Badan Siber dan Sandi Negara

Peningkatan Kemampuan Pendeteksian Dini dan Koordinasi dalam Rangka Cyber Situational Awareness

Sulistyo

Direktur Deteksi Ancaman, BSSN

INDONESIA 4.0

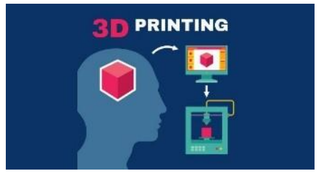
Sharing economy

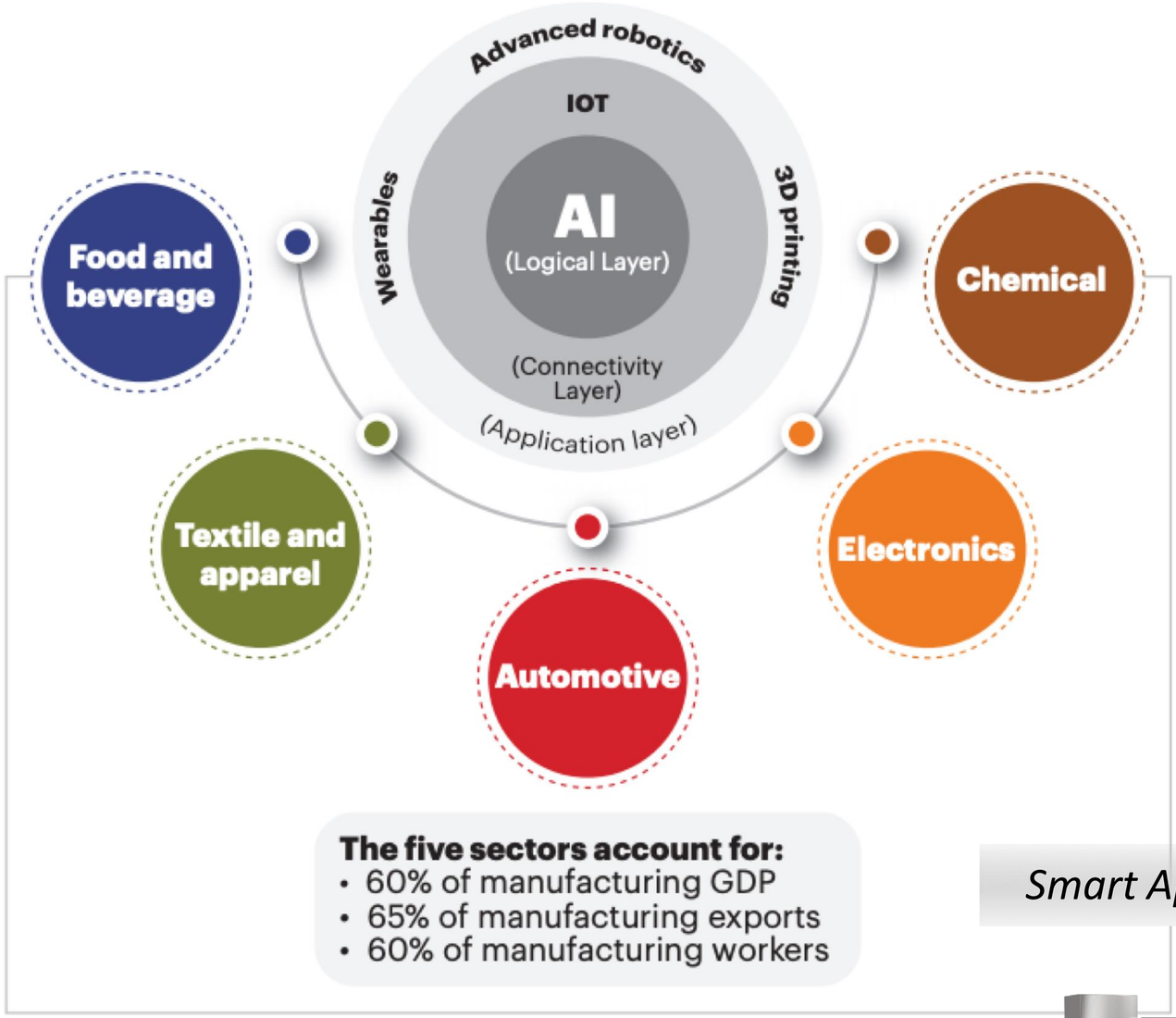
airbnb · swap · Zopa · Bcycle · CouchSurfing · BookMooch · Zilok.com · NETFLIX · carpooling.com · zipcar

Cloud Collaborative

Google Drive · Dropbox · Microsoft Office 365

Smart Manufacturing





The five sectors account for:
- 60% of manufacturing GDP
- 65% of manufacturing exports
- 60% of manufacturing workers

e-Government

Marketplace

Bukalapak.com · tokopedia

Smart City

Smart Appliances

BADAN SIBER DAN SANDI NEGARA

HOW SURVEILLANCE CAPITALISM WORK?

