EUROPEAN CYBERCRIME CENTRE (EC3)

Emmanuel KESSLER
Head of
Prevention&Outreach

DATA&CYBERCRIME…
THE LATEST TRENDS FROM IOCTA 2025

2025 AS AN ENDING YEAR…
FROM THE EUROPOL PERSPECTIVE

LOOKING AHEAD….
WHICH CHALLENGES, WHICH GOALS FOR EU ACTORS ?

IOCTA | 2025

Steal, deal and repeat:
How cybercriminals trade
and exploit your data

EUROPOL
EC3 | European Cybercrime Centre

Europol Unclassified – Basic Protection Level
NOT for public distribution

Europol Unclassified – Basic Protection Level

IOCTA | 2025

Steal, deal and repeat: How cybercriminals trade and exploit your data

THE COMPROMISED DATA ECOSYSTEM

Techniques
Social Engineering &
Attacks On Systems

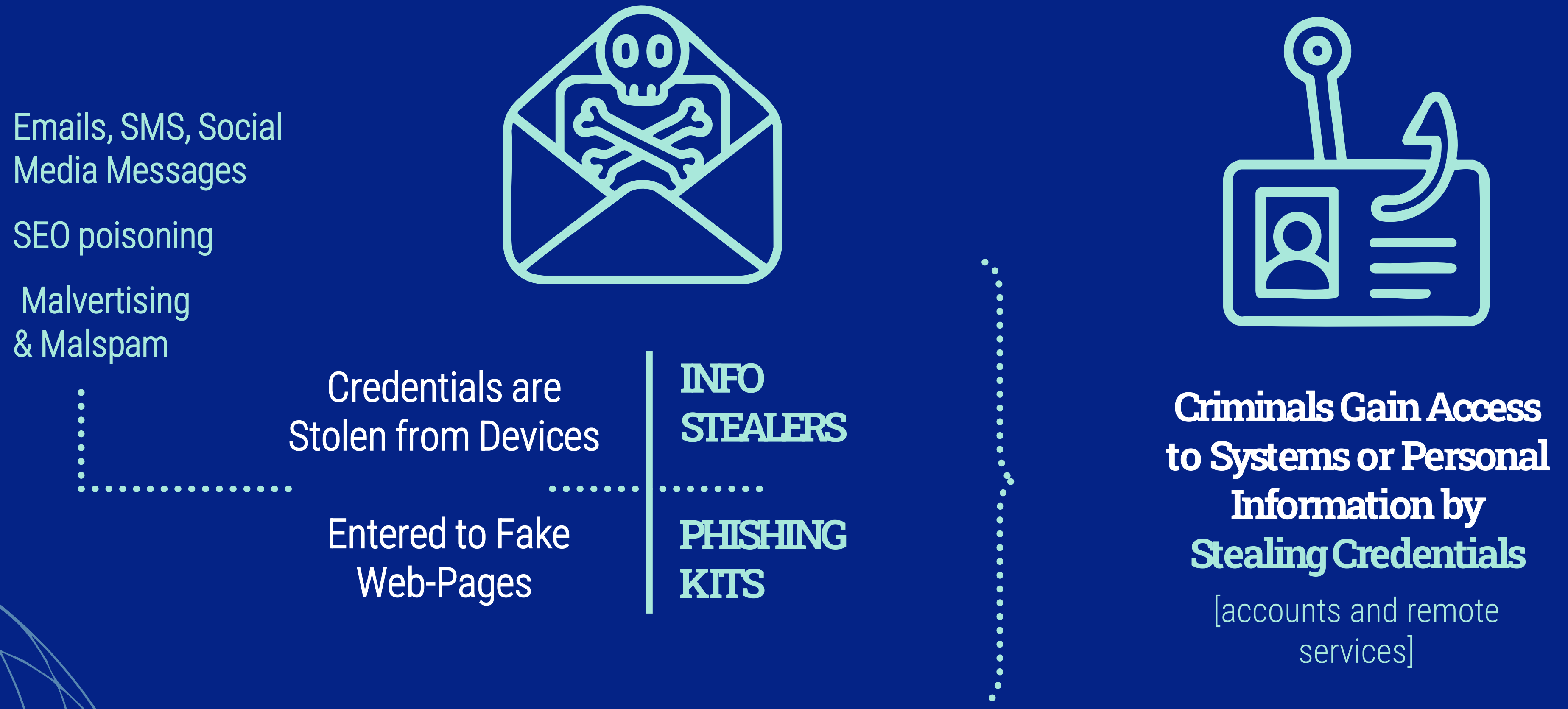
Criminal Actors
IABs & Data Brokers

Marketplaces
Compromised
Data, Tools &
Services

Exploitation
Online Fraud Schemes,
Cyber-attacks &
Hybrid Threats

DATA ACCESS

Exploiting Human Error



Emails, SMS, Social Media Messages

SEO poisoning

Malvertising & Malspam

Credentials are Stolen from Devices

INFO STEALERS

Entered to Fake Web-Pages

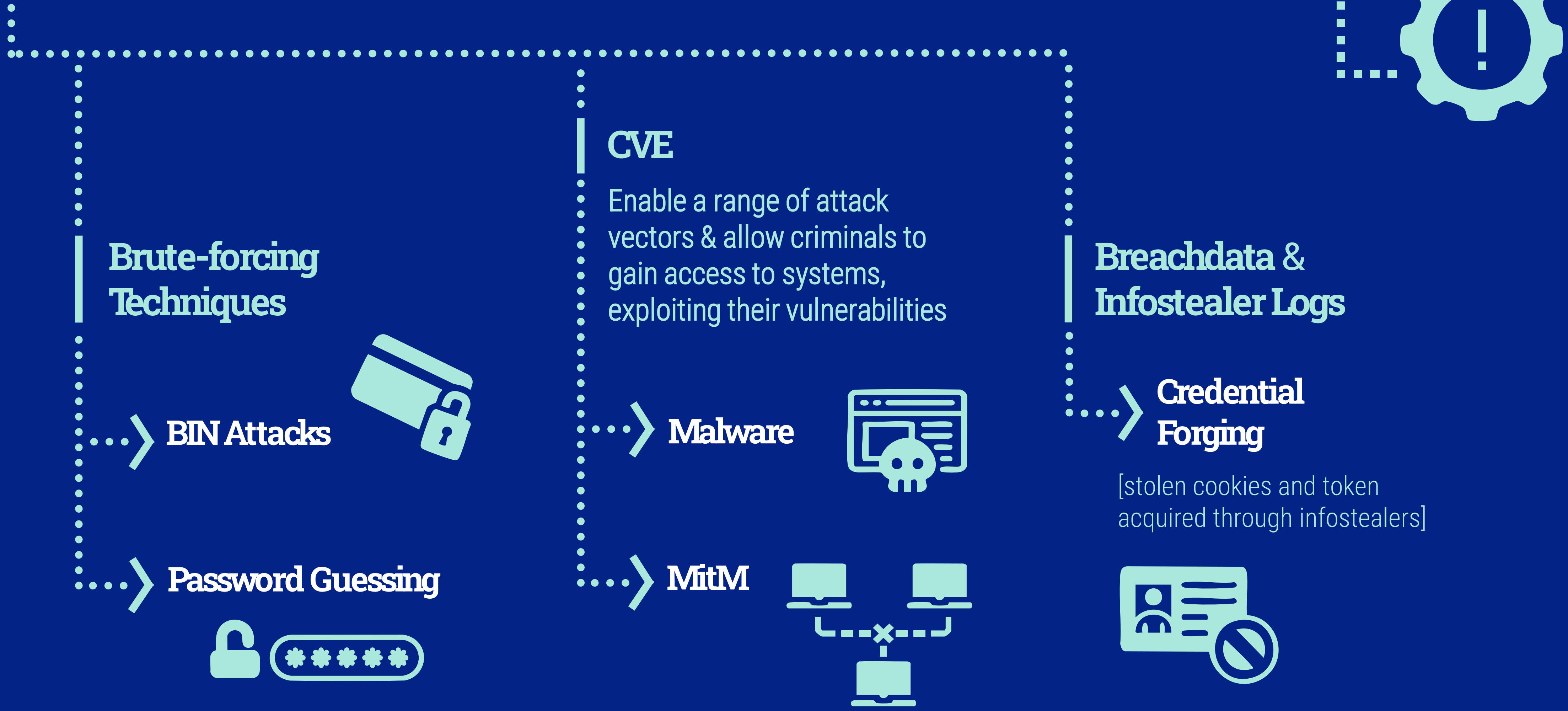
PHISHING KITS

Criminals Gain Access to Systems or Personal Information by Stealing Credentials

[accounts and remote services]

