The Evolution of Cyber Threat. Cyber security trends in Romania

Cătălin Aramă
Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)
catalin.arama@cert.ro

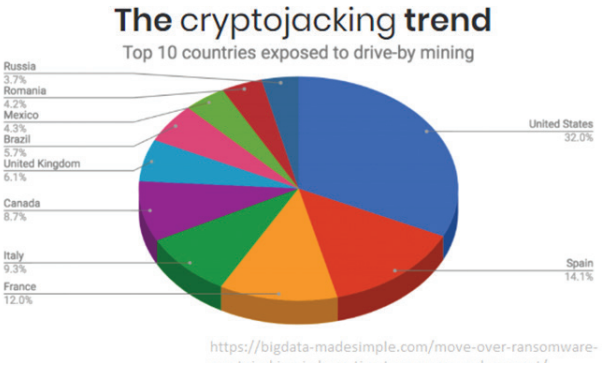
Abstract: Cyber attacks have seen an upward trend, being considered by the World Economic Forum as the fifth major global concern for 2019. A major part of the criminal activity has shifted from physical space to cyberspace. From the perspective of CERT-RO's specific activities and competences, 2018 saw an increase both in intensity and in the complexity of cyber-threatening modes, particularly, financial cyber-aggression. This motivation of cyber-aggression is and will continue to be one of the main factors that will determine cyber attackers to develop increasingly sophisticated attack techniques to harness all the opportunities that technology offers, to find new targets and exploit their vulnerabilities, even if it is thought to improve our daily lives.
Keywords: cyber security, cyber threats, cyber attacks, cryptojacking, malware

INTRODUCTION

Thus, in 2018, phishing cyber attacks have grown significantly. According to State of the Phish Report 2019, 83 percent of global info security respondents experienced phishing attacks in 2018 which is up from 76 percent in the previous year [1].

Relying on a well-engineered social engineering tailored to the needs of different types of consumers, the attackers explored and exploited both the classic e-mail method sent in the form of offers from known companies as well as the new/less used method to date phishing by phone.

Another way of displaying cyber threats in 2018 is cryptojacking attacks. In essence, it is about the use by attackers of the user resources (processing power) of sites for cryptomining malware.



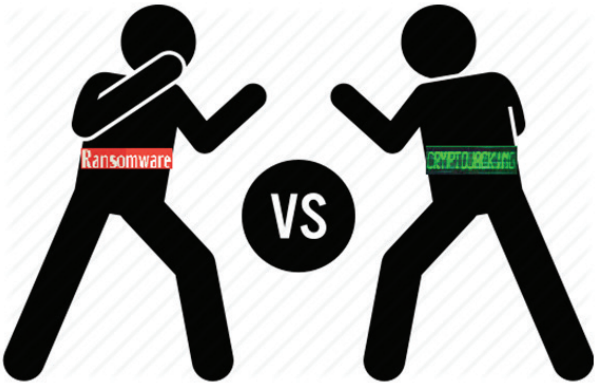
The number of crypto mining attacks increased by 956% in 2018 compared to the first half of 2017, cybersecurity firm Trend Micro reported on 29 August.

Over 787,000 crypto mining attacks were recorded in the first half of 2018, according to Trend Micro's Midyear Security Roundup report, bearing in mind that in the same period of 2017,

there were only 74,500 detections. These include both legal mining tools used in an incorrect and intentional manner.

According to the report, there have been identified "47 new cryptocurrency mining malware families," meaning that new hackers appeared on the market rather than former ones resumed their malware [2].

The ransomware attacks continue to be one of the tools used by cybercriminals to obtain undue benefits.



For the first time since 2013, according to the Internet Security Threat Report from February 2019, it was observed a decrease in ransomware activity during 2018, with the overall number of ransomware infections on endpoints dropping by 20 percent. WannaCry, copycat versions, and Petya, continued to inflate infection figures. When these worms are stripped out from the statistics, the drop in infection numbers is steeper: a 52 percent fall.

The danger of ransomware not only comes from the fact that it causes financial damage but also from the fact that it can lead to the degradation of human lives in cases when infrastructure of some health institutions are attacked.

Considering the Internet's topology and the fact that the work of many institutions/companies is based on interconnected computer systems and networks, a cyber-attack is not only local, but it can take effect in several states simultaneously. In this context, EU Directive 1148/2016 on measures for a high common level of network and information security was adopted by the European Union so that each EU Member State adopts and implements a set of measures that can guarantee an adequate level of cyber security.