Extractive Process

scanning of email

capture of voice communication

bypass privacy setting

through online services

extensive search big data

tracking mobile location

wearable tech & recognition

Data Sources

Data Flow from Corporate and Government Databases

Facebook “likes”, Google Search, email, dan location, social network, ecommerce, phonecall, and more

Everything resources from smartphones, satellites, google earth

Information Analysis

Facebook and Other Social Media can Accurately Predict

Sexual Orientation

Ethnicity and culture

Political and Religion Views

Whetever you use (drugs, money, etc)

Sentiment & Expression

Surveillance Capitalism Theory

- Prediction
- Surveillance Privacy
- Financial Oriented

“Commodification of Personal Information from Data Collection and Data Processing to have various advantages”

- shoshana Zuboff -

SAMPLE SURVEILLANCE CAPITALISM

Technology Company

amazon

BL BukalapakFacebook

Google Duolingo

ebay

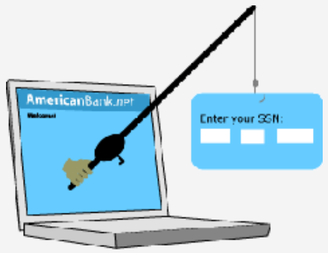
Surveillance Capitalism Approach

Target Market

HOW STATE/NON STATE GET INFORMATION

Phising dan zero day Attack

A handful of users are targeted by phising attack, include mail phising, web phising, etc



Backdoor

The user machine is accessed remotely using **malware** and **backdoor**

Lateral Movement

=

Attacker elevates access to important user, service and admin accounts, and specific system

Data Gathering

All data is acquired from target servers and storage to get sensitive information

Exfiltrate

Data is exfiltrated via encrypted files over ftp to external and compromised machine

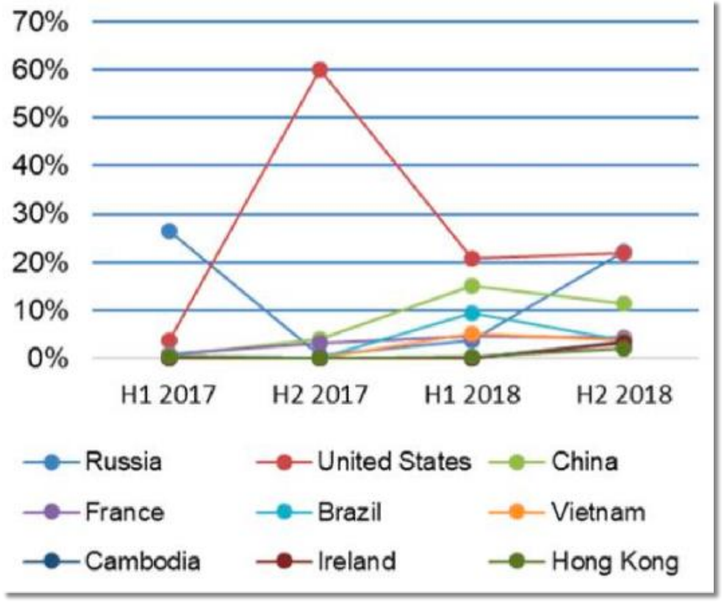
MALWARE and APT GROUP ATTENTION

Malware Type	Percentage (%)			
	H1 2017	H2 2017	H1 2018	H2 2018
Trojan	60.17%	55.73%	73.56%	98.89%
Downloaders	2.95%	2.91%	1.90%	0.59%
Backdoor	9.74%	18.92%	1.78%	0.43%
Worm	27.11%	19.55%	0.01%	0.05%
Ransomware	0.03%	2.89%	22.76%	0.04%

