MEET YOUR ATTACKER

TAXONOMY & ANALYSIS OF A SCADA ATTACKER

YEHONATAN KFIR

CTO, RADIFLOW

radiflow
Secure your Assets

TABLE OF CONTENTS

Meet your attacker: SCADA attackers Taxonomy and Analysis *3*

Taxonomy 4

Non-Technical Properties 4

Technical Properties 5

Case Analysis 6

Type of Attackers 7

Summary 9

About the author 9

About Radiflow 9

Appendix A – References *10*

MEET YOUR ATTACKER: SCADA ATTACKERS TAXONOMY AND ANALYSIS

Cyber Incident reporting in SCADA systems gives us invaluable insight into the burgeoning threat landscape. Incident case reports help the security community understand what threats we face and thus enable organizations to establish a robust defence strategy. In recent years, there has been an increase in cyber security awareness and the adoption of detection tools. As a consequence, the number of reported incidents and campaigns targeting SCADA networks has increased.

With the increase in the number of released reports, it is not uncommon to see various reports focusing on the same incidents. For example, the Ukrainian outage that happened in December 2015 appeared in **more than 30 reports**, all from prestigious research centers. As in many other cases, each of those reports used its own methodology and chose to emphasize different aspects of the case.

The increase in the number of reports, each with different analysis methodology, makes it challenging to derive a coherent and clear conclusion from the cases. Additionally, with the obstacle of an agreed analysis methodology, the reports are opened to be biased (un-intentionally) by the authors' knowledge and point of view. The lack of a single taxonomy to analyze incidents leads to difficulties in understanding the threat landscape in an unbiased way.

In this paper, we suggest an evidence-based taxonomy to analyze SCADA related incidents. In this taxonomy, we distinguish between properties which are more technical (e.g. the type of malware used) and non-technical (e.g. desired impact). In addition, with Radiflow's methodology, the technical properties should be analyzed merely based on the *demonstrated capabilities* of the attackers in each case. By *demonstrated capabilities* we refer to capabilities that are based on evidence collected by different research organizations. As for the non-technological, our analysis is also based on threat intelligent sources.

Radiflow's taxonomy analyzes several historical cases. Analysis is based on previous reports that we have aligned to our own taxonomy. From each report we only analyze information that is backed-up by evidence mentioned in those reports. Based on this methodology, we believe it is more accurate to review the evolution of the threats over the years.

In the following sections we describe our taxonomy, and the analysis of the cases using our taxonomy. In the last section, we discuss some of the trends that can be easily derived from the taxonomy-based analysis.

We believe this coherent taxonomy and case analysis allows us to define a clearer model of a cyber attacker in a SCADA system. Specifically, this analysis allows risk managers to understand the different types of attackers that are currently active, and the different capabilities each type of attacker has. In addition, it allows SCADA operators and CISOs to plan their security defenses according to those demonstrated attacker models.

TAXONOMY

The taxonomy used is summarized in the following table:

	○	◑	●
Targeted Industry	Mostly IT	IT and OT	Only OT
Desired Impact	Not SCADA Specific	SCADA Specific, Confidentiality	SCADA Specific, Availability & Integrity
Actual Impact	No Impact on Availability and Integrity	Impact on Availability and Integrity of non-critical processes	Impact on Availability and Integrity of critical processes
Physical Process Expertise	None	Narrow Case Specific	Industry Specific
Dormant Duration	Weeks or more	Days	Hours or less
Type of Malware	General IT Malware, or No Malware	Generic IT Malware / Backdoor, with add-on modules for SCADA	Relevant ONLY for SCADA
Industrial Protocols Expertise	Non-SCADA protocols	Open Specification	Proprietary Protocols
Assets Configuration Changes	No attempt to change Logic or Firmware	Changing the Logic	Changing the firmware
Vulnerability Type	Windows/ Linux OS	OT windows-based Software (e.g. HMI)	Embedded controllers
Vulnerabilities Used	With proof-of-concept to mature public exploit or none	Known, without exploit	Unknown, Zero-Days

NON-TECHNICAL PROPERTIES

Targeted Industry – Cyber security cases are often not standalone incidents and are likely to be part of a larger campaign. We distinguish between three types of campaigns. First are cases which were part of an IT campaign. The next are examples that were part of an intentional campaign to target OT and IT networks. Lastly are cases that were part of targeted OT specific campaigns.

