A THREAT FOR THE TRAINS: RANSOMWARE AS A NEW RISK

Daniel Vaczi and Tamas Szadeczky*

Óbuda University, Doctoral School of Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.17.1.1
Preliminary report

Received: 11 October 2018.
Accepted: 31 December 2018.

ABSTRACT

Nowadays we cannot speak about cybersecurity as a simple problem. It is not just about users cannot properly use the devices because of a malware settle in their computers.

Now professionals have to work in a more complex system. The information technology meshes most of our life. Begin with people use their smartphones over that companies lead most of their processes via computers.

Nations want that their citizens can live in a healthier, more comfortable, economical place, so they started to think about how can they warrant a better life. Result in this governments started to make critical infrastructure more economical with the help of information technology. That is how Smart Cities began to evolve. However, bringing into practice these innovations is still not enough. If we use any technology, we shall use it securely, that is why we must build our advanced city as a secure Smart City. If not, our systems can be attacked in different ways.

In the view of last years, we can accept, that ransomware can make considerable problems in different systems. Last time NotPetya caused many problems in Ukraine's infrastructure. The metro and the airport information technology systems were also victims of this malicious code. The security of the transportation is essential not just because of public transport one of the leading part of Smart Cities, but because in these public vehicles many people travel day by day, so these are critical infrastructures.

This article is processing what could happen if Hungarian train management systems got attacked by ransomware. What are the risks and how should we protect against them?

KEYWORDS

malware, ransomware, transport management systems

CLASSIFICATION

ACM: K.6.5.2
JEL: R41

*Corresponding author, η: szadeczky.tamas@kvk.uni-obuda.hu; +36 1 666 5170;
1084 Budapest, Tavaszmezo u. 17., Hungary

INTRODUCTION

As computers adhere to our life, we should prepare for new threats. Besides that information technologies help us to live our life easier, faster and more comfortable we can also run into trouble because of them. If we are looking around in the place where we are right now, there is an excellent chance that we can find many electrical devices. As time is moving forward, those objects become smarter and smarter. In this case, it just means that our articles of personal use are connected to the internet and may be integrated with a processor what helps to the electrical stuff serve our growing latent needs. Not just our homes and offices are going to be smarter with the help of the Internet of Things (IoT) devices, but also our cities. The concept of Smart Cities is more known and popular day by day. It means that we would like to turn our Planet and our environment more livable. For example, we would like to use the energy sources efficiently and also we would like to optimise our transport no matter if it is personal or public. Nowadays we can hear a lot about smart cars using artificial intelligence, which is one of the new and future ways of transporting. On the other hand many urban development programs purpose the expansion of public transport with the help of networking, analysis and machine learning. As we can see, those developments are heading to computers more heavily.

Unfortunately, this modern, information technology (IT) centralised word has a dark side also. In the last years, we can see new attacking trend in the cyberspace [1]. It has many dimensions. Cyberwars, an attack against companies or persons. On the one hand, we can found offensive where the attacker does not care who will be the victim; the only goal is the successfulness. On the other hand, there is a pre-elected person, group or company. The motivation of the attacker also can be different for example information and money gathering, ransom, gaining access to systems, destroying infrastructures, political or military motivation, and influencing.

ABOUT THE RESEARCH

Nowadays ransomware is one of those threats what makes the IT security professionals annoyed. This malware can block a company’s life if the security system is unwell designed. The problem in a standard IT system is easily visible. Ransomware encrypts the whole disk with the data of the company, or it makes the device unreachable locks the input tools are locked. The higher problem when in a not protected critical infrastructure is under attack. The public transportation’s IT systems are like that. Weakly protected, but if a planned attack can be successful, it can cause serious injuries or even death.

The authors researched the threat of ransomware in the available scientific articles, including categorisations, main scientific issues and protection possibilities. The focus of the research was the applicability of general ransomware issues to railway traffic control systems, to determine its susceptibility. The article is a preliminary research article about ongoing research shown in the acknowledgements.

RANSOMWARE AS A THREAT

The attackers have many opportunities to achieve their goal. They can use many tools on the different platforms depending on what is their motivation. In recent years, so-called ransomware attacks got attention. If ransomware successfully infects a device the content of it will not be available. Depending on the type of malware, it can just lock the screen and in the same time prohibit the access or encrypt the important files of the user or the Master Boot Record (MBR), perhaps other file indexes.

