Secura

A BUREAU VERITAS COMPANY

OTCAD

OPERATIONAL TECHNOLOGY CYBER ATTACK DATABASE

Stash Kempinski
Secura, September 2021

SECURA

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands
Follow us on

T +31 (0)88 888 3100
E info@secura.com
W secura.com

1. Introduction

The Operational Technology Cyber Attack Database (OTCAD) consists of OT-related cyber attacks mapped to MITRE's ATT&CK® for ICS [1]. At its release, OTCAD contains data of 133 publicly known cyber attacks on OT between 1988 and 2020. Although databases similar to OTCAD exist already, a database of this size has not yet been publicly mapped to a single framework before. The lack of such mapping used to make it hard and time consuming to structurally analyze the OT threat landscape, e.g. to find changes in adversary behavior over time. OTCAD aims to solve this problem by creating a publicly accessible database that can be extended and adjusted through collaborative means, which is made easy with the use of ATT&CK for ICS. This whitepaper presents the different information sources used to find the cyber attacks, ranging from sector-specific (white) papers to publicly available databases, and criteria used to create OTCAD. Furthermore, it presents and discusses some of the trends that exist within OTCAD as an example of its capabilities. The raw data, consisting of the mapping and sources of each attack, and scripts to quickly interact with OTCAD can be found on the Secura Github page[1].

[1] https://github.com/SecuraBV

Contents

2. MITRE ATT&CK for ICS

MITRE's ATT&CK® (*Adversarial Tactics, Techniques, and Common Knowledge*) is a free-to-use framework that contains common goals and methods used within the different stages of a cyber attack. The methods, called *techniques*, describe the different courses of action an adversary can take to perform a particular *tactic* (goal). These techniques and tactics consist of common concepts in cyber security. This makes it easy to map attacks to the framework and is, in combination with its wide recognition, the reason why this framework is chosen to map onto.

ATT&CK was originally developed for enterprise cyber security, but has recently expanded to different, specialized domains such as mobile and Industrial Control Systems (ICS). The first version of ATT&CK for ICS was released in 2020 and contains only relevant tactics and techniques for ICS. For example, the tactics *Inhibit Response Function* and *Impair Process Control* were added. Both these techniques are only applicable to ICS environments, opposed to enterprise environments, due to their relation to cyber-physical systems. Contrarily, the *Resource Development* tactic is not included in the ATT&CK for ICS framework as there is still little known about ICS adversary operations and their development techniques.

Version 8 of ATT&CK for ICS is chosen as the preferred version for OTCAD even though version 9 has been released during its creation. This choice is further explained in Section 5.1, after the mapping and trends in Section 3 and 4 respectively, as the information presented in these sections are essential to follow the reasoning. Both versions can be found in Appendix A as reference.

3. Mapping

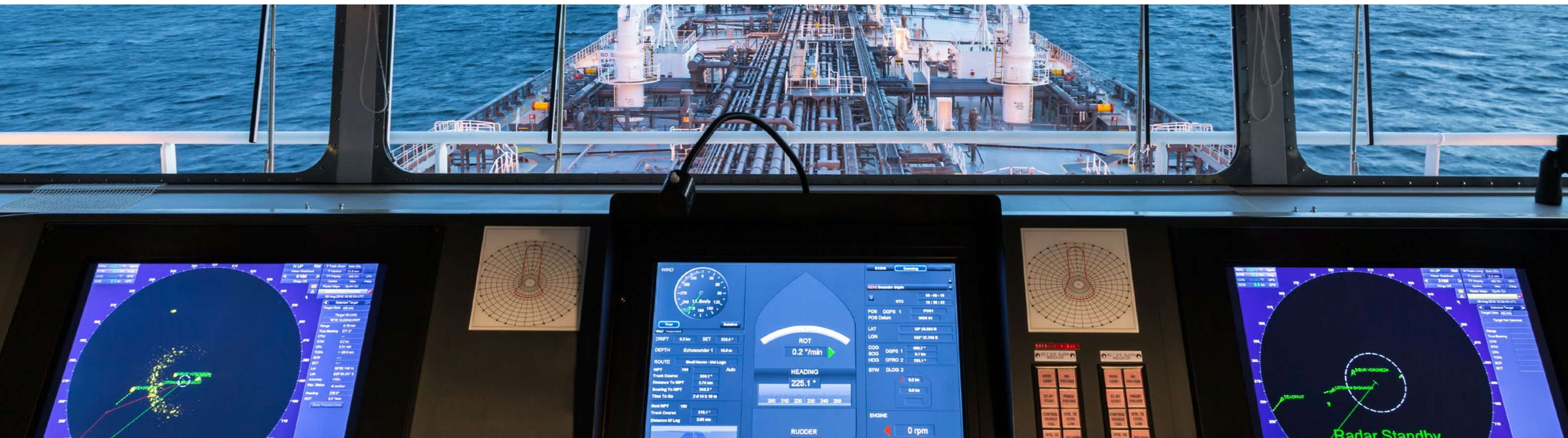
The cyber attacks in the initial release of OTCAD are found through various information sources, which are presented in Section 3.2. These “primary” sources, contain lists of attacks on OT, but in most cases these sources itself did not contain enough usable information to properly map the attacks to ATT&CK for ICS. As a result, other “secondary” sources, such as news articles, had to be found to gather mappable information. The secondary sources are included in OTCAD itself and not further discussed in this white paper. Both the primary and secondary sources were evaluated against the same criteria to maintain a high standard of trustworthiness.

