RANSOMWARE IN INDUSTRIAL CONTROL SYSTEMS. WHAT COMES AFTER WANNACRY AND PETYA GLOBAL ATTACKS?

MARCELO AYRES BRANQUINHO
Ti Safe Segurança da Informação, Brazil

ABSTRACT

The cyber security of critical global infrastructures was tested last May 12nd with the global attack via Wannacry, a technically simple Ransomware that used an old Windows operating system vulnerability to propagate. Although it was an important attack and with serious consequences, it was an attack that could be restrained with the use of basic countermeasures like the simple update of the Windows operating system. This paper aims to detail the serious consequences of a Ransomware infection in critical infrastructure Industrial Control Systems networks. The work was developed based on the good practices of ANSI / ISA-99 (current IEC 62443) and aims to raise the awareness of global companies regarding the immediate need for investments in cyber security in industrial networks. To illustrate the consequences of a Ransomware attack on industrial control systems, case studies of two attacks on Brazilian industrial control systems were listed. The first attack occurred in a furniture factory and the second in a control center of a major power utility. In both cases this study detailed the type of Malware used, the consequences of the attack, financial losses and countermeasures made to return to operation. The conclusion of the work sparks reflection on what is to come after the Wannacry and Petya global attacks, mentioning the new ones that are being developed at this time, and what impact should be expected if these new attacks hit critical infrastructure networks with low level of cyber security implemented.

Keywords: ransomware, security, malware, attacks.

1 INTRODUCTION

Critical infrastructures are facilities, services and goods that, if interrupted or destroyed, will have a serious social, economic and/or political impact. Here, we can mention some examples, as companies dedicated to:

- Generation and distribution of electricity;
- Telecommunications;
- Water supply;
- Food production and distribution;
- Heating (natural gas, fuel oil);
- Public health;
- Transportation Systems;
- Financial services;
- Security Services (police, army);

Infrastructure Control Systems have the role of keeping our society and economy functioning, either by providing energy for our homes and our work, by routing our telephone calls, by purifying the water we drink, by heating or cooling our homes, by caring for our patients, or by keeping our banks functioning in a way that facilitates the turn of capital by our economy, or even our armed forces that defend us from external threats, in short, all those activities that, even if we do not realize, are gears that without which the big

WIT Transactions on The Built Environment, Vol 174, © 2018 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE170301

machine which is our country, would cease to function or would do so precariously. So it is important to highlight what these assets are, their locations and how to protect them, whether in a terrorist attack, a war or even a natural disaster.

The current supervisory control and data acquisition systems that make up critical infrastructure control networks do not look like their early versions, launched in the 1970s. At that time, when a company was automated, operations were implemented separately in "islands" and humans were responsible for synchronizing the production steps. Currently, supervisory systems have complex functionalities, integrating these "islands" and composing a fundamental database for decision making. As a natural consequence, enterprise resource planning systems of the corporate networks were connected to the automation environment for the provisioning and production control.

Despite the evolution of the systems, the automation technology has not incorporated known security controls in Information Technology, giving vulnerabilities that, when exploited, can generate damages to the health, the environment and the infrastructure of the plant, besides Interruptions in production. In the integration of automation technology) and I.T. networks, development platforms have also suffered (and continue to suffer) a migration process. From the old supervisory systems developed in operating platforms in Unix systems, executed in specific machines like the Digital Vax and Alpha, it is observed the change to systems developed for platforms in x86 architecture (like Windows Server and Linux). This migration allowed the reduction of costs with infrastructure and application development, as well as drastically reduced the development time of projects. However, the changes caused the automation networks to live with new vulnerabilities that they were not designed to handle [1].

2 THE EVOLUTION OF HACKING

In the early days of computing, young people spent days and nights studying every bit in search of vulnerabilities and other shortcomings in the programs of that time. Their dream was to explore some system of a famous company, or some government organization, their goals were varied, some said they liked adrenaline, some overcome challenges, some only sought fame and recognition from the community, everything was just adventure and ego games. Over time, not only the interests of young nerds were changing, people from the corporate world began to see in it a huge source of espionage and a select and lucrative market.

The activity of hackers and hacktivists (activists who use digital means to practice their actions) from all over the world in corporate and government systems are reported by the press every day. These attacks are especially striking because they show how their attack tools are increasingly powerful and available to the general public, enabling even the least knowledgeable to attack their targets.

