SANS ICS Industrial Control Systems

January 5, 2016

Authors:
Robert M. Lee
Michael J. Assante
Tim Conway

ICS Defense Use Case (DUC) # 4:

Analysis of the recent reports of attacks on US infrastructure by Iranian Actors

Note: We are providing a summary of the available information and have not validated if the incident happened the way that has been described in the publicly available reporting. We are providing this summary of information, as we believe elements of the story being conveyed provide a learning opportunity for ICS defenders.

Incident Summary

On December 20, 2015 a report was released from the Wall Street Journal titled "Iranian Hackers Infiltrated New York Dam in 2013[1]". This report provided details of a cyber incident occurring at the Bowman Avenue Dam near Rye, N.Y. in 2013. The day after the WSJ story debuted, the Associated Press released the results of a yearlong AP Media Editors examination of the U.S. energy infrastructure's vulnerability to cyber attack. The AP report published on December 21, 2015 is titled "AP Investigation: US power grid vulnerable to foreign hacks[2]". The AP report provided details of sensitive information discovered by a security researcher, that contained passwords, engineering drawings, and network communications diagrams for a large power producer with assets in the US and Canada. The data breach was reportedly performed in 2013 by infiltrating a trusted vendor network and obtaining the files related to the power producer. Both stories examined incidents that were believed to have been conducted by Iranian cyber actors.

The SASN ICS' Defense Use Cases (DUC) provided in the past have focused on a reported incident or on a single report released. In this case, the authors of this DUC feel defenders can learn important lessons by collectively examining both the AP report and the WSJ report as a single DUC. While the reports do not overlap in regards to target infrastructure, as one focuses on flood control infrastructure and the second focuses on power infrastructure, the reports can be

[1] http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559

[2] http://bigstory.ap.org/article/c8d531ec05e0403a90e9d3ec0b8f83c2/ap-investigation-us-power-grid-vulnerable-foreign-hacks

pieced together as a view of common challenges facing defenders.

Credibility[3]: **4** (WSJ) and **4** (AP)

The Wall Street Journal report has been assigned a credibility score of a 4 as it cites current and former US officials, confirmed FBI involvement and contact with the asset owners and operators. Preventing the assignment of a 5 as confirmed is the claim in the report detailing the attacks sourced from Iranian hackers and the title of the article which indicated infiltration occurred whereas the article only cites probing activity. As detailed in the report there is potential confusion due to multiple US agency involvement, unclear internet addresses, and rules governing domestic surveillance. This potential confusion contributed to where the adversaries were targeting. This confusion over the target of the malicious communication sent intelligence officials in search of multiple possible destinations, yet there does not appear to be a corresponding reluctance to identify the source of the malicious communication to Iran in spite of the same if not more unclear confusion associated with Iranian IP address space. If the report equally pointed out the uncertainty in confirming the destination as in determining the source, the credibility would have remained a 5 as the events have been confirmed, however the source of the events are only determined as probably true (4).

The components of the AP report that focus on the data breach that impacted Calpine have been determined to be confirmed due to cited statements from a named Calpine official spokesman. The report also builds off of a public Cylance report on activity they have labeled as Operation Cleaver[4]. While the AP report identifies the IP address space as Iranian and some additional indicators identifying Iranian origin, they also carefully point out that while the hacking group coming from IP address space in Tehran, there also contained evidence to hide or mask the source of the communications and knowledge that members of the hacking group were located in the Netherlands, Canada, and the United Kingdom. There are many additional items throughout the AP report that sites other reports in relation to ICS related incidents, each of which may be a lower credibility score, however the authors of this DUC are focusing on the unique reporting of the Calpine data theft incident in the determination of the credibility score and the defender lessons learned. The score of a 4 was assigned instead of a 5 due to language in the report including "Cyberattackers had opened a pathway into the networks running the United States power grid." Review of the materials support a focus by an adversary on Calpine however the report notes that Calpine's statements indicate they do not believe Calpine or other segments of the power grid were actually breached. The information stolen is valuable to attackers, as it significantly cuts reconnaissance time and prepares the attacker

[3] Credibility of the information is rated in a scale from [0] Cannot be determined, [1] Improbable, [2] Doubtful, [3] Possibly true, [4] Probably true, [5] Confirmed

[4] https://www.cylance.com/operation-cleaver-cylance

to achieve faster discovery and more fruitful lateral movement plans, but did not increase the vulnerability of the power grid or open up attack paths.

Amount of Technical Information Available[5]: **2** (WSJ) and **1** (AP)
The WSJ report provided some details in regards to how the adversary may have gained access to the target environment, and some details in regards to how the activity was detected by US intelligence agencies. There was no additional information provided in regards to the assessment of what actions were taken by the adversary other than characterizing them as "probing" in nature which would be synonymous with reconnaissance activity. This does not indicate that an actual breach occurred and may be the result of Internet connected and unauthenticated systems. It is unclear how that determination was made or if the dam's control capabilities were even available remotely for the targeted facility. For these reasons the WSJ report has been assigned a technical score of 2 indicating a lack of most of the data but the presence of some technical details are available to assist the authors of this DUC in identifying specific defender lessons learned.

