RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Project 2020: Preparing Your Organization for Future Cyber Threats Today

SESSION ID: CLE-T08

Ken Low CISSP GSLC

Director of Cybersecurity Programs, Asia Pacific
TREND MICRO

TREND MICRO™

#RSAC


2020
by
TREND
MICRO

PROJECT 2020

An initiative of the International Cyber Security Protection Alliance (ICSPA).

AIM

To anticipate the future of cybercrime, enabling governments, businesses and citizens to prepare themselves for the challenges and opportunities of the coming decade.

ACTIVITIES

Including common threat reporting, strategic foresight exercises, policy guidance and capacity building.

SCENARIOS

Not predictions of a single future. Rather, they are descriptions of a possible future which focus on the impact of cybercrime from the perspectives of an

- Ordinary Internet user,
- A manufacturer,
- A communications service provider and a government.

They take their inspiration from analysis of the current threat landscape, the expert opinion of ICSPA members and extensive horizon scanning, particularly of emerging technologies.

VIEW FROM 2014

Mobile

Cloud/ Virtualisation

Consumerisation/BYOD

Social Networking/Media

New ways to hide

SSL/TLS Attacks

Rogue Certificates

Cyber Weapons

New threat actors

Online Financial Service Attacks

Crime as a Service

Data-Stealing Trojans

High Profile Data Loss

Web Exploits

SCADA

Spam goes Legit

Social Engineering

Hacktivism

APT

Embedded Hardware

Malware outside the OS

Legislation working against security

TREND MICRO

THE SCENARIOS

These focus deliberately on the criminal and economic aspects of cyber security in 2020

Drawing out the dependencies between different technologies and different sectors of society

