UNODC
United Nations Office on Drugs and Crime

COVID-19 RESPONSE

Vienna, 14/04/2020

CYBERCRIME AND COVID19: Risks and Responses

KEY JUDGMENTS

- **Cybercrime is evolving and growing in response to the COVID19 pandemic.** Online fraud, extortion and online child sexual abuse targets individuals whilst ransomware primarily compromises systems – including hospitals. Governments will continue to be targeted by malware. The increasing spread of misinformation and disinformation will continue to confuse the public and undermine the scientific response.
- **Home-based working has increased the potential cybercrime victim-pool. People take greater risks online at home which inadvertently exposes corporate IT to cybercriminals.** Phishing will continue to enable malicious access to critical systems for criminals and other advanced actors.
- **The quantity of specialist law enforcement counter-cybercrime personnel will be reduced throughout most of 2020. Cybercrime will increase in the short-term, and victims will likely face delays in achieving justice**. Cybercriminals will exploit perceived operational gaps. Counterintuitively, this will create tactical and strategic law-enforcement opportunities.

Context

1. This briefing provides a snapshot of cybercrime threats within the context of the COVID19 pandemic. It has been sourced from confidential debriefs of UNODC law enforcement, governmental, NGO, academic, media, open-source and private sector partners around the world during early April 2020. Recommendations are presented at the end of each thematic section.

Picture-of-Threat: evolving, increasing and exploiting

2. Comprehensive social distancing measures are now in place around the world. This has led to a significant increase in the use of online communication by public authorities, businesses and individuals alike. Many are unfamiliar with the use of online technology at this scale. This has presented a large, attractive and vulnerable target-set for cybercriminals to exploit. Combined with remote working and schooling, there are more Internet users, who are less knowledgeable of threats and are likely to take more risks whilst online at home than they would at work or school.
3. Cybercriminals have evolved their criminality to exploit the social, legal and psychological nuances associated with COVID19. School-age children, both the new and more frequent users of the Internet, are being proactively targeted by online sex offenders. This includes offenders seeking to groom[1] and

[1] https://www.esafety.gov.au/parents/big-issues/unwanted-contact

sextort[2] individual children, through to broader infiltration in online classes[3] now referred to as "Zoom-bombing".

4. Cybercriminals are increasingly preying on people's fear of the COVID19 virus: offering fake cures for sale on the Internet and defrauding through the sale of non-existent hand-sanitizer and medical Personal Protective Equipment (PPE), medicines or hygiene products. Other frauds include the offer of services such as unsound investment advice (including cryptocurrencies) and incorrect medical advice and diagnosis. One major online pornography site offered free subscription to users from one country, thus increasing the risks of malware downloads and sextortion.

5. Senior Citizens, who are often less sensitised to online risks, are explicitly profiled and targeted by cybercriminals to download and forward ransomware-infected links through COVID19 spam emails and spread disinformation amongst friends and family. Cybercriminals continue to seek to extort by claiming to know – and reveal - the victim's alleged use of online pornography.

6. Business Email Compromise[4] (phishing-compromised email accounts which pretend to be a senior official in the target organization) continues to use social-engineering, enhanced by the added urgency of the pandemic, to encourage the movement of funds to a criminal bank, foreign exchange or cryptocurrency account, or is used to obtain sensitive data for malicious use including espionage.

7. Darknet forums continue to sell compromised data – including that of high-profile officials and celebrities. Criminals new to "cybercrime" are seeking advice from others on how to best exploit the COVID19 pandemic for profit. Some cybercriminals have sought to dissuade other cybercriminals from targeting hospitals and vaccine-testing laboratories from Distributed Denial of Service (DDOS) and ransomware attacks. Predatory child sex offenders continue to discuss which social network and photo-sharing sites are likely to give them the easiest access to children to abuse. Offenders also continue to debate how to best identify and defeat undercover police officers online.

8. In addition to traditional cybercriminals, Advanced Persistent Threat (APT) groups continue to evolve and exploit the pandemic. APTs continue to target Critical National Infrastructure including hospitals and vaccine development labs with malware, ransomware and DDoS attacks. The motivation behind such attacks is not simply profit-based as malware often provides access to login credentials and other sensitive information of intelligence value.

9. The success of much of the COVID19-related cyber-criminality relies upon email phishing attacks as the initial vector of infection. When people click on a link or a document, the account is compromised. The compromise may be visible to the victim but, more often, the compromise is covert and enables the criminal to establish and maintain long-term access to the account, organization and associated IT. In addition to gathering sensitive information, the APT actor can deface websites, change the detail of documents, delete data and disseminate misinformation and disinformation.

