PAR
JON SHAMAH
EUROPEAN EID SUBJECT MATTER EXPERT

PAR
ERIC BLOT-LEFÈVRE
TRUSTSEED SAS

The Route to a Trustworthy Internet

The European commission is taking many actions to combat cyber-crime and to ensure a trustworthy Internet: "The European Commission aims for a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace." (EU Cyber Security Strategy, 2013).

C Cyber-crime may quite often be only one element of a more complex play where the motive is not apparent and as with any crime, it is important to recognise the Means, Motive, and Opportunity in order to categorise the cyber-criminal activity, and so devise counters and remediation.

However, here, I shall only examine certain aspects of cyber-crime that potentially can hugely hamper economic growth and so should be a high priority to be combatted.

LOW-VALUE 'BULK' CYBER-CRIME

The Digital Economy provides a target-rich environment for crime. The simplest form of crime is identity theft as a result of obtaining usernames and passwords either obtained directly by traditional deception (either on-line or physically), or by the easier and often more economic method of bulk purchasing compromised usernames and passwords/pin-codes from wholesalers on 'the Dark Web'.

Fraudulent transactions can also be created by intervening between a genuine internet user and its transacting party, such as a bank account holder and the internet bank.

These can offer substantial amounts of money, but often as a result of aggregating many smaller transactions that remain un-noticed or too small for action by police. Many individuals and companies remain somewhat 'buffered' from the effects by insurances and bank refunds of fraudulent transactions.

However, when aggregated across many countries, these bulk crimes can add up to quite large value gains by criminals, who do not need to respect geography or jurisdictions.

HIGH-VALUE/HIGH-IMPACT TARGETED CYBER-CRIME

Consider the example of a large publically quoted corporation, with a well-established brand and public trust. Traditionally, in the pre-internet age, a threat to the brand, and a well-crafted extortion note might well convince management that capitulation may be less of a financial loss than fighting. However in this internet age, the threat of releasing confidential data (either real or imaginary) may be enough to extort large amounts from a concerned Board of Directors.

The internet age, and automated share dealing provides an ideal opportunity to execute a 'victimless crime' of even greater magnitude. Imagine actually publicising that this large publically quoted corporation has suffered a major data breach. Knowing the details of when that information will be leaked to the press, provides a significant opportunity to 'insider-trade' and take advantage of stock movements, even if the disruption in stock values

> *The threat of releasing confidential data may be enough to extort large amounts*

are only transient. Significantly higher amounts of cash can be realised than those of the direct extortion approach.

EU EFFORTS TO FIGHT CYBER-CRIME

A lot of good work has been done on cyber-only initiatives. EU organisations such as ENISA, the European Agency for Network and Information Security, is providing much support to industry in the form of reports and analysis, as well as the exchange of information, best practices and knowledge.

The NIS platform is another good example of the EU stimulating activity via public-private joint initiatives. The NIS platform is intended to bring together policy and technical experts to debate the current and future challenges, identifying and develop incentives to adopt good cybersecurity practices and to promote the development and the adoption of secure ICT solutions.

THE TRUST SERVICES REGULATIONS

After the very mediocre success of the Electronic Signature Directive of 1999, the issue of Trust has been further recognised at regulatory level and a new Trust Services Regulation (eIDAS) has been passed and will come into force in June 2016. This new regulation – compulsory rather than optional as with the e-Signature Directive – will set clear rules on interoperability of both personal and company identification with e-signatures and time-stamping guaranteeing transactions. eIDAS is a huge opportunity to further boost the digital economy. Countries will need to first establish security infrastructure and digital trust in accordance with this regulation. This will hold operators of independent trust services liable to each other, protecting identities, privacy and fiscal value.

EFFECTIVE PRACTICAL SPECIFIC ANTI CYBER-CRIME MEASURES

Establishing Computer Emergency Teams (CERTs) in each Member State is a major step forwards for larger governmental organisations to protect themselves. They provide pro-active monitoring and technical remediation, but are only part of the protection from the more complex threats.

Security Operation Centres (SOCs), traditionally operated by large Service Providers offer security services to corporates.

SMES - THE SOFT UNDERBELLY

However, even this use of CERTs and SOCs is available only to those that can afford to engage them and aim to protect against targeted attacks. Small/Medium Enterprises (SMEs) have in the past, been under-recognised by the EU, leaving many initiatives to be enacted a country level only, albeit with some central support. The SME ecosystem is potentially much more vulnerable to the impact of cyber-crime than larger companies, who have the resources to better protect themselves. SMEs also comprise the majority of the economy within the EU.

> *Cyber-Crime is old style criminality dressed-up in modern clothes*

COSTAR, a 'Trust In Digital Life' incubator initiative aims to provide SOC-like capabilities for SMEs. It provides many of the SOC benefits at an economic level which would be affordable to even the smallest SMEs, through innovative technologies and methods and draws on collaboration between many public and private organisations using their expertise, and also uniquely providing local support when needed.

The COSTAR initiative is becoming a role model for industry and government together protecting SMEs.

CONCLUSIONS

Cyber-Crime is old style criminality dressed-up in modern clothes and taking advantage of modern technology to tap into more and varied victims.

Much of organised crime has already adapted its tried and tested techniques to the additional opportunities. Organised Crime recognises that criminal justice and policing lag far behind and are still struggling to break the mind-set that cyber-crime should be treated separately from other forms of criminality.

While there are many parallel initiatives, Europe has to continually adapt and improve its efforts to successfully combat Cyber-crime. The European Commission is now moving centre-stage in these efforts to improve the trustworthiness of the Internet and the Digital Economy, but must increase its speed to keep up with organised crime, through utilising, leveraging and stimulating effective existing technologies besides fundamental research. ●