EUROPEAN CYBERCRIME CENTRE

EC3 EUROPOL

The Hague, January 2017

Intelligence Notification No. 1/2017

CYBER BITS
Series: Trend

Predictions 2017

What happened?

The end of the year and beginning of the new one is usually the time for summaries and attempts to guess what the future will bring. The security industry is no different in this respect, in fact even a forerunner for this. As in past years, security experts prepared in-depth analysis and reports, wrote blog posts, looked into security oriented glass balls and spoke to fortune tellers to offer their best guess of what 2017 will be like. The Cyber Intelligence Team has followed the industry's predictions and, similarly to last year, this Cyber Bits is an attempt to highlight the most popular and probable events from the plethora of threats and challenges that information security might be facing in 2017.

How does it work?

Similarly to last year (and not surprisingly), ransomware keeps holding the number one position in almost all 2017 predictions. In 2016 we saw a rapid development of new ransomware families and ingenious extortion ideas. According to Trend Micro, ransomware growth will plateau in 2017 but attack methods and targets will diversify. Researchers agree that ransomware will attack cloud based data centres. Experts emphasised that ransomware will continue attacking mobile devices, however the focus will change. Mobile devices are usually backed up to the cloud, therefore the success of direct ransom payments to unlock devices is often limited. Researchers at McAfee suggest that mobile malware authors will combine mobile device locks with other forms of attack as credential theft and consequently, we will witness the reappearance of banking Trojans.

According to WatchGuard we will soon see a "Ransomworm" - a type of ransomware designed to duplicate itself, spreading the infection across the entire network.

Tripwire and F-Secure also talk about the "return of the worm" but in the context of Internet of Things (IoT) applications as prime targets. Continuous issues with security in IoT devices allows for easy infections. An affected appliance would contain a code that attempts to copy itself to routers via Wi-Fi. Once a router becomes infected, the worm would try to find and replicate itself to more routers. A Wi-Fi worm is seen as a logical extension of what we have seen last year with Mirai.

Researchers agree that DDoS attacks orchestrated with the use of IoT devices and Mirai-like malware will continue. CISO of LogRhythm goes as far as predicting that in 2017 we could experience a total shutdown of the Internet for up to 24 hours. Such attacks against service oriented websites, news, companies and political sites will become the norm whether conducted for financial gain or any other purpose. Events of this kind are expected to force manufacturers to apply security solutions and develop regulations concerning vendors' responsibilities around IoT device software updates.

It does not come as a surprise that malware is becoming smarter. Cybercriminals will continue to migrate towards script-based malware due to improvements in Machine Learning (ML) solutions. Script-based malware threats are typically tougher to detect, and therefore are becoming increasingly common in both email campaigns and lateral movement. Macro-based malware in particular will keep switching to unexpected formats as an evasion technique. Criminals will continue to hide malicious code in unused sectors, and maliciously modifying master file tables and volume boot records to load malware before security software loads is becoming more prevalent.

The majority of security researchers stressed the importance of the application of Artificial Intelligence (AI) and Machine Learning solutions in threat detection. Development of AI and ML in the past year promises more accurate and intelligent predictions of attacks, however the same solution can be used by criminals to accelerate social engineering and malware attacks.

AI solutions also replace traditional interaction with a computer. The emergence of voice activated AI platforms such as Siri, Google Home or Amazon Echo represents a new level of human and technology convergence. As the line between artificial and human intelligence blurs, machine will become more a part of human beings and human experience according to Forcepoint.

Organisations will continue to look at adaptive and behaviour-based authentication to balance security and operational concerns. Behavioural technologies such as pressure, typing speed and fingerprints will be embedded into newly released products.

2016 was a year of car hacking, and 2017 will be dominated by "Dronejacking". Researchers have presented potential scenarios ranging from intercepting signals and redirecting drones, whereby an attacker could carry out espionage and explosive attacks.

The above outlines what we can expect in terms of technology, however humans are the ones who use these solutions and are often considered the weakest link. While AI and ML solutions advance, researchers believe that social engineering techniques will still bring income to criminals. Business E-mail Compromise is anticipated to increase in the coming months. Hactivism and espionage are here to stay. Cyber-propaganda is expected to become a norm. The explosion of fakes ads and purchased "likes" will erode trust. Groups that are able to navigate public opinion using these means in a strategic manner will be able to achieve their goals. Ghosts from the past aka data breaches will continue to surface. The darkest visions forecast that the first nation state cyber-attacks will be conducted and acknowledged as an act of war and as a consequence it will likely lead to a civilian casualties.
Although cyber war and civilian fatality is still a prediction, many see the implementation of the General Data Protection Regulation (GDPR) as Armageddon, which will affect all companies collecting data on European Union citizens. GDPR will enter into force only in May 2018 but 2017 is going to be a period of preparation and transition.

Why do you need to know?

- Knowing what may come helps to prepare defences.
- Looking to the future and carrying out horizon scanning has become a regular practice in most organisations as it supports the decision making process.

EC3 would welcome feedback on this note. Please mail to **O31@europol.europa.eu**.
(note that "O" is *a letter not a number)*

Resources:

Symantec—https://www.symantec.com/connect/blogs/security-2017-and-beyond-symantec-s-predictions-year-ahead
TrendMicro—http://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017
McAfee—http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf
Watchguard http://www.watchguard.com/wgrd-resource-center/2017-security-predictions/2017-security-predictions-infographic
Forcepoint— https://www.forcepoint.com/sites/default/files/resources/files/2017-security-predictions-infographic-en.pdf
Beyond Trust—https://www.beyondtrust.com/blog/ten-cyber-security-predictions-2017/
Government technology