vb 2019 LONDON 2 – 4 October 2019

FANTASTIC INFORMATION AND WHERE TO FIND IT: A GUIDEBOOK TO OPEN-SOURCE OT RECONNAISSANCE

Daniel Kapellmann Zafra
FireEye, USA

danielkapellmann.z@fireeye.com

ABSTRACT

Since at least 2015, we have tracked a cluster of Russian-sponsored cyber espionage activity targeting the energy sector, known as TEMP.Isotope. The group has leveraged watering holes and spear-phishing campaigns to infiltrate information technology (IT) networks, harvest credentials, and exfiltrate information about industrial networks. The documentation retrieved by TEMP.Isotope is critical for engineering future attacks targeting operational technology (OT) networks that are designed to control and monitor physical processes. The extracted information can be used by threat actors to better understand the network architecture and physical processes taking place in the facility, to visualize what equipment the victim uses, identify associated suppliers and contractors, and figure out what tools they will need to build or acquire in order to conduct further attacks.

Although we have observed an uptick in the number of nation-state sponsored threat actors seeking to obtain information about operational technology environments by targeting organizations directly, we highlight that it is also possible to find this type of information in mainstream open-source sites and repositories. In this paper, we explain some of the main motivations that drive threat actors to perform reconnaissance on industrial networks. We then illustrate some of the tactics that have been used by threat actors to extract OT documentation from corporate IT networks. Finally, we present our findings from browsing popular sites in search of information that can be leveraged to learn about the industrial control systems (ICS) networks. Our paper includes examples from cybersecurity products, popular online retail stores, manual libraries, vendor websites, coding and mobile application repositories.

FANTASTIC INFORMATION AND WHERE TO FIND IT: A GUIDEBOOK TO OPEN-SOURCE OT RECONNAISSANCE

Cybersecurity professionals may never cease to be amazed by the large amount of sensitive information that is available online. Hidden within an unimaginable volume of data lie fantastic documents that are waiting to be found by those who know what to look for. As a result, open-source reconnaissance represents not only a valuable tool for penetration testers and researchers, but also a great opportunity for threat actors seeking to learn about their targets.

IT professionals – and malicious actors – often engage in an initial process of reconnaissance or intelligence gathering to learn about a target organization and explore possible weaknesses. During this process, the actor commonly attempts to map networks and discover their topology, scan for open ports and services, retrieve device and configuration logs, or harvest data from DNS and Whois, among other things [1].

However, in the case of operational technology (OT) security, the reconnaissance process is slightly different. Given the complexity of physical processes in industrial and critical infrastructure organizations, researchers and malicious actors often need to carry out extensive research to understand the process components and architecture in order to develop or acquire the tools that enable them to reach their ultimate goals. Small changes in the parameters that define physical processes or specialized equipment can have undesired impacts that the researcher or threat actor would normally want to be aware of.

In this paper, we explain some of the main motivations that drive threat actors to perform reconnaissance on industrial networks and present our findings from browsing popular sites in search of information that can be leveraged to learn about OT networks. We highlight that all of the resources we present for finding fantastic information are available publicly, or limited only by non-restrictive monetary compensations.

SCOPING OPEN-SOURCE OT RECONNAISSANCE

OT consists of hardware and software systems that are grouped to monitor or control physical equipment, processes or events. It is commonly used in the context of industrial operations including industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, networking components and other IT equipment required to facilitate process automation. OT is used in production line management, mining operations controls, utilities, and automated manufacturing, among other industrial activities [2]. Unlike attacks targeting IT networks, in the case of OT an incident may result in safety implications that range from equipment destruction and product disruption to environmental damage or even the loss of human life.

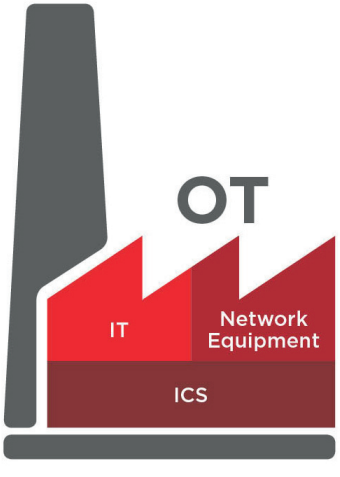

Figure 1: Simplified diagram of OT components.