The AP report provided some insight into where the sensitive information was obtained from without specific details into who the targeted vendor was or any additional details on the vendor environment vulnerabilities, exploits utilized, or targeted vendor architecture. For these reasons the AP report has been assigned a technical score of 1 indicating high-level summary details are available to assist the authors of this DUC in identifying specific defender lessons learned without specific technical details.

Attacker & TTP Description

Attacker: While the WSJ report has identified Iranian attackers and the AP article has hinted at Iranian attackers, the authors of this DUC will characterize the adversary sequence of events based on the targets and what has been confirmed as successful outcomes of the adversary actions. The authors of this DUC will not consider whether the adversaries were or were not from Iran or if they were or were not state sponsored. As of the writing of this article, an Iranian hactivist[6] has claimed responsibility for the incident identified in the WSJ report. No one has claimed responsibility for the incident identified in the AP report although Cylance's Operation Cleaver report also identified these incidents as Iranian in nature.

[5] Amount of Technical Information Available is an analyst's evaluation and description of the details available to deconstruct the attack provided with a rating scale from [0] No specifics, [1] high-level summary only, [2] Some details, [3] Many details, [4] Extensive details, [5] Comprehensive details with supporting evidence

[6] https://www.secureworldexpo.com/tags/bowman-avenue-dam

Capability: Beginning with the WSJ report, the target site identified in the report currently appears to have a system that is responsible for automating the sluice gate. The system will vary the outlet opening based on water elevation measurements. This would be the target of a determined adversary looking to overflow the dam as they could possibly manipulate readings from the measurement system and force the sluice gate into a full open position impacting water levels upstream or downstream or force the gate into a full closed position. This activity would impact water levels upstream or downstream.

These actions could have negative effects on wildlife, homes, and resident safety. The particular dam mentioned, has existed with a fixed open orifice of 15 ft by 2.5 ft wide with a fixed timber gate. The capability for forcing the gate full open has been the case since 1941 when the dam was rebuilt[7]. An adversary may want to force the sluice gate closed but they would have to be very patient and wait for the next 100 year storm to realize their objective.

Notably, it appears this activity would not have been possible for a remote adversary due to what appears to be a limitation of control due to project implementation timing. Statements made by the Rye City Manager[8] indicate that the sluice gate was installed when the adversary appeared to gain access, however ***the automated controls were not active, and therefore the adversary could not impact the operation of the gate.***

For this reason it is difficult to determine if the adversary chose to only probe devices on the network and chose not to control or if they had nothing they could control. In either case it is difficult to measure the adversary capability based on this contained environment as the only available options to the adversary were to gain remote access and perform asset reconnaissance or to gain access to an unauthenticated Internet accessible device and read information off of it. There was no capability of a follow on attack. If somehow there was though the impact of an attack at this facility would have been very limited.

Regarding the AP report and the data exfiltration campaign against a vendor of a power producer in the US and Canada there was no reported compromise of an ICS facility. As indicated by the score of 1 in the technical information category, it is impossible to determine the capability of the adversary conducting this data theft campaign or derive the possible intent based on the level of investment that was made to achieve a goal.

[7] http://www.egovlink.com/public_documents300/rye/published_documents/Engineering/Flood%20Studies/Project%20Report%20-%20Flood%20Mitigation%20Study%20-%20Bowman%20Avenue%20Dam%20Site.pdf

[8] http://patch.com/new-york/pelham/astorino-demands-answers-rye-dam-cyber-security-breach-0

For example, if details were available about the vendor that was targeted an analysis could be performed regarding the vendor security profile, how they conduct request for proposals, how they exchanged data with their customers, how their field engineers protect sensitive data when they visit customer sites, and a number of other open source analysis attempts could be made to determine the difficulty of targeting the vendor to gain access to 3rd party data. If the adversary was targeting Calpine specifically and performed reconnaissance against the target it is possible that they determined the path of least resistance into Calpine's networks was through a 3rd party vendor network. This could have served as motive to move to target the contractor's environment and obtain the data they desired but that is purely speculation. More likely from previously analyzed campaigns similar in nature, this was a campaign of efforts by a focused adversary and while the targets, Calpine and potentially other energy providers, may have been set the adversary's collection efforts were opportunistic in nature.

Given the type of data, amount of data stolen, and type of targets over an extended period of time the authors of this DUC have come to the conclusion that the adversary group was capable, organized, and funded. If for example an adversary targeted many vendors or individuals through a phishing campaign with a malicious attachment, succeeded with one, obtained a foothold on an individual's workstation with access to a project file share folder that contained customer project datasheets, diagrams, and engineering drawings, then they simply used FTP to move the files to an open university file share, then the authors of this DUC would assign a lower capability to that adversary. Lacking technical details and adversary intent makes it difficult to determine the capabilities of the adversary identified in the AP report. The conclusion put forth in the media stating that this activity is definitively Iranian in nature was not able to be reproduced by the authors of this DUC.

