

DEC{CODE}{2020} ELEVATE


TRANSFORM RAPIDLY, SEAMLESSLY, SECURELY




A Virtual Conference
www.decodeph.com


DEC{O}DE{2020} ELEVATE

TRANSFORM RAPIDLY, SEAMLESSLY, SECURELY

 NOVEMBER 10 to 12, 2020

 10:45AM – 4:00PM

 vfairs.decodeph.com

 3000 Attendees

 40 Sessions

Coverage:
IT Professionals in the
Philippines (nationwide)

ABOUT DECODE

DECODE is the premier cyber security conference in the Philippines hosted by Trend Micro. It aims to decode to local technology professionals the up-to-date information about the threat landscape, industry trends, and new technologies in order to empower them to secure the digital infrastructures of their organizations, as well as to inspire them to embark on a continuous learning journey.

DECODE HISTORY:

- 2019: Gear Up! Defending our Connected World.
- 2018: Connected Threat Intelligence
- 2017: Transforming Security

THE THEME FOR DECODE 2020

ELEVATE

Transform rapidly, seamlessly, securely.

With the understanding of the new threats comes acceptance that all organizations need to transform. What does transformation entail? What are the security precautions we need to take? IT professionals must always be equipped not only with the right tools, but with the right skills and knowledge. In the fight to keep the connected world safe and secure, these cyber defenders must elevate beyond the ordinary and transform rapidly, seamlessly, securely.

DEC`0`DE {2020}

ELEVATE

TRANSFORM RAPIDLY, SEAMLESSLY, SECURELY

Industry

Technology and IT Services	41%
Academia	16%
Banking, Finance, Insurance	13%
Government & Law Enforcement	7%
Business & Professional Services	4%
Others (i.e. Telco, Manufacturing, etc.)	19%

Attendance Turnout

Confirmed Registration vs
Actual Attendance

2019	44%
2018	41%
2017	38%

Attendee Profile

based on Decode 2019 Participant Analysis

Roles & Job Function

Security Analyst / Consultant	14%
Information Security Professional	9%
System / Network Administrator	9%
Developer / Programmer	7%
Instructor	5%
Others (i.e. IT engr, Tech Support etc.)	56%

Cybersecurity Skills Gap in the Philippines

Survey Results (Respondents are IT Organization Leaders)

Fundamental Cybersecurity Skills



Risk analysis and Mitigation, and Security Analysis are the top fundamental cybersecurity skills

Threat to Cybersecurity



Non-technological means of security compromise (e.g. social hacking) are considered to be a major threat to cybersecurity

Only half of the responders consider ransomware to be a critical threat



IT Role Demand



IT role demands are stratified. There is variation in the demand for cybersecurity-related roles

IT Role Attrition



5 out of the top 10 IT roles with high attrition are cybersecurity-related roles

Investments Related to Cybersecurity

Infrastructure investments (network, hardware, software) make up most of their spending, followed closely by people related investments.



Most organizations spend a fair amount in outsourcing security management



Cybersecurity Skills Gap in the Philippines (Survey Results)

What do you think is/are the fundamental cybersecurity skill(s) of an IT professional, that should be common across all functions and roles?

ANSWER CHOICES	RESPONSES
Risk analysis and mitigation	65%
Security analysis	65%
Intrusion detection	62%
Building a well-rounded skillset	60%
Thinking like a hacker	59%
Malware analysis and reversing	48%
Cloud security	40%
Programming know-how	36%

What is the biggest threat to cybersecurity in the Philippines?

ANSWER CHOICES	RESPONSES
Social Hacking	79%
Unpatched Vulnerabilities	59%
Ransomware	49%
Distributed denial of service (DDoS) Attacks	36%
Others (please specify)	5%

What is the most in-demand job/role/function in the IT industry in the Philippines?

ANSWER CHOICES	RESPONSES
Information Security Professional	64%
Security Analyst/Consultant	31%
Network Security Professional	28%
Network Administrator	26%
Security Administrator	21%
Information Systems Analyst/Officer	19%
System Administrator	19%
IT Officer/Administrator	18%
Anti-Malware Specialist/Analyst	15%
Developer/Programmer	15%

What is the job/role/function where attrition is the highest?

ANSWER CHOICES	RESPONSES
Information Security Professional	43%
Network Security Professional	27%
Forensics Specialist/Analyst	20%
Security Analyst/Consultant	19%
Security Administrator	19%
Anti-Malware Specialist/Analyst	19%
Developer/Programmer	18%
IT Engineer/Staff	13%
IT Research and Development Specialist	12%
System Administrator	11%

Cybersecurity Investments

47%

Spend **BIG** investments on **Infrastructure**

35%

Spend **BIG** investments on **People**

32%

Spend **FAIR** investments on **Outsourced Security Management**

DECODE{2020}
ELEVATE
TRANSFORM RAPIDLY, SEAMLESSLY, SECURELY

40+
sessions

6 KEYNOTES

33 Breakout Sessions

2 Plenary Sessions

1 Panel Discussion

PROGRAM

	START	END	NOV 10 <i>Tuesday</i>	NOV 11 <i>Wednesday</i>	NOV 12 <i>Thursday</i>
Side Tracks	8:00	10:30	Get IT Girl (Girls in Tech)	DECODE Student Track	Get IT Girl Skill Building Track
Opening & Keynotes	10:45	11:00	Opening by Host James Deakin	Opening by Host James Deakin	Opening by Host James Deakin
	11:00	11:30	Trend Micro Keynote Martin Rösler	Trend Micro Keynote Myla Pilao	Trend Micro Keynote Robert McArdle
	11:30	12:00	Guest Keynote Michelle Hathaway <i>Hathaway Global Strategies LLC</i>	Guest Keynote Philip Casanova <i>Principal Technologist, SGV</i>	Guest Keynote Craig Jones <i>Director, Interpol Cybercrime</i>
<i>Break</i>	12:00	13:00			
Tracks	13:00	13:30	Track A B C -1	Track A B C -1	Track A B C -1
	13:30	13:45	Networking Lounge		
	13:45	14:15	Track A B C -2	Track A B C -2	Track A B C -2
	14:15	14:30	Networking Lounge		
	14:30	15:00	Track A B C -3	Track A B C -3	Track A B C -3
	15:00	15:15	Networking Lounge		
	15:15	15:45	Track A B C -4	Track A B C -4	Panel Discussion
Plenary / Panel / Closing	15:45	16:00	Networking Lounge		
	16:00	16:30	PLENARY SESSION	PLENARY SESSION	Recap and Closing
	16:30	16:45	Recap and Closing		

KEYNOTES



The Game Changer – How the Pandemic is Changing Your World

Martin Rösler

Senior Director of Forward-Looking Threat Research (FTR)
Trend Micro

Innovation or Disruption: Examining Scenarios at the Intersection of Technological Development

Myla Pilao

Director of Technology Marketing
Trend Micro



Cybercrime in 2020 and Beyond: Not Everything Changes in a Pandemic

Robert McArdle

Director for Cybercrime Research of Forward-Looking
Threat Research (FTR)
Trend Micro



KEYNOTES



Exposed: Attack Surfaces Widen as the World Increasingly Relies on Digital Infrastructures

Melissa Hathaway

President
Hathaway Global, LLC

Principles to Live By for Cybersecurity Leaders

Philip Casanova

Principal, Technology Consulting Cybersecurity, Privacy,
and Trusted Technology
SyCip Gorres Velayo & Co



Cybercrime Through the Lens of Law Enforcement
and Private Partners

Craig Jones

Director of Cybercrime
Interpol



TRACKS / BREAKOUTS

SECURING PRIVACY
and IDENTITY,
COMPLIANCE

**NO MORE
SECRETS**

**BUSINESS
UNUSUAL**

CYBERCRIME,
VULNERABILITIES,
EMERGING and FUTURE
THREATS

AI, ML, IoT, IIoT,
Cloud

**THE DIGITAL
FRONTIER**

**SECURING
THE
SECURITY
LANDSCAPE**

FORENSICS,
INVESTIGATIONS,
INTELLIGENCE and
RESPONSE

DECODE{2020}
ELEVATE
TRANSFORM RAPIDLY, SEAMLESSLY, SECURELY

DECODE 2020 SPEAKERS

An abstract graphic on the right side of the slide, composed of various colored triangles (red, cyan, lime green, white) arranged in a complex, overlapping pattern that suggests movement or a stylized shape.

