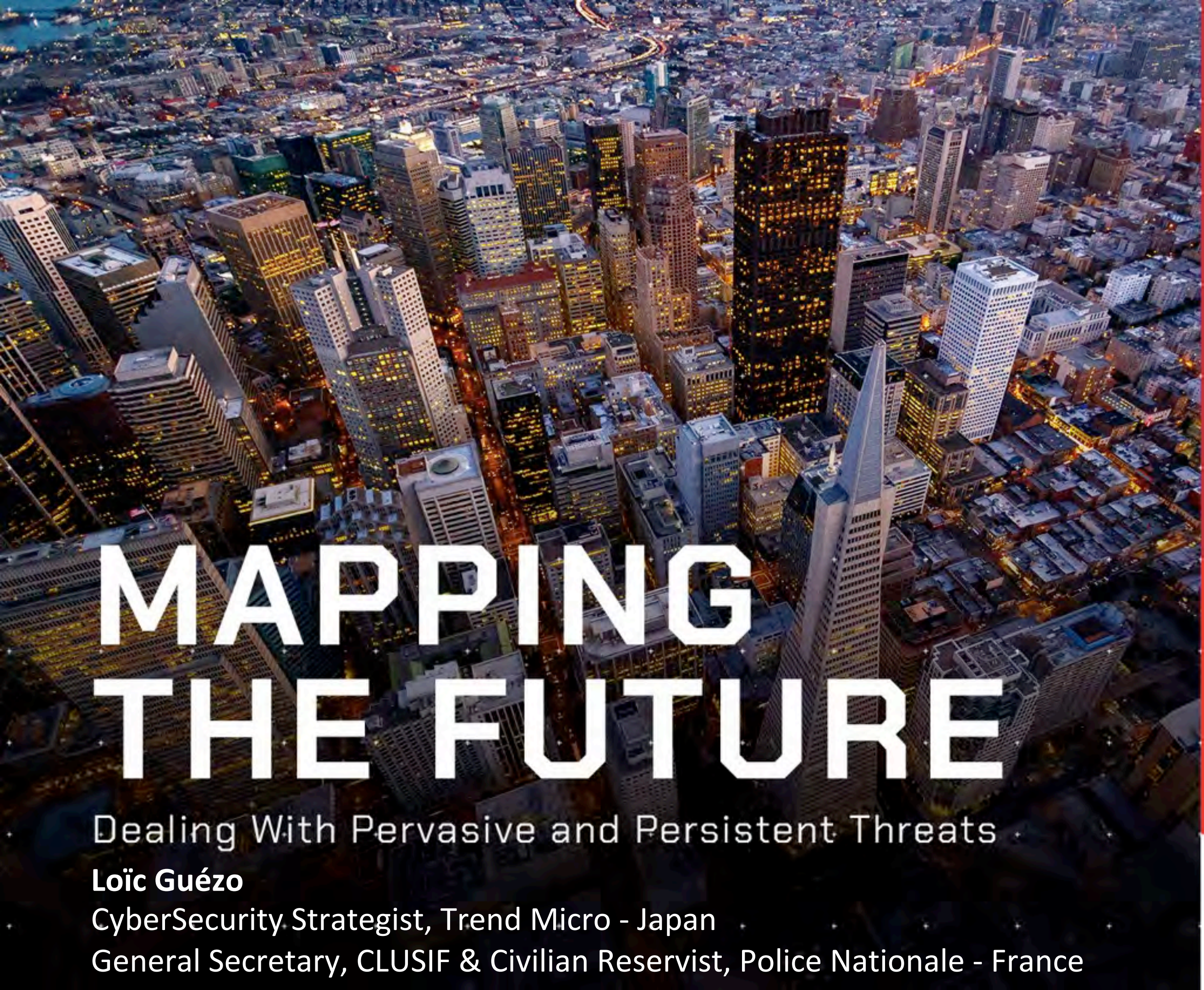


MAPPING THE FUTURE

Dealing With Pervasive and Persistent Threats

Loïc Guézo
CyberSecurity Strategist, Trend Micro - Japan
General Secretary, CLUSIF & Civilian Reservist, Police Nationale - France

Based on
TREND MICRO SECURITY PREDICTIONS FOR 2019

TREND MICRO | research

Technology Trends, 2019 and Beyond

- Cloud computing adoption
- ML and AI using bigger data
- 5G rollout in 2020
- Smart devices, homes, factories (IoT and IIoT)