The mapping methodology in OTCAD follows the American Cybersecurity & Infrastructure Security Agency (CISA) best practice guidance for MITRE ATT&CK mappings[2]. Following these best practices means that attacks are only mapped to the techniques actually used by the adversary, opposed to all techniques present in an attack. This ensures that closely related techniques are not mapped together by default, which could create possibly misleading statistics about adversary behavior. For example, *spearphishing attachment* and *replication through removable media* result mostly in a compromised engineering workstation, but this does not necessarily mean that the *engineering workstation compromise* technique is used. Only if engineering workstation compromise is used directly by the adversaries, e.g. they stole a workstation to send a *spearphishing attachment*, it is also mapped.

To make a distinction between information not being available or tactics not being used in an attack, *unknown* and *not applicable* are added to each tactic as mapping option. The *unknown* option means that the related tactic was used, but there was no criteria-meeting information available to determine which technique was used. The *not applicable* option in turn means that there was criteria-meeting information indicating that the related tactic was not used. Note that OTCAD cannot be completely objective as the used information can possibly be interpreted in different ways. However, these different interpretations will not lead to significant changes within the resulting statistics of OTCAD.

OTCAD also classifies the attackers and industry sectors for each attack (when possible). The attacker classifications consist of the following types: targeted attack, untargeted attack, disgruntled employee, and unknown. The RISI database[2] its industry classification is used for the industry sectors, namely: pulp and paper, power & utilities, food & beverage, electronic manufacturing, transportation, petroleum, water/waste water, chemical, metals, automotive, general manufacturing, and pharmaceutical, other, and unknown.

[2] https://us-cert.cisa.gov/ncas/current-activity/2021/06/02/cisa-releases-best-practices-mapping-mitre-attckr Accessed June 3rd, 2021



3.1. Criteria

The following criteria are used to determine if attacks are included in OTCAD and how they are mapped to the different tactics and techniques. These criteria are chosen in such a way that OTCAD is as factual as possible, and to make sure that it is not diluted by a single speculative report.

- The information on which the mapping is based must be publicly available. This makes sure that OTCAD's data is verifiable.
- From information sources, only the information presented as facts is considered. Speculations or strong indications are not included.
- The attack must have a human factor, either as malware creator or active adversary. Cyber security incidents that are solely caused by a hardware failure are not included in OTCAD.
- Attacks must have had an operational impact. If an attack only impacted the IT-systems of an organization it is not included in OTCAD, even if the victim organization revolves around OT.
- A series of attacks that is known to be true, but without concrete victims is only counted once.

It is important to note that these criteria exclude DUQU[3] because there are no actual (publicly known) incidents involving this malware. Another note is that the Night Dragon attacks[4] are only included once, as McAfee confirms that there were attacks but no concrete numbers are given.

3.2. Primary Sources

For the initial release of OTCAD, cyber attacks from five papers and two databases are used. The first paper is by Hassanzadeh *et al.*[5] and gives an overview of cyber security incidents within the water sector between 2000 and 2019. The second paper is by Fischer *et al.*[6], it contains a comprehensive list of cyber attacks in the energy sector between 1982 and 2017. The third paper is by Hemsley and Fisher[7] and evaluates ICS cyber-incidents between 2000 and 2017. The fourth paper is by Miller and Rowe[8], this paper gives an overview of SCADA and critical infrastructure cyber-incidents between 1982 and 2012. The last paper used as information source is by Applied Risk[9] and gives an overview of cyber attacks in 2020.

The first database used is the RISI database[2], this database contains industrial security incidents between 1982 and 2015 with varying reliability levels. From this database only the incidents with the highest reliability level are used. The second database is the VERIS Community Database[10], a community driven database that contains both IT and OT related cyber security incidents. This database categorizes incidents per sector using the North American Industry Classification System (NAICS)[11], the following codes are used as initial filter for the database:

- 11 - Agriculture, Forestry, Fishing and Hunting
- 21 - Mining, Quarrying, and Oil and Gas Extraction
- 23 - Construction
- 31, 32, 33 - Manufacturing
- 48, 49 - Transportation and Warehousing
- 562 - Waste Management and Remediation Services
- 622 - Hospitals

Furthermore, if the malware used in a cyber attack is known, information about that malware is used in addition to the reported information using the same criteria (when applicable).

3.3. Outcome

From the 133 attacks that meet the criteria, there are 72 attacks that could be mapped to atleast one technique. Furthermore, 25 attacks could be completely mapped, meaning that each tactic has atleast one technique mapped (including not applicable). The statistics presented in this section are from the subset of attacks with at least one technique mapped. The ranking of attacker and sector classifications can be found in Table 1 and Table 2 respectively. The statistics from the mapping to ATT&CK for ICS can be found in Table 3 where the techniques are ranked from most to least occurring. The added unknown and not applicable mapping options are underlined as extra indication that these do not belong to ATT&CK for ICS. The top and bottom numbers next to the techniques show the amount and percentage that each technique occurs in OTCAD respectively.

Targeted attack	35
Untargeted attack	14
Disgruntled employee	13
Unknown	10

Table 1: Attacker classification ranking.

Power and Utilities	17	Automotive	5	Electronic Manufacturing	1
Transportation	14	Metal	3	Chemical	1
Petroleum	9	General Manufacturing	3	Pharmaceutical	1
Water/Waste Water	7	Pulp and Paper	1	Unknown	1
Other	7	Food & Beverage	2		

Table 2: Number of attacks per sector.