Martin Roesler



Martin Roesler holds a Dipl.-Ing.(FH) degree in civil engineering and has been working in the computer security field since 1990. Having a penchant for technology — he actually lives in a Smart Home lab —, he enjoys learning about the latest tech trends and the innovations they contribute to the society.

Currently, Martin is the Senior Director of the Trend Micro Forward-Looking Threat Research (FTR) team. He built the FTR team in 2009 and has since been in charged of underground research, eCrime investigation services, and global law enforcement collaboration. Besides these, he specializes in Smart Technologies like Smart Homes and other internet-connected devices.

The Covid-19 pandemic is impacting people around the globe: millions of people got sick, the global economic growth dropped by more than 9%, and we are in a horse race to speed up medical progress and secure vaccine resources.

But besides all these direct impacts, there is another massive, long-term impact that needs to be addressed. Industries as well as ordinary users across the globe are faced with new cybersecurity risks and threats that could significantly impact the way they go about their dailies. In this session, Martin will be looking at some of the new cyber risks, threats, and challenges that the world is facing today.



Myla Pilao



Innovation or Disruption: Examining Scenarios at the Intersection of Technological Development

Myla leads the security research communications at Trend Micro, she heads the division of the company that monitors the security threat landscape, including high-profile attacks, like advanced persistent threats (APTs) and prevalent digital security risks . She supervises the development of critical information to broaden understanding of cyber security.

Myla contributes technical guidance in the development of strategic cybersecurity frameworks as she share her insights on digital threats and their real-world impact, along with countermeasure strategies for the computing public.

Myla is an active supporter of and advocate for the protection of children online. She also supports international movements that work on stopping the online commercial distribution of inappropriate images of children.

Connected technology has permeated even into the most intimate units of human life, while simultaneously making strides in wider and more encompassing aspects of society. Today, organizations aim to remain at the cusp of the latest technological trends and developments to improve their operations as well as remain competitive and relevant in the global market. This transformation introduces an unprecedented level of convenience and functionality, but it also demands the prominent presence of cybersecurity in every connected environment.

In this session, Myla will be examining how countries and organizations are being disrupted by a myriad of digital threats and risks, and why it's crucial that they reexamine their existing security architecture to make it robust against present cyberthreats.



Robert McArdle



Robert McArdle is the Director for Cybercrime Research of the Forward-Looking Threat Research (FTR) team, where he is involved in analyzing the latest cybercrime threats, researching the future threat landscape and Open Source Intelligence (OSINT), and coordinating investigations with international law enforcement agencies.

Robert also lectures for MSc modules in Malware Analysis for University College Dublin and Cork Institute of Technology. In addition, he has previously mentored for the SANS Incident Handling and Hacker Exploits Certificate (GCIH) and their Security Essentials Certificate (GSEC).

2020 has been a year of change far beyond even the wildest predictions. Besides the toll on our health, the pandemic has disrupted entire industries and fast-tracked changes in digitization that would otherwise have taken years to happen. This speed of change makes events and the ways we worked and interacted online in the past seem like a distant memory, despite being only a few months ago. If you want to confirm this time distortion for yourself, close your eyes and think of how long it feels since you last heard the words... "Taal Volcano eruption."

In this session, Robert will be exploring these effects and the state of cybercrime today. He will also be predicting, as best as one can in 2020, how cybercrime will evolve in the future.



Exposed: Attack Surfaces Widen as the World Increasingly Relies on Digital Infrastructures

Melissa Hathaway

President
Hathaway Global, LLC



Melissa Hathaway is a leading expert in cyberspace policy and cybersecurity and served in two U.S. presidential administrations. Melissa brings a unique combination of policy and technical expertise, as well as board room experience to help others better understand the intersection of government policy, developing technological and industry trends, and economic drivers that impact acquisition and business development strategy in this field.

Critical infrastructures and services are fragile. The pandemic has caused the world to work from home and learn from home — using the technologies that had actually been available for at least the past decade. Telemedicine, remote learning, and on-line education were among the early adopters of these technologies out of necessity. But even the Global 1000 businesses adapted and adopted quickly and have reported positive results regarding their increased productivity and meeting key performance criteria. And while our internet service providers (ISPs) and telecommunications companies are trying to build more capacity in the system, they are also experiencing more and more outages, knocking us offline when we need to be online. The supporting digital infrastructures are fragile and, in addition to glitches and outages, malicious actors are taking advantage of our increased reliance on digital tools and broader exposure to cyber risks to ramp scam individuals, ransom businesses, disrupt critical infrastructures, and attack governments at all levels.



Philip Casanova

Principal | Technology Consulting |
Cybersecurity, Privacy, and Trusted Technology
SyCip Gorres Velayo & Co



Philip Casanova is a Partner in SyCip Gorres Velayo & Co. (SGV)'s Technology Consulting practice, focusing on cybersecurity. He is a seasoned cybersecurity professional with nearly 25 years of experience as a consultant and as a Chief Information Security Officer (CISO). He has held cybersecurity leadership roles as the CISO of financial services institutions in the Philippines, other Asian regions, and North America, particularly New York. He is one of the signatories of the Philippine National Standards for Information Security under DTI.

Philip will be sharing timeless principles that he learned in his over two-decade journey as a cybersecurity professional.

His presentation aims to strengthen the mindset, persona, and posture of current and aspiring cybersecurity leaders in this evolving cyber threat landscape. Learning these principles can help cybersecurity leaders be consistent in decision making, opinions and recommendations.



Craig Jones

Director of Cybercrime
Interpol



Originally from New Zealand, Craig Jones leads INTERPOL's Global Cybercrime Programme. The objectives of this Programme are to reduce the global impact of cybercrime and protect communities for a safer world. Under this mandate, he focuses on operational delivery, cyber threat response and capabilities development in support of 194 INTERPOL member countries.

Fighting cybercrime is a task that no organization can effectively do on its own – not law enforcement agencies, governments, or private organizations. This is because cybercrime is a unique breed of crime –the cybercriminal can be on the other side of the world, but a huge chunk of useful evidence and intelligence can sit on the logs of ISPs, hosting providers, and cybersecurity companies, among other entities.

In this session, Craig will be discussing why it is crucial that law enforcement agencies and private partners collaborate in investigations to thwart cybercriminal operations and reduce the risks it could pose to ordinary users and enterprises.

DECODE



Jay Yaneza

Director of Managed XDR

Trend Micro

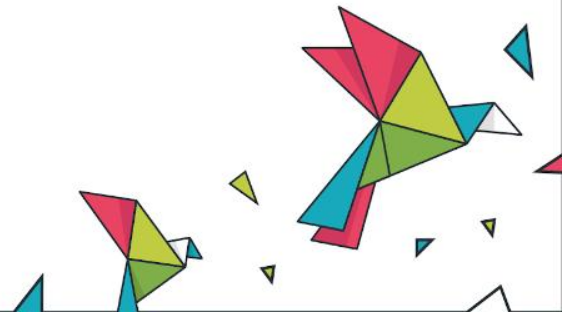
Jay is the director for the Trend Micro Managed Detection and Response Operations and is based in the US. An open source enthusiast and seasonal programmer, he actively investigates noteworthy incidents within the North America Business Unit (NABU) caused by interesting threats or targeted attacks.

TBD

How Threat Actors Move



DEC`0`DE



Alexander Caciuloiu

Cybercrime Project Coordinator
Regional Office for Southeast Asia and the Pacific
UN Office on Drugs and Crime (UNODC)

Alexandru Caciuloiu is the United Nations Office on Drugs and Crime (UNODC) Cybercrime and Cryptocurrency Advisor and Regional Coordinator for Southeast Asia and the Pacific. He is responsible for building and strengthening the region's capabilities and response to cybercrime and cybersecurity. He provides technical assistance, expertise, capacity-building as well as assistance with policy making and legislative harmonization.



BUSINESS UNUSUAL

Darknet and Cryptocurrency Trends in Southeast Asia

TBD

The background is a solid teal color. On the left side, there is a large, complex geometric shape composed of several triangles in shades of red, green, and white. This shape appears to be a stylized, multi-faceted object. Scattered throughout the lower half of the image are smaller, similar geometric shapes in the same color palette, some pointing upwards and some downwards, creating a sense of movement and depth.

