Internet Organised Crime Threat Assessment (IOCTA) 2020

Nicole van der Meulen
Head of Policy & Development team
EC3

PART I

Approach

IOCTA 2020

Approach

Aim

- inform decision-makers at strategic, tactical and operational levels
- contribute to the setting of the next priorities in 2021.

Scope

- EMPACT priority-relevant cybercrime threat
- LE-relevant cybercrime cross-cutting factors and challenges

Methodology

Semi-structured interviews:

- member state representatives
- Europol partner countries
- EC3's strategic advisory group representatives.

PART II

Developments

IOCTA 2020

IOCTA 2020: Key Threats

- Social engineering, malware and ransomware remain top threats
- Cryptocurrencies continue to facilitate payments for various forms of cybercrime
- Reporting challenges hinder the ability to create an accurate overview of crime
- Criminals take advantage of the COVID-19 crisis

The 2020 cyber threat landscape

Cybercrime evolution:

- Fundamentals firmly rooted
- Cybercriminals refine their artisanship
- CaaS raises capability among threat actors

Criminals drive enterprise mindsets in their approach:

- Improving crime methodologies and odds of success
- The cyber-element infiltrates almost all areas of crime

Threat actors abused the COVID-19 pandemic crisis narrative in criminal activities.

- Crisis amplified existing problems with people working from home and spending time online, particularly seen in CSE/CSAM

PART III

Key Findings

IOCTA 2020

Key findings

Cross-cutting crime facilitators

- Social engineering still top threat
- Cryptocurrencies facilitate criminal transactions
- Underreporting → crime overview inaccurate
- Technological developments prevent LE access to e-evidence

Key findings

Cyber-dependent crime

- Ransomware more targeted, sophisticated and adaptive
- Increased damage on supply chains and critical infrastructure
- Malware: modular and other versatile use malware as benchmarks
- DDoS: targeted, automated and increasingly adaptive

Key findings

Child Sexual Exploitation (CSE) Online

- CSAM growth impacts LE capacity
- Encrypted chat applications pose a significant threat for abuse, hindering online CSE detection
- Offender online communities exhibit resilience and evolve
- Livestreaming becoming mainstream. Producing CSAM also occurs in the EU
- Commercialization becoming a widespread issue

Key findings

Payment fraud

- Steep rise in SIM swapping
- BEC becomes more sophisticated and targeted
- Online investment fraud is one of the fastest growing crimes affecting EU citizens.
- CNPF increases with criminals diversifying targets and electronic-skimming modus operandi.

IOCTA 2020 Highlights

CSE/CSAM

- Overwhelming number of complaints requiring investigation
- Increasingly profit-driven and commercialized
- Referrals and reports from NCMEC and hotlines

Phishing Attacks

- Faster and more automated
- Criminals adopting a holistic strategy.
- More authentic-looking messages and sites
- Situational awareness: COVID-19 narrative

Ransomware

- Targets organisations rather than persons
- GDPR fines used as added leverage
- Fear of re-victimization: reluctant to report crime
- Ransom demand negotiating

Malware

- Banking Trojans → advanced modular Malware
- Different strains used in combination attacks
- Commodity malware lowering barriers to entry into cybercrime.

Threat Actors

- More operational security
- Hide tracks:
  - Privacy-enhanced policies
  - Bulletproof hosting
  - Cryptocurrencies and privacy-oriented techniques

Reporting challenges

- Broad and static crime registration systems
- Difficult to quantify resource requests
- Insufficient cybercrime awareness among the public and local police

PART IV

Recommendations

IOCTA 2020

Recommendations

Coordination and cooperation

- □ More efficient national level coordination
- □ Cooperation with hosting services, social media platforms & ISPs
- □ Focused legislation and policies
- □ Dedicated task-force approaches
- □ Centralised pre-investigative actions within the EU

Information sharing

- □ Trust: structured info sharing
- □ Culture of acceptance and transparency – safe crime reporting
- □ Implementing channels for faster info sharing

Prevention and awareness

- □ Educate online behavior and operational hygiene
- □ Improve cyber readiness with crisis management and disaster recovery plans
- □ Evaluation schemes to assess IT security
- □ Establish rules & guidelines to increase resilience

Capacity-building

- □ Integrate cyber elements into LE readiness at the police academy level (cyber specialization)
- □ Combine technical expertise (civilian) and criminal case expertise (LE) for effective investigations

Thank you for your attention

Any questions?

www.europol.europa.eu