Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems

Aaron Zimba, Zhaoshun Wang, Hongsong Chen

PII: S2405-9595(17)30330-2
DOI: https://doi.org/10.1016/j.icte.2017.12.007
Reference: ICTE 123

To appear in: *ICT Express*

Received date : 3 November 2017
Accepted date : 27 December 2017

Please cite this article as: A. Zimba, Z. Wang, H. Chen, Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems, *ICT Express* (2018), https://doi.org/10.1016/j.icte.2017.12.007

ICT Express
Information & Communications Technology

Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems

Aaron Zimba[1]*, Zhaoshun Wang[2], Hongsong Chen[3]

[1] Department of Computer Science and Technology, University of Science and Technology Beijing, Beijing, China (e-mail: azimba@xs.ustb.edu.cn)
[2] Department of Computer Science and Technology, University of Science and Technology Beijing, Beijing, China (e-mail: zhswang@sohu.com)
[3] Department of Computer Science and Technology, University of Science and Technology Beijing, Beijing, China (e-mail: chenhs@ustb.edu.cn)
* Corresponding author

ABSTRACT
The inevitable integration of critical infrastructure to public networks has exposed the underlying industrial control systems to various attack vectors. In this paper, we model multi-stage crypto ransomware attacks, which are today an emerging cyber threat to critical infrastructure. We evaluate our modeling approach using multi-stage attacks by the infamous WannaCry ransomware. The static malware analysis results uncover the techniques employed by the ransomware to discover vulnerable nodes in different SCADA and production subnets, and for the subsequent network propagation. Based on the uncovered artefacts, we recommend a cascaded network segmentation approach, which prioritizes the security of production network devices.

Index Terms: Critical Infrastructure, Cyber-attack, Industrial Control System, Crypto Ransomware, Vulnerability

I. INTRODUCTION

Industrial Control Systems (ICS) oversee many of today's Critical Infrastructure (CI), which include smart grids, electrical power plants, nuclear power plants, air traffic control, water and waste treatment plants, transportation etc. CI provides essential services and resources required for basic human needs. Due to their importance, they have traditionally been safeguarded and secluded from other publicly available systems [1]. The emphasis, as far as security is concerned, has been on physical security and environmental safety. This is evidenced by the tight physical security and safety systems present in almost all critical infrastructure. Notwithstanding the aforementioned, the advent of robust and advanced technologies, the Internet in particular, has seen the gradual disappearance of the "air-gap" between CI and public systems. The demand to enhance productivity by reducing manufacturing and operational costs has led to the adoption of technologies that have eventually led to the integration of CIs into public systems such as the Internet [2]. Moreover, the integration of enterprise and corporate systems with the Internet have provided new avenues for real-time data acquisition, which has considerably fostered efficiency. Nevertheless, considering the diversity of CI sectors, the integration of CIs with public or corporate networks has been diverse and lack a standard secure framework [3]. Thus, the approach in securing these integrated systems has largely been determined by the different security goals of organizations, which are inadvertently dictated by the underlying business objectives. Since the IP protocol (the protocol upon which private and public networks are built) is unsecure, cyber-attacks have found their way into CIs, which for a long time have been believed to be isolated and secure. This has resulted in cyber-threats, where the different network design patterns in CIs have resulted in a number of attack entry points into CIs. Figure 1 depicts the threat model against CI and ICS, which shows the various attack entry points.