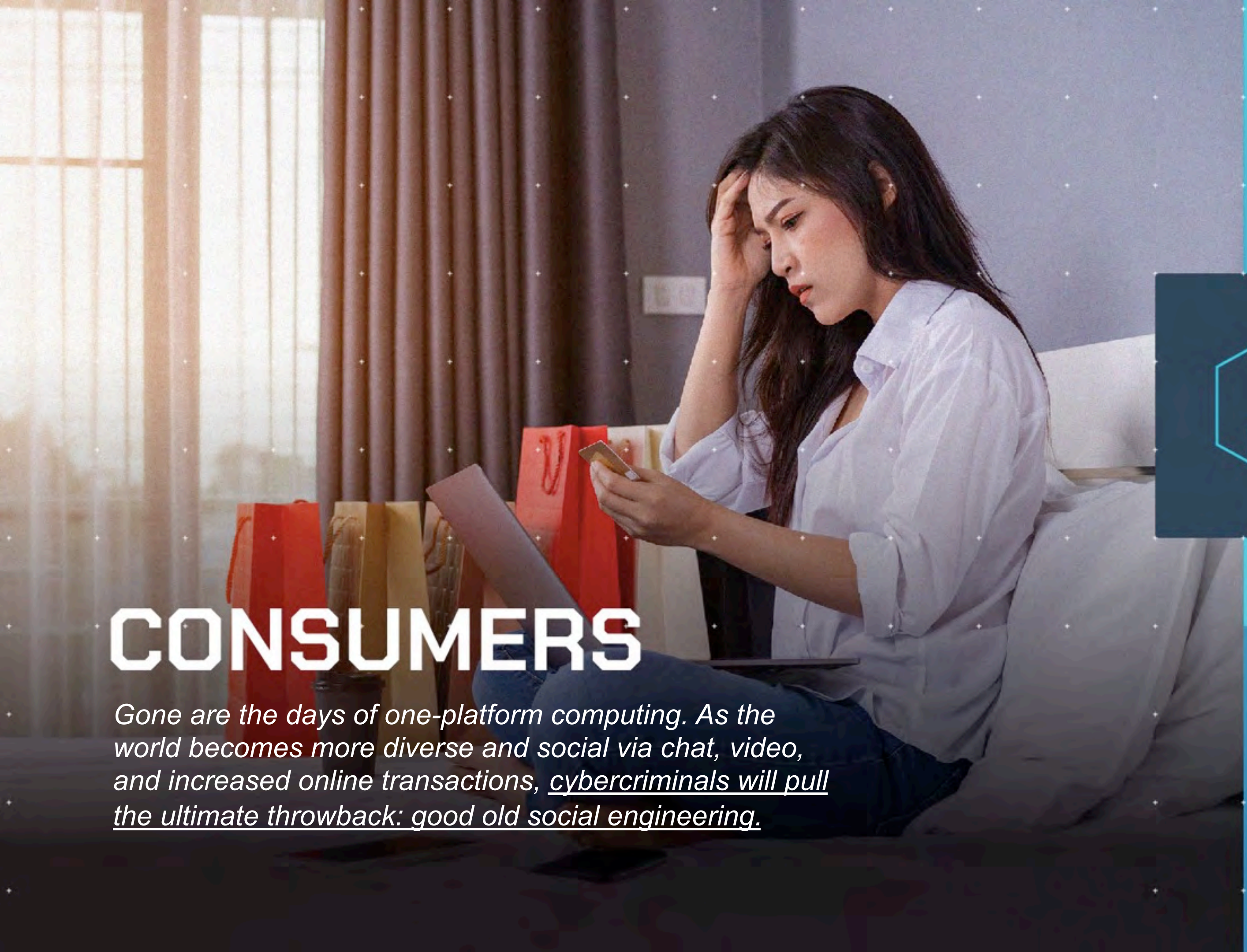
Data, knowledge, and functionality will move at a much faster pace and will permeate different aspects of professional and personal lives.

User Behavior and Sociopolitical Landscape, 2019 and Beyond

- Chat and video for online communications
- Rise of WFH, i.e., work from smart homes
- Fracture in sentiments more pronounced because of social media
- Important elections in different countries like EU upcoming

Security for these different segments will be affected by these developments differently.

CONTENTS

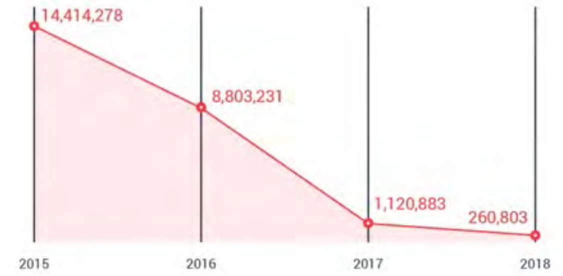


CONSUMERS

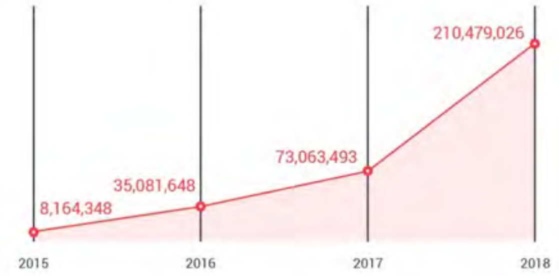
Gone are the days of one-platform computing. As the world becomes more diverse and social via chat, video, and increased online transactions, cybercriminals will pull the ultimate throwback: good old social engineering.

►Social Engineering via Phishing Will Replace Exploit Kits as Attack Vector

- As the state of "monoculture" declines, exploit kit attacks will decline, and cybercriminals will use social engineering even more
- There will be more cases of phishing not only in email but also in SMS and chat; SIM-jacking
- Sporting events, upcoming elections, and sociopolitical developments will be used as premise for social engineering attacks



Exploit kit activity



Phishing-related URLs blocked

►Chatbots Will Be Abused

- Similar to old telephone attacks that used prerecorded messages, IVR
- Impact: manipulation of orders, installation of RAT, extortion