The authors of this DUC would typically look to assess capabilities based on what a material attack would require the adversary to achieve. Consider an assessment of adversary ICS capabilities by looking at the following:

- Evidence of demonstrated skill sets in multiple disciplines
- Demonstrated ability to gain access and ability to pivot within target network
- Clear knowledge of specific information for the target
    - Detailed configuration information
    - Control system understanding of protocols, logic, and operational effects
    - Access to current operational functions, and logic

Based on the details of the WSJ report, the adversary demonstrated a skill set to identify access points and gain information from the environment. Based on the facility they accessed, none of the other assessment criteria can be evaluated. Based on the details of the AP report the adversary also demonstrated an ability to gain access to a target environment and possibly pivot within the target network but never breached an ICS organization or its ICS Both cases highlight the concern around Internet connected systems and the need to safeguard sensitive information both on and off the network.

Opportunity: The facility identified in the WSJ report had recently updated to a new sluice gate and therefore appeared to have added operational elements that could potentially be targeted and manipulated. The opportunity to do so at this facility was new and therefore possibly not fully understood, security hardened, and potentially the ideal time to act. Unfortunately for the adversary, it was so new that it was not yet complete and therefore could not be manipulated to cause an adverse effect. However, the report did note that the adversary was able to probe the device because it was connected via a cellular modem. This Internet connected device would have been discoverable via multiple adversary methods and may have been discoverable as simply as using the Internet connected device search engine Shodan. Internet connected control devices are of significant concern to the security of the ICS and will always provide an increased opportunity for adversary actions.

Regarding the AP report it is difficult to determine the opportunity available to an adversary as it is uncertain if they were targeting the vendor or Calpine indirectly through the vendor. As it remains unknown who the vendor is, the authors of this DUC can only examine opportunity of targeting Calpine through information obtained or indirectly through a 3rd party vendor. In August of 2013 when the breach began there was potentially an opportunity for an adversary to target Calpine through a 3rd party vendor as they had just announced the commercial operation of two new power plants in California[9]. Of interest these two plants were under a joint funded project with another organization and likely a large number of contractors and vendors who all would have access to various sensitive documents in relation to the project. However, it should be noted that sources cited in the AP report indicated that some of the documents discovered dated back to 2002 and therefore it would have been a vendor with a long-standing relationship with Calpine not just associated with the two new plants. The new power plants' public announcements though may have increased the interest of the adversary through open source reconnaissance efforts common in

[9] http://investor.calpine.com/investor-relations/news-releases/news-release-details/2013/Two-New-Calpine-Power-Plants-Begin-Commercial-Operations-in-California/default.aspx

adversary campaigns.

Adversaries looking to exploit ICS environments may elect to leverage opportunities related to geopolitical or target specific events, technologies, systems, or architectures. Opportunity based considerations focused on causing an ICS effect may include:

- Single targets with common systems and configurations
- Multiple systems with common centralized control points
- ICS Impact duration long-term or short-term
- Capabilities required to achieve desired results
- Risk level of performing the operation and being discovered

Motivation: The WSJ report indicates Iranian adversaries and makes reference to potential increased capabilities in nation state cyber capabilities, following the Stuxnet attack against Iran's Natanz facility. This would point to a potential motivation driven by geopolitical conditions, however this cannot be confirmed and there is currently at least one competing theory due to the Iranian hactivist group claiming responsibility. The AP reported incident is less clear without referencing what is known from the Clyance report about the larger adversary campaign. In the AP report the focus rested on information that was exfiltrated by the attacker and recovered by Cylance. This could be for the purposes of simply exfiltrating to evaluate future value, sought after the breach to plan follow on targeted attacks, or for the purposes of industrial espionage. Motivation for both reports is uncertain, as each may have involved actors and campaigns that included more broad objectives. It is also important to note that specific attribution in both cases, as reported, is challenging.

ICS Cyber Kill Chain Mapping – Bowman Avenue Dam

The ICS Cyber Kill Chain was published in 2015 by Michael Assante and Robert M. Lee as an adaptation of the traditional cyber kill chain developed by Lockheed Martin analysts as it applied to ICS.[10] The ICS Cyber Kill Chain details the steps an adversary must move through to perform a high confidence attack on the ICS process and/or to cause physical damage to equipment in a predictable and controllable way as displayed in Figure 1.

