Threats which waiting "The information security" in 2018

مرکز سمت للدراسات
SMT Studies Center

Tuesday, 2 January 2018

special reading 6

Many experts concluded about foreseeing the situation of "The information security" in 2018, to a number of trends which most of them agree on the nature and quality of the successive threats and are likely to face the informational pattern in the next year, especially when it comes to information networking and e-security.

The ISF report, in addition to the “Secureworks” report and many other experts and researchers in the fields of technology, concluded that there are many security threats facing IT networks and the qualitative shift in the nature of cyber-attacks, and we can summarized it in:

The escalation of cyber threats(1)

In 2018 , It is likely that the cyber-attacks will intensify in accordance with different objectives, all of which will lead to the economic segment as well as the political qualifiers, as well as the qualitative development that makes it difficult to detect and follow up the perpetrators of network criminals. In the event that it falls within the framework of "electronic ransom". For example, the phenomenon of electronic currencies such as “Biqtuin” which allows to obscure the movement of funds through the use of disguises such as mixing and changing the addresses of currencies and the so-called "electronic currency laundering."

The escalation of electronic piracy

In 2018, it is likely to witness a continued e-mail attacks and email counterfeiting attacks, also it is expected that this type of attack will increase because of the poor capabilities and high profitability of attackers. Such as the e-mail piracy of the UAE

*Political studies unit

ambassador in Washington, Yusuf Al Otaiba, and the publication of important documents on the UAE's policies about a number of files in the Arab region.

The situation of "cyber-attacks"(2) is likely to be activated, with the expectation of the return of the Russian-American international inversion theory as well as the Chinese and Iranian moves, so it is likely to be among the biggest threats to the world in 2018, especially since 2017 has witnessed attacks From North Korea, Iran and Russia against agencies, banks and military installations around the world.

The escalation of electronic fraud

Threats associated with cyber-attacks against banks are expected to continue, especially which the "organized crime groups" are increasingly using e-fraud to generate revenue. Some of these groups will also focus on banks operating in areas outside Europe and the United States, which are known to adopt relatively weak defense strategies for cyber-attacks, and are less complex than their counterparts in the West.

*Political studies unit

Malware attacks under the "electronic fraud" umbrella will not be limited to the major banks, as asset management institutions, large savings account holders, and payroll supervisors are also likely to be targeted by the “electronic fraud”.

The organizing of the artificial intelligence’s techniques:

The use of artificial intelligence and machine learning will continue to protect data in 2018. The number of information security experts and institutions who are aware of the benefits of artificial intelligence and machine learning to simplify and improve attacks detection and response, especially when This is supported by analysis of attack data by expert analysts.

Also, the experience of the UAE community is the most prominent in the Arab world in relying on applications of artificial intelligence in its daily life. The results of the "Digital Consumer" study published by the Executive Management and Strategic Consulting in August 2017, which included 26 thousand people In 26 countries, that more than two-thirds of UAE society, equivalent to about 68%, rely on smart applications, compared to 31% in other countries surveyed, as well as "satisfaction" more than three-quarters of respondents (76% UAE) to use artificial intelligence applications for only 44% And 86% of UAE respondents were interested in using new chipsets, compared to 77% in Singapore, 63% in the United States and 52% in the United Kingdom(3).

*Political studies unit

The escalation of using the digital transactions (block-chain)

Block-chain is a revolutionary technique that will have significant implications for management, marketing, finance and all jobs requiring a broker in 2018.

The UAE and Saudi Arabia have announced their intention to issue the first official digital currency to be traded between the two countries through the cluster chain system. Also in August 2017, six of the world's largest banks agreed to move towards the use of the mass chain in the circulation of digital money.

*Political studies unit

Also, the collapse of the global financial system in 2008 was the key to the creation of such a new currency exchange system without the need for banks and financial institutions. For example, despite the wide influence of Bitquin as a digital currency, and the biggest effect would be the same system as the "block- chain."

