Commercialization of cybercrime through Cybercrime-as-a-Service now poses a global threat

According to CIO Insight, a threat index created by network control solution provider Infoblox showed that cybercrime-as-a-service is growing at an explosive pace. The DNS Threat Index measures the number of malicious websites relative to a baseline average from 2013 to 2014. With this baseline defined as 100, the index for the most recent reporting period, the first quarter of 2016 stands at 137. It stood at 128 in Q4 of 2015, representing an impressive growth rate of 7 percent over a single quarter. Verizon's tenth annual breach report found that the number of ransomware attacks doubled compared to the previous year.

Cybercrime-as-a-service (CaaS) help Bad actors and cyber criminals with an expanding range of resources, tools and technologies from exploit kits to ransomware to build threats and launch attacks. Large number of malicious sites offer a wide range of services for cybercriminals to leverage. Exploit kits that automate the development and delivery of malware are a well-established industry. The now-defunct Angler exploit kit was the industry leader, although an older exploit kit, RIG, has undergone a new surge in popularity.

The hottest growth segment in cybercrime-as-a-service is ransomware, a technique which quietly encrypts files before freezing a computer or server and demanding money to decrypt a company or individual's data. The number of ransomware domains tracked in the DNS Threat Index has increased 35 times from its baseline value. Cyber attacks deploying ransomware to demand money from victims have soared 50 per cent in the last

year, hitting financial services, healthcare and the public sector the hardest, according to Verizon's closely watched annual data breach report.A separate report by security firm Symantec found that the average amount paid by victims of ransomware had risen to $1,077 (£834).

Ransomware has hit the big time – not just in the sheer number of malicious websites involved, but also in the scale of attacks and the nature of the targets. Ransomware used to be associated with small-scale attacks aimed largely at consumers or small businesses. Now, enterprise-strength ransomware attacks can target even the largest organizations. According to Marc Spitler, senior manager in Verizon's security research division, attacks on businesses were stealthier. Often, he said, attackers burrowed deeper into a company's infrastructure to find key databases that were then scrambled before payment was sought.

In most attacks, booby-trapped attachments sent via email were the main delivery mechanism for ransomware and other malware, found the report. "These attacks are all about getting a foothold on a system," he said, adding that once attackers were inside an organisation they typically looked to use the back doors for many different types of attack.

Darren Thomson, chief technology officer for Symantec in Europe, said its statistics suggest about one in every 131 email messages was now harbouring some kind of cyber-threat. "They are arriving in Word documents and Excel spreadsheets," he said, "the messages people get many times a day."

Despite this increase and the related media coverage surrounding the use of ransomware, many organizations still rely on out of date security solutions and aren't investing in security precautions. In essence, they're opting to pay a ransom demand
rather than to invest in security services that could mitigate

against a cyber attack, according to Verizon Report.

Cybercrime as a Global Threat

Until this year, the majority of malicious domains were registered in the U.S., including both domains created for cybercrime and previously legitimate domains hijacked by bad actors. U.S.-registered domains still account for the largest share of new malicious domains (41 percent).

But five other countries now account for half of new malicious domains: Portugal, Russia, Netherlands, the U.K. and Iceland. These countries' web presences share little in common beyond being favorites of the cybercrime-as-a-service industry, which is clearly adept at shifting resources at will.

For prospective targets such as you and your organization, there is no difference between attackers who leverage CaaS tool and those who use their own resources. If there is a specific lesson to be learned, it is that cybersecurity cannot be provided in isolation but must draw on cooperation to build a defensive system as flexible and powerful as the fast-growing cybercrime ecosystem.

Cybercrime is increasing in scale and impact

The advent of the Internet of Everything (IoE) combined with the ever increasing number of Internet users globally creates a broader attack surface, new attack vectors and more points of entry, including social engineering methods, for criminals to exploit, making endpoint security even more important.