[10] https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

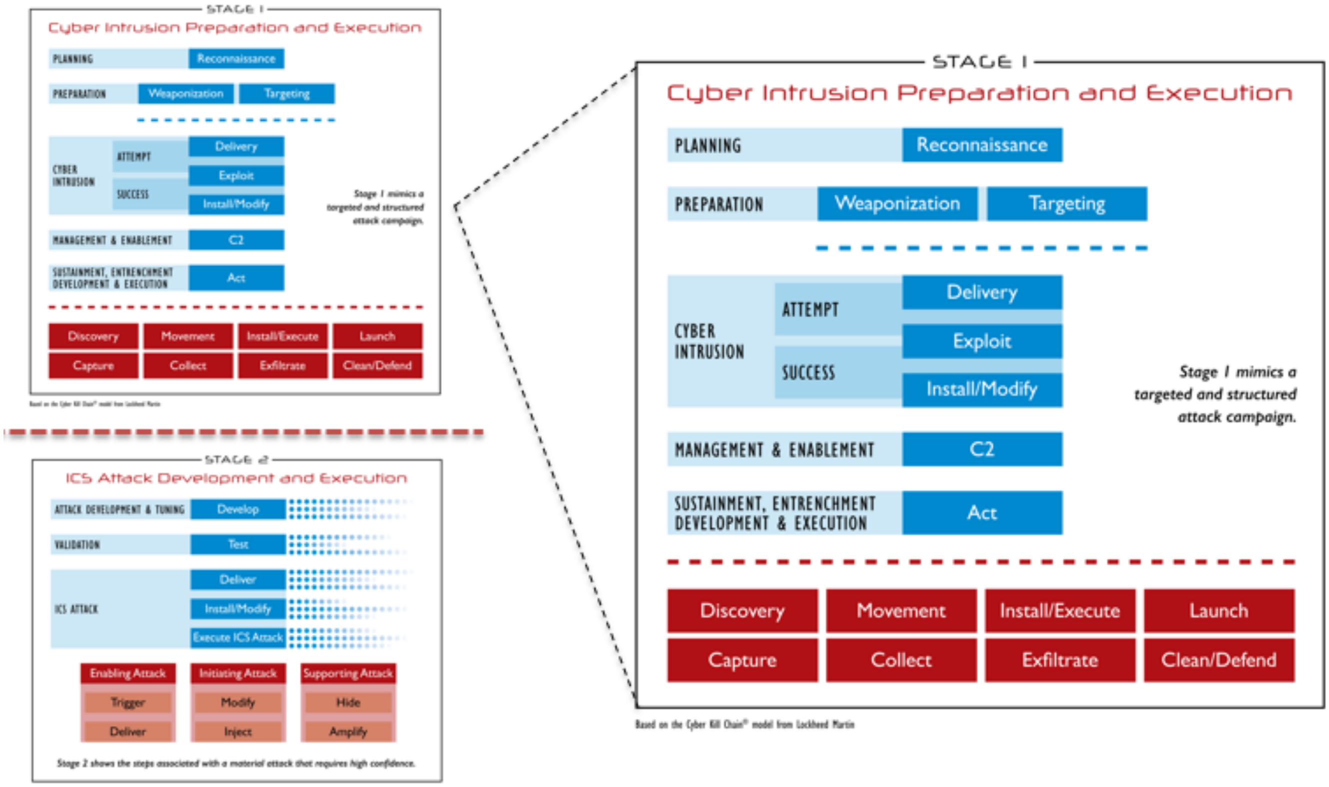


Figure 1: The ICS Cyber Kill Chain with Stage 1 Highlighted

One of the benefits of the ICS Cyber Kill Chain is that it puts forth that properly architected ICS networks are more defensible than traditional information technology networks. There are more opportunities for defenders to identify adversary activity and counter it while there are more complex systems and communication methods that an adversary must become familiar with. However, improperly architecting the ICS and its accompanying networks can lead to a shortened adversary kill chain which occurred with the Bowman Avenue Dam incident.

The WSJ put forth that the control system at the dam was accessed and probed. This would correspond to cyber intrusion type activity and not an attack. Specifically, this would indicate adversary reconnaissance efforts and because the system was specifically probed it also indicates targeting in the ICS Cyber Kill Chain. Depending on the type of access the system could give the adversary there may not have been any need for weaponization to take place. If an adversary is able to perform reconnaissance and then targeting of control systems and their networks there is often enough functionality to perform the cyber intrusion itself (delivery, exploitation, and installation) using native features, commands, and protocols within the system. This has not been reported to have occurred in the Bowman Avenue Dam incident though and the adversary’s activity were entirely confined to the beginning steps of stage one of the ICS Cyber Kill Chain.

The connection of the system directly to the Internet via a cellular modem eliminated the need for the adversary to move through a business network and DMZ. While the adversary still must move through the same kill chain phases it significantly decreases the adversary's time required in doing so to the disadvantage of the defender. Increasing the adversary's time during an operation is one of the few significant costs to the adversary that the defender can impose and additionally affords defender's additional time and opportunities to identify and remediate the intrusion before an attack can take place.

The alleged link to Iran in the incident is not disputed in this DUC although it is questionable without more information presented; therefore for the ICS Cyber Kill Chain the Iranian actor will be used as the aggressor but this should not imply the Iranian government or a higher confidence in the assessment than has been stated previously. Additionally, due to information uncovered for this DUC about the control elements in place at the Bowman Avenue Dam at the time of the adversary's presence it would have been improbable for the adversary to have achieved an attack with impact. Therefore, in the ICS Kill Chain stage two and the ability to impact the dam are marked out as shown in Figure 2.

