly to protect critical assets.

Himani's expertise and contributions have been pivotal in establishing Unosecur as a trusted partner for cloud-native companies seeking comprehensive identity threat defense solutions.

AXIDIAN SHIELD - IDENTITY THREAT DETECTION AND RESPONSE (ITDR)

Abstract:

As attacks become cheaper and simpler to execute, the entry barriers for attackers are lower, making cyber threats accessible even to less sophisticated actors. Additionally, the profitability of cybercrime, driven by the growth of ransomware and data theft markets, incentivizes attackers further. With an increasing volume of attacks, even a modest success rate results in a higher number of breaches, raising the stakes for organizations worldwide. This reality underscores the urgent need for robust, proactive security measures like Identity Threat Detection and Response (ITDR) solutions, which can effectively counteract sophisticated credential-based threats.

Kirill Bondarenko
Axidian

Bio:

Regional Director and Expert with 18 years of experience in international IT/Cyber Security creating products and services focused on enterprise security and workflow automation using Artificial Intelligence, Facial Recognition, OCR and Identity security technologies to make the world a better place.

THIRD PARTY VENDOR RISK MANAGEMENT (PANEL DISCUSSION)

Akkaiah Janagaraj
LTIMindtree

Ashok Kumar Jeyachandran
G3 Cyberspace

Bio:

A passionate cybersecurity leader, A Janagaraj is the global cybersecurity practice unit head of LTIMindtree. He has a professional track record of successfully establishing cybersecurity programs and helping Fortune 500 clients drive security transformation initiatives. Under his leadership, LTIMindtree brings tailored next-gen cybersecurity solutions for its clients worldwide.

Janag - as he is fondly called, leads the overall cybersecurity practice development, delivery excellence, tech innovation, process improvisation, new-age solution development for global clients, in collaboration with ecosystem partners and alliances.

Janag has over three decades of industry experience in cybersecurity and Information Technology, with a successful track record of driving security modernization in diverse industry contexts, managing complex transformations, strategic partnerships and building high-performance teams.

Prior to LTIMindtree, Janag was the Global Practice head for Cyber Security Practice at HCL. Previously, he also held a leadership role in PWC India, leading cyber business in the financial sector.

Janag is a management graduate from Welinker Institute of Management, Mumbai. He is a prolific speaker for various industry and professional bodies like ISF India, ISACA & CII and is passionate about continuous learning. He is based in Chennai, India with his family.

Bio:

I am Ashok Kumar, with over 18 years of experience in Cybersecurity, Governance, Risk & Compliance (GRC), Enterprise Risk Management, Business Continuity Management (BCM), Audit, Data Privacy, and Vendor Risk Assessment.

I have demonstrated expertise in enterprise risk management with a deep understanding of cyber threats, vulnerabilities, probability, and impact. My career includes 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, and Lead in Information Security, BCM, and GDPR at Equiniti.

I am recognized for my knowledge in TPRM, BCM, Cybersecurity, and Data Privacy. Currently, I am embarking on a new journey as an entrepreneur, developing a cybersecurity compliance product.

THIRD PARTY VENDOR RISK MANAGEMENT (PANEL DISCUSSION)

Subramanian Vaithi
Nium

Bio:

With over 16 years of experience spanning Internal Audit, Risk Management, Cybersecurity, and Consulting, Vaithi has a proven track record of driving strategic risk initiatives for global organizations. Vaithi has worked with renowned firms such as Ernst & Young, IBM, Cognizant Technologies, and Standard Chartered Bank, bringing a wealth of expertise in managing complex risk and compliance landscapes.

In his current role, Vaithi heads the Enterprise Risk Management function at NIUM, a leading global fintech company, where he is responsible for designing and implementing robust risk frameworks to support the organization's growth and resilience.

Vaithi holds esteemed certifications, including CIA, CISSP, CISA, CEH, and Certified IT Disaster Recovery Professional, and has earned a Diploma in Cyber Laws from NALSAR University.

THIRD PARTY VENDOR RISK MANAGEMENT (PANEL DISCUSSION)

Sarita Padmini
Protiviti

Bio:

Sarita Padmini is an accomplished leader in Cybersecurity and Data Privacy with extensive experience in various sectors. Having amassed a wealth of experience in esteemed organizations like PWC, IBM, HCL, she has cultivated a robust background, honed their expertise, and acquired comprehensive industry knowledge. Currently, Sarita Padmini holds the position of Director - Cyber Security and Data Privacy under the Technology consulting unit of Protiviti India Member Private Limited and an active Board Member at WiCyS - Women in Cybersecurity India Affiliate. She is responsible for leading cybersecurity & data privacy projects for her clients and analysing the evolving security and privacy challenges and developing innovative solutions for her clients.

Sarita has contributed to large scale national projects such as secure implementation of Ayushman Bharat Health Account Number (Unique Health ID of India), Pradhan Mantri Jan Arogya Yojana, Invest India, India's National ID project - Aadhaar and other digital innovation. She has curated long term strategic partnerships for her organizations with key cross-sectoral national and international institutions such as Data Security Council of India (DSCI), CERT-In, National Critical Information Infrastructure Protection Centre (NCIIPC), ISACA, United Nations Organization, GSMA. She has spearheaded multiple initiatives to support Women-in-Tech at her organization, promoting gender diversity and inclusion in the field of technology. She holds several professional certifications and has achieved notable accomplishments in her career.

Overall, with immense pride as a working mother, Sarita Padmini exemplifies a highly skilled cybersecurity professional dedicated to analysing security challenges and delivering effective solutions to her clients. Her extensive experience, leadership acumen, and cross-sector expertise position her as a valuable advisor in the realms of cyber security and data privacy.

THIRD PARTY VENDOR RISK MANAGEMENT (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.

AVAR

Association of anti Virus Asia Researchers

Enabling International Cyber Security Collaboration Since 1998

in /avar-asia/ X /avar_asia f /aavar.org

www.aavar.org

CONTENTS

Abstracts

CONTENTS

Panel Discussions