Paramount to any SCADA system is availability and integrity. Confidentiality, although very important in some cases, is more often a lower requirement. With respect to those SCADA requirements, we define two properties: (1) the attacker's desired impact; (2) and the actual impact achieved.

Desired Impact – We distinguish between three types of impact desired by the attackers. The least SCADA specific intentions are those cases where no intentions demonstrated an attack on any SCADA systems. The next level focuses on the intention to create an impact on the confidentiality of the system. The most severe cases are those where the attacker demonstrates the intention to impact the availability and integrity of the SCADA system.

Actual Impact – We distinguish between three types of actual impact achieved by the attacker. In the lower scale, we marked cases where there was no actual impact on the

availability and integrity of the system. The next level focuses on the impact on availability or integrity of non-critical processes / services. At the higher level are cases where there was impact on availability and integrity of critical processes / services.

Physical Process Expertise – Creating a desired impact on a SCADA system requires a domain expertise in the physical process that is controlled by the SCADA system. Demonstrating expertise in a wider physical process implies evidence of more experienced and flexible attackers that can move from one target to another. In this property, we distinguish between three levels of expertise. At the lower scale, a case where attackers did not demonstrate any specific domain expertise, related to the physical process. The next level focuses on cases where the attackers demonstrate a case-specific knowledge, which is very hard to leverage with other targets. The most dangerous are cases where the attackers demonstrate an industry wide expertise, e.g. understanding how a power grid network works.

Dormant Duration – In general, compromising SCADA systems may take time. During this time the attacker has compromised assets in the SCADA under his control (or partial control). We distinguish between three dormant durations: weeks, days and hours. The rationale behind this deviation is that the longer an attack is dormant, the higher the probability is that the SCADA owner will detect it.

TECHNICAL PROPERTIES

This is the second group of properties related to the technical expertise demonstrated by the attackers and the tools they used.

Type of Malware – This property distinguishes between the type of malware used and the level of industrial network knowledge required to be successful. In the lower scale, there are cases where generic IT malware was used, with no special development adaptions for OT environment. The next level focuses on cases with malware that had an add-on module for SCADA, while the malware itself could be used for both OT and IT networks. Lastly, cases where malware with capabilities that are useful only in SCADA networks that were clearly developed for the OT environment.

Industrial Protocols Expertise – SCADA systems use different protocols than traditional IT networks. Those protocols include traditional IT protocols, as well as open specification and proprietary industrial protocols. This property distinguishes between cases where the attackers demonstrated a different level of industrial protocol expertise. In the lower scale are cases where the attackers did not demonstrate any industrial protocol expertise. The second level are cases where attackers demonstrate

understanding of open specification industrial protocols. Lastly and most notably, are cases where the attackers demonstrate reverse-engineering capabilities, using proprietary, close-specification protocols.

Assets Configuration Changes – Most cyber-attacks require to infiltrate and change assets behavior. In SCADA networks beside the regular servers, there are a variety of embedded devices, such as controllers, RTUs, IEDs, etc. This property is focused on the level of configuration of changes attempted to be made in the network. In the lower scale cases where there was no configuration change to embedded devices, and (maybe) only to servers. The next level are cases where the logic or the set points of controllers were changed. At the higher level are cases where the firmware version of the embedded devices were attempted to be changed.

Vulnerability Type – This property describes the level of SCADA specific vulnerabilities used in the case. At the lower scale vulnerabilities related to operating system, which are common in IT networks and are not specific for SCADA. In other words, those are mainly vulnerabilities related to Windows and Linux operating systems. The next level are vulnerabilities in Window-based applications and those that related to the SCADA network (e.g. vulnerabilities in Human-Machine-Interface products). Lastly, vulnerabilities that related to controllers and other SCADA-specific devices.

Vulnerabilities Used – The property distinguishes between three levels of vulnerabilities that were used. At the lower scale are cases where the attackers used known vulnerabilities that already had an exploit by the time they used it. The next level are cases where the vulnerability was known, but no exploit was published. This required the attacker to develop their own exploit and research this specific vulnerability – knowing its existence. Lastly, the most expert attackers are those who used zero-day vulnerabilities.