Institutional sites, user databases and passwords, and the famous "*defacements*" no longer seem so attractive, and attackers have realized that their attacks can be far more powerful and destructive if carried out against industrial systems because they have very shallow security - when it exists - and have far greater consequences.

If we imagine that the water we drink, the electricity that comes to our homes, the signaling of mass transport (including air traffic), the control of hydroelectric and nuclear power plants, are controlled by computer systems that may be potential targets for hackers, we have a scenario with a potentially large risk. What would happen, for example, in the case of an invasion in control systems of a water treatment plant responsible for the control of the chemical reagents that are mixed to purify the water that the population drinks? What if a hacking attack were able to disable, even temporarily, hydroelectric and nuclear power plants causing blackouts in cities? All these threats to critical infrastructure are now very real.

3 MALWARE, WEAPON OF HACKERS

Malware (Malicious Software), is a common term in the world of information security, but a bit confusing to other professionals. Commonly known and widespread as Viruses, malware groups any software or program created with the intent to host functions to penetrate systems, break security rules, steal information, and serve as the basis for other illegal and/or harmful operations. The development of modern Malware is today the main hacker activity in the world, allowing them a quick financial return, mainly through attacks by a specific type of malware, the Ransomware.

Ransomware is a type of malware that restricts access to the infected system and charges a redemption (usually in bitcoins) so that access can be restored, if redemption does not occur, files can be lost and even exposed on the Internet.

Ransomware can spread within an industrial control system network in a number of ways, including:

- Through exploits. software or scripts designed to exploit a particular vulnerability and gain code execution.
- Through removable media (Flash Drives, External Hard Disks) with autorun enabled, exploits to the file browser, DLL injection or deliberate execution.
- Through shared folders on the network, just like removable media.
- Through communication between servers of different automation plants (object linking and embedding for process control, for example).
- By the use of mobile gateways in the automation network and direct communication with the internet without filters exposing to malicious URLs or malicious files.
- Through email attachments and malicious links on social networks.

Ransomware infections are one of the biggest nightmares of industrial network managers. In addition to the destructive features inherent in Ransomware, scatter mechanisms typically flood automation networks with unwanted data packets and gradually affect the response time of the real-time network until it completely paralyzes it. If compared to an information technology network, the consequences are much worse as they directly affect operations on supervisory control and data acquisition systems by:

- • Blocking access to supervisory stations and human machine interfaces;
- • Encrypting supervisory control and data acquisition programming stations;
- • Encrypting historical and production databases;
- • Encrypting engineering workstations;
- • Blocking access to utility systems;
- • Infecting other plants through the automation network and site-to-site virtual private networks.

4 THE FIRST RANSOMWARE GLOBAL ATTACKS

May 12th, 2017 was marked by a series of attacks on a global scale, making use of the updated version of a crypto-ransomware named WannaCrypt0r. News and reports indicate that public and private organizations around the world have been impacted.

WannaCrypt0r attacks start their organization cycle through a phishing e-mail attack, which includes a malicious link or PDF document. The successful phishing attack results in the delivery of the WannaCrypt0r ransomware on the local machine and consequently attempts to spread on a large-scale network using SMB protocol, attacking the "EternalBlue" vulnerability (CVE-2017-0144) in Microsoft Windows operating systems. This vulnerability was corrected by Microsoft in March 2017 with the MS17-010 patch.

In the UK, a researcher known by the nickname "Malware Tech" was able to accidentally stop the spread of the attack. The researcher realized that the program was trying to contact an unusual internet address (iuqerfsodp9ifjaposdfjhgosurijfae wrwergwea.com), which was not registered. He spent the equivalent of $35 to buy this address and noticed that the registration operation interrupted the program's process of propagating [2].

However, the damage had already been done and the consequences were disastrous for businesses and governments around the globe. More than 200,000 organizations in 150 countries, including energy distribution companies, railways, automobile industries and governments have been affected.

As anticipated, shortly after the attacks by WannaCrypt0r, a new generation of attacks even more powerful occurred on June 27th, 2017, this time based on a new generation of Ransomware called NotPetya.

NotPetya's modus operandi is basically the same as WannaCrypt0r, but with one important difference: WannaCrypt0r encrypted access to files while NotPetya completely blocks access to the computer.

The machine infected by NotPetya immediately loses its ability to offer access to Windows. While WannaCrypt0r made hospitals not have access to patient files, for example, NotPetya can hide the operating system and prevent the victim from making any use of the machine [3].

