Quick action will best serve telecoms carriers

WannaCry? Accelerated action will best serve telecoms carriers

In May 2015, Juniper published research entitled 'The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation' that predicted the cost of data breaches would quadruple from 2015, hitting a global cost of $2.1 trillion globally by 2019.

As anticipated, cyber-guerillas have been ramping up their campaigns to profit from the misery they bring to the world. The high-profile "WannaCry" ransomware attack over the weekend (just two years into Juniper's predicted four-year nightmare vision) is just the latest. And it is truly tragic: it appears that the attack exploits vulnerabilities that were known by security agencies (at least, allegedly, by the United States National Security Agency – NSA) more than four years ago. Even more tragic, if true, is the assertion that the NSA also created the tools required to launch an attack; tools which are believed to have become available to cyber-criminals.

In contrast, about a week before "WannaCry" made the headlines, there was another attack. It was reported that some customers of O2-Telefonica in Germany have had their bank accounts emptied by cyber-criminals. The attacks required two main steps – the first of which was for the thieves to acquire usernames and passwords to gain access to online banking applications. However, in order to authorize payments requested via the website, the banks used a second mechanism to "authenticate" the customer (so-called two-factor authentication, 2FA). The chosen mechanism, used across a wide range of industries, was to deliver a one-time password (typically 4 to 6 digits) via text messaging (SMS) to the genuine customer's mobile phone. The second part of the attack was, therefore, to intercept that text message that the bank was trying to deliver – and it is this aspect that makes the news significant: it was the first publicly reported case of an attack that leveraged vulnerabilities in carriers' network SS7 signaling.

So how does the SMS interception (and subsequent bank-account-draining) relate to "WannaCry"?

Well, as with "WannaCry", the vulnerability exploited has been known for years – the difference is that the vulnerability of carrier network SS7 signaling was disclosed to the affected carriers, rather than being kept secret and being weaponized by the discoverer.

This early disclosure of vulnerabilities to the systems manufacturers is cited by many as a cornerstone of effective security: provide the manufacturer with the opportunity to fix the vulnerability before malware is created to exploit it. While this sounds logical enough and appears generally to apply well to IT systems, the application of this paradigm to telecoms seems to have hit a road-block.

Despite being increasingly built of the same fabric (software) as any other IT system, upgrading the telecoms network through the addition of security patches just hadn't happened with the required urgency, and this is despite the availability of advanced signaling firewall solutions since the vulnerabilities were first published (late 2014).

Telefonica-O2 have taken a courageous step to go public with this news, and it's probably just the tip of the iceberg. It is extremely likely that customers of other carriers have also been impacted: not just in Germany, but potentially in any country in the world where SMS is used to deliver authentication codes. Furthermore, the vulnerabilities in SS7 signaling go way further than intercepting SMS.

Despite the slow-start to bolstering network signaling security, recently carriers have been accelerating their plans. By sharing their story Telefonica has taken a lead in driving a re-doubling of efforts amongst their peers, to ensure the broader telecoms industry can serve their customers securely.

Moreover, we hope this marks the first step towards a permanently accelerated reaction to cyber-threats. The war against cyber-crime is going to continue, and it's going to continue to evolve. We have the technology ready to tackle the threat – but we need carriers that are equally ready to adopt it.