►E-Celeb Accounts Will Be Abused in Watering Hole Attacks

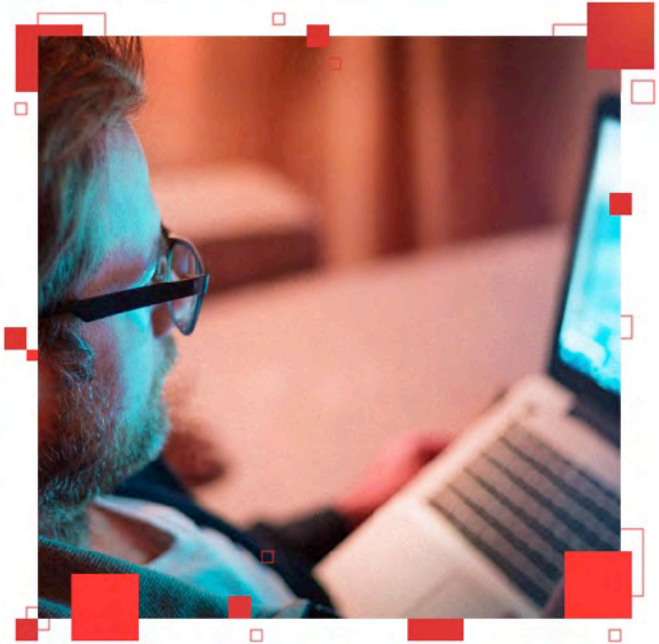
- Famous YouTubers and other "online-famous" personalities' social media accounts have millions of followers, making them attractive launchpads for attacks
- Impact: followers infected with various malware or hijacked for DDoS, cryptojacking, troll accounts

►Actual Mass Real-World Use of Breached Credentials Will Be Seen

- Credential stuffing has become more rampant
- Users recycle passwords across various sites
- Applications: for rewards, mileage, benefits, troll accounts

►Sextortion Cases Will Rise

- Highly personal nature of attack will force young adults and teenagers to comply with extortionists’ demands
- These attacks will claim more lives



ENTERPRISES

Risks related to the WFH trend, GDPR compliance difficulties, social engineering, BEC, automation, and extortion will become causes for concern.

►Home Networks in Work-From-Home Scenarios Will Open Enterprises to BYOD-like Security Risks

- Intersection of rise of remote-working/WFH arrangements and presence of more smart devices in the home
- Printers, network storage devices, etc. in the home double as employee devices
- Every unsecure home device is an entry point into the *enterprise* network

►GDPR Regulators Will Penalize the First High-Profile Violator the Full 4%

- Regulators will make an example out of a large, noncompliant company, fining it the full 4% of its global annual turnover
- Some agencies are already *inundated* with new disclosures

►Real-World Events Will Be Used in Social Engineering Attacks

- Tokyo Olympics 2020, Brexit, Italian budget issues, and other sociopolitical developments will be used as social engineering lures
- “Notre Dame de Paris”, as explained by M.BONNEL during opening session

Photo by Gentrit Sylejmani on Unsplash

►Business Email Compromise Will Go 2 Levels Down the Org Chart

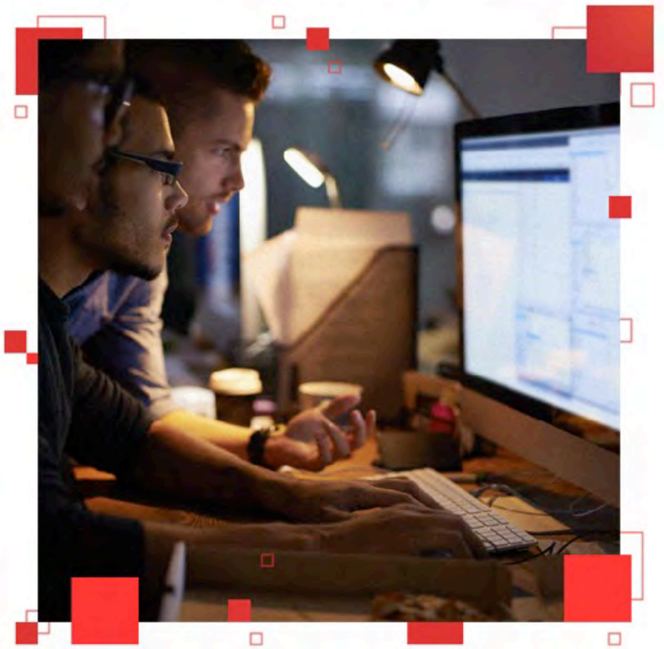
- Cybercriminals will target the CxO’s secretary or executive assistant, or a high-ranking director or manager in the finance department, etc.

►Automation Will Be a New Wrinkle in Business Process Compromise

- More aspects of monitoring and function are conducted through software or online applications
- Will also be used in supply chain attacks

►Digital Extortion’s Wide Field of Application Will Be Explored

- Online smear campaigns
- GDPR penalty will “guide” amount of ransomware demand



GOVERNMENTS

Upcoming major elections across the globe will test the mettle of social media improvements in combating fake news, innocent victims will become collateral damage in scenarios reminiscent of WannaCry and NotPetya, and governments will try to get ahead of IoT and IIoT risks.