DATA ACCESS

Attacks Against Systems



Brute-forcing Techniques

- BIN Attacks
- Password Guessing

CVE

Enable a range of attack vectors & allow criminals to gain access to systems, exploiting their vulnerabilities

- Malware
- MitM

Breachdata & Infostealer Logs

- Credential Forging

[stolen cookies and token acquired through infostealers]

CRIMINAL ACTORS

Data Brokers

Monetise Harvested Data To Highest Bidder

Data dumps
Stealer logs
Credit card data

IABs

Sell Access To Systems

[Direct collaboration with Criminal Networks]

Advanced / Targeted Social Engineering Campaigns
Zero-day Exploits

OFS & CSE

Exploit Personal Data and Utilise Data Immediately

Deception and Coercion of Victims

WHERE ARE DATA AND ACCESS COMMODIFIED?

Cybercriminal Platforms

Marketplaces, Forums & E2EE channels

DATA EXPLOITED

TOOLS & SERVICES

Unanalysed **Infostealer Logs** & Breached Data Dumps

Unanalysed Or Verified **Credit-card Dumps**

Account Login Credentials To Web-services

Criminal Services [MaaS, phishing & exploit kits, etc.]

Anti-detection Solutions [Proxies, BPH, ML, Manuals]

JAN 2025

Operation TALENT

Operation Talent is part of a international effort to **dismantle cybercrime forums worldwide**

Countries involved:
Australia, France, Germany, Greece, Italy, Romania, Spain, United States of America, Europol

Cracked & Nulled

"Cracked" and "Nulled" were two of the largest cybercrime forums in the world. These sites were used not only for **cybercrime discussions**, but also served as **marketplaces for illegal goods** and **cybercrime-as-a-service**.

RESULTS:

› **2 largest cybercrime forums in the world taken down** with more than 10 million users

This operation was coordinated by Germany

APRIL 2025

Operation Endgame

Follow-up leads to five detentions and interrogations as well as server takedowns

Coordinated by Europol, with support from Eurojust.

Participating countries: **Canada, Czech Republic, Denmark, France, Germany, Netherlands and United States of America.**

Anyone with information is invited to make contact through the new website: **operation-endgame.com**

The **Smokeloader** pay-per-install botnet was operated by the actor known as 'Superstar'. This individual used his botnet to run a pay-per-install service, enabling customers to **gain access to victims' machines**. Customers used the service to deploy malware for their own criminal activities.

April 9, 2025

RESULTS:

- **5 detentions and Interrogations**
- **Multiple servers takedowns**
- **House searches, arrest warrants or "knock and talks"**
  Focusing on Costumers of Crime as a Service
- **Reveal of the reasons why the botnet access had been purchased**
  Keylogging, webcam acces, ransomware, deployment, crypto mining, etc...

JULY 2025

Operation Eastwood

This operation **targeted the criminal network**, **NoName057(16)**, linked to 73 DDoS attacks per day of Ukrainian private and public actors.

Countries involved:
BE, CA, FI, FR, DE, IT, LT, PL, ES, CH, SE, NL, US

NONAME057(16)

NoName057(16) is a **cybercrime network** that **targets primarily Ukraine**, but also focuses on attacking **countries that support Ukraine** in the ongoing defence against the Russian war of aggression.

RESULTS:

- **9 Arrest Warrants issued, 2 of them executed**
- **+100 Servers disrupted worldwide**
- **24 House searches**
- **+1000 Supporters notified for their legal liability**

Europol and Eurojust played a central role in connecting investigators and coordinating enforcement actions.

MAY 2025

LUMMA Infostealer

Operation MaceFall

Europol's European Cybercrime Centre has worked with **Microsoft** to disrupt Lumma Stealer, the world's most significant infostealer threat.This joint operation targeted the sophisticated ecosystem that allowed criminals to exploit stolen information on a massive scale.

Countries/agencies involved:
Microsoft, US DOJ, JC3

LUMMA

LUMMA was a sophisticated tool that **enabled cybercriminals to collect sensitive data** (stolen credentials, financial data, and personal information) from compromised devices on a massive scale.

