Ensuring Industrial Safety and Security in times COVID-19 and beyond

Philipp Amann
Head of Strategy

European Cybercrime Centre
Europol
Europol’s Mandate

"Europol shall support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy"

(Europol Regulation)
Strategic overview and coordination
Regular coordination calls with EU bodies
Regular reporting to stakeholders

Products created asRestricted, BPL and Public versions, shared through SIENA, Europol LBs, Europol website, Social Media and the Europol Platform for Experts.
Criminal trends related to COVID-19: Cyber-Dependent Crime

Ransomware
- Faster and more targeted ransomware attacks
- Hospitals and health-related companies as a target of opportunity
- Known ransomware families

Phishing
COVID-19 topic used to lure victims to click fake links claiming to provide COVID-19 related information or attachments hiding or dropping malware

Malicious Domain Name
These registered domain names form the backbone of many criminal operations. There are currently ongoing discussions between EC3, DG HOME, registries/ars and the J-CAT to tackle the criminal use of malicious COVID related domains
Criminal trends related to COVID-19: Payment Fraud

**Card-present & Card-not-present-fraud**

- Overall, the impact of COVID-19 on non-cash payment fraud hasn’t been as significant as in other cybercrime areas. Card-present-fraud has significantly decreased, while Card-not-present-fraud has remained stable or slightly decreased.

**Legal Business Structures**

- Legal business structures, such as limited companies and other types of incorporated structures, are widely used to conduct COVID-19 related fraud schemes and other types of criminal activities.

- Many of these companies have been specifically established to conduct fraud schemes, distribute counterfeit goods or to handle and transfer fraudulently obtained funds.

- In some cases, criminal operators use the identities of genuine and legally operating companies. Several of these companies have lodged criminal complaints against criminals impersonating managers of the companies to conduct illicit transactions and deals.
Criminal trends related to COVID-19: Dark Web

Opportunities
- Perfect environment to sell fake and counterfeit articles, the most frequent being chloroquine, masks, vaccines and test kits.
- Increase in enabling crime, most significantly the scale of compromised data.

Demand
- COVID-19 related products - 645 listings across 12 markets, 222 unique;
- COVID-19 sales and discounts to stimulate demand/purchases;
- Increased demand for enablers as criminal business models change.

Distribution
- COVID-19 related items also offered on Telegram, Openbazaar and Discord;
- Forecast a significant surge with dark web dominating distribution in the post COVID-19 online culture.
Criminal trends related to COVID-19: Child Sexual Exploitation

Increase in...

- Increase of 141% in April and 68% in May 2020 in the number of reports (NCMEC)
- 200% increase in child abuse forum posts linking to child exploitation material
- Downloads on P2P sharing networks
- Discussions amongst offenders about online activity of children

Main risks

Grooming, SGEM, Sexual coercion and extortion, sexting, bullying, accessing pornography and violent content online, games with gambling-like elements, costs of in-game spending

Outlook

The global impact of COVID-19 means people are spending more time online. Children are:
- be more exposed to offenders
- be more inclined towards making explicit material to exchange with peers
- become lonely and isolated, thus willing to connect
Operational support
Operational Coordination

- **Operational, analytical and technical support** to concrete cybercrime COVID-19 related investigations in MS and TPs

- **Enhanced OSINT and cyber threat intelligence gathering and sharing**

- **Use of secure online collaboration/conferencing solution** for operational coordination and weekly remote operational meetings

- Two separate online rooms were used for secure chats within the **Virtual Command Post**
  1. J-CAT and EC3
  2. J-CAT, EC3, Eurojust
Prevention and Awareness
Europol.europa.eu/Covid-19

STAYING SAFE DURING COVID-19: WHAT YOU NEED TO KNOW

Criminals have quickly adapted their techniques to exploit our fears around the COVID-19 pandemic. Their main aim is profit by any means necessary.

Our desire for COVID-19 news is the perfect opportunity for criminals to dupe more victims looking for information and in-demand products and services.

COVID-19 – QUICK LINKS

Want to know more about COVID-19? Always check official channels like the World Health Organization or your national health authority.

COVID-19 landing page

Everything you need to know on staying safe online & offline during COVID-19

✓ Regularly updated
Pandemic profiteering

*March 2020*

Material available

Make your home a cyber safe stronghold

19 languages

Guidelines for safe teleworking

15 languages

Visual on criminals targeting senior citizens

English only

Clip on COVID-19 criminal profiles

English only

19 languages
Beyond the pandemic
30 April 2020
Material available

Watch out for the fakes! clip
English only

The new normal after COVID-19: a safety guide
8 languages and more in progress
No More Ransom (www.nomoreransom.org)

- +150 partners
- Website available in 36 languages
- +100 tools capable of decrypting +100 ransomware families
- +200k victims helped
Main Takeaway Points

- With restrictions in place and more people online, criminals have been quick in exploiting the crisis and in adapting their criminal business model.

- Worrying aspects are attacks on critical infrastructure and in particular against healthcare institutions (convergence of actors).

- Cyber threats require a networked response, including prevention and awareness (joint responsibility).
Main Takeaway Points

- Industrialization of Cybercrime – Crime-as-a-Service model
- Europol – the EU’s law enforcement agency to support MS
- Evolving threat landscape and various challenges
- Cybercrime at scale requires a networked response, including prevention
Thank you.