THE DIGITAL FRONTIER

AI, ML, IoT, IIoT, Cloud

These sessions are devoted to discussions surrounding the latest technological advances that are proving to be essential in cybersecurity: artificial intelligence (AI), machine learning (ML), internet of things (IoT), industrial internet of things (IIoT), and the cloud. In these sessions, speakers will be dissecting the most recent security risks and threats associated with the aforementioned technologies and provide useful knowledge that can help organizations beef up their security posture.

Magno Logan

Information Security Specialist

Deep Security Labs

Trend Micro

Magno Logan works as an Information Security Specialist for Trend Micro Cloud Research Team. He specializes in Cloud, Container and Application Security Research, Threat Modeling, Red Teaming, DevSecOps, and Kubernetes Security, among many others. He has been tapped as a resource speaker for numerous security conferences around the globe including US, Canada, Brazil and Portugal.



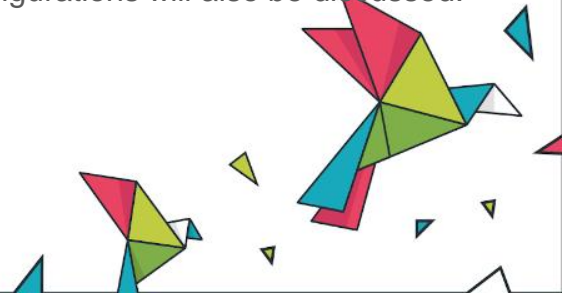
DECODE

THE DIGITAL FRONTIER

Kubernetes Security 101: Best Practices for Securing Your Cluster

This presentation aims to give an overview about how Kubernetes – an orchestration tool for scalable container deployment and management – works and to provide the best practices users can follow to secure their cluster when deploying and maintaining a cluster on their own or via managed services on Cloud Service Providers such as Google, AWS and Azure.

This session will be covering everything from the Master Node, starting with the Kube API server, also including the etcd, Role Based Access Control and Network Policies, and then the Worker Nodes, covering the kubelet, how to enable audit logs and how to protect your pods. CIS Benchmarks for Kubernetes and the default security configurations will also be discussed.



Alfredo Oliveira

Security Research Leader
Cloud and Container Threat Research
Trend Micro

Alfredo Oliveira is a Security Research Leader at Trend Micro, with over 10 years of working experience in the cybersecurity industry. He specializes in open source software, reverse engineering, malware analysis, honeypot deployment, data analysis, and, recently, container research.



DECODE

THE DIGITAL FRONTIER

Shedding Light on Security Considerations in Serverless Cloud Architectures

Serverless computing is a kind of cloud computing execution model that enables enterprises to use the computational power of a cloud service provider (CSP). It allows enterprises to focus on building apps and core products, rather than using manpower to maintain and secure server infrastructure. However, serverless technologies are not immune to risks and threats.

This presentation aims to shed light on the security considerations in serverless environments and help adopters in keeping their serverless deployments as secure as possible. It will be focusing on services offered by AWS, which has the widest range of offerings available in the serverless services market.



Joey Costoya

Senior Threat Researcher
Forward-Looking Threat Research
Trend Micro

Joey Costoya works as a Senior Threat Researcher under the Trend Micro Forward-Looking Threat Research (FTR) team. He was involved in developing novel infrastructure for threat analysis and an early pioneer of data streaming for big-data analytics. More recently, he has been building systems to aid threat research on hybrid, private, and public AWS cloud.



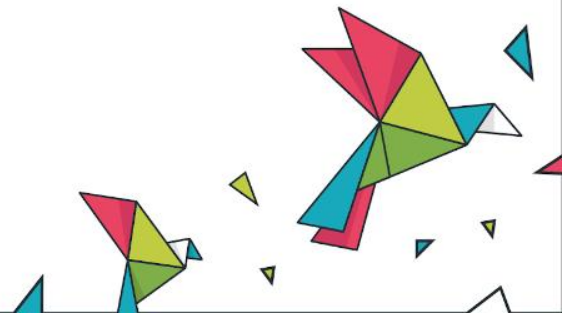
DECODE

THE DIGITAL FRONTIER

Cyberattack Trends in the Cloud

The benefits of migrating to and using cloud-based technologies also come with the risk of exposing organizations' infrastructure to the whole internet. To discover how exposed these cloud deployments are, Joey and his teammates conducted an in-depth survey of various cloud services and technologies, and identified a large number of exposed and badly configured cloud services, and in some cases, actively compromised cloud infrastructure.

This presentation will be exploring the various issues that they discovered, as well as the risks introduced to the organization. Furthermore, the presentation will touch on basic guidelines and best practices on how to secure your own cloud deployments.



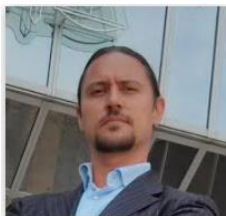
Vincenzo Ciancaglini

Senior Threat Researcher

Forward-Looking Threat Research

Trend Micro

Dr. Vincenzo Ciancaglini, who works at Trend Micro as a research scientist within the Forward-Looking Threat Research team (FTR), holds an M.Sc. in Telecommunications Engineering and an M.Sc. in Electrical Engineering, Wireless Systems. He develops new data analytics prototypes, identifies targeted attacks, and conducts research on new encrypted networks (darkweb) and Internet of Things (IoT).



DECODE

BUSINESS UNUSUAL

How Cybercriminals Misuse, Abuse AI and ML

While AI and ML can support businesses, critical infrastructures, and industries as well as help solve some of society's biggest challenges, these technologies can also enable a wide range of digital, physical, and political threats to surface.

This presentation will be discussing a research project, a joint effort among Europol, Trend Micro, and the United Nations Interregional Crime and Justice Research Institute (UNICRI), that shows the present state of the malicious uses and abuses of AI and ML technologies, and the plausible future scenarios in which cybercriminals might abuse these technologies for ill gain.



Shin Li

Senior Engineer
Cyber Safety Solution
Trend Micro



Shin Li graduated from National Cheng Kung University and has worked as a lecturer in several hardware-based associations and cybersecurity organizations for many years. He is effective at reviewing security issues from the perspective of hardware designers. He is currently working as a threat researcher at Trend Micro Security Cyber Security.

Ta-Lun Yen

Senior Engineer
IoT & ICS Security Research Labs
TXOne Networks Trend Micro

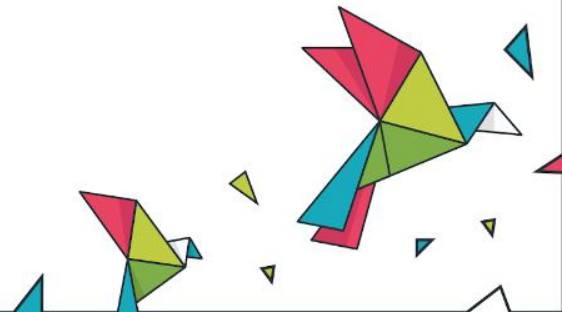


Ta-Lun Yen is a Trend Micro security researcher that specializes in reverse engineering, protocol analysis, wireless security, and IoT/ICS device security. He has been a member of the Taiwanese InfoSec community "UCCU Hacker" since 2018. He has presented at various conferences and events, including Black Hat EU 2019, HITCON 2018/2019, and TDOH-Conf 2018.

A Look at USBee Malware

During WW2, the U.S. used a flawed cryptographic device that relied on electro-mechanical relays in its operation. Eventually, researchers discovered they were able to detect electromagnetic spikes and eventually recover the plain text via radio. Decades later, Wim van Eck published an analysis on computer monitors, which describes a way to eavesdrop on CRT displays, in similar fashion with flawed U.S. device. Such research elevated alertness on research regarding side channel, and caused consternation in the community as such attacks required sophisticated equipment only available to organizations with a huge budget to expend.

In recent years, such topic has developed into a field of its own, and dubbed TEMPEST by NSA. In Black Hat USA 2020, researchers have revealed a method to eavesdrop on conversations via vibration patterns in a hanging light bulb, which only requires a line of sight to obtain. In this session, the researchers will be taking a closer look at USBee, a malware variant that uses electromagnetic emissions from an ordinary USB cable to exfiltrate data.