Threat actors targeting OT networks may rely on multiple sources to acquire information about target environments. These sources range from complex exfiltration mechanisms deployed directly in the target's corporate or industrial networks to low-cost open sources that are also used by regular consumers. This type of research can provide threat actors with valuable insights relating to an

organization's people, processes and technology with absolutely no risk of being discovered as the information is publicly available.

Information retrieved from open-source OT reconnaissance may reveal details about the target's preferred vendor and/or recently purchased, repaired or upgraded equipment; industrial processes; employee roles and duties; Internet-connected devices; network architecture and communication protocols; third-party service suppliers and so on. Attackers can use this information to:

- Leverage upstream equipment suppliers to compromise the victim and gain access to OT networks.
- Identify and target vendors and other contractors who have access to the final target's OT network – these upstream targets are often the weakest link in an organization's security.
- Learn about manufacturing environments and processes to figure out what tools they will need to build or acquire in order to conduct further attacks.
- Socially engineer key stakeholders that hold credentials to access OT networks or who possess documentation about network architecture and communication flows.

It is also important to highlight the fact that security has only recently registered as a priority for ICS asset owners. Traditionally, OT security relied on a model known as 'security through obscurity', where information about industrial networks and proprietary assets was available only to a select group of experts [3]. Information about OT was tightly protected and isolated from IT networks (the Internet was not even in the imagination of industrial organizations) as a safety measure to prevent external parties from learning about critical assets or internal processes. However, 'security through obscurity' is no longer appropriate for OT, given the increasing integration of corporate IT and modern control system architectures [4]. Today, threat actors have access to a broad range of resources to develop general OT knowledge and search for footprints left by industrial organizations, their employees and third-party contractors.

THE MAPPING MARAUDERS

In October 2017, the Cybersecurity and Infrastructure Security Agency (CISA) – best known as ICS-CERT at that time – released Alert TA17-293A on APT threat activity targeting energy and other critical infrastructure sectors [5]. This cluster of activity, which *FireEye Intelligence* has largely tracked as TEMP.Isotope, consisted of a long-term campaign leveraging spear-phishing and watering holes in industry websites to harvest credentials and perform reconnaissance of industrial control systems and critical infrastructure in countries including Turkey, Israel, Ireland, the US and the UK.

In March 2018, an updated version of the alert was published containing additional information on the threat actor's activity after having gained access to the targeted systems [6]. According to the alert, the actor accessed ICS engineering diagrams and documentation from victim corporate networks and public-facing websites. To provide an example, one of the documents retrieved from the corporate network included the visualization of an energy generation facility's human-machine interface (HMI) that the threat actor was able to visualize (see Figure 2).

TEMP.Isotope searched for file servers on victim corporate networks, where they attempted to find ICS-related files with naming conventions such as 'SCADA WIRING Diagram.pdf', 'SCADA PANEL LAYOUTS.xlsx' and others, according to the alert. However, not all the actor's research took place in company networks. TEMP.Isotope also explored publicly accessible websites for sensitive