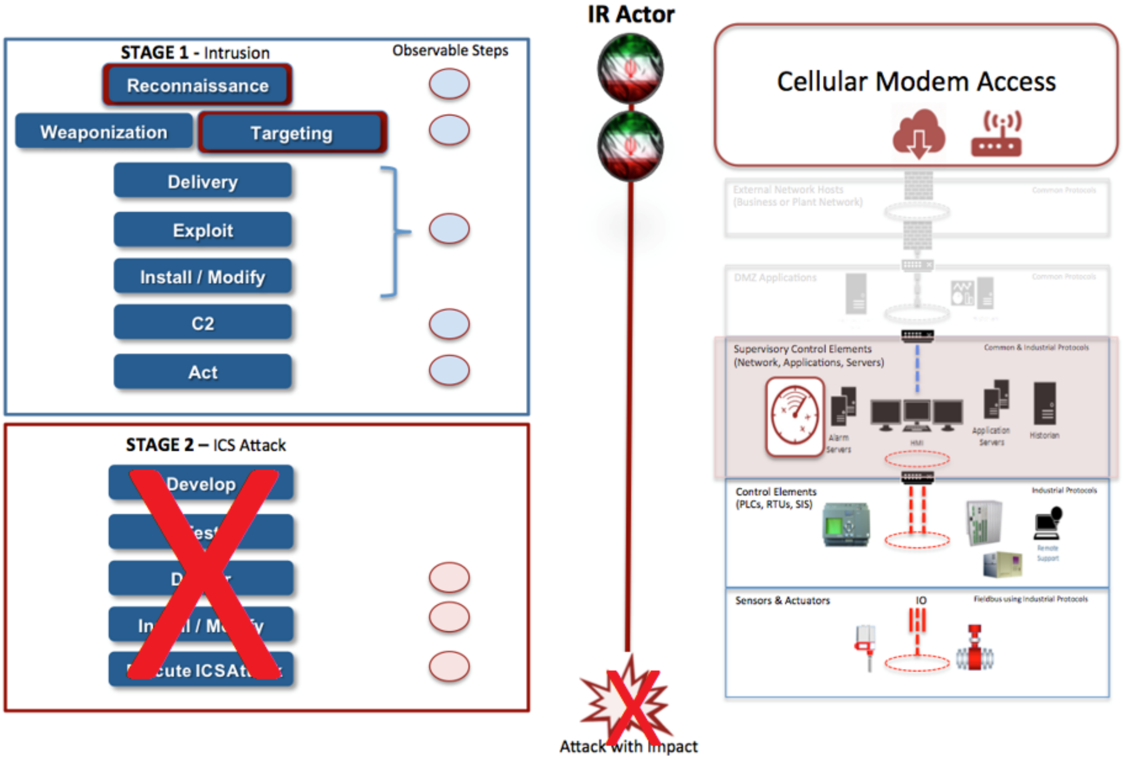


Figure 2: Bowman Avenue Dam Incident ICS Cyber Kill Chain

ICS Cyber Kill Chain Mapping – Calpine Data Theft

The AP research reported that there was no evidence to show that Calpine was breached. The data stolen pertaining to Calpine was taken from a third party contractor. Because no breach of Calpine took place the adversary did not begin the ICS Cyber Kill Chain as no ICS was at risk or targeted. However, the data reported to have been taken was absolutely useful to an adversary. Detailed schematics, information about passwords even if old, network diagrams, and logical addressing of the systems are all types of information that an adversary would hope to acquire about a target. These efforts would help develop a target profile and amplifying information to help quicken adversary activity inside the ICS network upon them gaining access. The type of information detailed does not sound as if it added a great deal of additional vulnerability to Calpine or the power grid but it would have provided the adversary with information helpful in shortening the time required to complete their kill chain in the event that they breached Calpine.

Although there was no ICS Cyber Kill Chain initiated there was the traditional cyber kill chain where the adversary targeted and breached the contractor networks. Based on the recovered documents the adversary would have had to fully compromise the contractor's networks and reach the act phase of the kill chain to exfiltrate information off of the network. Because the information does relate to ICS networks and would be useful to the adversary it can be classified as a stage 0 effort by the adversary against a target that could be used to start an ICS Cyber Kill Chain as shown in Figure 3.