Karla Agregado

Senior Engineer
Cyber Safety Solution
Trend Micro



Karla Agregado is a Senior Threat Researcher at Trend Micro who is currently working with the Machine Learning (ML) team. She's an expert in web analysis and has an in-depth understanding of the web threat landscape. In line with this knowledge, she applies different ML applications like feature creation based on the latest web threat techniques as a result of her continuous research.

Joy Avelino

Senior Engineer
IoT & ICS Security Research Labs
Trend Micro

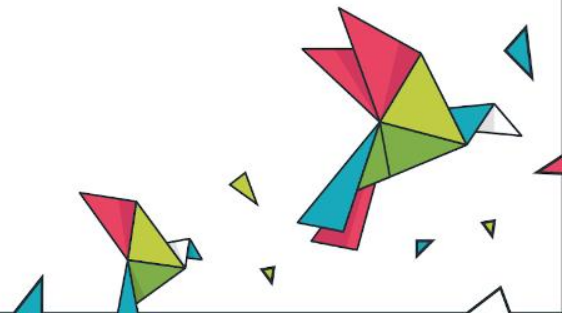


Joy Avelino is a Senior Threat Researcher at Trend Micro. In the recent years, she has regularly presented use cases of machine learning in the threat security industry based from actual results of machine learning POC projects. She has presented in previous academic conferences such as IEEE IISA 2014 and IEEE TENCON 2018.

A Web of Threats: How Machine Learning weave over the Web Threat Landscape

The ongoing pandemic compelled many organizations to shift from operating manually to maximizing various technologies for their day-to-day transactions. Due to this fact, there has been an increased traffic online, paving the way for threat actors to launch attacks against public and private institutions. For instance, there has been an increase in the number of phishing attacks using different web sharing services and cloud applications.

In this presentation, Karla and Joy will be diving deep into how the current global trends have shaped the web threat landscape with the help of machine learning (ML).



Jon Oliver

Director & Data Scientist
Threat Research
Trend Micro

Dr. Jon Oliver has been with Trend Micro for 13 years, and worked on a range of machine learning (ML)- and threat-based projects. The ML projects include ML for antispam, WRS categories, TrendX (files) and building TLSH. Jon has a PhD from Monash University and is an inventor of over 100 software patents.



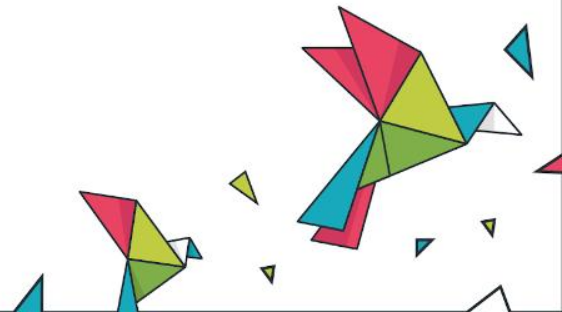
DEC`0`DE

THE DIGITAL FRONTIER

The Role of Machine Learning in Cybersecurity

There has been an ongoing evolution of the malware and security landscapes. In the last few years, we have seen the widespread adoption of machine learning (ML) into cybersecurity solutions. In response to this, we have seen changes in the methods adopted by malware authors to evade security solutions. It is a game of cat and mouse between the attackers and defenders, and unfortunately there are real-world consequences when cybercriminals succeed.

In this presentation, Jon will be looking at this ongoing evolution of security and malware. He will describe why ML is a key technology in understanding the interaction between malware and how security solutions can help maximize the benefits of ML-based security.



Isaac Reyes

Data Scientist & Co-Founder
StoryIQ

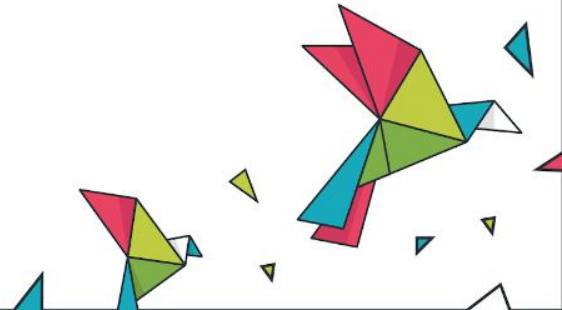
Isaac Reyes, Co-Founder at StoryIQ, is a TEDx speaker and international keynote presenter in data visualization and machine learning. He was the keynote speaker at the 2019 Open Data Science Conference in Brazil and over 2018-2019, his speaking tour visited 26 cities across five continents. His ultimate goal is to empower every organization to derive value from data.



Asking the Right Business Question — The Most Important Phase of the Data Science Process

Asking the right business question is easily the most important phase of any data science project. Despite this, many data science teams focus on the wrong business questions. Teams often select projects that are either not feasible or tackle problems that don't drive sufficient business value.

Isaac will be talking about a methodology for selecting the right business question, therefore ensuring that data science projects deliver real, risk controlled business value.



The background is a solid teal color. It is decorated with several abstract, multi-faceted geometric shapes in shades of red, green, and white. These shapes resemble stylized, low-poly birds or flying objects, scattered across the frame. Some are larger and more prominent, while others are smaller and more distant.

NO MORE SECRETS

SECURING PRIVACY and IDENTITY, COMPLIANCE

With news of high-profile incidents of company and consumer data exposure becoming a common occurrence recently, the need for stronger data protection measures is also becoming increasingly apparent. In these track sessions, speakers will be bringing a broad range of perspectives to trends and challenges related to data privacy, security, and compliance.

Feike Hacquebord

Senior Threat Researcher

Forward-Looking Threat Research

Trend Micro

Feike Hacquebord, Senior Threat Researcher, has over 15 years of experience conducting threat research. Since 2005, he has been a regular advisor of international law enforcement agencies and has assisted in high-profile investigations. Prior to joining Trend Micro, he earned a Ph.D. in theoretical physics from the University of Amsterdam.



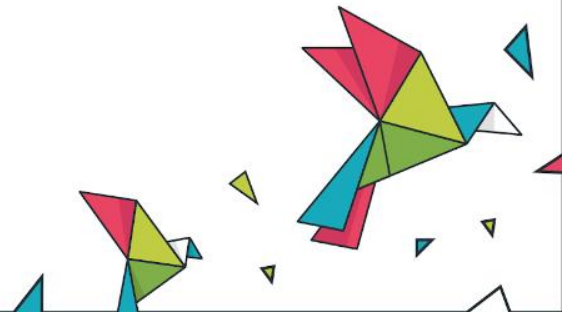
DECODE

NO MORE SECRETS

The Risks of Open Banking

As more industries adapt to cater to the increasingly mobile market, the financial industry is the latest to experience a shake-up. The Revised Payment Service Directive (PSD2) – also known as Open Banking – is a new set of rules for the European Union (EU) that's expected to affect the global financial industry.

With Open Banking, banks will have to provide APIs to share customers' banking data with third parties. Hear the results of Feike's research into the challenges of protecting the larger attack surface created by open banking and the potential security issues associated with APIs, banking apps, and protocols.



Drex Laggui

Principal Consultant
Laggui & Associates

Drex Laggui is a Highly Technical Consultant (HTC) for the Office of the Assistant Secretary for Digital Philippines (OASDP) at the Philippine Department of Information and Communications Technology (DICT). He is also a Post-Sales Technical Support Contractor for Verint (NASDAQ: VRNT), where he provides services that include detecting threats on a national scale, assessing impact of known threats, conducting cyber threat hunting to upcoming campaigns.

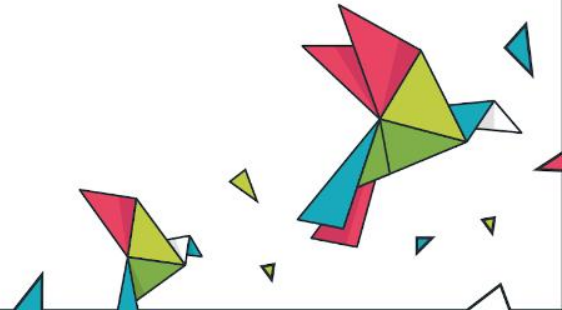


DECODE

NO MORE SECRETS

DIGITAL PRIVACY VS. PUBLIC SECURITY: Which Side Are You On?