The Directive was transposed into national law by Law no. 362/2018 and establishes obligations for security of information security for service providers in the seven economic sectors (energy, health, transport, banking, financial markets, water transport sector, digital infrastructure) and for digital service providers; to notify the security incidents identified. At the same time, the framework for cooperation at national level and participation at European and international level in the field of cyber security is established.

In the context of the latest legislative changes in Romania in the field of cyber security, a recipe recommended by one of the specialists from Kaspersky Lab for clubitc, caught our attention:

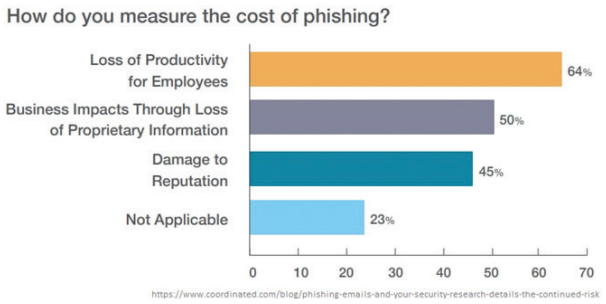
TOP 10 most widespread cryptor families

	Name	Verdicts	%
1	WannaCry	Trojan-Ransom.Win32.Wanna	28.72%
2	(generic verdict)	Trojan-Ransom.Win32.Phny	13.70%
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	12.31%
4	Cryakl	Trojan-Ransom.Win32.Cryakl	9.30%
5	(generic verdict)	Trojan-Ransom.Win32.Gen	2.99%
6	(generic verdict)	Trojan-Ransom.Win32.Cryptor	2.58%
7	PolyRansom/VirLock	Virus.Win32.PolyRansom	2.33%
8	Shade	Trojan-Ransom.Win32.Shade	1,99%
9	Crysis	Trojan-Ransom.Win32.Crusis	1.70%
10	(generic verdict)	Trojan-Ransom.Win32.Encoder	1.70%

https://securelist.com/it-threat-evoluat-evolution-q3-2018-statistics/88689/

"Companies that manage to create a culture of cyber security are the winning ones. Staff training in cyber security should be a priority" [3].

According to their research and other industry specialists, most cyber security incidents in a company are caused by employees' actions - over 80%.



The lack of training employees over opening suspicious emails, not changing the password periodically or installing dubious applications on the phone, elements that can translate into a security breach, do not just lead to financial losses. According to a graph in the State of the Phish 2018, the cost of a phishing attack is also reflected in the loss of employee productivity, business impact through loss of proprietary information and damage to reputation.

Besides an effective security solution tailored to the company profile, it is very important to be aware of the importance of cyber threats among employees. As a general rule, awareness should be a permanent effort to educate employees about company security policies and cyber threats, along with safeguards. Social engineering techniques continue to have a very high success rate, so companies' representatives should pay more attention.

In a context where Romania ranks first places in top countries where users faced the greatest risk of online infection, top countries exposed to drive-by mining, the secret of the success of an IT security program should be constancy and evaluation. As Bogdan Pismicenco said "Just like in a diet or sports performance, nothing changes overnight or after a two or three-week effort": for notable results, a lifestyle change is needed. In the case of companies, a rethink of cyber security is necessary. It can't be something that you do once a year and have the desired results, but is an ongoing effort" [3].

CONCLUSIONS

The world we live in becomes more and more interdependent day by day, largely due to developments in information and communication technology. Statistics highlight a change in the dynamics of cyber attacks. User education is imperative, whether we talk about users as employees or simply users in private life. Cyber security culture must assumed at individual level regardless of what role you have.

References

[1] *STATE OF THE PHISHING 2019 REPORT.* Last accessed on 14 March 2019 at: https://www. proofpoint.com/us/resources/threat-reports/state-of-phish

[2] *Unseen Threats, Imminent Losses* 2018 Midyear Security Roundup Last accessed on 14 March 2019 https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf

[3] Bogdan Pismicenco, Kaspersky Lab: *Companiile care reușesc să creeze o cultură a securității cibernetice sunt cele câștigătoare. Pregătirea angajaților în domeniul securității cibernetice ar trebui să fie o prioritate*. Last accessed on 14 March 2019 http://www.clubitc.ro/2019/01/04/bogdan-pismicenco-kaspersky-lab-companiile-care-reusesc-sa-creeze-o-cultura-a-securitatii-cibernetice-sunt-cele-castigatoare-pregatirea-angajatilor-in-domeniul-securitatii-cibernetice-ar-trebui-sa/