►The Fight Against Fake News Will Buckle Under the Pressure of Various Elections

- Improvements social media has made to fight fake news post-2016 will not be enough to keep up with the deluge of cyberpropaganda around major elections in 2019

►Innocent Victims Will Get Caught in the Crossfire as Countries Grow Their Cyber Presence

- Nations firming up their cyber capabilities will seek to support domestic hackers
- Spillover effects on innocent victims completely unrelated to these cyber responses like what happened with WannaCry and NotPetya

►Regulatory Oversight Will Intensify

- Precedent: California’s bill requiring manufacturers to enforce the use of strong passwords on their smart devices
- Local governments will prohibit the use of unsecure consumer and industrial IoT devices (eg. Japan Act to “check” IoTs)

SECURITY INDUSTRY

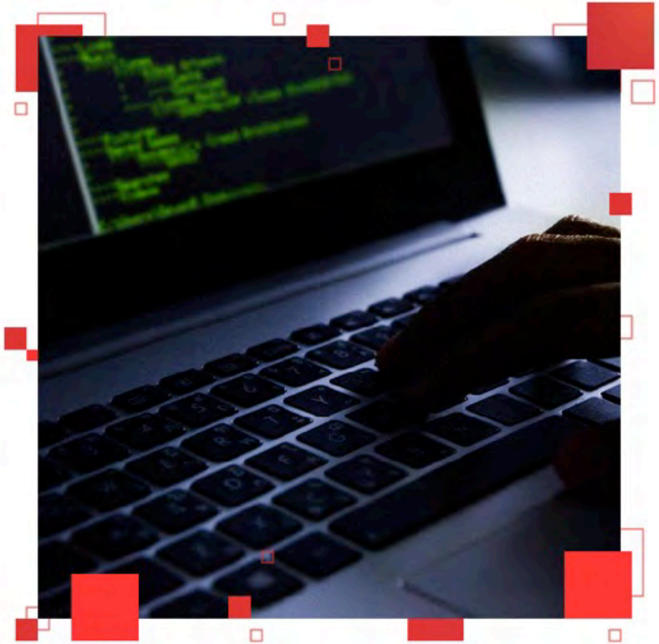
InfoSec and IT teams will see more cases of threat actors using "normal" objects to blend in the network, successful n-day exploit attacks, and more reasons to invest in AI for cybersecurity.

►Cybercriminals Will Use More Techniques to Blend In

- New ways of using normal computing objects for purposes other than their intended uses or designs — a practice known as “living off the land” — will continue to be discovered, documented, and shared:
    - Unconventional file extensions
    - Less reliance on actual executables, as in the use of “fileless” components, Powershell, scripts, and macros
    - Digitally signed malware
    - New activation methods
    - Abuse of email accounts or online storage services and apps
    - Minimally modifying or infecting legitimate system files

►99.99% of Exploit-Based Attacks Will Still Not Be Based on 0-Day Vulnerabilities

- Successful exploit-based attacks will involve vulnerabilities for which patches have been available for weeks or even months but have not been applied yet



►Highly Targeted Attacks Will Begin Using AI-Powered Techniques

- AI to predict the movements of executives or other persons of interest (hotels, routes, flights, other preferences, etc.)

INDUSTRIAL CONTROL SYSTEMS

Attacks against critical infrastructure and more HMI vulnerabilities will become a problem for owners of ICSs.

►Real-World Attacks Targeting ICSs Will Become a Rising Concern_

- Countries learning and exercising their cyber capabilities will conduct attacks against smaller players' critical infrastructure
- Impact: operational shutdowns, damaged equipment, indirect financial losses, and at worst, health and safety risks

►HMI Bugs Will Continue to Be the Primary Source of ICS Vulnerabilities

- These kinds of software are more readily available to vulnerability researchers
- HMI software is not as robustly secure as more established vendors
- The incorrect assumption that this kind of software will run only in isolated or on air-gapped environments

CLOUD INFRASTRUCTURE

Hybrid cloud users will face more security challenges like misconfigurations during migration, cloud cryptojacking, and cloud deployment software vulnerabilities.

►Misconfigured Security Settings During Cloud Migration Will Result in More Data Breaches