RESULTS:

- **Over 394 000** Windows computers identified
- **300 domains actioned** will be redirected to Microsoft sinkholes
- **Over 1 300** domains seized

Europol coordinated with law enforcement in Europe to ensure action was taken, leveraging intelligence provided by Microsoft.

FEB 2025

8BASE RANSOMWARE

Operation PHOBOS

Countries/Agencies involved:
BE, Czechia, FR, GER, JP, PL, RO, SG, ES, SE, CH OAG and Fedpol, TH CCIB, UK NCA, US DOJ, US FBI and US DC3

Europol and Eurojust played a central role in connecting investigators and coordinating enforcement actions. Europol's European Cybercrime Centre (EC3) has been supporting the investigation since February 2019.

A coordinated international law enforcement action has led to the **arrest of four individuals** leading the **8Base ransomware** group in Thailand. These individuals are suspected of deploying a variant of Phobos ransomware to **extort high value payments** from victims across Europe and beyond.

PHOBOS

Phobos ransomware has been a **long-standing cybercrime tool**, frequently used in large-scale attacks against businesses and organisations worldwide. Phobos **relies on high-volume attacks against small to medium-sized businesses**.

RESULTS:

- **27 servers** linked to the criminal network were taken down.
- **Arrest of an administrator** of Phobos in 2024
- **400 companies were warned** worldwide of ransomware attacks.

EUROPOL

EUROPOL UNCLASSIFIED – BASIC PROTECTION LEVEL

MAY 2025

DDoS-for-hire takedown

Operation PowerOFF

Countries/agencies involved:
GER, NL, PL, US DOJ, US FBI, US HSI, US DCIS

Europol provided analytical and operational support throughout the investigation.

A coordinated operation led by Polish authorities with the support of Europol and US law enforcement agencies resulted in the **arrest** of **administrators of a global DDoS-for-hire service** and the seizure of **associated domains**.

Stresser & Booter Services

Stresser & Booter Services are offer on-demand cyberattacks. These services **let users flood a target server** or website with enormous volumes of **fake traffic**, making them **inaccessible to real users**.

RESULTS:

- **4 administrators arrested**
- **1 suspect identified** and critical intelligence shared on others
- **9 domains seized**, associated with booter services
- **Warnings for users** seeking out DDoS-for-hire services

EUROPOL

Europol Unclassified - Basic Protection Level

OCT 2025

Operation SIMCARTEL

Agencies/Countries involved:
Austria, Estonia, Latvia,
Europol, Eurojust

Operation was led by Austrian, Estonian and Latvian investigators.

An action day performed in Latvia led to the **arrest cybercriminals** of Latvian nationality and the **seizure of infrastructure used to enable crimes** against thousands of victims across Europe.

RESULTS:

- **5 Arrests** of Cybercriminals from Latvia
- **1200 SIM boxes seized**
- **5 servers taken down**
- **40000 active SIM cards seized**
- **26 searches carried out**
- **4 luxury vehicles seized**
- **EUR 431 000 in suspects' bank accounts frozen**
- **USD 333 000 in suspects' crypto accounts frozen**

EUROPOL

Europol Unclassified - Basic Protection Level

MAY 2025

Operation RAPTOR

Countries involved:
Austria, Brazil, France, Germany, The Netherlands, Spain, South Korea, Switzerland, United Kingdom, USA

Operation was coordinated by Europol.

This operation **targeted dark web vendors and buyers** across four continents. Europol coordinated the enforcement actions.

RESULTS:

- **270 Arrests** across multiple countries
- **12500 counterfeit goods apprehended**
- **+184M in cash and cryptocurrencies apprehended**
- **+180 firearms apprehended**
- **+2 tonnes of drugs apprehended**
- **+4 tonnes of illegal tobacco apprehended**

EUROPOL

Europol Unclassified - Basic Protection Level

Law Enforcement Challenges

EUROPOL
EC3
European Cybercrime Centre

Anonymity

High volume/ low value crime

Cross-border jurisdiction

Artificial intelligence
Quantum computing

Tracing payments

Tracing communication

THANK YOU!

https://www.europol.europa.eu/rss.xml

@europol.eu

https://www.linkedin.com/company/europol/

https://www.facebook.com/europol

@europol

@europol-eu

https://www.youtube.com/user/EUROPOLtube

EUROPOL
EC3 | European Cybercrime Centre