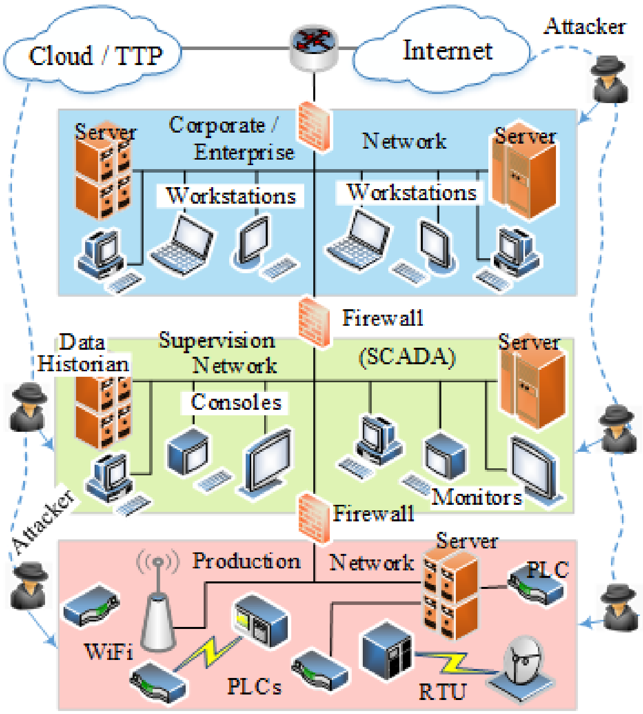


Figure 1. Threat model against CI and ICS

The production network is similar to the physical world and comprises sensors, actuators, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs) for remote access, and general Wi-Fi and RF networks. In some of the network design patterns, these low level components are directly connected to the Internet [4]. This is one entry point for malwares such as ransomwares. Some network design patterns only have a supervision network, which houses the Supervisory Control And Data Acquisition (SCADA) system to connect to the Internet. The attacker can thus infiltrate the supervision network upon vulnerability discovery and elevate the attack to the production network if possible. Some network design patterns connect the corporate and enterprise networks via a cascaded approach as in the Purdue Model [5]. In this case, the attack has to infiltrate the corporate network in order to reach the underlying ICS, provided such a design is categorically secured via a defense-in-depth strategy. The worst-case scenario is where the three networks are not properly segmented but designed in a single broadcast domain without proper demarcation points. Therefore, given a certain network design pattern, an attacker can, upon discovery of a vulnerability, deposit malware in the corresponding CI network. In this study, we aim to model and characterize the attack techniques employed by cyber attackers to infiltrate CIs through publicly accessible networks. To validate our modeling approach, we use ransomware attacks through reverse engineering (static malware analysis). We perform source code analysis on the infamous WannaCry ransomware, which has not spared CI, and uncover the underlying network attack techniques. In Section II, we present the attack model of ransomware on CI based on the corresponding threat model. We perform static code disassembly and malware analysis in Section III. The recommended best practices based on the observed attack patterns and the conclusions are provided in Section IV.

II. THE ATTACK MODEL

As shown in Figure 1, CI and ICS, once connected to the Internet whether directly or otherwise, present three points of entry through which the attacker can deliver the ransomware payload. The entry points are denoted as:

1) Corporate Network (CN)
2) Trusted Third Party (TTP) i.e. cloud outsourcing or technical support
3) Direct Internet Connection (DIC)

We model the attack process using an attack graph with three entry nodes denoting three infiltration sources. The other three sections of the graph denote vulnerable node instances in the three network types found in typical CI and ICS as illustrated in Figure 1. The edges between the node instances denote the exploitation of a vulnerability, which further enhances the traversal of the ransomware across the network. The threat actor of our attack model is a ransomware with worm-like capabilities (as those witnessed in WannaCry), which is capable of propagating the payload to adjacent network upon vulnerability exploitation [6]. The resultant attack model is shown in Figure 2. The target of any crypto ransomware attack is to breach availability by encrypting a victim's files, thereby rendering them inaccessible. In our model, the ransomware seeks to attack the SCADA or production networks to make CI and ICS data inaccessible. Therefore, even though ransomware attacks are indiscriminate, the presence of a ransomware in the corporate or enterprise network of a CI implementing the Purdue model does not constitute an actual attack. Rather, the network is used as a pivot to traverse the underlying SCADA or production network.