TBD



Andreas Gehrmann

Managing Director
SRMS & Associates Pte. Ltd.

Andreas Gerhmann is a Managing Director and Lead Consultant at SRMS Associates Pte. Ltd., a management consultancy firm. He has over 20 years of experience in auditing, training, consultancy, and business development in the Asia Pacific Region. He also has 15 years of experience in the field of information security, business continuity management, personal data protection, and supply chain security management.



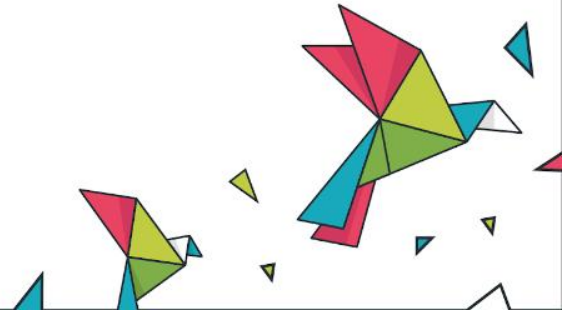
DEC}DE

NO MORE SECRETS

Personal Data Protection in the Time of COVID-19: Using Privacy Impact Assessment and Proper Security Controls for Compliance and Risk Management

Technology provides solutions for managing risks surrounding COVID-19 and controlling the spread of the virus. In the rush to come up with technical solutions, standard constraints on collecting and processing private data have been disregarded or waived and compromises on security have been often made.

In this presentation, Andreas will be illustrating the complex management and minimization of the impact of compromised personally identifiable information (PII) at the time of a pandemic. He will be introducing the concept of privacy by design and privacy impact assessment. In addition, he will be discussing the controls and tools needed to minimize the adverse and long-lasting impacts of solutions deployed to fight COVID-19.



Atty Michael Santos

Officer-In-Charge

Complaints and Investigations Division

National Privacy Commission

TBD

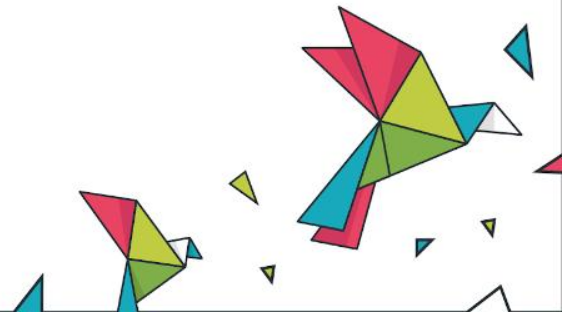
TBD

TBD



DEC`{}DE`

NO MORE SECRETS



The background is a solid teal color. On the left side, there is a large, complex geometric shape composed of several triangles in shades of pink, green, and white. Scattered across the bottom and right sides are smaller, similar geometric shapes in the same color palette, some pointing upwards and some downwards, creating a sense of movement and depth.

BUSINESS UNUSUAL

CYBERCRIME, VULNERABILITIES, EMERGING AND FUTURE THREATS

The sessions for this track will bring a focus on the shifting nature of cybercrime, the current set of tools and exploits that cybercriminals could use and abuse to facilitate attacks, and more. Speakers will be diving into the latest research and future areas of interest for organizations navigating the increasingly dynamic threat landscape.

Jaromir Horejsi

Senior Cyber Threat Researcher
Cyber Safety Solution
Trend Micro

Jaromir Horejsi is a threat researcher at Trend Micro. He specializes in hunting and reverse engineering threats that target Windows and Linux, such as APTs, DDoS botnets, banking Trojans, click fraud, and ransomware. He has presented his research works at RSAC, SAS, Virus Bulletin, HITB, FIRST, AVAR, Botconf, and CARO.



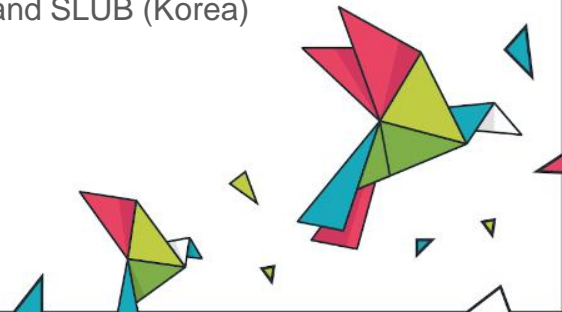
DEC`0`DE

BUSINESS UNUSUAL

Cyberespionage: Targeted Attacks Abusing Third-Party Cloud Services

To achieve their espionage goals, threat actors need a mechanism to exfiltrate data from their targets. Malware developers have a multitude of choices to achieve this task, for example, the design and implementation of a custom communication protocol, and the use of an existing protocol offered by cloud services.

This presentation will be discussing the benefits and limitations of implementing a custom communication protocol, and the cases where attackers abused third-party cloud services in selected targeted. These cases involve targeted threat actors across the globe, including Patchwork (South Asia), DRBControl(South East Asia), Confucius (South Asia), MuddyWater (Middle East), and SLUB (Korea)



Dusan Stevanovic

Senior Threat Researcher
Vulnerability Research Service
Trend Micro

Dusan Stevanovic has been a member of the Trend Micro Security Research Vulnerability Research Service (VRS) team since 2015. He researches and provides detection guidance for N-day vulnerabilities. This work also includes developing PoCs and exploits for the most recently-discovered critical vulnerabilities. Before joining VRS, he completed his PhD in Computer Science from York University in Toronto, Canada.



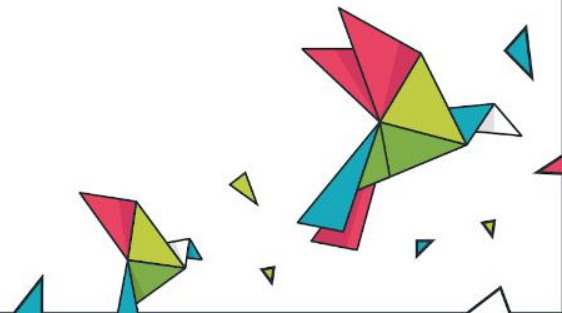
DECODE

BUSINESS UNUSUAL

Deserialization Vulnerabilities: From Theory to Practice

In this session, Dusan will provide an overview of the insecure object deserialization in Java and .NET and provide an in-depth look at 2 different cases of these vulnerabilities. In the first part of the presentation, Dusan will be delving into the basics of object serialization and provide insight into why deserialization attack surfaces exist in applications built on top of Java and .NET.

In the second part of the presentation, Dusan will be presenting an overview of three specific recent cases of deserialization vulnerabilities in Java and .NET, where he will provide an in-depth look at the vulnerability in the three scenarios and how to detect these forms of attacks.



Andy Niu

Senior Threat Researcher
Vulnerability Research Service
Trend Micro

Andy Niu works a Senior Consultant at Trend Micro. As a long time shellcode exploit developer, his work covers all kinds of vulnerabilities, stack buffer overflow, heap memory corruption, command injection, and many more.



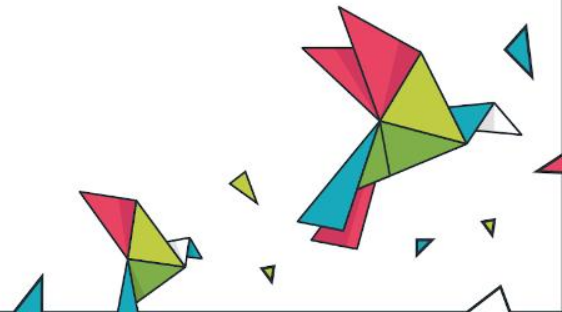
DECODE

BUSINESS UNUSUAL

From Use-After-Free To Remote Code Execution

User-After-Free (UAF) vulnerabilities have been widely used in developing web browser malware variants. A UAF vulnerability concerns the incorrect use of dynamic memory during program operation. If after freeing a memory location, a program does not clear the pointer to that memory, malicious actors can use the error to hack the program.

In this presentation, Andy will be introducing the technologies and tricks available to write a real shellcode exploit abusing a UAF vulnerability.



Vladimir Kropotov

Senior Threat Researcher
Forward-Looking Threat Research
Trend Micro

Vladimir Kropotov, who earned master's degrees in applied mathematics and information security, works as a Senior Threat Researcher within the Trend Micro Forward-Looking Threat Research (FTR) team. He previously built and led incident response teams at Fortune 500 companies. Vladimir has appeared at international conferences such as FIRST, CARO, HITB, PHDays, ZeroNights, Black Hat EU, and more.