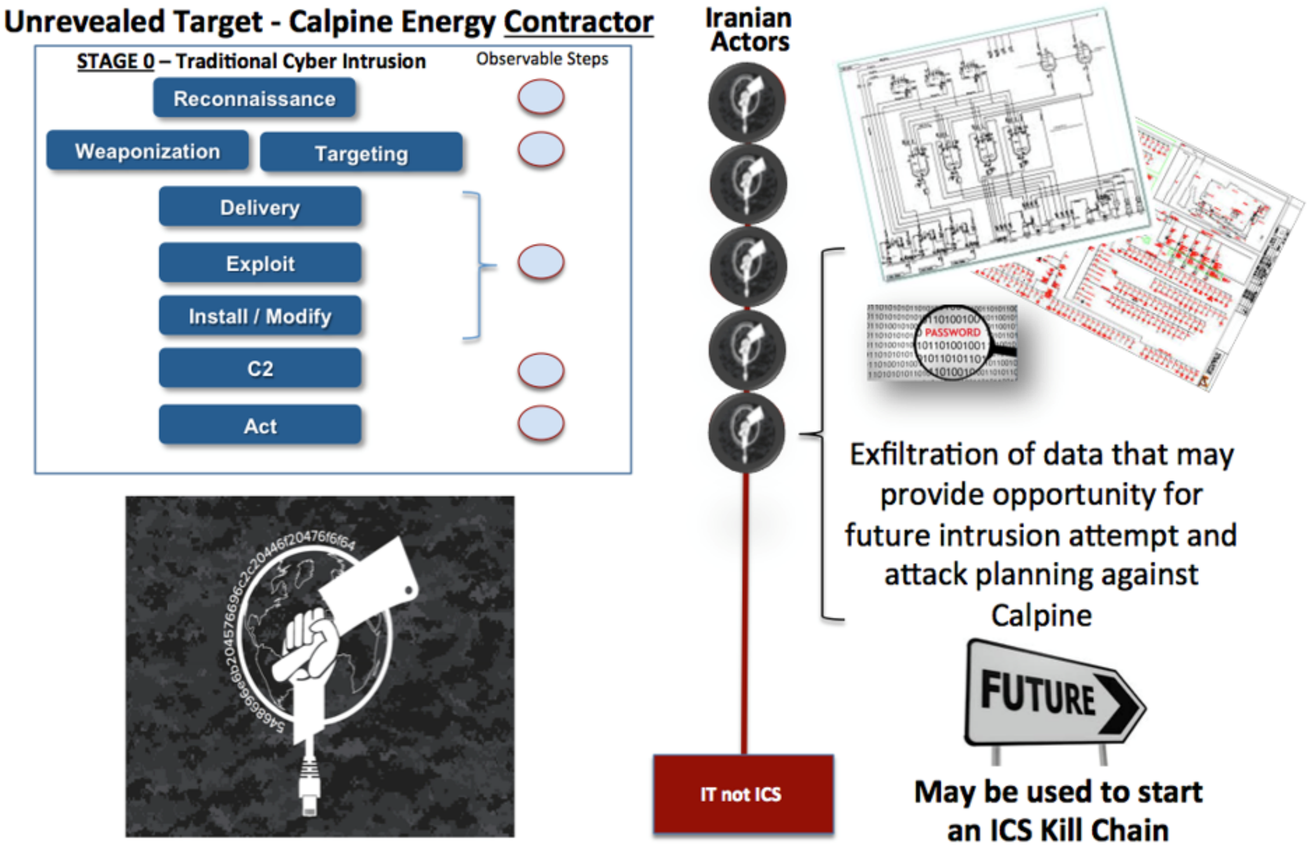

Unrevealed Target - Calpine Energy Contractor
STAGE 0 – Traditional Cyber Intrusion
Observable Steps
Reconnaissance
Weaponization
Targeting
Delivery
Exploit
Install / Modify
C2
Act
Iranian Actors
PASSWORD
Exfiltration of data that may provide opportunity for future intrusion attempt and attack planning against Calpine
FUTURE
May be used to start an ICS Kill Chain
IT not ICS

Figure 3: Kill Chain Mapping - Calpine Energy Contractor

It is important to note that most power system cyber incidents end in the Stage 1 of the ICS Kill-Chain. A number of recent campaigns such as APT 1 related intrusions of US energy infrastructure and the Havex campaign were focused on networks attached to the ICS, but no evidence has been presented that indicates more than some successful cross-overs into the ICS. The development and execution of a Stage 2 attack requires the adversary to plan to achieve a specific effect to the ICS or process. Intrusion into IT systems or even access to an ICS does not immediately position an attacker to disrupt the process or system under control. Developing and deploying an attack that can disrupt the system or manipulate the process can be challenging. Figure 4 provides a visual representation of the need to achieve a 'cross over' and take further actions that can manipulate the ICS to achieve some desired outcome. Causing a disruption to power should be easier than creating a power outage that lasts more than a few days. Developing a Stage 2 attack capable of damaging physical equipment under control is usually very difficult and complex.