Malware is becoming increasingly sophisticated, intelligent, versatile, available, and is affecting a broader range of targets and devices. E-commerce related fraud has increased in

line with the growing number of online payments, affecting major industries such as airlines and hotels. Key factors fuelling the increase are largescale data breaches supplying compromised card data to underground forums and a low prevalence of preventive measures implemented by merchants and the financial industry, such as 3D Secure.

In general, trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage. The EU will remain a key target for cybercrime activities because of its relative wealth, high degree of Internet penetration, its advanced Internet infrastructure and increasingly Internet-dependent economies and payment systems

Commercialization of cybercrime

Criminals are freely able to procure commercial services that facilitate almost any type of cybercrime, such as the rental of botnets, denial-of-service attacks, malware development, data theft and password cracking, according to the 2014 iOCTA report.

Cybercrime has become commercialized according to Crime-as-a-Service (CaaS) business model and financial gain accrued by cybercrime experts further stimulates the commercialization of cybercrime as well as its innovation and further sophistication. This has made the process of conducting cyber-attacks easier, facilitating a move by traditional organised crime groups (OCGs) into cybercrime areas.

The criminals are also abusing anonymisation techniques such as Darknets that allow citizens to communicate freely without the risk of being traced. However, the features of these privacy networks are also of primary interest to criminals that abuse such anonymity on a massive scale for illicit

online trade in drugs, weapons, stolen goods, forged IDs and child sexual exploitation.

Criminal marketplaces are complemented by anonymous payment mechanisms such as virtual currencies. While in principle legitimate, they are abused by criminals for criminal transactions and money laundering. Centralised schemes such as WebMoney are commonly exploited.

This new method of developing cyber-threats leaves little trace and poses a huge challenge to those trying to combat cybercrime, and is ultimately making the process of conducting cyber-attacks easier, especially for those with little or no experience or knowledge.

Combating cybercrime requires a different approach from that which has been traditionally taken in respect of most crimes. In contrast to the off-line world where criminals normally need to be physically present at the crime scene and can typically only commit one offence at a time (i.e. rob one bank or burgle one house at a time), criminals in cyberspace do not need to be close to the crime scene, they might never even travel to the target country, and can attack a large number of victims globally with minimum effort and risk by hiding their identity.

iOCTA Recommendations

The trans-national nature of cybercrime poses huge challenges for law enforcement to secure and analyse electronic evidence in countries from where the attacks originate, where there may be no or ineffective legal tools in place or insufficient capacity.

The report recommends that Law enforcement should increase its visibility and presence online to increase public confidence, create awareness campaigns about cyber threats and establish

norms of social conduct in cyberspace. The agencies should acquire necessary skills, expertise, knowledge and tools to perform cybercrime investigations, Big Data analysis and Internet of Everything (IoE) related digital forensics.

The dynamic, evolving and trans-national nature of cybercrime demands an equally diverse and flexible response by law enforcement in close international strategic and operational partnership with all relevant stakeholders. Legislators in the EU need to provide law enforcement with the legal instruments it requires to allow it to disrupt and investigate criminal activity, and to access the information it needs in order to apprehend criminals that undermine public safety and economic interests.

Law enforcement should concentrate on pro-active, intelligence-led approaches to combating cybercrime in a prioritised manner, focusing on high impact areas. In order to measure the scale and scope of cybercrime in a consistent way, there is a need for improved monitoring, reporting and sharing of cybercrime-related data in a standardised EU-wide manner.

Law enforcement should focus with priority on dismantling criminal infrastructure, disrupting the key services that support or enable cybercrime and prosecuting those responsible for malware development, as the numbers of highly skilled cybercriminals are limited and their skills are hard to replace. The increase of both cyber-enabled and facilitated crime should be met with a proportionate increase of relevant resources and skills within law.

The Internet Organised Crime Threat Assessment (iOCTA) informs decision makers at strategic, policy and tactical levels about on-going developments and emerging threats of cybercrime affecting governments, businesses and citizens in the EU.

References and Resources also include:

https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/

http://www.bbc.com/news/technology-39730407