10. **UNODC recommends that governments and the private sector increase public awareness campaigns which are culturally sensitive and easy to understand. Anonymous Online Child Sexual Abuse Reporting hotlines are a key facet of the response. We also recommend that security updates continue to be rigorously applied and information routinely backed-up.**

[2] https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion
[3] https://tcrn.ch/3buz3gW
[4] https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

Reduced law enforcement capacity and societal resilience

11. In many countries, specialist counter-cybercrime law enforcement personnel have been diverted from investigating cybercrime offences to supporting government measures, such as quarantine enforcement, against the COVID19 outbreak. Specialist officials have also become ill. Capacity is likely to reduce further in the coming weeks, reducing the capability of States to counter new and increasing cybercrime threats.

12. In several countries, investigative and judicial procedures are disrupted by the need to conduct these activities in-person, which is not possible due local public health measures. Other countries have rapidly moved to online judicial operations.

13. Misinformation and disinformation regarding the virus continues to spread primarily through social media and encrypted messaging services. Social media companies, also challenged by remote working, struggle to cope with the quantity of misinformation content, how to consistently apply internal policies and the impact of local legislation.

14. Misinformation, disinformation and attacks on Critical National Infrastructure undermine public trust and weaken the effectiveness of public safety measures.

15. **UNODC recommends that judicial procedures should continue online where possible, whilst ensuring that international standards and norms, due-process and the rule of law remain.**

16. **We also recommend that Social Media Companies do more to counter the spread of the COVID19 "misinfodemic", whilst protecting freedoms of speech. Fact-based science must be at the heart of the COVID19 response – we all have a critical role to play in this.**

Analysis

a. *The COVID19 pandemic poses an unprecedented global challenge to all of society. Many have transferred their physical activities to online operations, as have criminals. As cybercrime increases in complexity and victims increase in quantity, law enforcers in some countries are moved to other duties. The economic impact of COVID19 adds a further layer of complexity for the public and for government. A perfect storm of potential cybercriminality emerges.*

b. *Whilst COVID19 and cybercrime threats related to this crisis are global, responses must also be global: countering cybercrime in one jurisdiction reduces risk around the world. Information on new threats and crime types, like Europol's COVID19 analysis and INTERPOL's Cyber Threat Assessment, must continue to be shared internationally without delay. Online Child Sexual Abuse reporting hotlines are a critical tool in enabling the public to counter the threat.*

c. *Given the likely strain on both proactive and reactive law-enforcement, we assess that the capacity to actively investigate cybercrime will be challenged in the short-term – especially in countries with limited resources before the pandemic. Cybercriminals, including APT groups, will continue to exploit this. Public reporting of successful arrests or disruptions of cybercriminals who sought to exploit the current crisis must be enhanced. Highly impactive operations, like the Netherlands recent take-down of fifteen DDoS providers in one week[5], help to show visible impact and remind cybercriminals that operations continue around the world. Proactive undercover online operations against high-risk cybercrime actors must continue. Counter-intuitively, cybercriminals may take more risks online as*

[5] https://www.zdnet.com/article/dutch-police-take-down-15-ddos-services-in-a-week/

they perceive that the likelihood of detection has reduced. Specialist law enforcement investigations must, therefore, continue at pace.

d. *Public diplomacy and awareness-raising are critical for prevention and must empower vulnerable groups, especially children and seniors. Measures against misinformation and disinformation should provide assessed, credible and useful information: this must be done in a transparent and accountable manner.*

e. *All measures used to counter cybercrime must continue to be Proportionate, Legal, Accountable and Necessary. Technology is being used by many governments to assess, identify and trace potential COVID19 patients. This essential work must remain under review, with clear oversight, to ensure that surveillance measures are withdrawn once the aim of outbreak control is achieved. Now is the time to build cyber-confidence with the public and to work together to counter the most pressing threats of our time. and to build confidence internationally.*

f. *Now is not the time to de-invest in specialist cybercrime law enforcement. The capability and capacity to counter cybercrime are vital components for protecting Critical National Infrastructure, keeping children safe online, empowering industry, securing hospitals and supporting economic recovery from COVID19.*

g. *UNODC's specialist cybercrime staff are available, around the globe, to support Member States in countering cybercrime, 24 hours a day, 7 days a week. UNODC's public diplomacy resources are available at* https://www.unodc.org/unodc/en/covid-19.html *and include links to an Instagram Live session with the Secretary-General's Special Envoy on Youth, protective cyber advice for UN staff and the UN Secretariat-wide iSEEK Live event on cyber.*

Dissemination: this report (UNODC/CMLS/COVID19/Cyber1) may be shared without any prior reference to the originator.

ENDS