Initial access			Execution			Persistence			Evasion			Discovery			Lateral Movement		
Engineering Workstation Compromise	18	25%	Unknown	21	29%	Not applicable	24	33%	Not applicable	32	44%	Not applicable	30	42%	Not applicable	29	40%
Unknown	15	21%	User Execution	14	19%	Program Download	13	18%	Unknown	17	24%	Unknown	19	26%	Unknown	16	22%
Spearphishing Attachment	13	18%	Graphical User Interface	9	13%	Valid Accounts	13	18%	Masquerading	10	14%	Remote System Discovery	17	24%	Valid Accounts	13	18%
Exploit Public-facing Application	9	13%	Execution through API	8	11%	Unknown	13	18%	Exploitation for Evasion	7	10%	Network Service Scanning	7	10%	Exploitation of Remote Services	9	13%
External Remote Services	7	10%	Not applicable	7	10%	Hooking	9	13%	Indicator Removal on Host	8	11%	Control Device Identification	5	7%	External Remote Services	4	6%
Supply Chain Compromise	5	7%	Project File Infection	7	10%	Project File Infection	5	7%	Rootkit	4	6%	Network Connection Enumeration	5	7%	Remote File Copy	4	6%
Internet Accessible Device	4	6%	Scripting	6	8%	System Firmware	1	1%	Rogue Master Device	1	1%	I/O Module Discovery	3	4%	Program Organization Units	2	3%
Wireless Compromise	4	6%	Command-Line Interface	6	8%	Module Firmware	0	0%	Utilize/Change Operating Mode	1	1%	Network Sniffing	3	4%	Default Credentials	1	1%
Replication Through Removable Media	3	4%	Change Program State	4	6%				Spoof Reporting Message	0	0%	Serial Connection Enumeration	1	1%			
Not applicable	3	4%	Program Organization Units	3	4%												
Drive-by Compromise	2	3%	Man in the Middle	2	3%												
Data Historian Compromise	1	1%															

Collection			Command and Control			Inhibit Response Function			Impair Process Control			Impact		
Not applicable	31	43%	Not applicable	23	32%	Not applicable	24	33%	Not applicable	30	42%	Loss of Productivity and Revenue	20	28%
Unknown	21	29%	Standard Application Layer Protocol	18	25%	Unknown	20	28%	Unknown	22	31%	Loss of Availability	17	24%
Automated Collection	9	13%	Unknown	18	25%	Denial of Service	18	25%	Unauthorized Command Message	8	11%	Loss of Control	15	21%
Data from Information Repositories	7	10%	Commonly Used Port	17	24%	Data Destruction	12	17%	Service Stop	7	10%	Theft of Operational Information	15	21%
Screen Capture	4	6%	Connection Proxy	1	1%	Program Download	4	6%	Modify Parameter	6	8%	Loss of View	13	18%
Program Upload	3	4%				Alarm Suppression	2	3%	Masquerading	4	6%	Manipulation of Control	8	11%
Detect Operating Mode	2	3%				Block Command Message	2	3%	Change Program State	3	4%	Damage to Property	7	10%
Detect Program State	2	3%				Device Restart/Shutdown	2	3%	Program Download	3	4%	Denial of Control	7	10%
I/O Image	2	3%				Manipulate I/O Image	2	3%	Modify ControlLogic	2	3%	Loss of Safety	6	8%
Location Identification	2	3%				Rootkit	2	3%	Module Firmware	2	3%	Unknown	5	7%
Monitor Process State	2	3%				Utilize/Change Operating Mode	2	3%	Brute Force I/O	1	1%	Not applicable	4	6%
Role Identification	2	3%				Activate Firmware Update Mode	1	1%	Spoof Reporting Message	1	1%	Manipulation of View	3	4%
Point & Tag Identification	1	1%				Block Reporting Message	1	1%	Rogue Master Device	0	0%	Denial of View	2	3%
						Block Serial COM	1	1%						
						Modify Alarm Settings	1	1%						
						Modify Control Logic	1	1%						
						System Firmware	1	1%						

Table 3: The ATT&CK for ICS statistics from the dataset.

4. Trends

This section highlights some of the trends that can be observed within OTCAD while giving possible explanations for their existence. These trends, ranging from ranking-wide trends to single techniques, give insights in how the OT threat landscape has changed over the years. The presented trends in this section are not necessarily the only trends present in OTCAD, but they are interesting examples of OTCAD's capabilities.

4.1. Unknown & Not Applicable

As can be seen in Table 3, *unknown* and *not applicable* are at the top of the ranking for nearly all tactics, the exceptions being *initial access* and *impact*. This is not unexpected, the information related to these tactics is usually reported by news sources. The reason that *unknown* is ranked this high for the remaining tactics is because details about cyber attacks are either kept private or are simply not available (e.g. due to the lack of meaningful logging). Moreover, even if detailed information about attacks is available, for example official lawsuit documents[12], it does not necessarily mean that this information is usable in OTCAD.

On the other hand, the ranking of *not applicable* has possible explanations that differ per tactic. *Not applicable* scores lower for the *initial access, execution* and *impact* tactics. Given that these three tactics are the cornerstones of a cyber attack, this is not unexpected. The reason that *not applicable* is present in these three tactics has multiple reasons; for *impact* this includes a failed attack, for *execution* it simply means that there was no execution on a technological level. The three not applicable mappings on initial access are from disgruntled employees not in need to compromise anything as they had legitimate access to the systems needed to perform their attack.