If we see the lifecycle of a typical ransomware attack, the first step is the distribution with the help of e-mail attachments, website compromises or similar [2; p.152]. Then the malware infects the victim system and starts to communicate with the encryption-key servers. After the connection is made, it searches for the commonly used file types, and it is typically renaming, encrypting and renaming them again. If the victim is on the company network, the backup methodology will be attacked, too [2; p.151]. At the end of the process the user will see a ransom message what says if the user pays, usually, in Bitcoin or other cryptocurrencies, the attacker will provide the decryption key.

Maybe those are not the most sophisticated attacks, but they are effective. Because of such an attack the user is going to realise the importance of information security while losing personal data. If the family photos become encrypted and finally lost, that is something what everybody can realise. But not just the private sector can be a victim of ransomware. The public organisations and the governmental sector also can be attacked by ransomware. In this case, we can easily concede that critical infrastructures (e.g., transport, banking, energy, health sector) and critical information infrastructure (e.g., telecommunication, internet access, satellites) are an excellent goal to the criminals or maybe other malicious nations [3].

There were two huge global ransomware attacks in 2017. One of it is called WannaCry (also known as WanaCrypt0r or WannaCrypt) [4]. Among other things the British health sector had a severe breakdown because of that malware campaign. The other globally concerned one from 2017 is the NotPetya (in other names: Petya, Petrwrap, ExtPetr). It is mostly attacked targets in Ukraine, but it also impaired one of the biggest container ship companies, the Danish A.P. Moller – Maersk Group. As a result of the campaign the shipping company still has unknown containers. Metro and Airport IT system were also targets of this attack. As we can see in these examples, critical infrastructures are deeply concerned with this problem.

Because writing a ransomware code is one of the most straightforward malware programming tasks, attackers use it frequently. We also have to remark, that nowadays anybody can buy ransomware as a service. It has a name, called RaaS (Ransomware-as-a-Service) [2; p.145].

TYPES OF RANSOMWARE

Al-rimy et al. defined a ransomware taxonomy in their paper, shown in Figure 1 [2]. They distinguished consumer and organisation target based attacks. They also separated this malware what is the attacked platform (e.g., PC, mobile, cloud). In our view, the most essential taxonomy is the severity based one. We can distinguish between those that are detrimental and what is only called scareware. The latter is just a fake warning. With the help of this trick, the attacker asks for a ransom without real damage. That ransomware what cause damage can be categorised as locker and crypto. If the malware only locks the services and limit the applications, we call it locker-ransomware. If it encrypts the user's files named crypto-ransomware. Depending on the cypher algorithm it can be classified as symmetric crypto-ransomware (SCR), asymmetric crypto-ransomware (ACR) and hybrid key crypto-ransomware (HCR). The SCR operates mostly DES, AES and RC4, the ARC use such as RSA and HCR integrate both previous algorithms.

PROTECTION AGAINST RANSOMWARE

As we could see via WannaCry and NotPetya, well-written ransomware can cause huge trouble. In extreme cases, it threats also life. In the IT security profession, most of the people agree that the security awareness is crucial [5]. The users are not careful, do not think on security in typical situations and because of those, the attacker can trick them easily. Maybe we think that in critical infrastructure the co-workers are more aware, but they can also be spoofed [6].