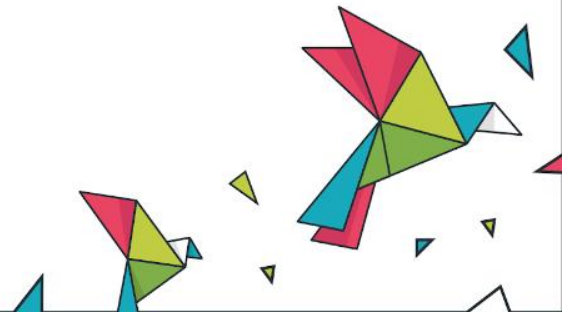


BUSINESS UNUSUAL

Past, Present, and Future of Cybercrime Infrastructure

Criminal infrastructure is an important chain that binds the whole underground ecosystem. This presentation will be focusing on the evolution of technologies and approaches which underground actors use to maintain and protect their infrastructures. It will show how actors abuse legitimate hosting and cloud services, exploit geographical and cross-jurisdictional issues to avoid takedowns, or even maintain server farms located in private houses in rural areas.

The presentation will also be discussing the shifts on underground hosting approaches, which are enforced by the introduction of new technologies. The presentation contains several case studies that are based on our investigations of cyber incidents.



Vincent Lee

Vulnerability Researcher
ZDI Vulnerability Analysis
Trend Micro

Vincent Lee is a Vulnerability Researcher at Trend Micro's Zero Day Initiative (ZDI) program. His primary role involves performing root cause analysis and determining the exploitability of ZDI submissions. He previously served as a researcher at TELUS Security Labs, where he looked at known security issues to provide detection guidance to a variety of security solution vendors.



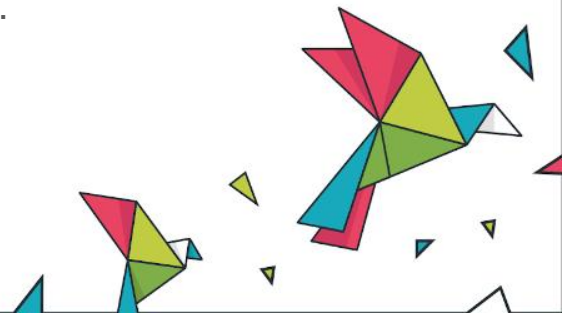
DECODE

BUSINESS UNUSUAL

Getting Started in Hardware Reversing with ZDI

Reverse engineering routers and IoT devices may seem daunting for beginners. In this session, Vincent will be guiding you through hardware reverse engineering and vulnerability hunting processes through vulnerabilities affecting two routers. He will explore the hardware architecture and design of the TP-Link TL-WR841N and the Belkin F7D2301 router.

In addition, he will be looking at the Linux-based firmware of the TP-Link and the RTOS-based firmware of the Belkin, then walk through the vulnerabilities reported in these routers.



Paul Pajares

Threat Researcher
Threat Hunting Team
Trend Micro

Paul Pajares works as a researcher within the Trend Micro Threat Hunting team. He has worked on web reputation services, threat sourcing, antivirus benchmarking, and threat hunting. As part of a strategic partnership between INTERPOL and Trend Micro, he is currently a seconded researcher in the former and is involved in different fields, such as cryptojacking mitigation, threat assessment, campaign awareness, and RFIs.



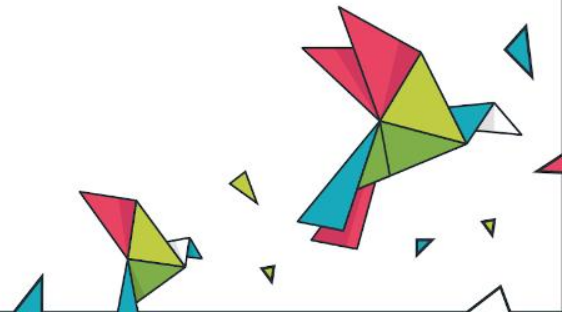
DECODE

BUSINESS UNUSUAL

Cyber Threat Intelligence Toward Cybercrime Investigation

Law enforcement (LE) agencies play a vital role in shaping down cybercrime trends. As a seconded researcher to an LE agency, Paul will be sharing some of his experiences on working with them.

Paul will also be discussing how Trend Micro's provision of expert insights and datasets help LE agencies proceed in some investigations. He will also be highlighting the dependencies of LE to private partners (cybersecurity firms) and vice versa by citing some cases. In addition, Paul will be sharing some tips and tricks on how to utilize threat intelligence in order to move forward.



Ricky Lawshae

Senior Security Researcher

DV Labs

Trend Micro`

Ricky Lawshae is a Senior Security Researcher for Trend Micro, focusing mainly on enterprise IoT. He has found and disclosed more than 50 vulnerabilities in devices from HID, Crestron, Oculus, and many more. His work has been featured in Forbes, Wired, and Hackaday. He has spoken at conferences around the world, including Defcon, Recon, Ruxcon, and Insomnihack.



DECODE

BUSINESS UNUSUAL

Pitfalls of OSS in IoT

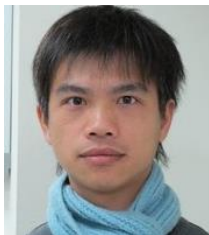
Open source software has become the standard foundation upon which most IoT devices are built these days. It helps to keep costs down and allows for easy customization in order to suit specific needs. However, there are some very common problems and potentially serious security ramifications that come along with those benefits.

In this presentation, Ricky will be discussing some of the more common pitfalls that users and developers need to be mindful of when using and modifying open source software. He will go over some real-world examples of vulnerabilities and exploits in IoT devices, how they were found, and how to avoid making the same mistakes in the future by following certain best practices.



Philippe Z Lin

Senior Threat Researcher
Forward-Looking Threat Research
Trend Micro



Philippe Lin works as a Senior Threat Researcher within the Trend Micro Forward-Looking Threat Research (FTR) team. He is mainly working on industrial embedded system, software defined radio and 4G/5G core network. He was a BIOS engineer, a maker, and an enthusiast of open source software.

Roel Reyes

Senior Threat Researcher
Forward-Looking Threat Research
Trend Micro



Roel Reyes is a Senior Threat Researcher within the Trend Micro Forward-Looking Threat Research (FTR) team. He is currently involved in threat research as well as on-premise or AWS cloud-based infrastructure builds. He started as a Quality Assurance Engineer and became part of the Web Reputation Services Team, developing solutions focused on system enhancements and improvements.

DECODE

BUSINESS UNUSUAL

Edge Computing

Facial recognition access control is one of the killer apps that benefit from the emerging edge computing architecture, which brings the processing power near the endpoints for faster processing speed, less latency and reduced demand of bandwidth.

This presentation will be discussing three popular facial recognition systems and the vulnerabilities that have identified, including: server command forgery, user arbitrary addition, privilege escalation, man-in-the-middle, and face database exposure. The presentation will also demonstrate how to leak employee pictures, automatically add unauthorized personnel as administrator, and impersonate a back-end server in order to open the doors and leave a false trace to deceive auditions.



PCol Michael Angelo Reyes Zuñiga

<Title of Talk>

Chief, Operations Management Division
Philippine National Police (PNP)
Anti Cybercrime Group (ACG)

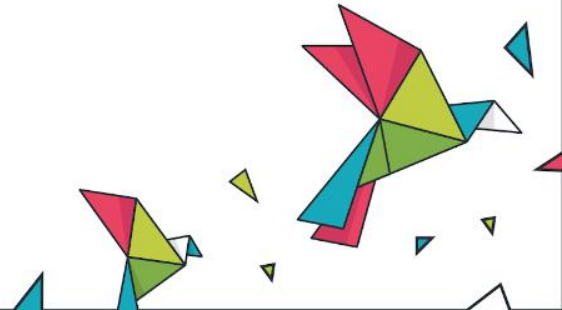
TBD

TBD



DECODE

BUSINESS UNUSUAL



Joseph Pacamarra

Co-Founder

CERT PH

Joseph Pacamarra, co-founder of Cyber Security Philippines CERT®, specializes in OSINT, CYBINT, insider threat, threat research, and DevSec, among many others. As a former Senior Security Analyst / Security Consultant at Trend Micro, he co-wrote the Consulting Services Program that covers Critical System, Network, Security Analysis and Monitoring for the Trend Micro Custom Defense Services.