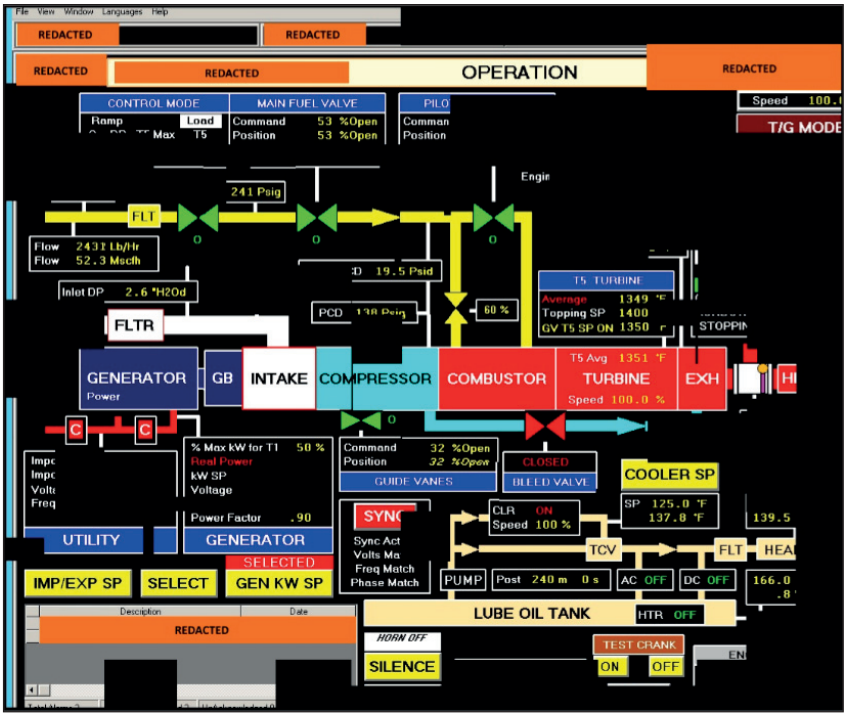

Figure 2: HMI screen reconstructed from fragments accessed by the threat actor described in Alert TA18-074A.

ICS information. For example, the actor downloaded a high-resolution photo from a victim's publicly accessible human resources page that displayed control systems' equipment models and status information in the background.

As illustrated by the former case, open-source OT intelligence can be found in the least expected places. Even though advanced threat actors often have enough resources to deploy complex exfiltration techniques for reconnaissance, low-cost and low-risk open sources are usually the starting point. Organizations that leave sensitive online footprints may become low-hanging fruits for opportunistic threat actors.

The TRITON incident provides an additional illustration of the usefulness of open sources in learning about OT. In December 2017, *FireEye* publicly released its first analysis of the TRITON attack, in which malicious actors used the TRITON custom attack framework to manipulate industrial safety systems at a critical infrastructure facility and inadvertently caused a process shutdown [7]. The threat actors behind the TRITON attack framework invested significant time learning about the Triconex Safety Instrumented System (SIS) controllers and TriStation, a proprietary network communications protocol.

Considering that TriStation is a proprietary protocol and there is no official public information detailing its structure, it remains a mystery as to what resources were used by the threat actor to

understand the protocol. In June 2018, *FireEye* reverse engineered the protocol and discussed some possible theories [8]. In at least a couple of them, open-source reconnaissance seemed to be a feasible path the attacker could have taken to better understand the protocol. For example, the threat actor could have bought or used a demo version of the *TriStation 1131* software, allowing them to reverse engineer some portions of the protocol. The attacker could have purchased the *Triconex* controller and software at a reasonable price from an online retail store for the purpose of testing and reverse engineering the product.

It is also worth highlighting that it only took a couple days for components of the TRITON attack framework to become broadly accessible in a *GitHub* repository once the incident had publicly been disclosed [9]. This is yet another example of the various open sources researchers can use to learn about an attack framework, but which threat actors can also leverage to improve their strategies.

A GUIDEBOOK FOR FANTASTIC OT RECONNAISSANCE

The elaboration of a guidebook for finding fantastic open-source information about OT is an art, not a science. Information about target organizations is often present in the most unusual locations. Researchers and threat actors that are both knowledgeable and creative will always find a way to find the information they seek. The following examples illustrate some peculiar sources of information that we have explored in *FireEye Intelligence*.

Malware analysis and sandboxing platforms

Open-source malware analysis and sandboxing platforms are often used by organizations to evaluate artifacts such as suspicious files and URLs. However, in some cases employees upload sensitive information and proprietary files without understanding the risks entailed by open-source tools – namely, that in some cases, other users can download these private files. Without realizing the consequences, employees may upload vital information such as technical documentation, registration of purchases and agreements with suppliers and lists of equipment components, among other things.

Diagrams and internal documentation enable threat actors to learn about an industrial environment, improve their search capabilities for retrieving further sensitive documentation, and ultimately engineer targeted attacks against operational environments. We highly recommend reading Ralph Langner's classic white paper 'To Kill a Centrifuge' for more examples of the types of information a threat actor requires to execute an attack against OT systems [10].

In January 2018, *FireEye Intelligence* performed a basic query of ICS-related files in some of these platforms. Multiple types of documents were found revealing sensitive information about industrial environments:

- Engineering diagrams
- Configuration documents
- Manuals and operation guidelines
- Industrial control systems software executables
- Purchasing documentation

Online retail stores, auction sites and vendor download centres

While the lack of accessibility to industrial equipment and software for testing and reverse engineering presents a barrier for threat actors attempting to design specialized malware, many components can be purchased via third-party distributors or web-based auction sites. Customers can circumvent primary vendor purchasing restrictions or obtain components for a lesser cost.