CASE ANALYSIS

Based on the above taxonomy, we analyzed 8 major cases from the past. The source of information for the cases has been taken from leading research and advisory centers, such as ICS-CERT, NIST, FireEye and Kaspersky. The full list of reports used for each case, can be found in Appendix A .

The summary of the cases can be seen in the following table:

Year	2010	2010	2013	2014	2015	2017	2017
Operation	Energetic Bear	Stuxnet	Research Hoenypots	Steel Plant Germany	Ukranian Outage	Triton	WannaCry / NotPetya / CryptoMiners
Industrial Vectors	General	Iran Nueclear	General	Plants	Power Grid	Safety	General
Targeted Industry	◑	●	◑		●	●	○
Desired Impact	◑	●	●	●	●	●	○
Actual Impact	○	●	○	●	●	●	◑
Physical Process Expertise	○	◑	○	●	●	●	○
Dormant Duration	○	○	●		○	○	●
Type of Malware	◑	●	○	●	◑	●	○
Industrial Protocols Expertise	◑	●	◑	●	◑	●	○
Assets Configuration Changes	○	◑	○	●	○	●	○
Vulnerabilities Used	○	●	○		○	●	◑
Vulnerability Type	◑	◑	○		●	●	○

In two cases, we faced some ambiguities from the public information. The first case is in the honeypot research carried out by TrendMicro. This research collected information from multiple SCADA honeypots across the world. Therefore, the honeypot case represents a variety of incidents, and not one specifically. Most of the incidents found in TrendMicro's research caused no effect on the availability or integrity of the SCADA honeypots. However, there were a few incidents in the research where attackers carried out some activities (probably, unintentionally) that may have caused impact on the availability. We chose to set the actual impact value according to the majority of impacts, which did not involve impact on availability or integrity.

The second ambiguity case is the cyber-attack on the steel plant in Germany. There is not a lot of accurate or publicly available information regarding this case. In a few properties we were not able to find sources, and we did not set values to those fields.

TYPE OF ATTACKERS

Based on the cases analyzed we can now distinguish between several types of attackers that are currently active in the ICS:

1. **Low-Skill Attackers Prototype** – The case analysis shows that there is a high correlation between low level attackers operating without intent to cause specific SCADA impact and those that attack to cause intentional medium impact. In several cases, the attackers did not demonstrate any SCADA specific knowledge or a specific desire to cause damage but were still able to create medium impact. Examples of this group are the WannaCry and NotPetya malware.

   Recent years and events would indicate that there is no need to be a SCADA expert in order to harm SCADA networks. Additionally, SCADA systems are suffering from medium impact on their availability, even from an attacker with no intent to create such impact.

   

   Those low-skill attacks also have a short dormant duration and have the property of using non-zero-day vulnerabilities.

   Such attacks allow the defender a small amount of time to respond and mitigate the threat. Since the impact is on availability and integrity, there is little benefit for detection-only strategies. The fact that non-zero days are used encourages prevention systems to be quickly updated to prevent those vulnerabilities.

   The main explanation for the phenomena of increased low-skilled, low-motivated attacks are two-fold; Firstly is the increased use of automatic hacking tools, such as AutoSploit. Radiflow has encountered cases where operators accidently connected their network to the internet and in less than one hour, their network was scanned, exploited and used to attack other services in the network. Secondly, SCADA networks are generally those with the weakest security. Wide attacks, even if not targeting SCADA, are more likely to infect the weak internet-connected SCADA networks.

2. **Highly Sophisticated Attackers** – Over recent years, there has been an increase in the number of sophisticated OT-specific attacks using in-depth OT know-how. More highly sophisticated attackers demonstrate a high level of motivation to impact availability and integrity. Those attackers have almost the opposite characteristics than the ones of the lower-skilled attacker. The cases of Stuxent, Ukrainian Outage and Triton are examples of attackers with a desire to cause damage and the motivation to impact availability. The attackers in those cases operated in the targeted network for weeks, if not months or longer.