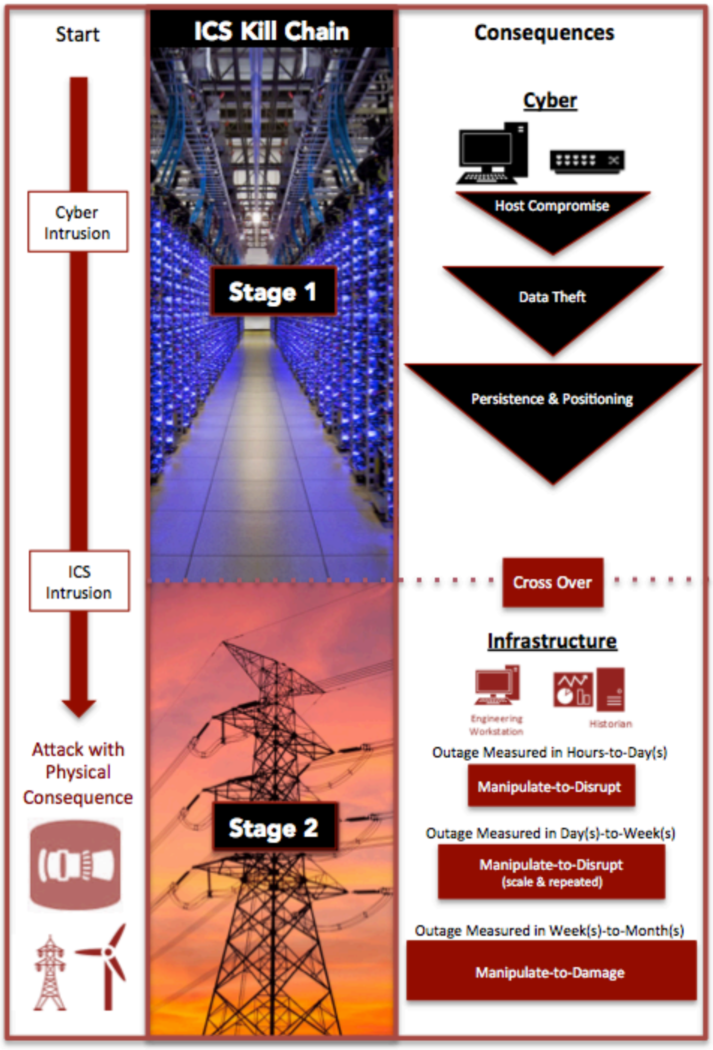

Start
ICS Kill Chain
Consequences
Cyber
Cyber Intrusion
Host Compromise
Stage 1
Data Theft
Persistence & Positioning
ICS Intrusion
Cross Over
Infrastructure
Engineering Workstation
Historian
Outage Measured in Hours-to-Day(s)
Manipulate-to-Disrupt
Attack with Physical Consequence
Stage 2
Outage Measured in Day(s)-to-Week(s)
Manipulate-to-Disrupt (scale & repeated)
Outage Measured in Week(s)-to-Month(s)
Manipulate-to-Damage

Figure 4: ICS Kill Chain Consequence Model for Power Systems

Conducting a Stage 2 attack often requires multi-disciple skills, proper access, and specific information about the process, technology, and setting. All of this comes together as attacker knowledge of the target and experience with ICS. There are different attack concepts and these approaches carry different requirements. There are some attack concepts that require detailed configuration information and others that require more knowledge of the operational procedures or an in-depth understanding of the control system. Simple network diagrams are helpful, but they do not provide the entire story necessary to plan and execute a Stage 2 attack.

Defense Lessons Learned

While some lessons learned are shared between the WSJ and AP reports, the authors of this DUC have identified a top 10 list of lessons learned with 5 items identified for each report. In all lessons learned provided, the authors have considered specific ICS attack enabling elements that adversary groups may focus on to gain access and achieve a desired ICS effect. This methodology is shown in Figure 5 and the following supporting lessons learned provide guidance to defenders.

In the WSJ report, the top 5 primary lessons learned are the following:

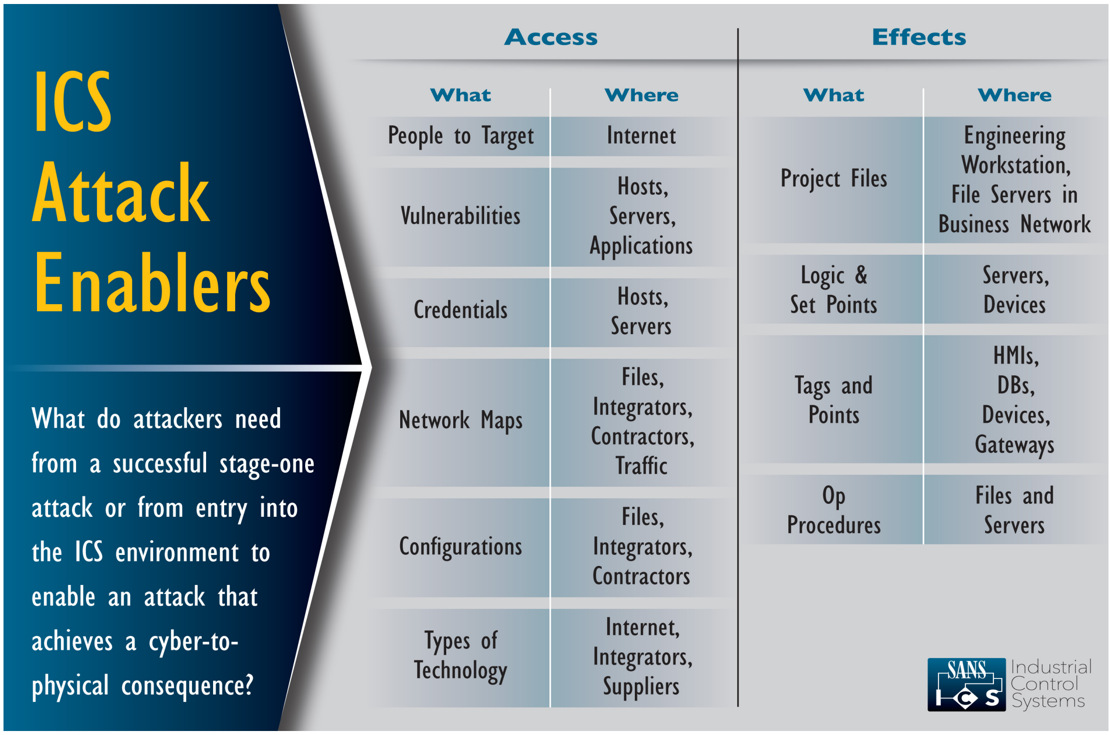
1) No target is too small (especially if the adversary is attempting to determine what target network they are in)
2) Ensure your architecture is appropriate for your operation and even if you have no ICS control capability available and simply wish to view the state of a system, do not directly connect to the Internet especially without robust authentication
3) As a component in your annual assessments perform reconnaissance on your own organizations' publically available information. Hire a consulting organization that specializes in performing the reconnaissance if necessary and mitigate the findings.
4) Media report findings and analysis should be examined for applicability to your own facility, as they may be overstated or may not apply. However, anticipate customers, utility commissioners, and lawmakers to ask questions regarding your level of protection.
5) Adversary groups are actively targeting facilities, you do not get to choose if you are a target, but you do get to choose how difficult of a target you will be.