Companies located in several countries also suffered losses with the wave of attacks. In Ukraine, while trying to make a simple cash withdrawal at ATMs, users were greeted with a message from hackers requesting an amount equivalent to U$300.00 to be able to access their bank account and perform operations [4].

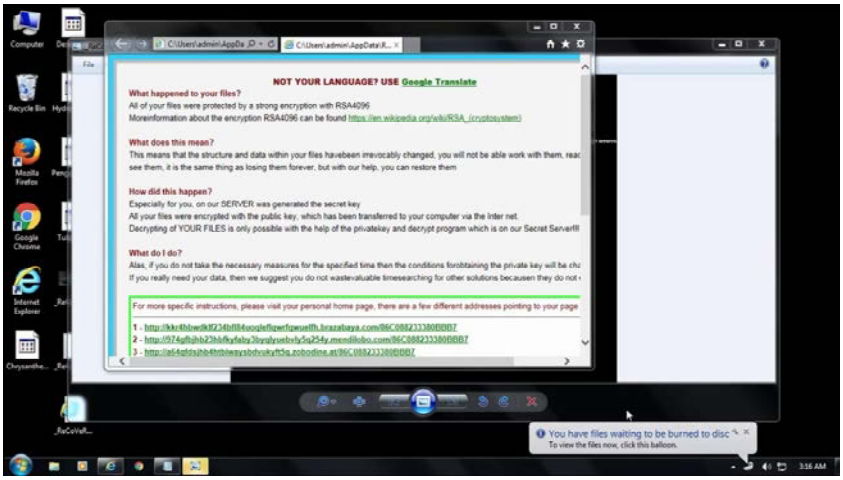
5 CASE STUDIES OF RANSOMWARE ATTACKS IN BRAZIL

To illustrate the consequences of an attack by Ransomware on critical infrastructures, this study presents two cases of attacks in Brazilian industrial control systems.

The first attack occurred in a furniture factory located in the state of Goias, in central-western Brazil. In this case a type of Ransomware called cryptoRSA4096-Ransomware infected the supervisory control and data acquisition systems (Windows operating system-based) supervisory stations and industry programming machines.

This attack led the industry to shut down for 15 days. With this the industry lost the data of customers and suppliers, the payroll and the supervision of the production. Although the amount of redemption demanded by the hackers was relatively low (approximately U$3,061.00), the company refused to pay, which generated a loss of approximately U$100,000.00 because of the stoppage in production and delays in deliveries.

The second case of attack by Ransomware occurred at a control center of a major power utility located in southern Brazil. In this case the Ransomware used for the attack was the CryptoLocker, which infected supervisory machines inside the control center.



NOT YOUR LANGUAGE? USE Google Translate

What happened to your files?
All of your files were protected by a strong encryption with RSA4096
Moreinformation about the encryption RSA4096 can be found https://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files havebeen irrevocably changed, you will not be able work with them, reac
see them, it is the same thing as losing them forever, but with our help, you can restore them

How did this happen?
Especially for you, on our SERVER was generated the secret key
All your files were encrypted with the public key, which has been transferred to your computer via the Inter net
Decrypting of YOUR FILES is only possible with the help of the privatekey and decrypt program which is on our Secret Server!!!

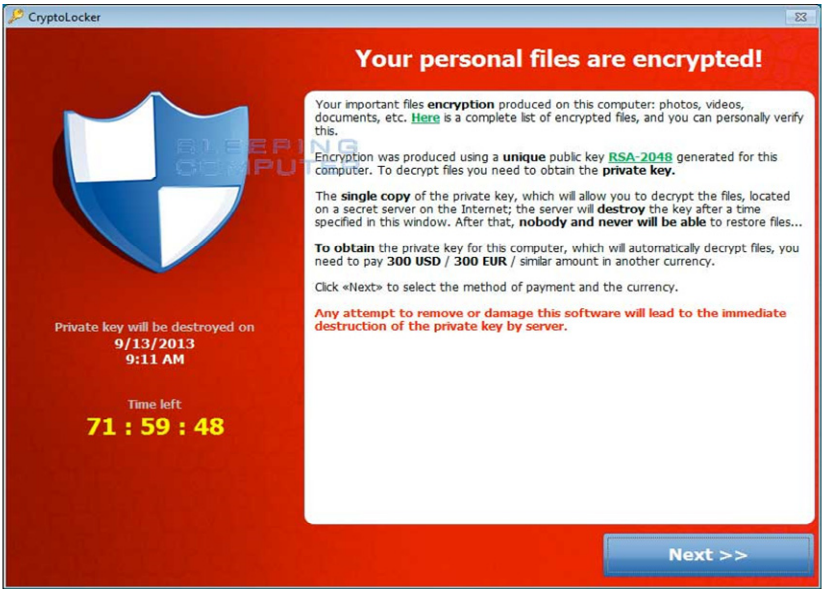
What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions forobtaining the private key will be cha
If you really need your data, then we suggest you do not wastevaluable timesearching for other solutions becausen they do not