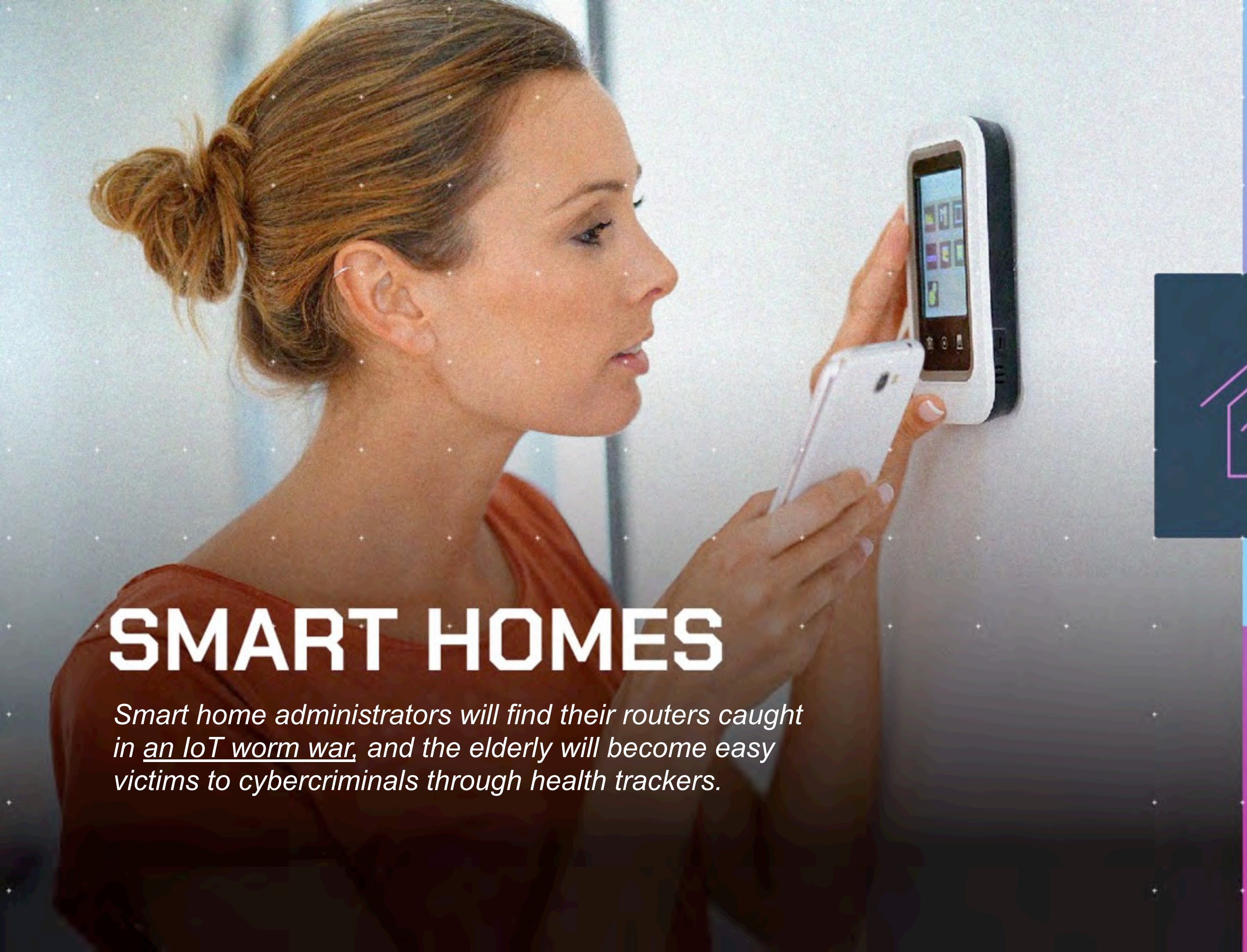
- More major data breach cases will come as a direct result of misconfigurations during migration
- Refining settings to be secure is often difficult especially for a large number of buckets and moving parts
- Each cloud migration is unique in terms of scope and pace

►Cloud Instances Will Be Used for Cryptocurrency Mining

- Mining via the cloud is easy to start and maintain
- More cybercriminals will hijack cloud accounts to mine cryptocurrency or maintain control over alternative ones
- Cloud bucket scanner tools are available
- Cryptojacking malware will throttle usage to minimize detection

►More Cloud-Related Software Vulnerabilities Will Be Discovered

- Cloud infrastructure vulnerability research will begin to gain ground
- Kubernetes vulnerabilities found in the past, a critical one found recently
- More than a dozen malicious Docker images found downloaded at least 5 million times



SMART HOMES

Smart home administrators will find their routers caught in an IoT worm war, and the elderly will become easy victims to cybercriminals through health trackers.

►The First Case of Senior Citizens Falling Easy Victims to Smart Health Device Attacks Will Emerge

- Companies are exploring the senior citizen customer base as potential users of smart trackers or other internet-connected health devices
- Senior citizens have been targets of phone scams because of their relative wealth, given their retirement savings
- Elderly users of health trackers will not be computer-savvy enough to check the privacy settings of these devices or to keep their accounts secure

►Cybercriminals Will Compete for Dominance in an Emerging IoT ‘Worm War’

- Recent router-based/IoT attacks are mostly based on the same leaked source code from Mirai
- They use the same handful of exploits and mostly bad login credentials, which means they are auto-scanning and discovering the same devices
- Since one malware needs to be in control of a single device, cybercriminals will add code to lock out “competitors”

►They Welcome the 5G Era !