   In order to defend against such attackers, it is required to have a monitoring system that is able to monitor all the levels where the attackers are operating, including proprietary protocols, zero-day vulnerability detection, anomalies in the physical process and configuration changes. However, this deep visibility is not enough. In order to distinguish between innocent, rare events and rare malicious attacks, the monitoring system should have an additional layer of robust analytics. These analytics are critical in order to provide the operators with a coherent understanding of all the events and the level of risk those event present on its network.

SUMMARY

In this paper we presented a taxonomy to analyze cyber case incidents in SCADA systems. We were able to show that there are at least two types of attackers. The first are low skilled attackers that use traditional IT tool sets. Although they possess low-level skills, they were able to impact SCADA systems shortly after the initial infection. For these types of attackers, it is recommended to use prevention capabilities on the entrance to the SCADA, and in-depth monitoring for cyber threats and network anomalies. Secondly, we discussed the more sophisticated attacker who stays undetected for long periods of time within the network. In order to detect these attackers, it is necessary to monitor the network for configuration changes and anomalies in the network and process behavior.

We suggest that when developing your SCADA/ICS network you take those two types of attackers into consideration, combining detection and prevention tools, while working alongside a trusted cyber security partner.

For more information on how Radiflow could help you detect, protect and secure your ICS/SCADA networks with cutting edge technology and unparalleled customer experience visit our website: www.radiflow.com

ABOUT THE AUTHOR

Yehonatan Kfir, CTO, Radiflow LTD, is an experienced security expert, Yehonatan Kfir has led Radiflow's technology innovation road-map since 2014. In his early career he served for 10 years in an IDF Intelligence Corp elite R&D Unit. In his last role in Unit 8200 he led product research at the Cyber Innovation division and led a project that won the Intelligence Corp Commander's Creative Thinking Award. Yehonatan has a BSc, an MSc and an MBA, and is currently working on his PhD in Cyber Security.

ABOUT RADIFLOW

Radiflow is a leading provider of cyber security solutions for critical infrastructure networks (i.e. SCADA), such as power utilities, oil & gas, water and others.

SCADA networks often extend across multiple remote sites, allowing automation devices to be controlled from the control center.

Radiflow's security tool-set validates the behaviour of both M2M applications and H2M (Human to Machine) sessions in distributed operational networks. Radiflow's security solutions are available both as in-line gateways for remote sites and as a non-intrusive IDS (Intrusion Detection System) that can be deployed per site or centrally.

Radiflow was founded in 2009 as part of the RAD group, a family of ICT vendors with over $1Bn annual revenues. Radiflow solutions were launched at the end of 2011, validated by leading research labs and successfully deployed by major utilities worldwide.

Radiflow's solutions are sold as either integrated into wider end-to-end solutions of global automation vendors or as a standalone security solution by local channel partners.

APPENDIX A – REFERENCES

Energetic Bear –

- Kaspersky, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf

Stuxnet –

- ICS-CERT, https://ics-cert.us-cert.gov/advisories/ICSA-10-201-01C
- ICS-CERT, https://ics-cert.us-cert.gov/advisories/ICSA-12-205-02

Research Honeypots –

- TrendMicro, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-scada-that-didnt-cry-wolf.pdf

Steel Plant Germany –

- SANS, https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Ukrainian Outage –

- ICS-CERT, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
- SANS, https://ics.sans.org/blog/2016/02/25/thoughts-on-the-ics-cert-ukraine-cyber-attack-report
- NERC, https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
- SEL, https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6774_UkraineCyber_DEW_20170130_Web7.pdf?v=20181015-210831

Triton –

- ICS-CERT, https://ics-cert.us-cert.gov/advisories/ICSA-18-107-02
- ICS-CERT, https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF
- FireEye, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

WannaCry –

- Kaspersky, https://ics-cert.kaspersky.com/reports/2017/06/22/wannacry-on-industrial-networks/
- Symantec, https://www.symantec.com/security-center/writeup/2017-051310-3522-99

NotPetya –

- US-CERT, https://www.us-cert.gov/ncas/alerts/TA17-181A

CryptoMinner –

- Radiflow, classified incident case research

(C) 2019 Radiflow Ltd. All rights reserved. Radiflow reserves the right to change product specifications without prior notice | www.radiflow.com | info@radiflow.com