The remaining tactics have *not applicable* at the top of their ranking. The first, *persistence* is explained through the lack of needing to stay persistent in a system, or even the lack of capabilities to stay persistent. For example, in the early 2000's worms were the main source of (OT) cyber attacks. One of these worms was the Slammer worm [13], this worm only resides in memory, meaning that rebooting the infected machine would remove the worm.

Nearly half of the attacks mapped (47%) did not include any *evasion* tactics. These attacks consists mostly of attacks with disruptive intentions, such as ransomware attacks and attacks by disgruntled employees. Both these types of attacks and attackers do not have any reason, nor the capabilities, to be evasive.

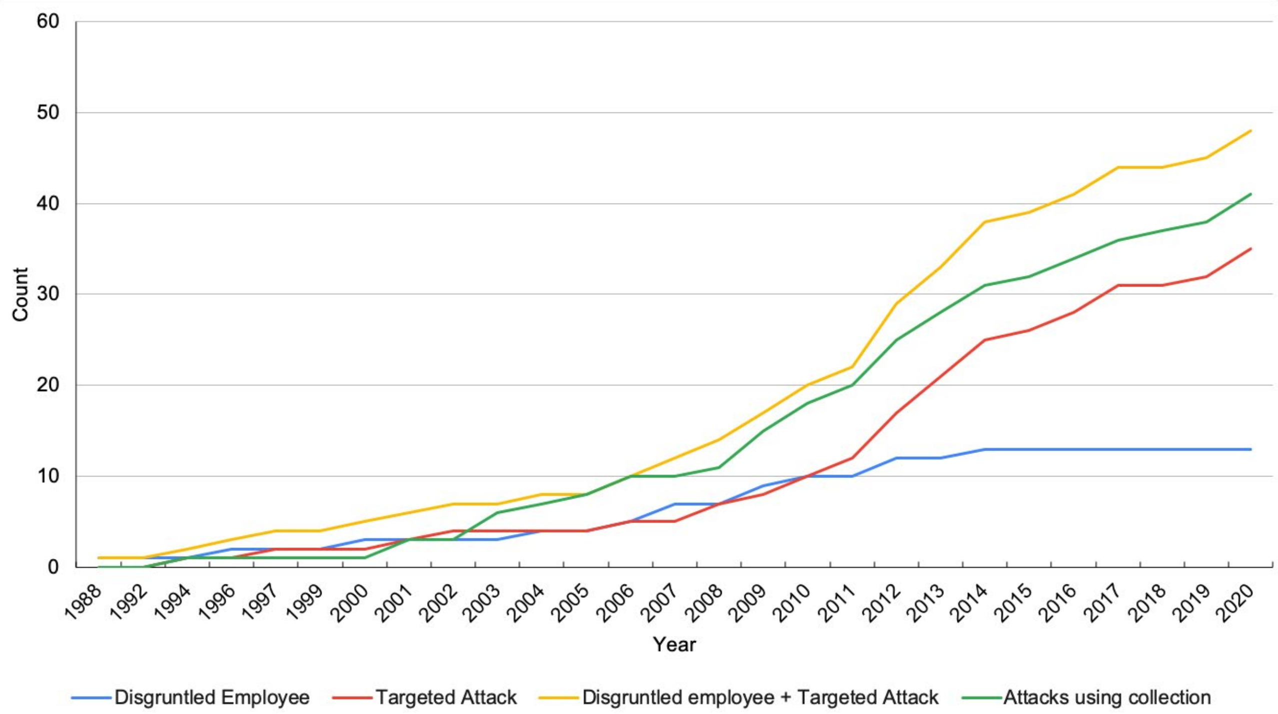


Figure 1: Cumulative occurrences of targeted attacker classifications and cyber attacks that included at least one collection technique.

Nineteen attacks have *not applicable* mapped to both *discovery* and *lateral movement*. This can be expected; most of the time the former is needed to successfully perform the latter. Other reasons include attacks where the adversary was an ex employee, hence no discovery needed as they had knowledge about the network, and attacks where compromising a single machine was enough already.

As can be seen in Figure 1, the *collection* of data by adversaries has a strong correlation with the attacks being classified as a *targeted attack* or *disgruntled employee*. This is in line with adversaries only being interested in data if they are targeting a specific organization.

There is not always a need for any from of *command and control*, for example in completely manual attacks [14] and self-replicating malware. The *not applicable* numbers for *command and control* are similar to multiple other tactics, however there is no correlation between them.
The *inhibit response function* tactic was in most cases *not applicable* due to most attacks lacking the need to actually prevent responding to the attacks (just like *evasion*). This tactic became more popular with the rise of ransomware where *data destruction* is an essential part of the attack.

Lastly, for the *impair process control* tactic to be applicable, attackers needed to have specific intentions. These intentions align with *targeted attacks*, which was not the case for most attacks present in OTCAD.

