Cyber security woes: WannaCry?

by Patryk Pawlak

For the average user, questions about access and secure use of the internet can be rather abstract. Or at least they were until last week when businesses, institutions and citizens across the globe fell victim to a new strain of ransomware known as WannaCry. The extensive media coverage of the havoc wreaked by this new malicious software – which encrypts a computer's files and then demands payment to unlock them – has exposed the many weaknesses of today's digital environment.

Lessons unlearned

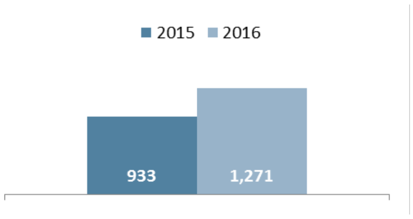
Cyber history provides many examples of crises that should make users, governments and businesses take immediate action. And yet, as WannaCry shows all these stakeholders are slow (or unwilling) to learn the lessons of these past experiences and implement effective countermeasures.

Ransomware – like many other digital threats – has been around for over a decade. When a new wave of more potent malware, dubbed Cryptolocker, emerged in 2013, it was the most sophisticated example to date and is thought to have generated about $3 million in ransom payments. Ransomware is the fastest growing malware threat, with over 4,000 ransomware attacks per day – a 300% increase between 2015 and 2016. This is partly due to the emergence of the Ransomware-as-a-Service (RaaS). The use of hard-to-trace cryptocurrency Bitcoin for ransom payments and the reliance on the 'Tor network' provide anonymity for its users. And yet, as the recent Global Survey on Internet Security and Trust shows, 24% of respondents admitted they would have no idea what to do if their computer were to be hit with ransomware, while only 16% indicated that they would retrieve their data from a backup.

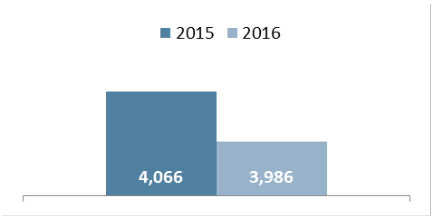
Online bank heists and large-scale attacks on internet infrastructure are becoming more common, too. In April 2016, a malware known as GozNym stole $4 million from more than 24 US and Canadian banks, credit unions and popular e-commerce platforms in just a few days. A week after GozNym's operators unleashed a new European configuration that attacked corporate and investment banks, as well as individual accounts.

Large-scale attacks aimed at paralysing the internet are also growing in strength. In October 2016, two high-powered distributed denial-of-service (DDoS) attacks flooded the servers of DynDNS – a company responsible for translating alphabetic domain names to the numerical IP addresses – until the system could no longer handle the high level of traffic. As a result, an estimated 1,200 websites were no longer accessible, including PayPal, Twitter, Amazon, Netflix and Spotify. The attack was possible due to the proliferation of the Mirai botnet, which hijacked 'Internet of Things' devices without adequate built-in security measures. While both events increased awareness about the vulnerability of internet infrastructure and stressed the importance of public-private cooperation, the perpetrators are always one step ahead.

Average global ransomware detections per day



Zero-day vulnerabilities, annual total
(vulnerabilities not discovered by vendors)



Data source: Internet Security Threat Report 2017, Symantec

It is not (just) business

The failure to prevent the WannaCry attack is a shared responsibility, with negligence seen on several levels. Critical infrastructure operators and service providers – like the UK's National Health Service – are dependent on off-the-shelf security solutions offered by technology companies and service providers. It is, therefore, up to technology designers and manufacturers to ensure that security measures are built-in from the start and not retrofit at later stages.

The role of the private sector – and IT companies in particular – is evolving from a mere provider of services or equipment to an important security provider. In the case of WannaCry, it was clearly Microsoft's decision not to issue security updates in older, unsupported versions of Windows that contributed to such a rapid spread of this ransomware. Such cases show that the issuing of product liability for software and hardware requires closer monitoring and decisive action, especially given the exponential growth of the 'Internet of Things'. But it also makes IT companies part of the conversation about emerging digital inequalities. As the international community continues its efforts towards bridging the digital divide, it would be regrettable to see 'cybersecurity poverty' become an issue in the decades to come. This, of course, does not diminish the importance of increasing awareness about digital risks among users and improving the level of cyber hygiene more broadly.

It is not (just) security

The issue of government responsibility in such instances is also hotly debated – not least because of routinely insufficient manpower and funding for building secure and resilient IT systems. The hacking method employed by the WannaCry perpetrators is believed to have been developed by the National Security Agency (NSA) as part of the government's stockpile of cyber weapons. But the NSA did not foresee that their hacking tool designed to exploit the vulnerabilities of Microsoft products – known as 'Eternal Blue' – would be leaked by a group of hackers called Shadow Brokers. This brings to the fore an important discussion about governments' role in determining which known vulnerabilities should be disclosed to companies and which should be guarded for potential offensive or defensive operations in the future. The bigger underlying question remains: which idea of cybersecurity prevails? One that places individual citizens at the centre and protects them against risks to energy, water or financial infrastructure, or a state-centric vision that focuses on defending citizens against state enemies?

A lesson to learn

With the recognition that cyberattacks will both broaden (thanks to increased connectivity) and deepen (due to technological advances), international cooperation is clearly key to assessing transversal cyber threats. However, the goal of building cyber resilient states and societies is not interpreted in the same way around the globe and there is a risk that certain countries may use cyberattacks to push for stronger government control over the internet. For instance, Russia and China are the main drivers behind the proposal for the International Code of Conduct by the Shanghai Cooperation Organisation – an initiative that the European Union has often criticised over its insufficient guarantees for the lack of both the protection of human rights online and the multi-stakeholder model of the cyber domain. Regarding the increasing vulnerability of digital infrastructure prompted by the unchecked proliferation of the 'Internet of Things' – currently estimated to number 17.6 billion connected devices – the International Telecommunication Union is promoting a new universal identifier known as 'Digital Object Architecture'. However, should this technology become universally applied, governments would gain access to unprecedented amounts of information on citizens, undermining their right to privacy and potentially other civil liberties.

The main remaining lesson, therefore, is the need to focus international efforts on solidifying, streamlining, and advancing the progress achieved already within the numerous existing cooperation frameworks, rather than reinvent the wheel.

Patryk Pawlak is the Brussels Executive Officer and is responsible for cyber-related issues at the EUISS.

© EU Institute for Security Studies | QN-AL-17-013-2A-N | ISBN 978-92-9198-520-3 | ISSN 2315-1129 | doi:10.2815/806115