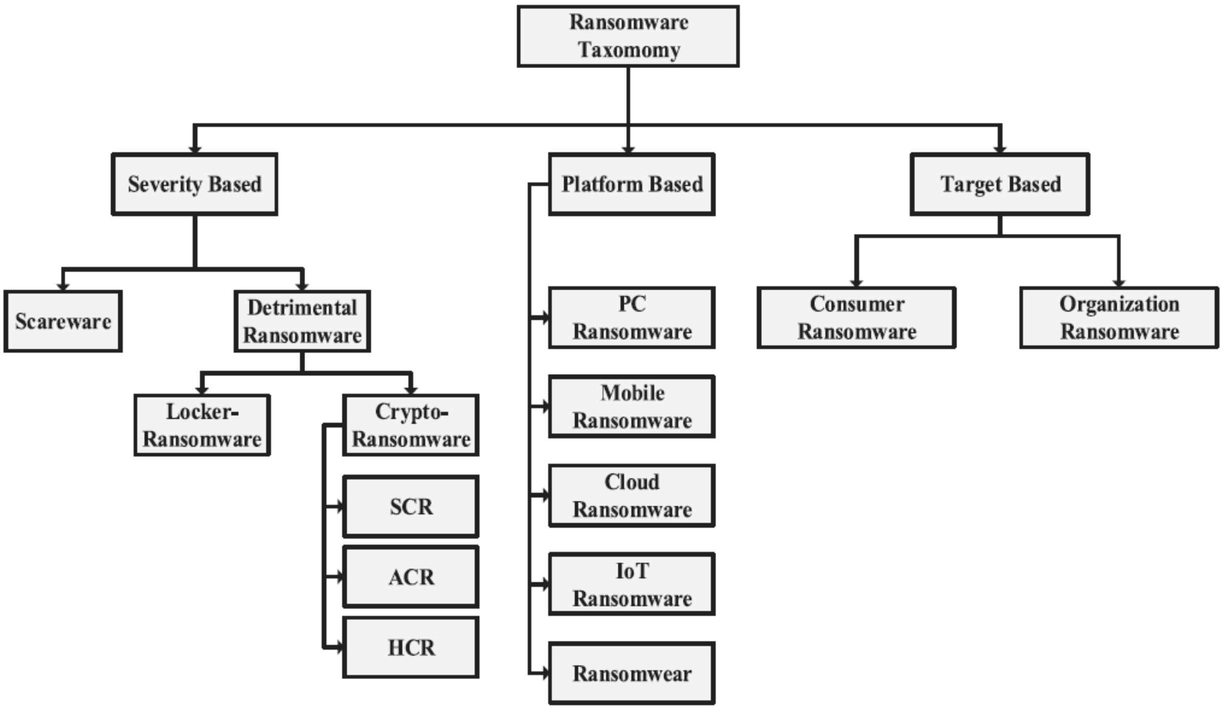

Figure 1. Taxonomy of ransomware [2].

The first step against any cyber-attack is to raise awareness and education level. Of course, this is not the only way to protect ourselves and our IT systems in the cyberspace. There is a need for technical countermeasures also, like system hardening and virus protection.

If a user opens an infected email attachment or surf a hacked webpage, a ransomware dropper can be downloaded. Those are the most common way to be attacked. However, if our IT system and processes are well prepared the malware has less chance to work. Steven Furnell and David Emm in their study introduce the three most crucial steps of defence against these malicious codes [4]. “A” as Anti-malware, “B” as Back-up and “C” as critical patching. Building an alarm system what gives us a signal if something strange or dangerous came into our system is necessary, even if it is not 100 % trustworthy. Then if we have a proper offline backup process in our system, we are able to recover the stored data. Finally, if we update the operating system, firmware and all possible software the ransomware cannot exploit the known vulnerabilities.

On the one hand those steps are too general, but if we look deep into the problem, those are necessary but not sufficient. Against the ransomware, the employees should notice if they are under attack and they have to know the needed steps to minimalise the loss. Knowing about the infected links and attachments is not equal to staying clear of them. Another easy but effective action is the unplugging of the computer. It can save many essential files.

SUSCEPTIBILITY OF RAILWAY TRAFFIC CONTROL

Transportation is always a crucial element of critical infrastructure. Sometimes people can forget how important the railway transportation is. It is not only about personal travel, but also a significant percent of cargo is transported by trains. As we can see, this kind of transportation is significantly vulnerable to the information technology aspect. There are many railway-related services what are now IT based. Timetable, geolocation, and surveillance of the trains are based on traditional IT-infrastructure. Typically this means a centralised IT service is running on a small number of servers. In this case, not just backups, but also high redundancy is required, which is a question of investment. If the geolocation-based controlling system became hamstring, it might have a severe impact on the train control. In this way, the standard traffic management process will not work. The fallback solution is the manual control of the switches, stations and trains, which have a low throughput. Safety systems are based more on specialised hardware. However, similarly to industrial control systems, if we connect them to the internet, they will be susceptible to hacker attacks [7]. If the security modules of the modern railway control systems are exploited with ransomware, many people's lives will be jeopardised. The ticketing systems typically include web interfaces. Thus web services and web applications might be hacked. If ransomware infects a ticketing system front- or backend, the online and ticket office sales and also the ticket control might have stopped. Thus not just the buying, but also the travel is jeopardised. Those things can cause a shortage of the income and the dissatisfaction of the travellers. Interconnection interfaces between international train management systems are also implemented via the internet.