4.2. Spearphishing

Even though *spearphising attachment* is the third ranked initial access technique, its first occurrence was only in 2011. If only attacks from 2011 onward would be taken into account, *spearphising attachment* would minimally be present in over 60% of the attacks. 2011 is also the same year in which targeted attacks became the most common attacker classification (see Figure 2) which is an attacker classification that is closely associated with spearphishing. The sudden speed at which the usage of spearphishing attachment increased is unique within OTCAD. The amount of *spearphising attachment* attacks (1.3 average occurrences per year) grew with about the same speed as all other *initial access* techniques combined (2 average occurrences per year) in that period.

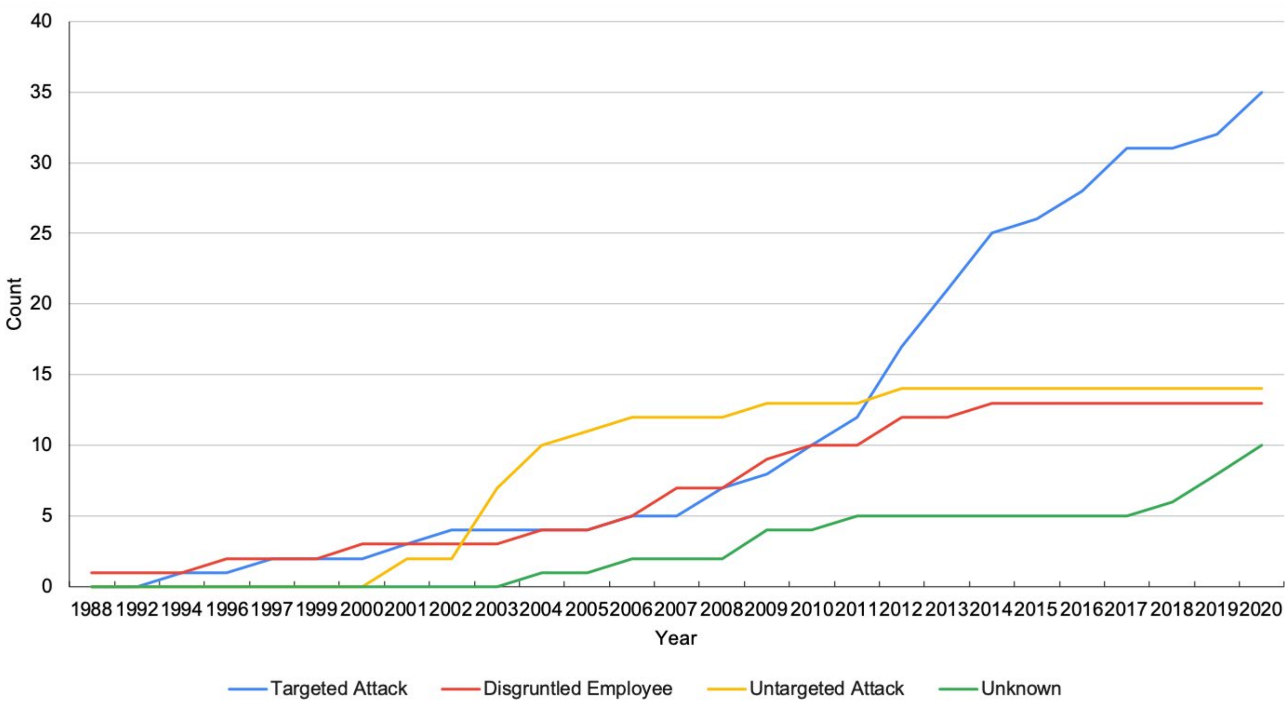


Figure 2: Cumulative attacker classifications per year.

4.3. Collection

Before 2008, the only four attacks (14% of the total attacks) could be mapped to a *collection* technique. Moreover, these four attacks all used *automated collection,* the variation in used techniques within *collection* only came after 2008. This contrast is only this big in this tactic, which can be seen in Figure 3. Starting from 2009 the techniques started to differ, and from 2014 onwards all techniques had been used at least once. Over these years the amount of attacks that included a known *collection* technique grew to 41 (57% othe total attacks).