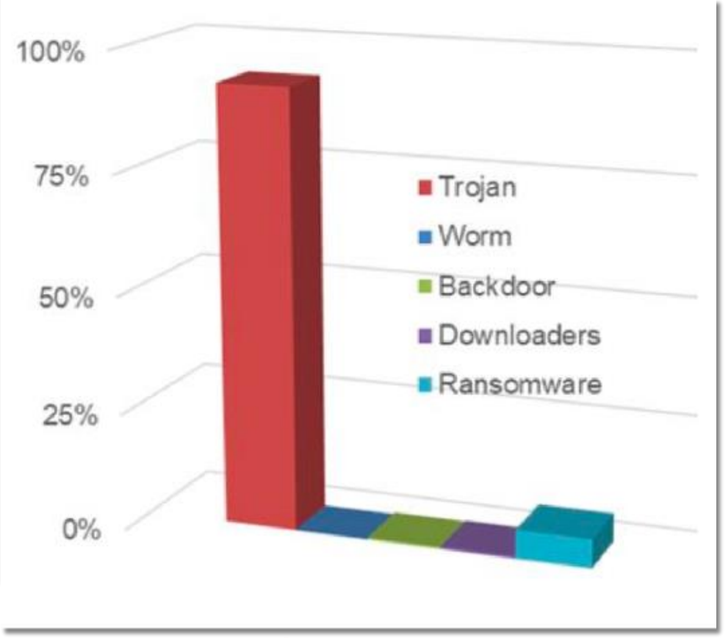
Malware reports comparison

	Malware detected in the region		Most Common Malware
	H1 2018	H2 2018	
Windows	**Total 57.58%** -Trojan 69.9% -Backdoor 2.3% -Downloader 27.8% -Others 0.0%	**Total 63.93%** -Trojan 75.6% -Backdoor 19.0% -Downloader 0.0% -Others 5.4%	Backdoor.Androm
GNU/Linux	**Total 34.82%** Trojan 25.4% Downloader 0.5% Others 74.2%	**Total 23.41%** Trojan 90.6% Downloader 0.4% Others 14.5%	Backdoor.JBOSS.SHELL

PC Malware



CNC callback source



Malware type H2 2018

Korea Utara

Rusia

China

US

lazarus
carbanak
cleavar
cobalt
caracal

gorgon
honeybee
naikon
poseidon
fin

APT Group

Sumber : OIC CERT Malware Trend Reports 2018

Threats Detection Strategy

Honeynet

Social Network Analysis

Cyber Threat Intelligence Sharing

Pemerintah

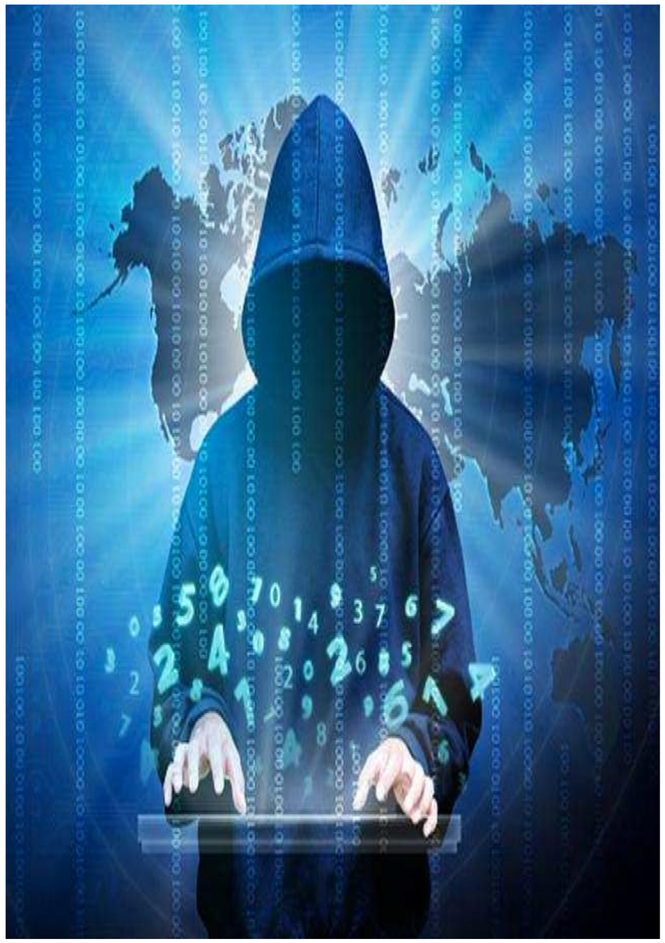
IIKN

Ekonomi Digital

Malware Threats

Social Culture Threats

Advanced Persistent Threat



PROGRESS HONEYNET BSSN

25 Pemerintah

6 Informasi Infrastruktur Kritikal Nasional

12 Universitas

18 Provinsi

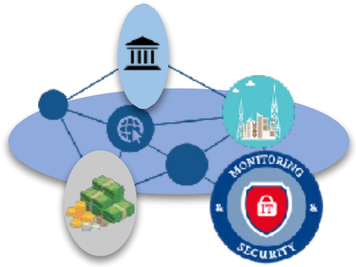
2018-2019

43 Jumlah Perangkat Honeypot

KEMANFAATAN HONEYNET

Profiling/Behavior Serangan Siber milik Stakeholders sebagai sistem deteksi dini

Platform Malware dan Threat Information Sharing yang dapat dimanfaatkan stakeholders



HONEYNET BSSN-IHP

Memperkuat Fungsi Security Perimeter Devices

Peningkatan People Capability dalam riset dan pengembangan dengan bekerjasama dengan Institusi Pendidikan

Berbasis Komunitas (Honeynet Global) dalam rangka mendukung World Class Cyber

THANK YOU !

mail : sulistyo@bssn.go.id