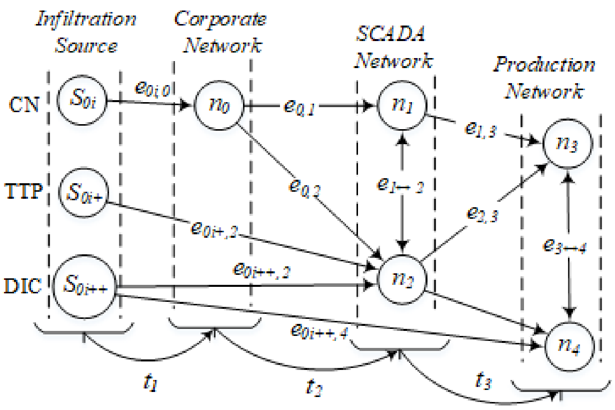


Figure 2. Attack model against CI and ICS

We differentiate three infiltration sources CN, TTP and DIC denoted by three sources S_{0i}, S_{0i+}, and S_{0i++}, respectively. The attack edge $e_{0i,0}$ denotes infiltration of the corporate network via an insider or outsider attack. We postulate the Markov assumption [7], and therefore constrain the history of how the corporate network gets infiltrated. However, exploit kits and email attachments are not uncommon in this regard [8]. It is clear that the attack edges $e_{0,1}$ and $e_{0,2}$ depict the exploitation of the enterprise network as a pivot to the supervision network. This is possible when the corporate subnet shares a trust relationship with the supervision network. In environments with firewalls and strict access policies through ACLs, the malware would leverage permissible network protocols such as SMB in the case of WannaCry. At node n_1, the malware checks whether the host being exploited has already been infected, and if has not, it proceeds to encrypt the targeted files. It then scans the current (SCADA) and adjacent (production) network for the sought after network vulnerabilities, and this is denoted by attack edges $e_{1,2}$ and $e_{1,3}$, respectively. Upon discovery of vulnerable node 3, it repeats the process as that at node n_1. On the other hand, if node n_1 has already been infected, the malware proceeds to the already discovered network via attack edges $e_{0,2}$and $e_{2,4}$. The attack paths generated from the first infiltration source CN are:

$$CN: \begin{cases} S_{0i} \rightarrow n_0 \rightarrow n_1 \\ S_{0i} \rightarrow n_0 \rightarrow n_2 \rightarrow n_4 \\ S_{0i} \rightarrow n_0 \rightarrow n_1 \rightarrow n_3 \rightarrow n_4 \end{cases}$$

It is worth noting that the attack edges $e_{1\leftrightarrow 2}$ and $e_{3\leftrightarrow 4}$ are bidirectional to denote two distinct attack instances, one where the node being exploited has already been infected and the other where it has not. In the former, the malware does not scan the local and adjacent networks, because the presence of an infection is an indicator that the networks have already been scanned.

In light of the above, the attack paths generated from the second infiltration source TTP following the same logic are:

$$TTP: \begin{cases} S_{0i+} \to n_2 \\ S_{0i+} \to n_2 \to n_4 \\ S_{0i+} \to n_2 \to n_3 \to n_4 \end{cases}$$

Although some attack paths generated in CN appear to be of the same weight as those of TTP, it is worth noting that the latter paths originate from a domain beyond the jurisdiction of CI and ICS. Therefore, they do not have the same degree of mitigation approach.

From the above, the attack paths generated by the malware originating from the DIC infiltration source are:

$$DIC: \begin{cases} S_{0i++} \to n_2 \\ S_{0i++} \to n_2 \to n_4 \\ S_{0i++} \to n_2 \to n_3 \to n_4 \\ S_{0i++} \to n_4 \end{cases}$$

The attack path $S_{0i++} \to n_4$ is of paramount interest to the attacker, because it delivers the malware right into the core of the CI through Internet-facing devices. Since the malware uses vulnerable nodes in different subnets as pivot nodes to get to the target, the attacks are henceforth classified as multi-stage attacks. Having defined the attack paths from the infiltration sources to the core of CI, we now perform malware analysis on the WannaCry ransomware, which attacked parts of the CI and ICS [9]. From the observed attack techniques, we further infer which of the above attack paths are applicable.

III. Illustrative Data and Analysis

Considering the nature of the attacking malware, we reverse engineer the code to extract three features of interest that enable the ransomware to effectuate a multi-stage DOS attack on CI. Figure 3 shows the steps we implemented to achieve the aforesaid.

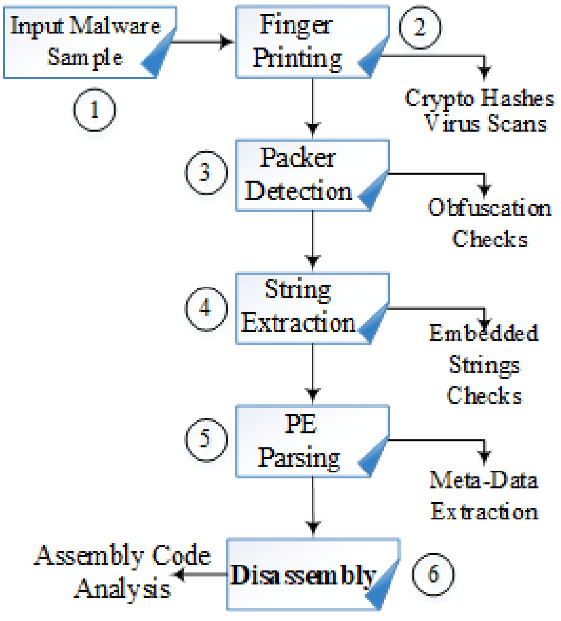


Figure 3. Static malware analysis workflow

In stage 1, we specify the ransomware family and strain. A crypto ransomware variant, WannaCry, was selected instead of a locker ransomware. WannaCry encrypts only the data files of a particular extension, unlike a locker ransomware, which attacks system files. In stage 2, we determine the ransomware's identity by running corresponding cryptographic hashes. We end this stage of external feature extraction by verifying the sample's authenticity using Virustotal.com with a confirmed score of 58/64. The sample's cryptographic hashes are:

MD5 : 5333fdb8a34f790538a9bd70de1011403

SHA-1 **:** f7c1a3b4e856eb523ae35eebcb7e9847ccda19e5

SHA256 :5adbd3f97a9c106aef9d9d6456c3fee0622ee93 92be323f42da0e41f5e7d5189

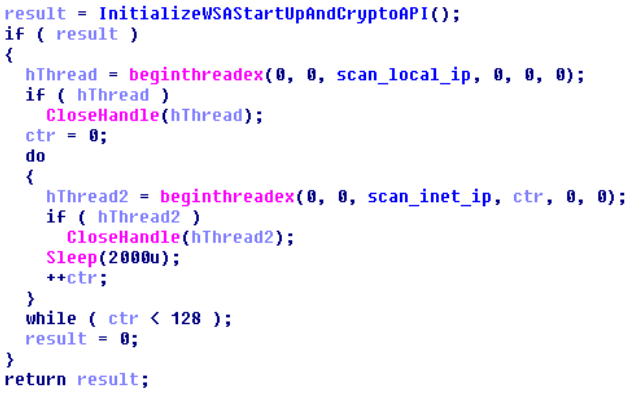
We check the packing to determine whether the sample's internal logic is obfuscated to disguise its operation in stage 3. We check for strings in stage 4 to find some encryption routines and to find out whether the sample uses a kill-switch domain. The sample for meta-data extraction is parsed in stage 5 and the source code is disassembled with an interactive disassembler in stage 6.

At runtime, the ransomware imports the external DLLs *{ADVAPI32.dll, KERNEL32.dll, MSVCP60.dll, MSVCRT.dll, WININET.dll, WS2_32.dll, iphlpapi.dll}* and loads the libraries *{secur32.dll, shell32.dll, wsock32, ws2_32, rpcrt4.dll, advapi32.dll}*. Clearly, the sample utilizes the Windows API and is thus tied to the Windows operating system. This implies that devices in CI running the Windows operating system are susceptible to this ransomware. It is not uncommon for CI devices connected to the Internet to be running Microsoft Windows, e.g. an oscilloscope at CERN running Windows XP [10]. The ransomware checks for the presence of a mutex *Global\MsWinZonesCacheCounterMutexA* before encryption to check if the host being exploited has already been infected. This is equivalent to the first attack action the malware performs upon infiltration of a device in the node set $\{n_0, n_1, n_2, n_3, n_4\}$, as depicted in the attack model. If the mutex exists, the ransomware does not encrypt the target files, but uses the `GetAdapterInfo ()` function to get subnet information in order to scan the entire local subnet scope. This is equivalent to attack actions $e_{1\leftrightarrow 2}$ and $e_{3\leftrightarrow 4}$ in the attack model. The ransomware leverages the EternalBlue exploit, which exploits the implementation of the SMB protocol [11] on Port 445. This implies that a CI network with devices running Windows operating system with file sharing via SMBv1 is a breeding ground for WannaCry. This exploit uses CVE vulnerabilities CVE-2017-0144 [12]. We can convert this CVSS base score value to a probability:

$$Pr(n_i \mid \forall\, c \,\in\, R_i) = {}^{BS_i}/_{10} \qquad (1)$$

This gives a marginal probability value of infecting a vulnerable node exhibiting the vulnerability $\Pr(n_i) = 0.81$. The highest likelihood of infiltrating a device in the core of the CI is thus $\Pr(n_4|S_{0i++})$ via attack edge $e_{0i++,4}$. Since $\Pr(n_i) \leq 1$ for nodes in the attack network, $\Pr(n_4|S_{0i++}) > \{\Pr(n_4|S_{0i}), \Pr(n_4|S_{0i+})\}$ always holds true, as far as the supervision and production networks are concerned. This implies that the devices directly connected to the public Internet in a CI pose the highest threat of infiltration to the aforementioned ransomware.