On the other hand, the escalation of the "block- chain" system poses two problems: (4)the first relates to transparency, especially in the absence of a central authority controlling and managing this system, and thus can be held accountable in the event of a system malfunction or piracy or fraud. The second is cost-related. Although the “block- chain” system itself is inexpensive, it requires a large number of computers with special specifications to enable transactions and transfers, as well as consuming a large amount of energy to terminate transactions, Recent high energy prices

Overall, we expected in 2018 to be "the uncertainty information" and is expected to be the scene of a qualitative reproduction in the world of technology and areas of "information security" support, with the aim of giving a new look to some existing old techniques, These operations are more focused on the field of “artificial intelligence”, in response to the growing structural gaps in information security and global digital security, which were revealed in 2017. And the most prominent of these are: the dilemma of cyber defense, threats of information monopoly and the risks of electronic currencies, which constitutes a great threat to the global security of information networks.

*Political studies unit

Resources

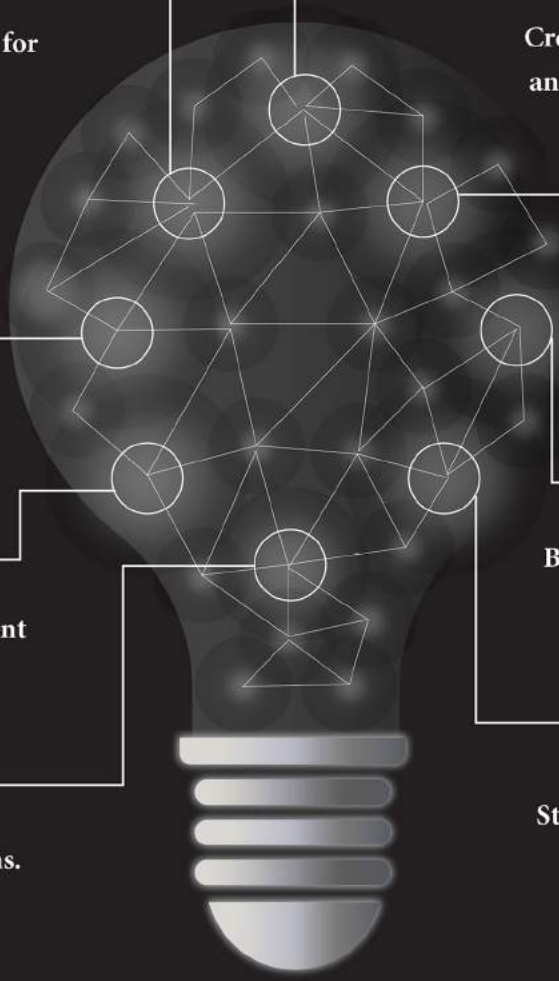
1 - https://www.secureworks.com/

2 - URI FRIEDMAN AND ANNABELLE TIMSIT, Global Conflicts to Watch in 2018,The Atlantic, https://goo.gl/q9mBPe

3 - إيهاب خليفة، إدارة التكنولوجيا: لماذا تهتم الإمارات بتنظيم تقنيات الذكاء الاصطناعي؟ مركز المستقبل للأبحاث والدراسات المتقدمة، 20 أكتوبر 2017. https://goo.gl/ddQj5h

4 - إيهاب خليفة، ثورة المعاملات الرقمية: لماذا تهدد "سلسلة الكتلة" ملايين الوظائف في العالم؟ مركز المستقبل للأبحاث والدراسات المتقدمة، 19 ديسمبر 2017. https://goo.gl/pLcx4h

What We Do



Providing studies and consultations for governments, organizations and decisions-makers

Create monitoring. Planning and analysis teams .FOCUS GROUP

Plans and strategies in global relations

Defeating Challenges Plans and recommendations

Businesses and organizations reputation management

Studies of : attitude assessment

Statistics and analytical studies

Forming studies and results teams. Discussion group

info@smtcenter.net

www.smtcenter.net/en @SMT_CENTER_EN @Smtcenteren @smt_center_en