Summary Report

Internet Security

2018 was a year that has brought significant changes in the cyberthreat landscape. Those changes had as source discrete developments in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors. Monetization motives have contributed to the appearance of crypto-miners in the top 15 threats. State-sponsored activities have led to the assumption that there is a shift towards reducing the use of complex malicious software and infrastructures and going towards low profile social engineering attacks. These developments are the subject of this threat landscape report.

Developments have been achieved from the side of defenders too. Through the emergence of active defence, threat agent profiling has led to a more efficient identification of attack practices and malicious artefacts, leading thus to more efficient defence techniques and attribution rates. Initial successes through the combination of cyberthreat intelligence (CTI) and traditional intelligence have been achieved. This is a clear indication about the need to open cyberthreat intelligence to other related disciplines with the aim to increase quality of assessments and attribution. Finally, defenders have increased the levels of training to compensate skill shortage in the area of cyberthreat intelligence. The vivid interest of stakeholders in such trainings is a clear indicator for their appetite in building capabilities and skills.

Recent political activities have underlined the emergence of various, quite novel developments in the perceived role of cyberspace for society and national security. Cyber-diplomacy, cyber-defence and cyberwar regulation have dominated the headlines. These developments, when transposed to actions, are expected to bring new requirements and new use cases for cyberthreat intelligence. Equally, through these developments, existing structures and processes in the area of cyberspace governance will undergo a considerable revision. These changes will affect international, European and Member States bodies. It is expected that threat actors are going to adapt their activities towards these changes, affecting thus the cyberthreat landscape in the years to come. In summary, the main trends in the 2018's cyberthreat landscape are:

- Mail and phishing messages have become the primary malware infection vector.
- Exploit Kits have lost their importance in the cyberthreat landscape.
- Cryptominers have become an important monetization vector for cyber-criminals.
- State-sponsored agents increasingly target banks by using attack-vectors utilised in cyber-crime.
- Skill and capability building are the main focus of defenders. Public organisations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.
- The technical orientation of most cyberthreat intelligence produced is considered an obstacle towards awareness raising at the level of security and executive management.

- Cyberthreat intelligence needs to respond to increasingly automated attacks through novel approaches to utilization of automated tools and skills.
- The emergence of IoT environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services. The need for generic IoT protection architectures/good practices will remain pressing.
- The absence of cyberthreat intelligence solutions for low-capability organisations/end-users needs to be addressed by vendors and governments.

In 2018, Cyberthreat Intelligence (CTI) has continued improving with regard to good practices, tools, training courses and standards. These developments are the response to an increasing demand for contextualized and actionable information about threats. Just as in 2017, large organisations continue to be the main customer base for CTI. It is worth mentioning, that CTI has matured in concert with other related cybersecurity disciplines, such as Security Operation Centres (SOC), threat hunting and Security Information and Event Management (SIEM). Nevertheless, CTI experts worry about the differences between cycles of cybersecurity related processes. In particular, syncing CTI with Incident Management, Vulnerability Management and Risk management seems to be a necessity in order to keep the focus on incidents that matter for the protection of respective "crown jewels".

Malware

Malware is the most frequently encountered cyberthreat and somehow involved in 30% of all data breach incidents reported334. During the reporting period, there are no evidences of a global malware outbreak similar to the ones that happened during 2017 (i.e. WannaCry and Petya). We have observed, though, the malware landscape evolved and malware authors are adjusting their TTPs in order to maximize their profits and effectiveness rates. Notable observations include the shift from ransomware to cryptojacking, the blurred lines between cyber criminals and cyber espionage actors, the high effectiveness of fileless attack techniques, the decline of exploit kits resulting in increased difficulty of delivering malware as well as the growing mobile threat landscape.

Web based attacks

Web based attacks are those that use web systems and services as the main surface for compromising the victim/target. This includes browser exploitations and injections (including extensions), websites, Content Management System (CMS) exploitation, and web services. For instance, drive-by, watering-hole, redirection and man-in-the-browser attacks are a few known categories of such attacks. Web based attacks continued to be observed as one of the most important threats due to their wide spread surface across the threat landscape, from general ad related spamming campaigns to banking trojans117 and multiple Advanced Persistent Threat (APT) groups118 facilitating such attacks as their techniques to target victims. This threat is expected to increase as more malware and exploitation techniques rely more heavily on it, as a delivery mechanism, during the end-to-end attack path.

