COVID-19 SPARKS UPWARD TREND IN CYBERCRIME

05 Oct 2020
Press Release

Europol’s 2020 cybercrime report updates on the latest trends and the current impact of cybercrime within the EU and beyond.

So much has changed since Europol published last year’s Internet Organised Crime Threat Assessment (IOCTA). The global COVID-19 pandemic that hit every corner of the world forced us to reimagine our societies and reinvent the way we work and live. During the lockdown, we turned to the internet for a sense of normality: shopping, working and learning online at a scale never seen before. It is in this new normal that Europol publishes its 7th annual IOCTA. The IOCTA seeks to map the cybercrime threat landscape and understand how law enforcement responds to it. Although the COVID-19 crisis showed us how criminals actively take advantage of society at its most vulnerable, this opportunistic behaviour of criminals should not overshadow the overall threat landscape. In many cases, COVID-19 has enhanced existing problems.

CROSS-CUTTING CRIME

Social engineering and phishing remain an effective threat to enable other types of cybercrime. Criminals use innovative methods to increase the volume and sophistication of their attacks, and inexperienced cybercriminals can carry out phishing campaigns more easily through crime as-a-service. Criminals quickly exploited the pandemic to attack vulnerable people; phishing, online scams and the spread of fake news became an ideal strategy for cybercriminals seeking to sell items they claim will prevent or cure COVID-19.
Encryption continues to be a clear feature of an increasing number of services and tools. One of the principal challenges for law enforcement is how to access and gather relevant data for criminal investigations. The value of being able to access data of criminal communication on an encrypted network is perhaps the most effective illustration of how encrypted data can provide law enforcement with crucial leads beyond the area of cybercrime.

MALWARE REIGNS SUPREME

Ransomware attacks have become more sophisticated, targeting specific organisations in the public and private sector through victim reconnaissance. While the COVID-19 pandemic has triggered an increase in cybercrime, ransomware attacks were targeting the healthcare industry long before the crisis. Moreover, criminals have included another layer to their ransomware attacks by threatening to auction off the comprised data, increasing the pressure on the victims to pay the ransom. Advanced forms of malware are a top threat in the EU: criminals have transformed some traditional banking Trojans into modular malware to cover more PC digital fingerprints, which are later sold for different needs.

CHILD SEXUAL ABUSE MATERIAL CONTINUES TO INCREASE

The main threats related to online child abuse exploitation have remained stable in recent years, however detection of online child sexual abuse material saw a sharp spike at the peak of the COVID-19 crisis. Offenders keep using a number of ways to hide this horrifying crime, such as P2P networks, social networking platforms and using encrypted communications applications. Dark web communities and forums are meeting places where participation is structured with affiliation rules to promote individuals based on their contribution to the community, which they do by recording and posting their abuse of children, encouraging others to do the same. Livestream of child abuse continues to increase, becoming even more popular than usual during the COVID-19 crisis when travel restrictions prevented offenders from physically abusing children. In some cases, video chat applications in payment systems are used which becomes one of the key challenges for law enforcement as this material is not recorded.

PAYMENT FRAUD: SIM SWAPPING A NEW TREND

SIM swapping, which allows perpetrators to take over accounts, is one of the new trends in this year’s IOCTA. As a type of account takeover, SIM swapping provides criminals access to sensitive user accounts. Criminals fraudulently swap or port victims’ SIMs to one in the criminals’ possession in order to intercept the one-time password step of the authentication process.

CRIMINAL ABUSE OF THE DARK WEB

In 2019 and early 2020 there was a high level of volatility on the dark web. The lifecycle of dark web market places has shortened and there is no clear dominant market that has risen over the past year. Tor remains the preferred infrastructure, however criminals have started to use other privacy-focused, decentralised marketplace platforms to sell their illegal goods. Although this is not a new
phenomenon, these sorts of platforms have started to increase over the last year. OpenBazaar is noteworthy, as certain threats have emerged on the platform over the past year such as COVID-19-related items during the pandemic.

“Catherine De Bolle, Europol’s Executive Director commented: “Cybercrime affects citizens, businesses and organisations across the EU. Europol plays a key role in countering cybercrime by working with our many partners in law enforcement and the private sector and by offering innovative solutions and effective, comprehensive support to investigations. I hope this analysis can inform effective responses to these evolving threats and make Europe safer”.

“Vice-President for Promoting our European Way of Life, Margaritis Schinas, who is leading the European Commission’s work on the European Security Union, said: «Cybercrime is a hard reality. While the digital transformation of our societies evolves, so does cybercrime which is becoming more present and sophisticated. We will spare no efforts to further enhance our cybersecurity and step up law enforcement capabilities to fight against these evolving threats. Europol has a major role to play».

“EU Commissioner for Home Affairs, Ylva Johansson, said: “The Coronavirus Pandemic has slowed many aspects of our normal lives. But it has unfortunately accelerated online criminal activity. Organised Crime exploits the vulnerable, be it the newly unemployed, exposed businesses, or, worst of all, children. This report shows the urgent need for the EU to step up the fight against organised crime [online] and confirms the essential role of Europol in that fight”.

“Edvardas Šileris, Head of European Cybercrime Centre said: “I am pleased to welcome the 2020 edition of the IOCTA – our flagship document, an essential resource for EU’s law enforcement and policy makers. I am very thankful to all the partners who have contributed to this year’s assessment and have helped us identify the key theme defining the current landscape: cybercrime is an evolution, not a revolution”.

The 2020 IOCTA contributes to setting priorities for the 2021 EMPACT operational plans, which follow the priorities defined as: disruption criminal activities, combating child sexual abuse and child sexual exploitation and targeting criminals involved in fraud and counterfeiting of non-cash means of
Download the IOCTA 2020 report.

<table>
<thead>
<tr>
<th>CRIME AREAS</th>
<th>Cybercrime</th>
<th>High-Tech crime</th>
<th>Social engineering</th>
<th>Child Sexual Exploitation</th>
<th>Online sexual coercion and extortion of children</th>
<th>Forgery of money and means of payment</th>
<th>Payment Fraud</th>
<th>Money Muling</th>
</tr>
</thead>
<tbody>
<tr>
<td>TARGET GROUPS</td>
<td>General Public</td>
<td>Law Enforcement</td>
<td>Academia</td>
<td>Professor</td>
<td>Students</td>
<td>Researcher</td>
<td>Press/Journalists</td>
<td>Other</td>
</tr>
<tr>
<td>ENTITIES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>