Even in the traffic control systems virtualisation and sometimes private clouds take place. From the CIA-triad (Confidentiality, Integrity and Availability) of information security, integrity deals with protection against malicious or unintentional modification of data stored in storages and sent through communication channels. According to standard information security, practice redundancy and error checking are the most common measures of integrity controls. In virtual data storages also concurrent and collaborative access issues became important. Availability is the ability to access data whenever required. Redundant data storage and processing, backup and business continuity management are the standard controls for that. Virtual systems are scalable, intelligent, flexible and redundant when they are built according to general best practice. However, the hypervisor is a new single point of failure because it is generally not redundant. Despite generally proper security controls, virtualised systems are not invulnerable. Amazon EC2 Easter outage in 2011 April was an example of cloud failures when more thousands of websites were unreachable because of a configuration error, which was possibly a human error. According to a study, the human factor is always an issue in information security. Therefore awareness should be increased [8, 9].

CONCLUSIONS

One can see that ransomware can cause massive damages. Maybe the impact is only a financial loss, but it can also risk human life. The only way to defend that system is proactivity.

In the case of railway companies, many different systems are being used. Also, some of them are non-conventional PC systems, but industrial IT elements. IT management should deal with the patching of those systems, despite the heterogeneous environment. Using anti-malware and universal threat management (UTM) is a matter of course. Last but not least we must raise the security awareness of the employees to avoid spreading the ransomware on the network with clicking on some malicious attachments.

ACKNOWLEDGMENTS

This article is based on the research conducted within the project "The Development of Integrated Intelligent Railway Information and Safety System", Application number: GINOP--2.2.1-15-2017-00098.

REFERENCES

[1] Yaqoob, I. et al.: *The rise of ransomware and emerging security challenges in the Internet of Things.*
Computer Networks **129**(2), 444-458, 2017,
http://dx.doi.org/10.1016/j.comnet.2017.09.003,

[2] Al-rimy, B.A.S.; Maarof, M.A. and Shaid, S.Z.M.: *Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions*.
Computers & Security **74**, 144-166, 2018,
http://dx.doi.org/10.1016/j.cose.2018.01.001,

[3] Rajnai, Z. and Puskas B.: *Requirements of the installation of the critical informational infrastructure and its management*.
Interdisciplinary Description of Complex Systems **13**(1), 48-56, 2015,
http://dx.doi.org/10.7906/indecs.13.1.7,

[4] Furnell, S. and Emm, D.: *The ABC of ransomware protection.*
Computer Fraud & Security **2017**(10), 5-11, 2017,
http://dx.doi.org/10.1016/S1361-3723(17)30089-1,

[5] Szadeczky, T.: *Information Security Law and Strategy in Hungary*.
Academic and Applied Research in Military and Public Management Science **14**(4), 281-289, 2015,

[6] Kiss, D. and Váczi D.: *Risks of attacks against human networks of companies and critical infrastructures according to network sciences*.
Hadtudomány **28**(1), 151-168, 2018,
http://dx.doi.org/10.17047/HADTUD.2018.28.1.151,

[7] Zimba, A.; Wang, Z. and Chen, H.: *Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems*.
ICT Express **4**(1), 14-18, 2018,
http://dx.doi.org/10.1016/j.icte.2017.12.007,

[8] Metalidou, E. et al.: *The Human Factor of Information Security: Unintentional Damage Perspective.*
Procedia – Social and Behavioral Sciences **147**, 424-428, 2014,
http://dx.doi.org/10.1016/j.sbspro.2014.07.133,

[9] Iantovics, L.B. et al.: *Review of Recent Trends in Measuring the Computing Systems Intelligence.*
Broad Research in Artificial Intelligence and Neuroscience **9**(2), 77-94, 2018,