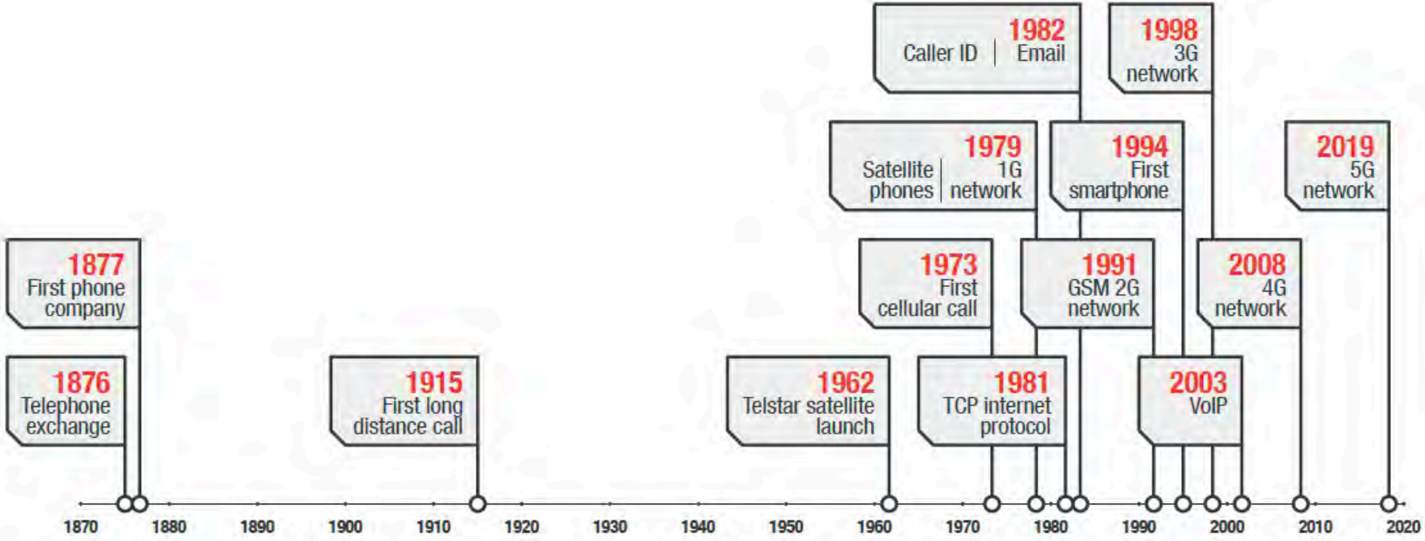


Figure 1. Timeline of telecom evolution to 5G[4,5]

►TELCO : from humans, circuits, packets to SMDN

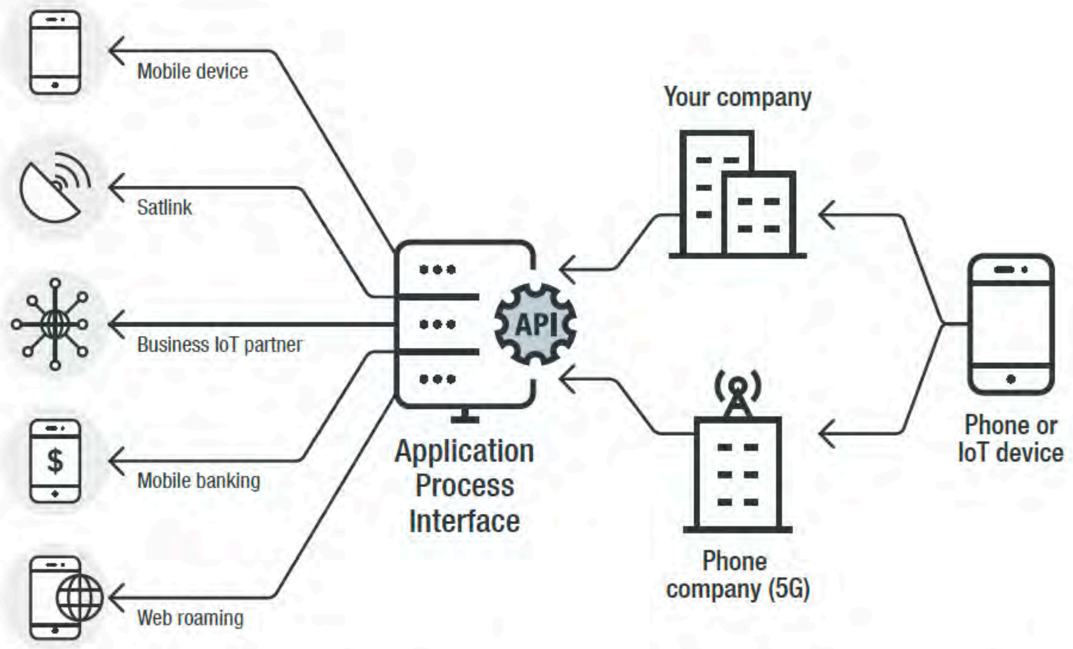
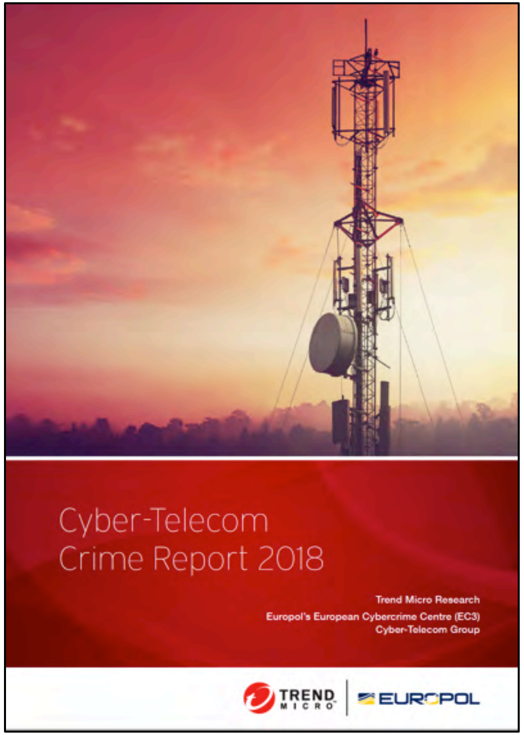


Figure 5. Software-defined networks are implemented across hundreds of identical low-cost computers, using software-based routing and nested tiers of automation to carry voice calls, data, and management traffic

►5G Era … and Cyber Telecom (CyTel) crime ?



Cyber-Telecom
Crime Report 2018

Trend Micro Research
Europol's European Cybercrime Centre (EC3)
Cyber-Telecom Group

TREND MICRO | EUROPOL

- Telecom has been part of the evolution of modern society. It is seminal in the operations and has become a major industry itself.
- The reality of its own threats and vulnerabilities exists : given how critical telecom is, its threat landscape should be explored and understood as telecom technology continues to thrive.