Identifying barriers to progress and effective security

Kinuko

23 years old

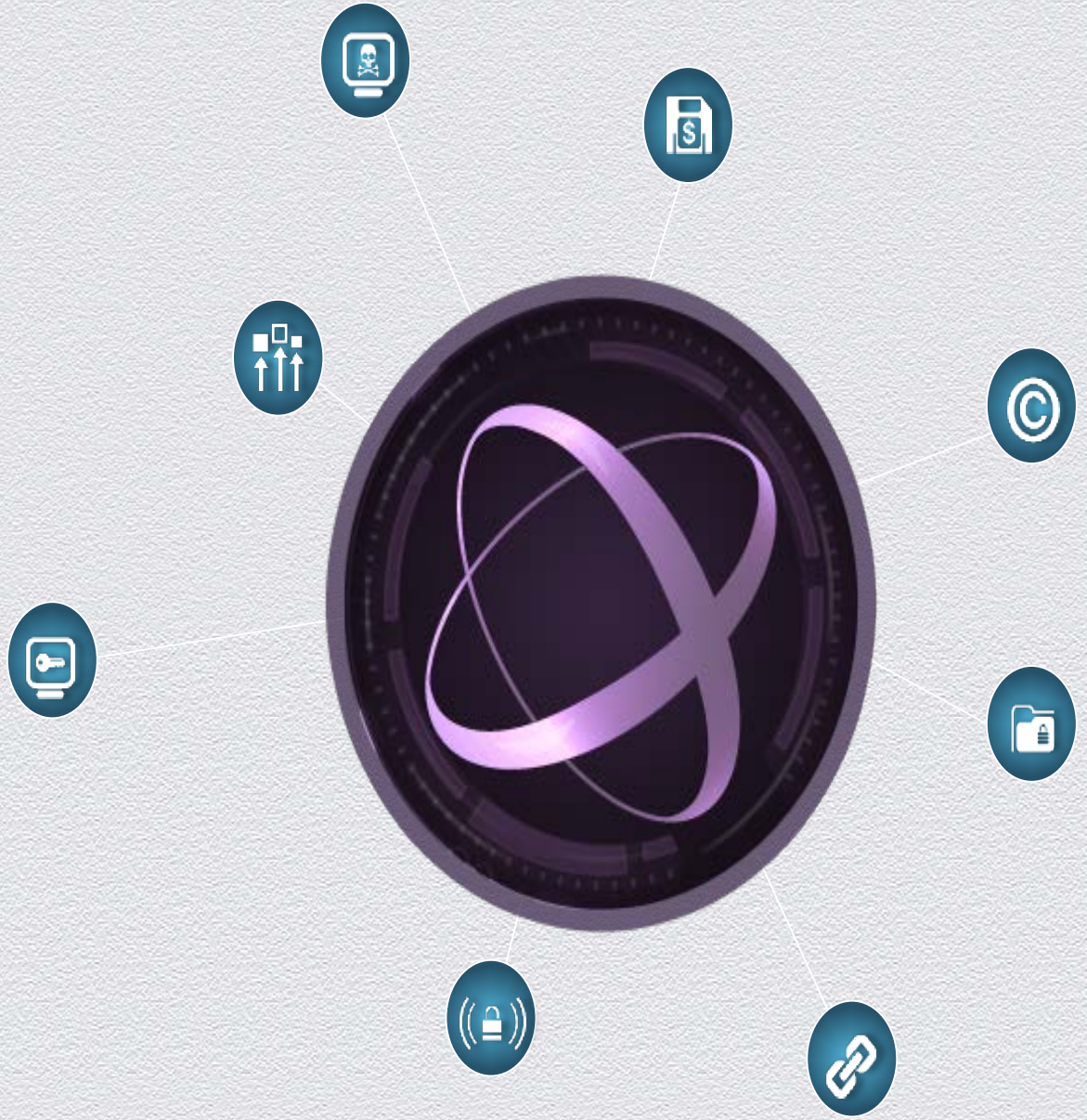
2nd generation digital native

a. Citizen – Kinuko

Key Features:

- Augmented reality and highly personalised content
- Technology assisted living for an ageing population
- Physical threats to the medically vulnerable
- Mature virtual property markets
- Personal data brokerage and identity management
- New forms and patterns of employment

Xinesys Enterprises & Lakoocha



b. Business - Xinesys Enterprises (SME) and Lakoocha (CSP)

Key Features:

- Enterprise virtualisation reaches maturity
- Supply and distribution chain automation
- New approaches to intellectual property, and Research and Technology (R&T)
- Greater storage of data = greater liability
- Communications as critical infrastructure
- Security scores as indicators of trustworthiness
- A dedicated Internet for secure payments

South Sylvania

c. Government - South Sylvania

Key Features:

- New tech powers, and R&T "leapfrogging"
- Internet diplomacy and international diplomacy one and the same
- Countries with lower levels of cybersecurity become "no go" areas, and havens for cybercriminals
- Increasing tensions between governments and multi-national corporations
- Attacks on critical information infrastructure result in physical destruction and violence (integrated transport networks and energy supply)
- Citizens demand greater government transparency - increasing focus on reputation management in government administrations

2020

IN A TRULY CONVERGED 2020, THE FOLLOWING CYBER-RELATED ACTIVITIES MAY BECOME MORE APPARENT:

- A market for scramblers of mood recognition, remote presence and near field communication technologies
- Highly distributed denial of service attacks using Cloud processing
- A move from device-based to Cloud-based botnets, hijacking distributed processing power
- A mature illicit market for virtual items, both stolen and counterfeit
- Distributed bulletproof and criminal processing
- Physical attacks against data centres and Internet exchanges
- Electronic attacks on critical infrastructure, including power supply, transport and data services
- Micro-criminality, including theft and fraudulent generation of micro payments
- Bio-hacks for multi-factor authentication components

TREND MICRO

2020

IN A TRULY CONVERGED 2020, THE FOLLOWING CYBER-RELATED ACTIVITIES MAY BECOME MORE APPARENT:

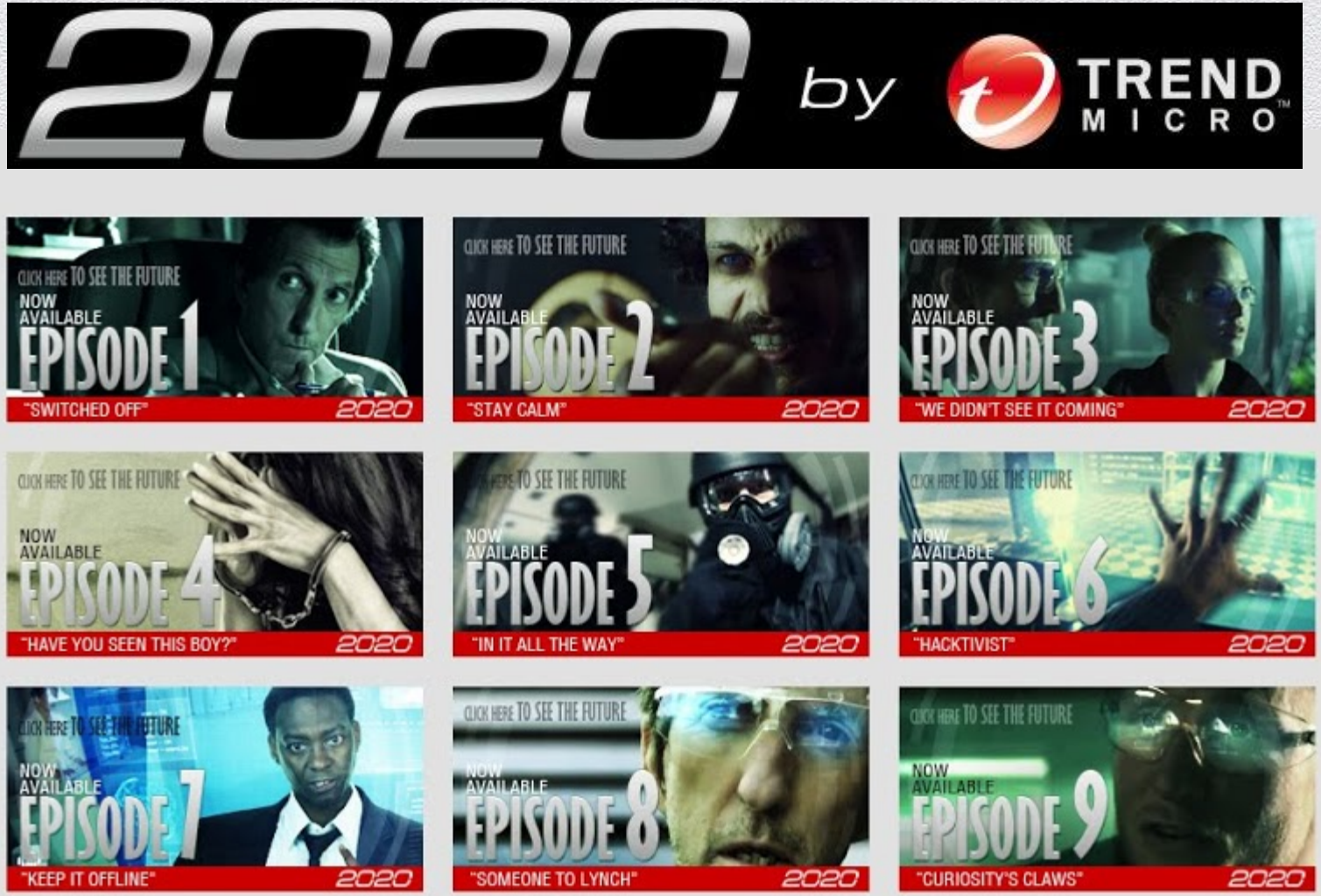
- Cyber-enabled violence against individuals, and malware for humans
- Cyber gang wars
- Advanced criminal intelligence gathering, including exploitation of big and intelligent data
- High impact, targeted identity theft and avatar hijack
- Sophisticated reputation manipulation
- Misuse of augmented reality for attacks and frauds based on social engineering
- Interference with unmanned vehicles and robotic devices
- Hacks against connected devices with direct physical impact (car-to-car communications, heads-up display and other wearable technology, etc.