NO MORE SECRETS

Insider Threat — The Enemy from Within

Insider threat is a malicious threat that comes from people within the organization, such as employees, former employees, contractors or business associates.

In this session, Joseph will be discussing the real-life concern of many organizations that rarely hits the news: the motive, detection, interdiction, tactics and strategy of insider threats, which are among the most devastating threats that any organization will ever encounter.

The background is a solid teal color. Scattered throughout are various geometric shapes, primarily triangles and polygons, in shades of red, green, and white. Some shapes are larger and more complex, while others are smaller and simpler. The shapes are distributed across the page, with a larger cluster on the left side and smaller ones scattered towards the bottom and right.

SECURING THE SECURITY LANDSCAPE

FORENSICS, INVESTIGATIONS, INTELLIGENCE and RESPONSE

The emergence of new and increasingly sophisticated cyberthreats highlight the need for better strategies for securing the computing environment. Speakers for this track will be taking a closer look at notable cybercrime investigations and state-of-the-art infrastructure defense and forensic techniques that could aid industries in their efforts to secure their digital assets and resources.

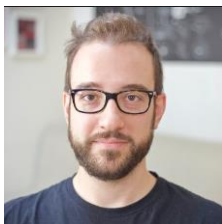
Federico Maggi

Senior Threat Researcher

Forward-Looking Threat Research

Trend Micro

Federico Maggi, a former assistant professor at Politecnico di Milano, currently works as a Senior Threat Researcher at Trend Micro. He specializes in conducting threat and security analysis virtually on any system. He has given several lectures and talks as an invited speaker at international venues and research schools, and also serves in the review or organizing committees of well-known conferences.



SECURING THE SECURITY LANDSCAPE

The Hidden Risks of Industrial Automation Programming and their Repercussions for Smart Factories

Robots and other programmable industrial machines are the backbone of the manufacturing industry. Without them, the large-scale and fast-paced production that our modern economy depends on would simply be impossible. However, as much as modern manufacturing is dependent on them, these machines themselves rely on legacy technology designed decades ago.

This presentation will be discussing the legacy programming environments of widely used industrial machines that harbor virtually undetectable vulnerabilities and malware. The security analysis of these environments, which was conducted in collaboration with Politecnico di Milano, reveals critical flaws and their repercussions for smart factories.

Josiah Hagen

Senior Security Researcher

DV Labs

Trend Micro

Josiah Hagen is a Security Researcher at Trend Micro Research. He has a BA in Mathematics and Computer Science from Oberlin College and has over 20 years of professional software development experience focusing on AI and ML techniques. His cybersecurity work ranges from ML detection of DGAs and EK obfuscation to scaling unsupervised techniques applied to various byte streams.



DECODE

SECURING THE SECURITY LANDSCAPE

A Survey of Similarity for Security

Detecting similar artifacts is crucial to identifying variants that malicious actors use to evade defenses. With static inspection of files or other parts of byte streams, using a similarity measure provides a quick mechanism to triage the vast sea of incoming unknowns.

This presentation will be discussing the development and evolution of similarity measures adopted by the security community, comparing approaches for their search and clustering effectiveness and their runtime performance. In particular, the presentation will explain the algorithms used by SSDeep, SDHash, TLSH, LZJ and JA3. A demonstration on why Trend Micro leads the industry in this field, and its application to security problems, will also be showcased.



Gilbert Sison

Cyber Threat Hunting Technical Lead
Incident Response
Trend Micro



Gilbert Sison is fortunate enough to do what he enjoys doing and that is to figure out how things work. All the experience, skills and knowledge he accumulated in his 15-year tenure in Trend Micro as an AV engineer, QA engineer, and threat researcher, are in full use in his role as a threat hunter for the Managed XDR team. As a threat hunter, he finds needles in haystacks to identify attacks.

Abraham Camba

Incident Response Analyst
Incident Response
Trend Micro

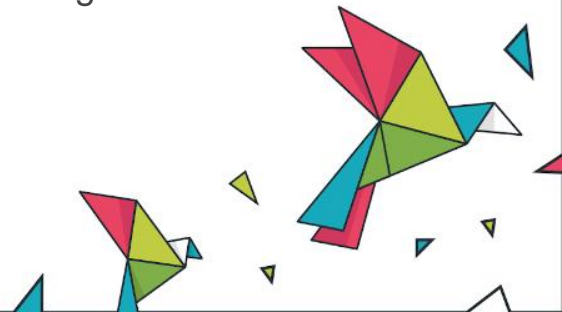


Abraham Camba, who graduated Cum Laude with a degree in Applied Physics from the University of the Philippines Diliman, is working with Trend Micro's Managed XDR team as an Incident Response Analyst. Joining Trend Micro in 2011, he has honed his skills in research, automation, programming, reverse engineering, and system development.

Fileless Control: Removing the Backdoor in Backdoor Shell

APT groups usually rely on backdoor shells to gain a foothold on the target environment. These tools open the victim machine to commands the attacker wants to perform from the outside of the system. Like any other piece of malware, having this tool run on a machine adds footprints that can be used to discover the attack.

In one case Gilbert and Abraham handled, the attacker did away with using backdoor shells and instead went full fileless. In this presentation, they will be discussing the tools the attacker used or may have used to achieve this. They will show the advantages and disadvantages the attacker has in using this approach.



Monte de Jesus

Senior Threat Researcher
Threat Hunting Team
Trend Micro

Monte de Jesus is a Senior Threat Hunting Engineer. He is also a Senior Smart Pattern Engineer that creates one-to-many detection signatures and served as a mentor to junior engineers. He has been a part of the US operation in Texas as a Volume Engineer that process bulk samples, which requires him to analyze malware and data, and develop and improve automation systems.

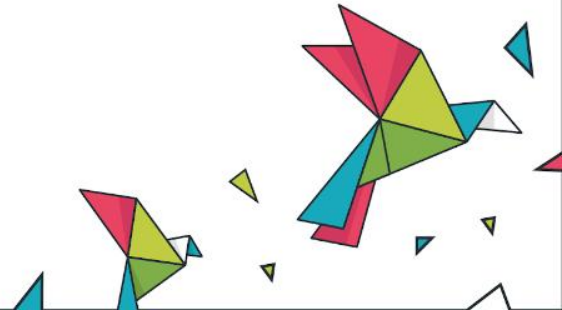


SECURING THE SECURITY LANDSCAPE

On the Radar: Exploring the Current Threat Hunting Process

Malware hunting still lacks a formal definition and base model today. Developing a hunting process and quantifying the success all depend on the hunter's goals. Another challenge posed by threat hunting is that it requires extensive resources ingesting and transforming hunting data into actionable intelligence.

In this session, Monte will be sharing Trend Micro's hunting process, particularly the process of collecting data from different channels using various method both manual or automated, and how to process, store, interpret, and define data into useful context such as defining malware landscape, campaign tracking, and network defense.



Marvin Cruz

Senior Threat Researcher
Cyber Safety Solutions
Trend Micro

Marvin Cruz is an experienced malware reverse engineer, digital forensic investigator, and security incident analyst. He is currently working at Trend Micro's biggest R&D center in Taipei, providing insight on emerging cyber threats and latest attacker's modus operandi. Despite his penchant for secrecy, several security blogs, invention, and patents are published on his credit.



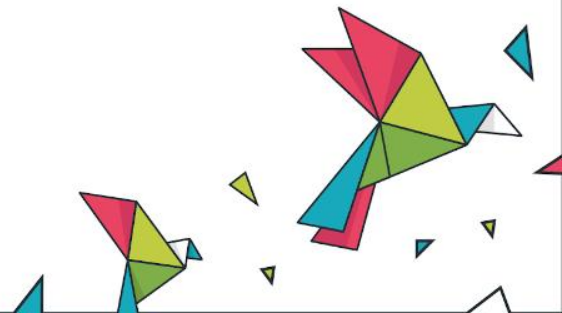
DECODE

SECURING THE SECURITY LANDSCAPE

The State of Ransomware in 2020

In this session, Marvin will be sharing an inside scoop on recent trend and changes in ransomware threat tactics, techniques, and procedures (TTP). Ransomware threat actors nowadays are no longer into the shotgun approach of mass-mailing targets with ransomware-laced emails but are more like a skilled sniper – a deliberate, patient, and resolute attacker with a clear focus on its target industry or company. Today, threat actors use phishing, info-stealers, exploits or outright purchase credentials in underground market to gain preliminary access to its victims.