- We collaborate here with Europol's European Cybercrime Centre (EC3) Cyber-Telecom Group.

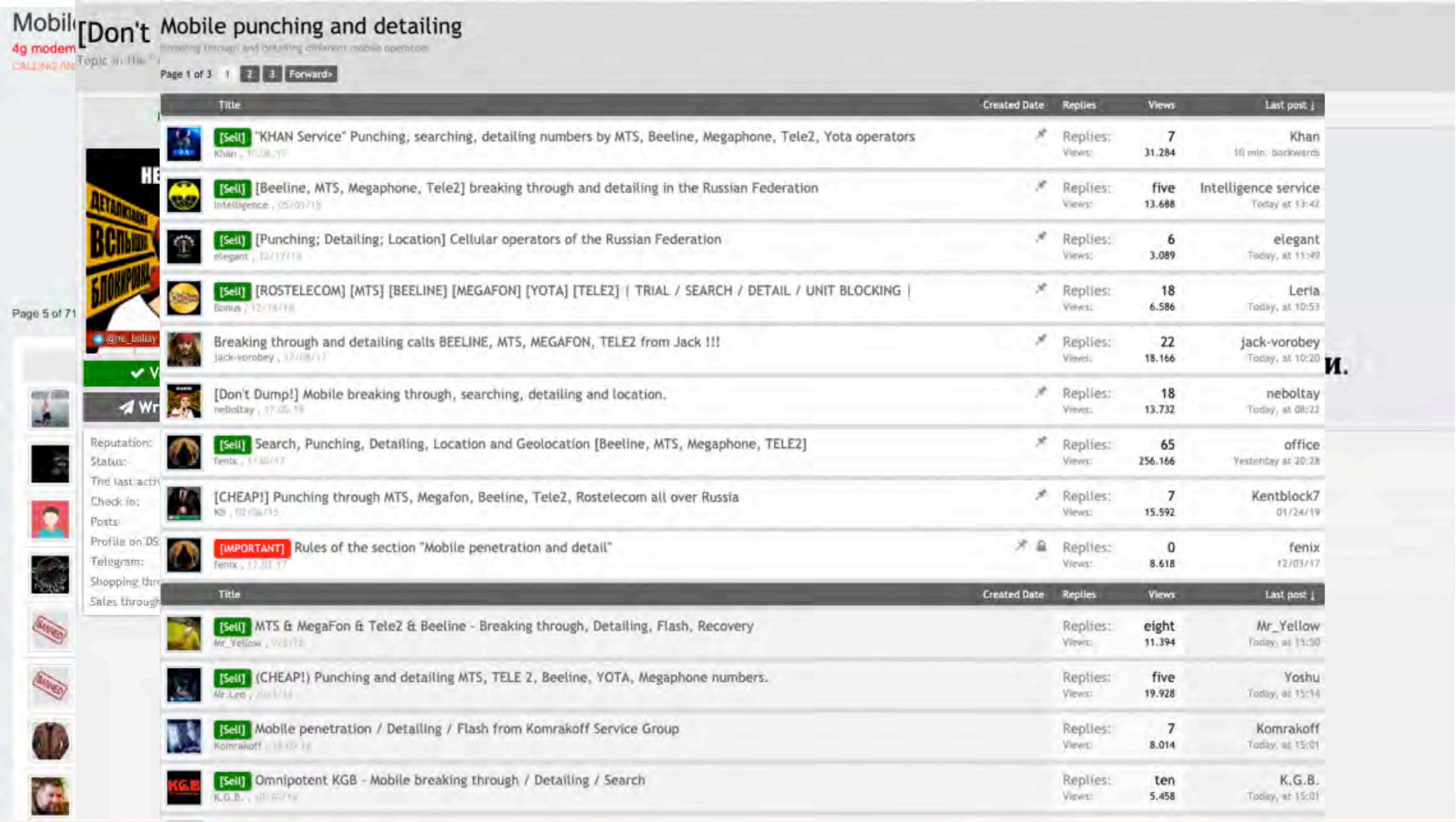
https://documents.trendmicro.com/assets/white_papers/wp-cyber-telecom-crime-report-2019.pdf

►Model in Projects

- CISOs strategize/budget 10 years ahead
- 90% of Telecom spend is CTO, 10% CIO
- Large telco project is $1 billion USD
- Large projects every 2 years

- Very little Telco-side SEC overview
- Security orchestration in SDMN (Software Defined Mobile Network) ?

►Some IRL “underground battles” examples …



Mobil

4g modem

[Don't

Topic in the "

Page 5 of 71

Reputation:
Status:
The last acti
Check in:
Posts:
Profile on DS
Telegram:
Shopping thr
Sales through