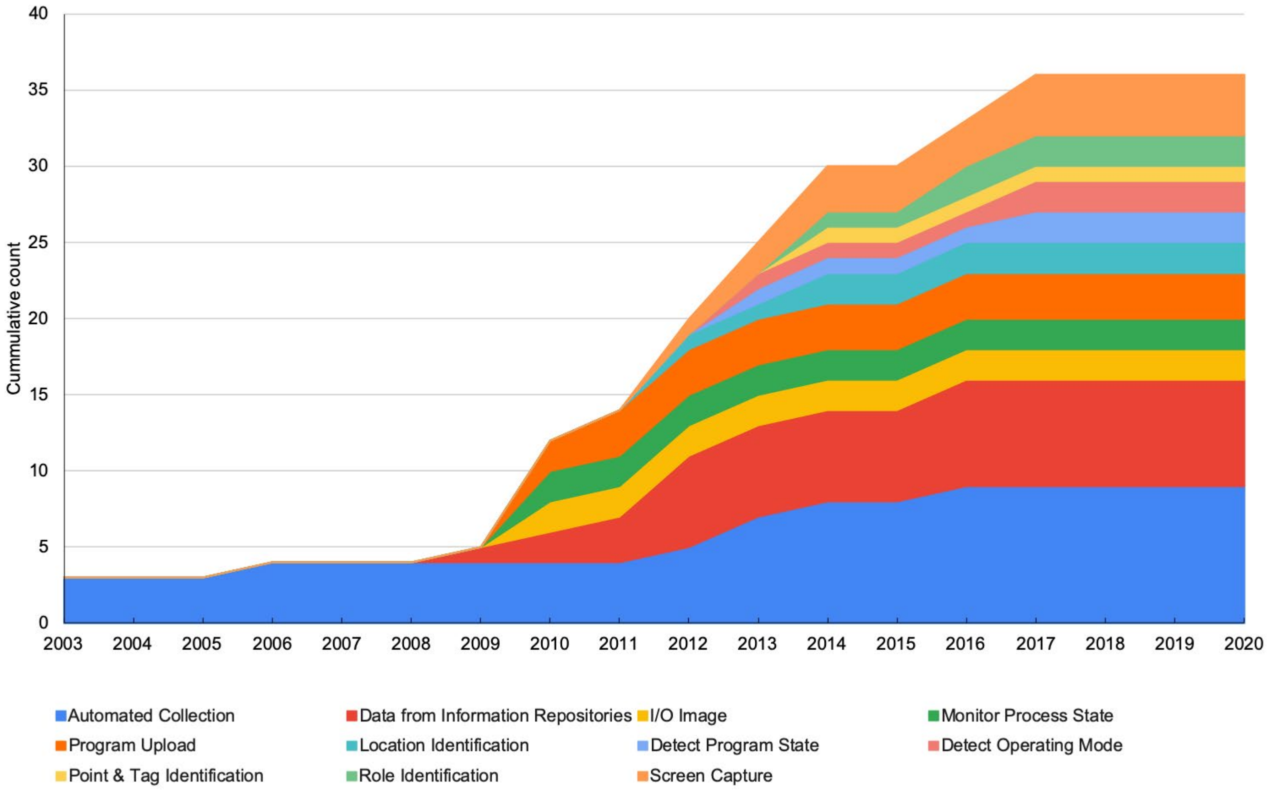


Figure 3: Cumulative occurrences of each collection technique stacked on top of each other.

5. Discussion

The creation of OTCAD faced two difficulties; the first one is the release of ATT&CK for ICS version 9 during its creation, the second one the lack of available information about cyber attacks. These difficulties will continue to create problems for OTCAD as ATT&CK for ICS will be updated regularly, and details about cyber attacks will continue to be kept incomplete. The consequences of these difficulties can already be seen in Table 3, *unknown* is ranked high in most tactics and the techniques in this table are already outdated. However, as will be explained in this section, these difficulties are not necessarily bad things and overcoming them is not mandatory for OTCAD's existence.

5.1. Version 8 vs Version 9

Version 9 of the ATT&CK for ICS matrix has two directly noticeable changes compared to version 8; the first is the addition of the *privilege escalation* tactic, the second is the big reduction in *impair process control* techniques (from eleven to five techniques). Other, smaller, changes are related to the removal and addition of techniques in each tactic. The update did not include any form of reasoning for these changes, which makes it harder to understand the vision of the creators.

Even though the updates brings varying levels of improvements, version 9 is not an improvement from OTCAD's perspective. A reason for version 9 to be less aligning with OTCAD's purpose is that ATT&CK frameworks are "based on real-world observations", meaning that removed techniques might not be observed any more. However, it is important that these techniques should stay preserved for incentives like OTCAD.

The biggest positive change from version 8 to version 9 is the change of *external remote services* to *remote services* in *lateral movement*. This change allows users of ATT&CK for ICS to map a lateral movement technique to adversaries using legitimate services which are being used as intended. *Remote services* is also added to the *initial access* tactic, which acknowledges that misconfigured services can be a way for adversaries to access an internal network as well. Note that this differs from *external remote services*, these are the intended services to access an internal network.

The negative changes that version 9 introduced (from OTCAD's perspective) on the other hand were big enough to decide to not use this newer version. Mapped techniques (e.g. *masquerading* in *impair process control*) are removed from tactics, or moved to different tactics, while techniques that have not been mapped to are still in the version 9 (e.g. *spoof reporting message* in evasion). The addition of techniques is not necessarily good either; the added techniques in version 9's *initial access* makes it a very cluttered tactic due to the low level of uniqueness between some of the techniques. There are now three remote services related techniques in initial access; *remote services* itself, *exploitation of remote services*, and *external remote services*. These techniques do not cover the whole range of remote services related techniques. A complete list should actually include four techniques but "exploitation of external remote services" is missing. A plausible reason for this is that the creators of ATT&CK for ICS did not observe this technique being used in the ICS threat landscape. The introduction of sub-techniques in ATT&CK for ICS would create a less cluttered framework, this would allow for the remote services sub-techniques to be grouped under a single "access through services" technique.

However, a lot of variation does not directly mean a cluttered tactic. The variation within version 8's *impair process control* enabled fine-grained mapping due to the level of uniqueness between techniques within this tactic. When looking at the ranking of *impair process control* techniques (as presented in Table 3), it shows that the least mapped techniques are kept rather than the most mapped ones. The most mapped technique that is changed within *impair process control* is *service stop*, which is moved to *inhibit response function*. Although *service stop* fits in *inhibit response function*, it should also be present in impair process control as it can be used to "disrupt control logic and cause determinantal effects to processes being controlled in the target environment".

A possible way to use each version its strengths is by combining the versions, but this would break compatibility with existing tools. One of these tools is the MITRE ATT&CK Navigator[3], which is essential to quickly adjust and add cyber attacks to OTCAD. Furthermore, combining versions will only lead to confusion when newer versions get released. Lastly, it would mean that OTCAD maps to a non-existing ATT&CK for ICS version, so essentially OTCAD would not map to ATT&CK for ICS.