Web application attacks

Web Application Attacks are regarded as direct or indirect attempts to exploit a vulnerability or weakness in the services and applications on the web, abusing their APIs, runtime environments or services. In other words, the simple abuse of an active or passive component of a software available via web. Notably, these types of attacks overlap with web-based quite often due the shared services on the application side and attack surface on the threat side. Web applications are becoming more interesting targets for adversaries as more businesses and firms are becoming dependent on web services, both in revenue and reputation. However, the trend of attacks during the reporting period shows a slight decrease in these type of attacks . Nevertheless, more firms are seeing what OWASP categorises as automated attacks143 during their first sixty day of appearance144, showing more efficient and automated exploiting capabilities on the adversary side. On the other side as web applications represent a large part of attacks on the internet, enterprises and organisations are investing more on web applications detection, protection and defense systems in 2018, which presents a positive move in the industry.

Phishing

Phishing is the mechanism of crafting messages that use social engineering techniques so that the recipient will be lured and "take the bait". More specifically, phishers try to lure the recipients of phishing emails and messages to open a malicious attachment, click on an unsafe URL, hand over their credentials via legitimate looking phishing pages, wire money, etc. Phishing is the preferred way of compromising organisations179 and it has been reported that 75% of EU’s Member States disclosed cases of phishing241 . Phishing is so heavily leveraged that over 90% of malware infections and 72% of data breaches in organisations originate from phishing attacks.

Denial of services

(Distributed) Denial of Services is one of the highly impactful threats in cyber landscape that has been targeting almost any business or organisation. It has been quite clear that preserving a solid defence for such threat has become extensively important for different organisations. According to Arbor Networks, the strong demand for mitigation services provided by managed service providers in this field is notable with financial services, e-commerce, cloud providers and governments on the top. Also, Law enforcement activities in this realm have played a key role for fighting against such malicious activities by running operations to take down services like “webstressor.org” during the first half of 2018. Although this has been a great achievement, DDoS for hire services like this are not few and still the landscape is seeing activities with similar characteristics. On the other side the increase in the number of connected services globally and their dependency on the Internet of Things (IOTs) to run and facilitate such services raised concerns over threats like DoS attacks to potentially cause nation wide failures for businesses and critical systems. One example of such services is the concept of connected hospitals and related services. Yet with all the mitigation and preventative activities across the world reports and researches suggest that the number of DDoS activities are on the rise (16% increase). Although we might not be observing too many large attacks.

Spam

Spam is the abusive use of email and messaging technologies to flood users with unsolicited messages. Spam dates back to the beginning of the Internet and is mainly distributed by large spam botnets. Although it is continuously reducing in volume, spam is still one of the major attack vectors observed in the wild. During the last years spam has evolved, (i.e. spam via social media and messengers) and it is assessed that it will continue to be used241. Spam is regarded a threat because of its low cost to send messages while it is time consuming and costly for spam recipients and service providers in terms of network bandwidth and storage. The good news here is that, the coordinated law enforcement activities for botnet takedowns and the advances in anti-spam technologies have resulted in lowering the spam numbers during the last years.

Conclusions

Non-targeted threats spreading contagiously in the cyberspace tend to last longer (or not to disappear at all). This is mainly due to the reduced adoption by individuals and organizations of cyber hygiene practices (cryptographic keys and user credentials protection, etc.), adherence to good security practices (revised security policies, two face authentication (2FA), etc.) and systems still operating without any security updates, to name a few. The same is valid to justify the lengthy time taken by many organizations to acknowledge and respond to an incident. This situation urges organizations to include cybersecurity into their risk management functions and identify clear strategies to anticipate and/or respond to crises.

Cyberthreat intelligence has evolved in the last 7-8 years from the need to follow up on a rapidly changing cyberthreat landscape. This rapid development was purely technology driven and narrowly scoped. Its relevance highly matured traditional intelligence has been recently recognized. The advantages that can be materialised when coupling traditional intelligence and cyberthreat intelligence have not yet been implemented. Individual events in the reporting period549 have demonstrated the increases in efficiency when combining these two disciplines. Though the deployment of cyberdefence practices may facilitate mutual fertilization between these two disciplines, public and private organisation will need to benefit from these synergies too. This is yet another opportunity for Europe - but also for international players -to implement a synergy that will boost cybersecurity to new quality and maturity level.