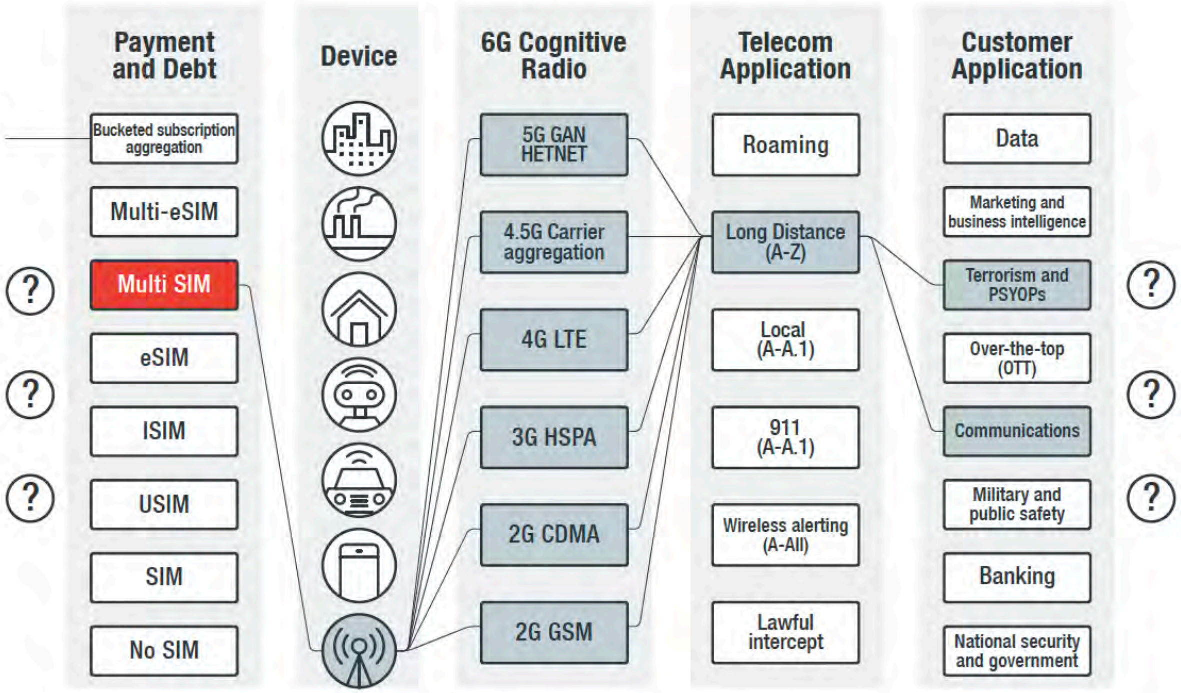
Mobile punching and detailing

Breaking through and detailing different mobile operators

Page 1 of 3 1 2 3 Forward>

Title	Created Date	Replies	Views	Last post ↓
[Sell] "KHAN Service" Punching, searching, detailing numbers by MTS, Beeline, Megaphone, Tele2, Yota operators Khan , 10.08.17		Replies: Views:	7 31.284	Khan 10 min. backwards
[Sell] [Beeline, MTS, Megaphone, Tele2] breaking through and detailing in the Russian Federation Intelligence , 05/01/15		Replies: Views:	five 13.688	Intelligence service Today at 13:42
[Sell] [Punching; Detailing; Location] Cellular operators of the Russian Federation elegant , 12/17/18		Replies: Views:	6 3.089	elegant Today, at 11:49
[Sell] [ROSTELECOM] [MTS] [BEELINE] [MEGAFON] [YOTA] [TELE2] | TRIAL / SEARCH / DETAIL / UNIT BLOCKING | Bonus , 12/16/18		Replies: Views:	18 6.586	Leria Today, at 10:53
Breaking through and detailing calls BEELINE, MTS, MEGAFON, TELE2 from Jack !!! jack-vorobey , 17/08/17		Replies: Views:	22 18.166	jack-vorobey Today, at 10:20
[Don't Dump!] Mobile breaking through, searching, detailing and location. neboltay , 17.05.18		Replies: Views:	18 13.732	neboltay Today, at 08:22
[Sell] Search, Punching, Detailing, Location and Geolocation [Beeline, MTS, Megaphone, TELE2] fenix , 11/30/17		Replies: Views:	65 256.166	office Yesterday at 20:28
[CHEAP!] Punching through MTS, Megafon, Beeline, Tele2, Rostelecom all over Russia Kb , 02/06/15		Replies: Views:	7 15.592	Kentblock7 01/24/19
[IMPORTANT] Rules of the section "Mobile penetration and detail" fenix , 12.03.17		Replies: Views:	0 8.618	fenix 12/03/17
Title	**Created Date**	**Replies**	**Views**	**Last post ↓**
[Sell] MTS & MegaFon & Tele2 & Beeline - Breaking through, Detailing, Flash, Recovery Mr_Yellow , [illegible]		Replies: Views:	eight 11.394	Mr_Yellow Today, at 15:50
[Sell] (CHEAP!) Punching and detailing MTS, TELE 2, Beeline, YOTA, Megaphone numbers. Mr.Leo , [illegible]		Replies: Views:	five 19.928	Yoshu Today, at 15:14
[Sell] Mobile penetration / Detailing / Flash from Komrakoff Service Group Komrakoff , [illegible]		Replies: Views:	7 8.014	Komrakoff Today, at 15:01
[Sell] Omnipotent KGB - Mobile breaking through / Detailing / Search K.G.B. , [illegible]		Replies: Views:	ten 5.458	K.G.B. Today, at 15:01

►Proposal for threat modeling



Note: The blue line shows the path that telecom attacks including fraud can take.

Figure 26. Voice phishing threat model

► CLUSIF

- In France, CLUSIF = Club de la Sécurité de l’Information Français (750 members)
- Many WGs, including a new WG « 5G Cyber Risks »

- Initially leaded by … Huawei France
- Set « on hold » for differents reasons
- Possible restart with NOKIA support

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com