Overview

On October 20, 2020, the European Union Agency for Cybersecurity (ENISA) issued its annual Threat Landscape 2020 publication summarizing the main cyber threats and providing insights on the evolution of threats encountered between January 2019-April 2020.

For the first time, this year's publication is divided into 22 separate reports; it comes with no surprises that it concludes that cyberattacks are generally becoming more sophisticated, targeted and often undetected.

In this alert, we discuss one of the 22 reports, i.e., the Sectoral and Thematic Analysis Report reviewing cyber threats to specific sectors (health, finance, manufacturing, education, etc.) and technologies, particularly 5G, Internet of Things (IoT) and smart cars. The report presents the most common techniques of cyberattacks and the level of exposure of different sectors, many of which were affected heavily in the recent pandemic. These insights are drawn by using contextualized cyber threat intelligence (CTI) based on sectoral incident statistics. A tool that has become widely spread for cybersecurity assessments.

COVID-19 – The Super Spreader of Cyberattacks

As with all business operations, COVID-19 has affected the cybersecurity arena, especially as IT departments were forced to decentralize the targets shifted from corporations to individuals who have seen the most cyberattacks in the past year. It also comes as no surprise that the health/medical sector has been increasingly targeted by cyberattacks in the past year - mainly through malware, being the biggest cybersecurity threat over the past year, insider threat and web application attacks. Malicious attackers have used phishing campaigns and ransomware attacks to obtain sensitive data.

Since the beginning of the pandemic, cybercriminals have been particularly attracted and driven by financial rewards related to the COVID-19 funding. The pandemic further affected the education and public administration sector. The vast amount of funding related to the COVID-19 pandemic has led to increased attacks on social services. Educational research programs were increasingly affected by cyber espionage, as a method to obtain insider information related to COVID-19 research. Similarly, cybercriminals, in an attempt to leak information, increasingly attacked the professional and digital services industry by web application attacks, insider threats and malware.

Sectoral Analysis and Its Inherent Imperfections
While ENISA calls for the urgent need of sectoral incident statistics to ensure the analysis of sectoral threats, it also points to uncertainties stemming from this approach. The numerous incidents that are classified as “unknown” (i.e., both not capable of being allocated to a given sector, for between 1.5% to 5% of the cases but also where the attack techniques are not determined – for around 15% of the cases), may lead to a distorted portrayal of the order of targets of cyberattacks. A siloed approach to a sectoral incident statistic by definition does not capture the dependencies of attacks across verticals risking a duplication in numbers. Another challenge, common to data collection, is comparing statistics when the criteria for collecting the relevant data is not consistent among all collectors. These are just some of the challenges of data gathering related to cyberattacks the report raised.

Emerging Technologies Require a Different Approach to Assessing Cyber Threats

In its analysis, ENISA addresses, for the first time, the use of contextualized CTI to reduce the risk of cyberattacks on emerging technology sectors, such as 5G, IoT and smart cars.

Unlike established technological solutions, emerging technologies rarely have sufficient data sets of prior cyberattacks, making it difficult to develop and rely on sectoral incident statistics and ultimately to analyze and mitigate future risks.

In order to apply CTI to emerging technologies, ENISA performed a threat assessment of asset categories instead. The result is a seven-page summary of the identification of key asset groups and their corresponding threats exposure of 5G networks, IoT and smart cars. We provide some elements on each of them below.

- While 5G opens up unprecedented opportunities for innovative use cases across industries, cybercriminals are already attacking the network’s vulnerabilities. 5G’s dynamic software-based systems have far more traffic routing points with every routing point increasing the attack surface for cybercriminals. Moreover, the 5G network enables device authentication, device encryption, device ID, and credentialing, but the proliferation of end points, as encouraged by the technology also carry security dangers. Vulnerabilities in devices could be exploited by attackers to access confidential proprietary data, steal user information or inject dormant malware.

- The exponential use of IoT enables the deployment of more devices, sensors, and sophisticated software applications. It is the foundation to bring smart homes, smart cities or smart offices to life. Yet, with whole environments such as cities, utility grids or homes being dependent on technology, any potential failure causes more damage. Cybercriminals motivated by the potential extent of their attack may be able to shut down whole cities and deny individuals access to their homes or offices. Often times, malware or additional harmful software is installed to disrupt the IoT, and to exploit users and data for materialistic gains, such as intellectual property theft, identity theft, brand theft, and fraud.

- The report noted that smart cars are exposed to an active threat frontier that continuously expands in scale and sophistication. The inherent vulnerability of the software, on which smart cars are based on, lead to numerous threats. Some of which include identity theft, general theft as well as the introduction of any malicious software controlling the vehicle. Bluetooth attacks, for example, can also easily be used to steal sensitive data. It will soon become apparent whether the automotive industry will embrace this new challenge and fulfill its responsibilities to effectively address cyber risks while continuously advancing its technologies.

This report is yet another reason as to why it is crucial and indispensable to organizations operating in today’s technological world to know the cyberspace they are in, but even more importantly who would be their enemies.

“If you know the enemy and you know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle” (the Art of War, S. Tzu).

Practices
Privacy & Cybersecurity

© 2021 STEPTOE & JOHNSON LLP. ALL RIGHTS RESERVED. ATTORNEY ADVERTISING.