Cybercriminal Threats

3. Cybercriminal Threats

At the most simplistic level, the cybercriminal threats envisaged in the narratives can be broken down into the following categories:

- Intrusion for monetary or other benefit
- Interception for espionage
- Manipulation of information or networks
- Data destruction
- Misuse of processing power
- Counterfeit items
- Evasion tools and techniques



2020.trendmicro.com

Preparing for 2020

KEY CONSIDERATIONS FOR STAKEHOLDERS:

- Who owns the data in networked systems, and for how long?
- Who will distinguish between data misuse and legitimate use, and will we achieve consistency? What data will the authorities be able to access and use for the purposes of preventing and disrupting criminal activity?
- Who covers (and recovers) the losses, both financial and in terms of data recovery?
- Who secures the joints between services, applications and networks? And how can objects which use different technologies operate safely in the same environment?
- Do we want local governance and security solutions, or global ones?
- Will we be able to transit to new forms of governance and business models without causing global shocks, schisms and significant financial damage?

Beyond 2020

- Remote presence and virtual reality technologies (early adoption by mainstream)
- Truly immersive technologies with human cognitive processes will bring new harms (especially psychological) as well as benefits
- Mainstream adoption of augmented reality, virtual reality and sensor technology
- “Singularity” of man and machine (Ray Kurzweil)
- Quantum computing?

A world safe for exchanging digital information

CEO	Eva Chen
Founded	1988, United States
Headquarters	Tokyo, Japan
Employees	5,217
Offices	36
2013 Sales	$1.1B USD

New malware every ½ second

Global Threat Intelligence
- 1,200+ experts worldwide

96% of the top 50 global corporations.

100% of the top 10 automotive companies.

100% of the top 10 telecom companies.

80% of the top 10 banks.

90% of the top 10 oil companies.

TREND MICRO™

#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Search : Keyword English

INTERPOL 100 YEARS OF INTERNATIONAL POLICE COOPERATION

WANTED PERSONS
MISSING PERSONS
INTERPOL WORLDWIDE

HOME | ABOUT INTERPOL | NEWS AND MEDIA | MEMBER COUNTRIES | INTERPOL EXPERTISE | CRIME AREAS

- Media room
- News
- Speeches
- Events
- Publications
- Videos
- Photos

All news | Share | Print

Photos : 2

24 June 2013 - Media release

INTERPOL and Trend Micro to collaborate against cybercrime

LYON, France – INTERPOL and Trend Micro Inc. have announced that the security software leader is to collaborate with the world police body to support global law enforcement programmes to combat cybercrime. The announcement is the latest in INTERPOL's efforts to boost the global fight against cybercrime by engaging with private sector leaders.

Following talks on Friday at INTERPOL's General Secretariat headquarters between INTERPOL Secretary General Ronald K. Noble and Trend Micro's Chief Executive Officer, Eva Chen, Trend Micro is set to deliver training programmes to INTERPOL, government and police agencies in various participating countries to address emerging digital crime at the national and international level.

Including expertise and best practices, training will encompass e-learning modules, classroom-based training sessions, workshops and professional certifications.

"We are honoured to have earned the trust of INTERPOL to provide our expertise to keep digital information safe while exposing illegal activities," said Eva Chen, CEO, Trend Micro. "Our team is on the frontlines of the quickly-evolving threat landscape and we look forward to sharing our analysis and insight to support global law enforcement. Alignment between public and private organizations will play a critical role against cybercrime and it will take collaboration such as this to be successful."

Trend Micro will also help support the development of an INTERPOL cyber alert by providing expert cyber-threat analysis at INTERPOL's Global Complex for Innovation (IGCI) when it opens in Singapore in 2014. This cyber-specific alert created by the IGCI will be used to share information on cybercrime with not only the law enforcement community but also the general public.

"Due to the complexity of the cyber-threat landscape, investigation of cybercrimes is profoundly different in nature to traditional crime, requiring high-level technical expertise and large-scale cross-jurisdictional investigations," said INTERPOL Secretary General Ronald K. Noble.

"It is essential that law enforcement collaborate across sectors with Internet security experts such as Trend Micro so as to develop the technical expertise, tools and infrastructure necessary to effectively

SEE ALSO

- Cybercrime
- The INTERPOL Global Complex for Innovation

TREND MICRO


2020 by TREND MICRO
VISIT 2020.TRENDMICRO.COM AND WATCH THE SERIES

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Project 2020: Preparing Your Organization for Future Cyber Threats Today

SESSION ID: CLE-T08

Ken Low CISSP GSLC

Director of Cybersecurity Programs, Asia Pacific
TREND MICRO

#RSAC