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page

1 - http://kkr4hbwdktf234bf84uoglefiqwrfqwuelfh.brazabaya.com/86C088233380BBB7
2 - http://974gfbjhb23hbfkyfaby3byqlyuebvly5q254y.mendilobo.com/86C088233380BBB7
3 - http://a64qfdsjhb4htbiwaysbdvukyft5q.zobodine.at/86C088233380BBB7

You have files waiting to be burned to disc
To view the files now, click this balloon.

Figure 1: Print screen of infected supervision station.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/13/2013
9:11 AM

Time left
71 : 59 : 48

Figure 2: Print screen of an infected supervision station.

The Infection Vector was a flash drive used in the USB port of the supervisory station. Ransomware has spread through shared files and folders mapped on the network infecting 3 other monitoring stations located in the same segment of the automation network. The main consequence was the momentary loss of supervision and control of energy distribution.

The hackers asked for a ransom of U$ 300.00 per infected machine (in the case 4 machines were infected), but the utility did not pay the ransom. No financial loss occurred because the control was automatically transferred to a second control center that was not physically connected to the main control center. Infected machines could be reinstalled through clean, current backups.

6 CONCLUSION: WHAT TO EXPECT FROM THE FUTURE?

The analysis of the WannaCrypt0r and NotPetya malicious codes reveals something in common: both made use of the same security vulnerability called *EternalBlue*. Exploit was featured as part of the files published by the hacking group known as Shadow Brokers. The group claimed to have stolen EternalBlue as part of a series of hacking tools from the US National Security Agency.

It is strongly believed that the NSA was responsible for the development of the exploit- which is officially known as MS17-010 – or purchased from others.

Since ShadowBrokers published EternalBlue online, it was used in the development of malware by hacker groups. The culminations of this development were WannaCrypt0r and NotPetya [5].

It seems that these global attacks were just the beginning of something much worse that is about to come. The success of the first global attacks will surely encourage hacking groups around the world to develop increasingly powerful Ransomwares focused on shutting down essential services in industrial control systems networks. Like EternalBlue, there are many other exploits (including those exploiting zero day vulnerabilities) that will certainly be used by hacking groups in upcoming attacks.

The trend is that each new global attack will be more powerful than the previous one, and that it will use vulnerabilities without known patches, which will mean that the attacks will be unstoppable.

Critical global infrastructures should immediately protect themselves by increasing investment in cyber security and improving the maturity of their defenses according to the best practices of the global cyber security frameworks such as the IEC-62433, or they will be victims of the new and powerful attacks that will emerge very soon.

REFERENCES

[1] Segurança de Automação Industrial e SCADA/Marcelo Ayres Branquinho et al. 1. ed. - Rio de Janeiro: Elsevier, 2014.

[2] Ten Sistemas e Redes (No date) Ransomware e o ataque global do dia 12 de maio. Available: http://www.ten.com.br/ransomware-e-o-ataque-global-do-dia-12-de-maio/ Accessed on: 1 Aug. 2017.

[3] Tecnologia IG (No date) Entenda por que o ataque com ransomware NotPetya é mais grave que o WannaCry. Available: http://tecnologia.ig.com.br/2017-06-27/ransomware-notpetya-wannacry.html. Accessed on: 1 Aug. 2017

[4] Tecnoblogs Tecnologia e Informações (No date) Vírus Petya atinge Bancos, Aeroportos Hospitais e até Chernobyl. Available: http://tecnoblogs.com.br/virus-petya-atinge-bancos-aeroportos-hospitais-e-ate-chernobyl/ Accessed on: 1 Aug. 2017.

[5] Wired (No date), WannaCry and Petya are just the beginning. It's going to be an "ugly few years". Available: http://www.wired.co.uk/article/whats-next-petya-ransomware-wannacry Accessed on: 1 Aug. 2017.