It is worth noting that though the local IP subnet scan is multithreaded, the ransomware limits it to 10 IP addresses per scan, to avoid detection from the CPU overhead. Further, in an effort to scan external IP networks, the ransomware spawns 128 threads to scan public IP addresses. This would be a subset of scanning adjacent networks as portrayed in the attack model. Figure 4 shows a code snippet of WannaCry's local and external IP network scans.



```
result = InitializeWSAStartUpAndCryptoAPI();
if ( result )
{
  hThread = beginthreadex(0, 0, scan_local_ip, 0, 0, 0);
  if ( hThread )
    CloseHandle(hThread);
  ctr = 0;
  do
  {
    hThread2 = beginthreadex(0, 0, scan_inet_ip, ctr, 0, 0);
    if ( hThread2 )
      CloseHandle(hThread2);
    Sleep(2000u);
    ++ctr;
  }
  while ( ctr < 128 );
  result = 0;
}
return result;
```

Figure 4. Local and public IP address scans

The ransomware sample uses a hybrid cryptosystem to effectuate file encryption. It uses a symmetric AES-128 cipher for actual file encryption, and an asymmetric RSA-2048 public key to encrypt the symmetric key. The corresponding master private RSA key is held by the attacker, while the public RSA key is implanted in the ransomware payload. The malware uses the operating system's *CryptoAPI* to access the *CryptEncrypt ( )* function to implement the encryption process. These are up-to-date resilient ciphers, which are computationally impossible to crack without the corresponding decryption keys [13]. Access to the encrypted files by subsequent decryption is granted only upon meeting the ransom demand, and that too without a guarantee. Otherwise, the affected portion of the network remains incapacitated.

By employing the above techniques, WannaCry was able to implement multi-stage attacks on CI devices, both for those that were directly connected to the Internet and those connected through some other intermediate networks. This was witnessed on attacks on hospitals [14] and public transport systems [15], which resulted in several system failures in CI.

IV. Conclusions

In this study, we modeled different crypto ransomware multi-stage attacks emanating from various infiltration sources in CI. We verified our modeling approach with WannaCry attacks. The static malware analysis results show the different techniques employed by the ransomware to propagate and attack CI components across various network partitions. Since the integration of CI and ICS to the Internet seems inevitable, the hierarchy in securing CI and ICS should prioritize production networks first, followed by supervision/SCADA networks. A cascaded network segmentation with DMZ will minimize the exposure of production network devices to cyber threats, provided such components are not Internet-facing. Such defense-in-depth security strategies should be supplemented with intrusion detection systems in each network segment.

References

[1] E. Byres and J. Lowe. "The myths and facts behind cyber security risks for industrial control systems." In Proc. of the VDE Kongress, vol. 116, pp. 213-218. 2004.

[2] L. Obregon "Secure architecture for industrial control systems." SANS Institute InfoSec Reading Room (2015).

[3] E.D. Knapp and J.T. Langill. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[4] H. Ghani, A. Khelil, N. Suri, G. Csertán, L.Gönczy, G. Urbanics, and J. Clarke. "Assessing the security of internet-connected critical infrastructures." Security and Communication Networks 7, no. 12, pp.2713-2725. 2014.

[5] S. Marrone."Towards a Unified Definition of Cyber and Physical Vulnerability in Critical Infrastructures." In Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on, pp. 167-173. IEEE, 2017.

[6] K. Ganame, M.A. Allaire, G. Zagdene and O. Boudar. "Network Behavioral Analysis for Zero-Day Malware Detection–A Case Study." In International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, pp. 169-181. Springer, Cham, 2017.

[7] D. Gonzales, J.M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods. "Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds." IEEE Transactions on Cloud Computing 5, no. 3, pp.523-536. 2017.

[8] R. Brewer. "Ransomware attacks: detection, prevention and cure." Network Security 2016, no. 9 pp.5-9. 2016.

[9] G. Swenson. "Bolstering Government Cybersecurity Lessons Learned from WannaCry." NIST 2017.

[10] S. Lüders (2014, Aug.) Why Control System Cyber-Security. BlackHat Conference. [Online]. Available: https://www.blackhat.com/docs/us-14/materials/us-14-Luders-Why-Control-System-Cyber-Security-Sucks.pdf

[11] S. Shao, C.Tunc, P. Satam and S. Hariri. "Real-Time IRC Threat Detection Framework." In Foundations and Applications of Self* Systems (FAS* W), 2017 IEEE 2nd International Workshops on, pp. 318-323. IEEE, 2017.

[12] CVE-2017-0144 Detail (2017, Oct). [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-0144

[13] A. Al Hasib, and A.A.M.M. Haque. "A comparative study of the performance and security issues of AES and RSA cryptography." In Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on, vol. 2, pp. 505-510. IEEE, 2008.

[14] T.A. Mattei. "Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack." World Neurosurgery 104, pp. 972-974. Elsevier 2017.

[15] N. Huq, R. Vosseler and M.orton Swimmer. (2017) "Cyberattacks Against Intelligent Transportation Systems" TrendMicro TrendsLabs, 2017. [Online] Available: https://documents.trendmicro.com/assets/white_papers/wp-cyberattacks-against-intelligent-transportation-systems.pdf