Marvin will also be discussing what action defenders need to do and think about to address this change in ransomware TTPs.



Muqeeet Ali

Senior Security Researcher

DV Labs

Trend Micro`

Muqeeet Ali is working as a Senior Security Researcher at Trend Micro since September 2017. Previously, he obtained Masters and PhD degrees in Computer Science from University of Texas at Austin in 2013 and 2017 respectively. He has broad research interests in the areas of networking, security and machine learning. Recently, he has been interested in scaling machine learning techniques to make sense of security threats present in the wild.



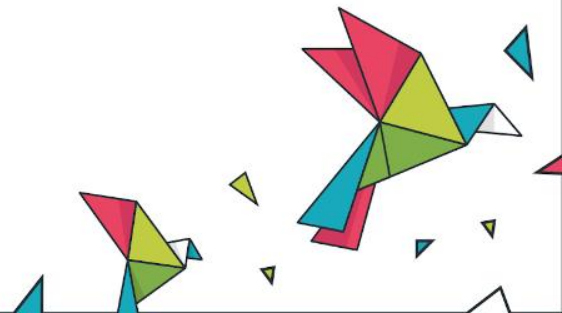
DEC{CODE

SECURING THE SECURITY LANDSCAPE

Scalable Malware Clustering

Similarity hashing is an important tool for searching and analyzing malware samples which are similar to known malware samples. TLSH has been found to be particularly well-suited for finding related malware (and goodware) samples from known malware (and goodware) samples. In particular, TLSH has been shown to be good at finding the different variants of a given malware.

Previous works at Trend Micro have shown that TLSH hashes can be used to build fast search and clustering techniques, which can scale to tens of millions of items. In this presentation, Muqeeet will be presenting techniques that can scale to even larger data sizes by doing clustering in stages.



Lord Remorin

Senior Threat Researcher
Forward-Looking Threat Research
Trend Micro

Lord Remorin is a Senior Threat Researcher within the Trend Micro Forward-Looking Threat Research (FTR) team. He began his career with TrendLabs Philippines in 2009 where he acquired his experience on malware analysis, forensic investigation and development of malware reversing and automation tools. Currently, he is based in the US, focusing on cybercrime investigations and honeypot technology.



DECODE

SECURING THE SECURITY LANDSCAPE

Building and Running a Realistic Factory Honeypot

Designing realistic ICS honeypot requires a substantial time and resource investment, and in-depth knowledge not only of the technical aspects, but of industrial automation process. Over the past couple months of planning, Lord and his teammates designed and built a factory honeypot, one that appeared so real that it was mistakenly identified as real production environment.

Lord will be sharing their experience on how much effort they went through to make a realistic honeypot. Then, he will highlight incidents they came across with while running the honeypot since May 2019. Lastly, he will be discussing recommendations and lessons they learned and answer the question: Did they do enough to attract cybercriminals who thought they were targeting a real factory?



Lala Manly

Senior Threat Researcher
Threat Hunting Team
Trend Micro

Lala Manly Reyes is a graduate of BS Mathematics major in Computer Science from Pamantasan ng Lungsod ng Maynila. She has been working in Trend Micro since 2006, and currently holds the position of Senior Researcher in the Threat Hunting Team. She has extensive experience in research and content analysis for email security, and has worked on various antispam projects, including machine learning (SVM) solution for spam mail.



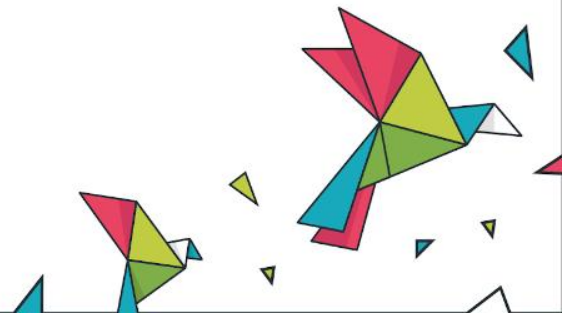
DEC`0`DE

SECURING THE SECURITY LANDSCAPE

Understanding and Curbing Online Phishing Attacks

Phishing has been a long-time cyberthreat and perhaps the simplest technique used for identity theft. On a daily basis, cybercriminals deploy thousands of phishing pages and register several malicious domains to host phishing sites. The Covid-19 pandemic crisis did not halt the perpetrators to defraud online users. In fact, it has vastly improved their techniques on social engineering schemes.

In this session, Lala will be presenting an overview of phishing attacks and how they work. She will examine some of the latest techniques adopted by cybercriminals. Lastly, she will be providing some phishing attack countermeasures to ensure that users will know how to recognize and avoid such cyberthreat.



Matsukawa Bakuei

Senior Security Specialist
Forward Looking Threat Research
Trend Micro

Matsukawa Bakuei, who has been with Trend Micro since 1997, joined the Forward-Looking Threat Research (FTR) team in 2012. Under INTERPOL and Trend Micro's strategic partnership, he also worked for the former where he was involved in the SIMDA botnet takedown, BEC investigations, West African Underground research, and more. Cybercrime and Industry 4.0/Manufacturing are his current research specializations.



SECURING THE SECURITY LANDSCAPE

Threats to Critical ICS/SCADA Endpoints

At last year's Decode, Matsukawa's colleague Ryan Flores had a presentation about Industry 4.0 and the cyberthreats affecting relevant industries. While it is interesting to find out that old Conficker worms are prevalent in industrial environments, they wanted to dig deeper and find out what cyberthreats are really affecting the critical endpoints tasked at controlling various industrial equipment – the ICS/SCADA computer.

This presentation will be showing how they built their catalogue of industrial software and fingerprint endpoints for the presence of ICS/SCADA processes, and, with this information at hand, how they monitor these critical endpoints for cyberattacks.

JV Roig

Senior Cloud Architect
Cascadeo Corporation

JV Roig works as a Senior Cloud Architect for Cascadeo Corporation, a Seattle-based premiere cloud consulting company recently acquired by Globe Telecom. Aside from routinely having to deal with security as one of the pillars of any well-architected solution for clients, JV also engages in security research in his off-time, thinking about what-ifs or revisiting things often overlooked or misunderstood.



DECODE

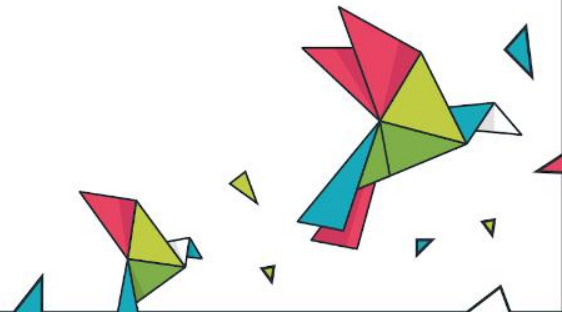
SECURING THE SECURITY LANDSCAPE

Honeypots, Honeyports, and 'Trollports': An Ecosystem-Wide Solution to the 'Firewall Spotlight Problem'

Firewalls are our friends. Unfortunately, firewalls have this weird and almost counterintuitive effect – it highlights where our crown jewels are. In a nutshell, because a typical "safe" configuration exposes only legitimate service ports, a firewall also inadvertently becomes a spotlight for attackers. JV calls this the “firewall spotlight problem.”

It's no wonder then that services like Shodan and its more criminally inclined botnet counterparts are extremely useful – the firewall spotlight problem makes it so that exposed ports are often regarded as legitimate services the vast majority of the time, making internet-wide scanning a good investment.

In this session, JV will be exploring how honeypots, honeyports, and “trollports” can rebalance this asymmetry in favor of defenders.



DEC{CODE}{2020}
ELEVATE
TRANSFORM RAPIDLY, SEAMLESSLY, SECURELY

THANK YOU!

DECODE 2020 Task Force

info@decodeph.com