In June 2018 *FireEye Intelligence* searched some online retail and vendor sites for available ICS components. During the exercise, we identified hardware components such as safety systems and satellite communication equipment. Firmware and software from major ICS vendors was also available.

While we continue to assess that only sophisticated and well-funded threat actors currently possess the expertise and resources needed to reverse engineer industrial components and produce highly targeted ICS-focused malware (e.g. TRITON), the increasing availability of the systems and software in this type of channel continues to lower that bar.

Manual repositories and vendor websites

Technical documentation and manuals about some industrial equipment is broadly available in online repositories alongside consumer-focused products that range from computer accessories and video surveillance systems to humidifiers, video game consoles, stoves, furniture and cars. (Yes, I said humidifiers!)

Figure 3: Honeywell manuals by category as presented on Manuals Directory [11].

In February 2019, *FireEye Intelligence* explored some online repositories and vendor websites. The focus of this exercise was to identify information that could help threat actors learn about targeted ICS products, their inner workings, functionalities and device compatibilities. The identified documentation could also be useful for initial research to support the reverse engineering of hardware or software, retrieve information about product features, and sometimes even identify production sites where the technology has been implemented.

Specialized and consumer search engines

Since the creation of the *Shodan* search engine in 2009 [12], multiple researchers have explored alternatives for finding Internet-connected OT equipment using specialized search engines. For many years, a project called *Shodan Intelligence Extraction* (*SHINE*) amazed ICS security professionals by sharing information about a significantly large number of exposed IP addresses that appeared to belong to SCADA and control systems devices [13]. The platform later released a web page showing queries for a set of popular control systems equipment, software, and communication protocols [14].

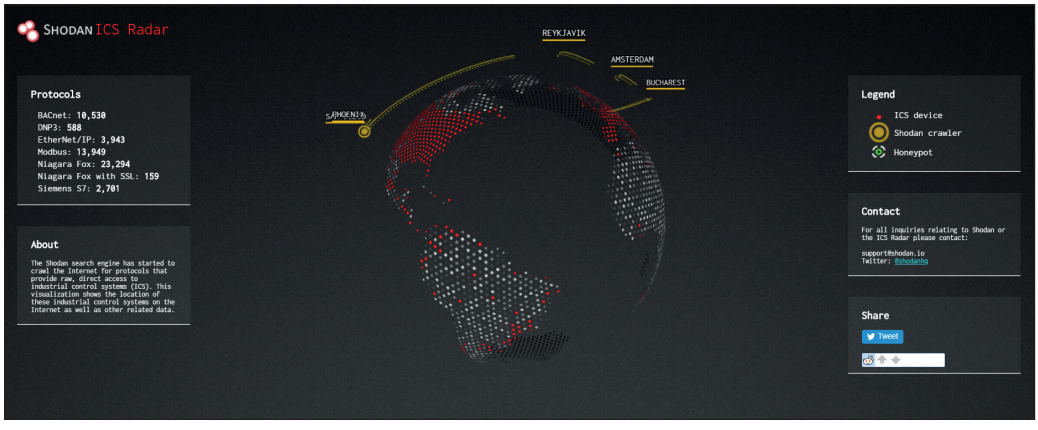

Figure 4: Shodan ICS Radar [15].

Although awareness of the severity of exposing OT equipment online has increased significantly during the past few years, new research continues to be released regularly. For example, in 2018 *Trend Micro* released a report called 'Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries', compiling exposed HMIs found by a group of researchers in facilities from the water and energy industries [16]. However, the simplicity of these platforms is such that it is not only large-scale security firms that have gained visibility into exposed devices. Smaller research organizations and threat actors have also explored these avenues. Other regularly used engines include *Censys*, *ZoomEye* and *OShadan*.

Researchers and threat actors can also find exposed devices using consumer search engines such as *Google* or *Bing*. By querying for certain keywords and parameters it is possible to identify equipment that should probably not be available online. This methodology is commonly known as dorking, and it has also been broadly explored by OT security professionals [17, 18, 19]. While certainly not the most formal concept, others refer to this type of browsing colloquially as 'Google Fu'.