The AP report provides another set of 5 lessons learned:

1) Adversaries are in search of data that can be used to increase the understanding of process design and engineering. Why adversaries are targeting operational data may be of interest to some, however as a defender it is most important to identify and protect the data that is being targeted. Campaigns like these should lead to an increased security posture for your organization as it may be a prelude to an organized intrusion attempt.
2) Adversaries can target and obtain sensitive ICS data without actually targeting the ICS. Broaden your defenses, to include the controls focused on sensitive information regardless of where that information is stored.
3) Consider how you share data with contractors and vendors. From those who provide long-term service, to those who shared data related to a project.
4) Utilize a common language for what defines an ICS attack. Obtaining

sensitive data from a vendor network is a concerning achievement by an adversary, however it is not an attack nor does it open a "pathway into the networks running the United States power grid."

5) Even if sensitive information is old, it is likely still of great value to an adversary. Knowledge of systems in place, will likely steer an adversary to a particular ICS vendor of choice, vulnerabilities to research, architecture connectivity details, personnel information, physical locations of devices, and support systems critical to the operation.



ICS Attack Enablers

What do attackers need from a successful stage-one attack or from entry into the ICS environment to enable an attack that achieves a cyber-to-physical consequence?

Access

What	Where
People to Target	Internet
Vulnerabilities	Hosts, Servers, Applications
Credentials	Hosts, Servers
Network Maps	Files, Integrators, Contractors, Traffic
Configurations	Files, Integrators, Contractors
Types of Technology	Internet, Integrators, Suppliers

Effects

What	Where
Project Files	Engineering Workstation, File Servers in Business Network
Logic & Set Points	Servers, Devices
Tags and Points	HMIs, DBs, Devices, Gateways
Op Procedures	Files and Servers

Figure 5: ICS Attack Enablers

Implications / Predictions

The events reported in both the WSJ and AP articles indicate ongoing campaigns continue to surface defender implications that need to be considered. These targeted incidents require defenders to develop a focused investment in detection and response capabilities, as prevention efforts may fail. The authors of this DUC believe asset owners and operators who continue to improve their detection and response capabilities, will begin requiring third party vendors and contractors to demonstrate an equivalent security posture to protect the assets used by the 3rd party or the sensitive information they have access to. It is also quite likely that utility commissioners, and law makers will request information on the actions being taken to mitigate the expanding 3rd party cyber security risk and attack surfaces identified in media reports.[11]

Conclusion

The authors of this DUC believe there are many lessons learned for defenders within both of these media reports. Both reports and the journalists did a fantastic job of highlighting ongoing interest by threats into targeting ICS networks and data about those networks. Both reports overstated some of the impact of the threats observed but offered a good opportunity for a discussion about how to impact ICS and what the community cares most about to defend. In neither case were ICS networks and components attacked nor was there ever potential impact for loss of safety or human life. It is imperative for the ICS community to take reported threats seriously but do follow on analysis instead of relying on news media to accurately understand the intricacies of ICS security and threat impact. More importantly, more information sharing must take place in the ICS community about threats to have an accurate story told.

Throughout the ICS community there are appropriate ways to share information safely through sector specific Information Sharing and Analysis Centers (ISACs). As pointed out in the yearlong AP examination of the state of the nation's infrastructure, they made a Freedom of Information Act (FOIA) request to the FBI that was not fulfilled. It was also identified in the AP article that the NERC E-ISAC, which handles information sharing and analysis for the electric sector, treats the information received as confidential and exempt from disclosure under FOIA. The entire infrastructure community will benefit from general reporting of incidents and specifically what the ICS kill-chain looked like from an attacker perspective. You should protect sensitive details about your organization but more freely share about how the attacks happen. If someone would like to share information and an appropriate ISAC or organization is not identifiable please feel free to contact the authors of this report without including specific or sensitive information; the authors will make points of contact available for assistance.

Follow us on Twitter for additional updates:
https://twitter.com/SANSICS
https://twitter.com/robertmlee
https://twitter.com/assante_michael

[11] See July 2015 NOPR from FERC discussing the possibilities and merits of a supply chain standard https://www.ferc.gov/whats-new/comm-meet/2015/071615/E-1.pdf