[2] https://mitre-attack.github.io/attack-navigator/

As both ATT&CK for ICS and OTCAD will be updated regularly in the future, we will re-evaluate which ATT&CK for ICS version is suitable for OTCAD when appropriate. Furthermore, these re-evaluations can be done in collaboration with the OT cyber security community when users have had time to use OTCAD.

5.2. Lack of Information

Publicly disclosed information is important from a researchers perspective, as it enables initiatives like OTCAD to exist and be verifiable. However, the amount of publicly disclosed information is currently lacking. From the collected attacks, only 54% had publicly disclosed information that was both criteria meeting and mappable. Even with cyber security being taken more seriously over the last years, there has been no significant increase in publicly disclosed information. As can be seen in Figure 4, this roughly even split of cyber attacks that had mappable information and those who had not is continuously present over the years. The amount of collected cyber attacks is also not representative for the total amount of cyber attacks that happened within OTCAD's timeline. For example, the US ICS-CERT (Computer Emergency Response Team) reported 257 incidents in 2013 [15], but only 4 cyber attacks from 2013 are included in OTCAD. Although not all these incidents would meet OTCAD's criteria, it still shows that a lot of cyber attacks are not publicly disclosed. This makes it harder to create a complete picture of the threat landscape, as unique attacks might be overlooked.

On the other hand, publishing detailed information about cyber attacks might expose previously undisclosed vulnerabilities or enable adversaries to mimic the used tactics and techniques. This in turn can hurt other organizations as adversaries can usually respond faster to new findings. Especially in OT this can be problematic, because mitigating vulnerabilities can be costly and time consuming. Moreover, publishing details about cyber attacks can be seen as negative publicity, hence there is no real incentive (other than for research purposes) to release information.

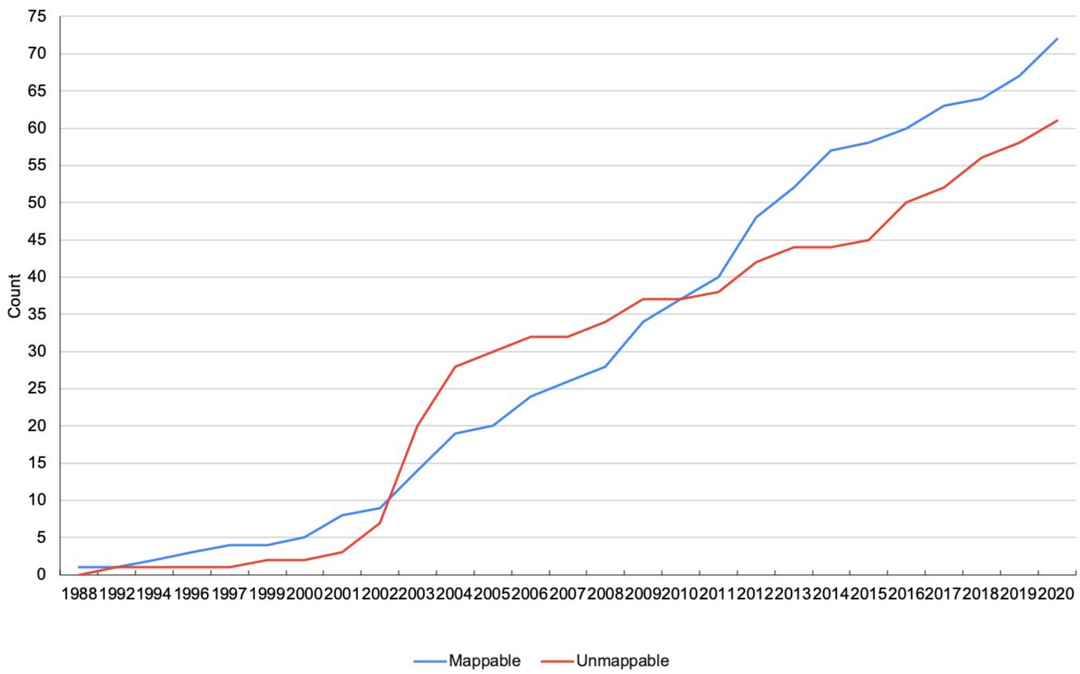
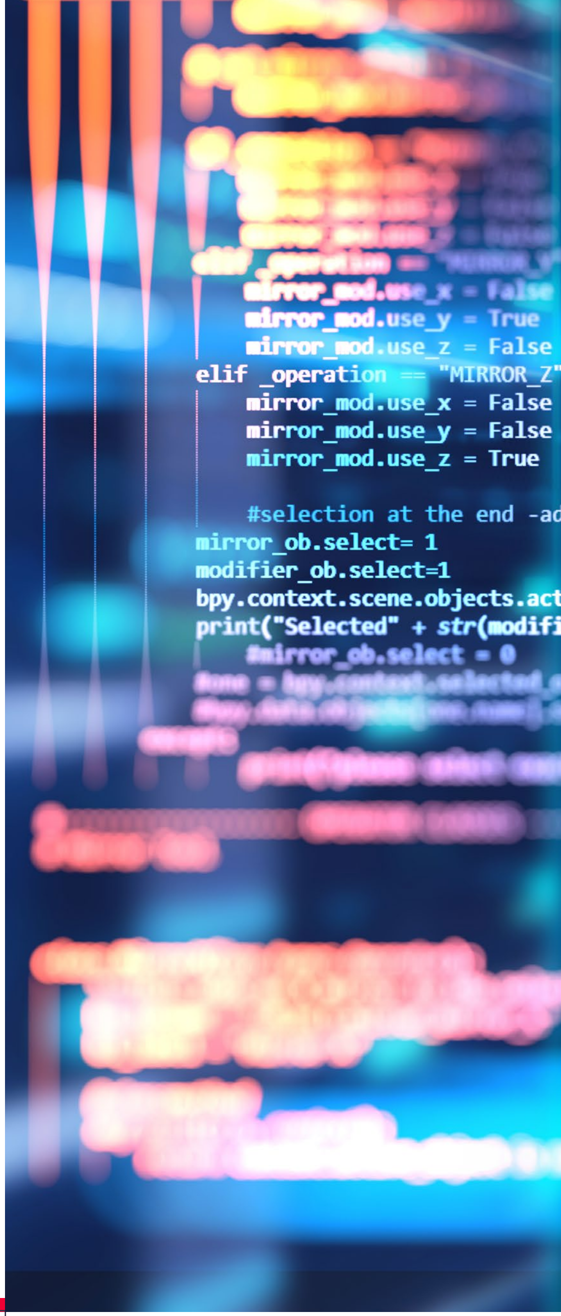