Social media

Last but not least, social media plays a significant role in open-source OT reconnaissance as a primary method for social engineering. Social media profiles often contain valuable information about the targets that may range from personal preferences (useful for crafting spear-phishing emails), to work expertise and projects (e.g. publications on *LinkedIn* revealing the role an individual played in a major OT project). This type of information is useful for developing mechanisms for exploiting vulnerabilities in people's behaviour, which is often recognized as the easiest path to break the security chain.

Social engineering offers a low-cost avenue for threat actors to gather technical information about target facilities and evade perimeter security controls by gaining access to employee credentials or privileged information. Social engineering attacks aimed at gaining access to ICS networks often focus on engineers and technicians. Given that ICS networks are often separated from public corporate networks via air gaps and other security mechanisms, social engineering represents an attractive avenue for acquiring access to privileged ICS accounts.

In a specific instance, *FireEye Intelligence* found an old post in the review section of an *Android* SCADA mobile application. The post had been written by an engineer from an oil and gas automation solutions company and included an explanation of the purpose for which the application was used. Using this information, we were able to identify details relating to the submitter, coworkers, the equipment used in the facility, and even other sites at which the same solution was implemented.

THOSE WHO SEEK SHALL FIND

The OSINT resources for OT reconnaissance that we have explored in this paper are by no means an exhaustive representation of all the available alternatives. Other OT cybersecurity researchers have talked about this in the past, revealing some fantastic information that could lead to incidents impacting human lives and public safety [20]. Those who have enough patience, determination and creativity will surely continue to find new avenues through which to identify publicly available information that should probably not be present online.

However, there are two important lessons that this research should highlight:

- **Security by obscurity is dead.** People and organizations leave digital footprints that are often visible for determined researchers and threat actors. Diagrams, internal documentation and other details enable threat actors to learn about an industrial environment, improve their search capabilities, and ultimately engineer targeted attacks against operational environments.
- **It's all about awareness.** Companies that do not implement proper information-handling procedures and security awareness programs risk becoming low-hanging fruits for attackers who scan these sources for actionable information.

REFERENCES

[1] Chapple, M.; Seidl, D. Reconnaissance and Intelligence Gathering. CompTIA CySA+ Study Guide. John Wiley & Sons 2017. pp. 34-36.

[2] Harp, D. R.; Gregory-Brown, B. IT/OT Convergence Bridging the Divide. https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf.

[3] Byres, E. The Industrial Cybersecurity Problem. 2013. https://www.isa.org/pdfs/the-industrial-cybersecurity-problem/.

[4] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. 2016. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[5] Cybersecurity and Infrastructure Security Agency. Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors. https://www.us-cert.gov/ncas/alerts/TA17-293A.

[6] Cybersecurity Infrastructure and Security Agency. Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. https://www.us-cert.gov/ncas/alerts/TA18-074A.

[7] Miller, S.; Brubaker, N.; Kapellmann Zafra, D.; Caban, D. TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping. https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html.

[8] Miller, S.; Reese, E. A Totally Tubular Treatise on TRITON and TriStation. https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html.

[9] MDudek-ICS. TRISIS-TRITON-HATMAN. https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN/commits/master?after=d08c9464d451f38c7a4c182d9aabd58d0dc84b0e+34.

[10] Langner, R. To Kill a Centrifuge. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

[11] Honeywell manuals. http://www.manualsdir.com/brands/honeywell.html#categories.

[12] Shodan. https://www.shodan.io/.

[13] Radvanovsky, B. Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting. https://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting.

[14] Industrial Control Systems. https://www.shodan.io/explore/category/industrial-control-systems.

[15] Shodan ICS radar. https://ics-radar.shodan.io/.

[16] Hilt, S.; Huq, N.; Kropotov, V.; McArdle, R.; Pernet, C.; Reyes, R. Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries. https://documents.trendmicro.com/assets/white_papers/wp-exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries.pdf.

[17] SCADA Dorks Database (SDD). http://www.critifence.com/scada-dorks-database/.

[18] Scada_dorks.xls. https://github.com/w3h/icsmaster/graphs/contributors.

[19] Google Dorking and Shodan. https://www.elp.com/articles/powergrid_international/print/volume-21/issue-11/features/google-dorking-and-shodan.html.

[20] Sistrunk, C.; Krypt3ia; SynAc. WE ARE THE ARTILLERY Using Google Fu To Take Down The Grids. https://www.youtube.com/watch?v=MjuzLOo_tV8.