Figure 4: Cumulative mappable and unmappable cyber attack occurrences within OTCAD.

6. Conclusion

With the release of OTCAD, there is now a publicly available database of OT-related cyber attacks that are mapped to MITRE's ATT&CK® for ICS. The wide usage of ATT&CK within the cybersecurity domain makes OTCAD easy to use for interested parties.The criteria set for OTCAD ensures that its data stays credible and verifiable, so users can be confident that the statistics they extract from OTCAD are as correct as possible. OTCAD can be used to provide historical insights, and to recognize cyber attack trends within OT. Furthermore, OTCAD can easily be extended by its users which, next to adding new cyber attacks to the database, opens up more research possibilities.



About Secura

Secura is your independent cybersecurity expert. Secura provides insights to protect valuable assets and data. We make cybersecurity tangible and measurable in the field of IT, OT and IoT. With security advice, testing, training and certification services, Secura approaches cybersecurity holistically and covers all aspects from people, policies, organizational processes to networks, systems, applications and data.

For more information, please visit: **secura.com.**

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter: secura.com/subscribe.

Follow us on

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

References

[1] “MITRE ATT&CK,” [Online]. Available: https://attack.mitre.org/.

[2] “RISI database,” [Online]. Available: https : / / www . risidata . com/ (visited on Mar. 15, 2021).

[3] “W32.Duqu: The precursor to the next Stuxnet,” Symantec, Nov. 2011. [Online]. Available: https://docs.broadcom.com/doc/w32-duqu-11-en (visited on May 26, 2021).

[4] “Global Energy Cyberattacks: “Night Dragon”,” McAfee, Feb. 2011.

[5] A. Hassanzadeh, A. Rasekh, S. Galelli, et al., “A Review of Cybersecurity Incidents in the Water Sector,” Journal of Environmental Engineering, Sep. 2019.

[6] L. Fischer, M. Uslar, D. Morrill, M. D¨oring, and E. Haesen, “Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector,” Ecofys, Oct. 2018.

[7] K. Hemsley and R. Fisher, “History of Industrial Control System Cyber Incidents,” Idaho National Laboratory, Dec. 2018.

[8] B. Miller and D. Rowe, “A Survey of SCADA and Critical Infrastructure Incidents,” SIG- ITE’12, Oct. 2012.

[9] “The State of Industrial Cyber Security 2020,” Applied Risk, Nov. 2020.

[10] “The VERIS Community Database,” [Online]. Available: https://github.com/vz- risk/ vcdb (visited on Mar. 31, 2021).

[11] “North American Industry Classification System,” [Online]. Available: https://www.census. gov/naics/?58967?yearbck=2017 (visited on Mar. 31, 2021).

[12] “United States of America v. Mario Azar,” District Court for the central district of California, Feb. 2009.

[13] “Worm:W32/Slammer,” [Online]. Available: https://www.f-secure.com/v-descs/mssqlm.shtml (visited on Mar. 18, 2021).

[14] “Antwerp incident highlights maritime IT security risk,” Seatrade Maritime News, Oct. 2013. [Online]. Available: https://www.seatrade- maritime.com/europe/antwerp- incident- highlights-maritime-it-security-risk (visited on Apr. 16, 2021).

[15] “ICS-CERT: Year in Review 2013,” [Online]. Available: https://web.archive.org/web/ 20150714024506/https://ics-cert.us-cert.gov/ sites/default/files/documents/ Year_In_Review_FY2013_Final.pdf (visited on May 26, 2021).

Appendix ATT&CK for ICS matrices

Even though the v9 matrix is, at the time of writing, the latest version of the matrix and thus easily findable online, it is included here for archiving purposes. Table 4 and 5 present the v8 and v9 ATT&CK for ICS matrices respectively.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Table 4: ATT&CK for ICS v8 matrix

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

Table 5: ATT&CK for ICS v9 matrix

Secura

A BUREAU VERITAS COMPANY

BUREAU VERITAS 1828

BUREAU VERITAS

Shaping a World of Trust