June 12th, 2020

Authors:
Tim Conway
Robert M. Lee
Jeff Shearer

ICS Defense Use Case (DUC) # 7:

Analysis of the recent report of supply chain attacks on US electric infrastructure by Chinese Actors

Event Summary

On May 1, 2020 an Executive Order was released, titled "Securing the United States Bulk-Power System".[1] The Executive Order (EO) prohibits the acquisition, importation, transfer, or installation of certain "bulk-power system electric equipment" where the transaction involves property in which a foreign country or national has any interest. The EO authorizes the U.S. Secretary of Energy to establish criteria pertaining to specific equipment and vendors in regard to new procurement activities, in addition to the development of strategies to manage existing equipment. The EO states "Within 150 days of the date of this order, the Secretary, in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other agencies, shall publish rules or regulations implementing the authorities delegated to the Secretary by this order." While much work needs to be done during the 150 days since the order was issued, and the industry has numerous questions in regards to what the order will mean for their existing infrastructure and for future capital projects, there is also a number of stakeholders wondering if something happened to heighten the need for the Executive Order now. In a May 11th, 2020 blog post on the Control Global site, author Joe Weiss[2] posted an article titled "Emergency Executive Order 13920 – Response to a real nation-state cyberattack against the US grid". [3]

Claims of real nation-state cyberattacks attacks against U.S. critical infrastructure will generate requests across the public and private sector seeking guidance on actions to take and information requests to inform risk assessments and prioritization efforts. In addition to the wave of activity generated from the initial

[1]https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/

[2] Joe Weiss is a recognized Control Systems Cybersecurity Expert and active contributor to industry standards development for years

[3]https://www.controlglobal.com/blogs/unfettered/emergency-executive-order-13920-response-to-a-real-nation-state-cyberattack-against-the-us-grid/

claim, it is also important to understand the follow-on effects of interest to the asset owner and operator stakeholder community of the claims. A secondary event worthy of mention as an example is the references to the Control Global blog claims of the nation-state cyberattack against the US grid from the GridSecurityNow.org blog post. A post on GridSecurityNow.org provides details of a formal complaint that was filed with The Federal Energy Regulatory Commission (FERC) from Michael Mabee[4] with references to the Control Global blog post from Joe Weiss and the connection it makes between the Executive Order, nation state cyberattacks against the US grid, and current CIP-013 supply chain mitigation efforts underway across North America.[5] The complaint calls upon FERC to address gaps in the supply chain standard CIP-013. The formal complaint was FERC filed on the 12th and created on the 13th under Docket number EL20-46-000[6].

It can be important for analysts to track associated extensions to reports as it branches off into other reporting outlets. As claims extend beyond the initial source, there are potentials for additional supporting or confirming pieces of information being merged in and there is potential for calls to action based on the information. An example of another derivative report adding information can be seen in a May 20th article in CSO which was released reporting more widely on the claims made in the original May 11th blog from Joe Weiss in Control Global.[7]

The SANS ICS' Defense Use Case (DUC) series of papers seek to analyze reported incidents or events of significant interest to the ICS community. In these documents the SANS ICS team first speaks to the credibility and technical details of the claims and then analyzes the defense outcomes regardless of the credibility.

Credibility[8]: **0**

The Control Global blog posting has been assigned a credibility score of 0 (Cannot Be Determined) as it does not cite any sources of information beyond a statement from the author. The claims are significant and relate to an alleged discovery at a utility where the individual making the claim does not appear to be directly employed currently and would therefore likely not have first-hand access to information supporting the claim. If for example the claim was being made from or sourced to an individual who was working for the utility referenced in the

[4] Michael Mabee is an author focusing on securing the electric grid and civil defense

[5] https://michaelmabee.info/supply-chain-cybersecurity/

[6] https://elibrary.ferc.gov/idmws/docket_sheet.asp?docket=EL20-46&Subdocket=000

[7] https://www.csoonline.com/article/3544299/executive-order-boots-foreign-adversaries-from-us-electric-grid-over-security-concerns.html

[8] 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

claim, then the credibility score would have been impacted favorably as direct firsthand information is preferred when assessing credibility of a claim. In this blog post and in derivative reporting, there are no references to information sources or how the information was obtained. Two important claims are made within the blog post:

1) "So why the EO now? Government and public utility procurement rules often push organizations into buying equipment due to price and without regard to origin or risk. In this case, it resulted in a utility having to procure a very large bulk transmission transformer from China. **When the Chinese transformer was delivered to a US utility, the site acceptance testing identified electronics that should NOT have been part of the transformer – hardware backdoors**. That transformer now resides at a government installation."

2) "**What the Chinese did was install hardware backdoors that can cause an Aurora or other type of damaging event at a time of their choosing."**

For item 1) the blog post does not provide any information sources, citation of information sources at the impacted utility, vendor of the identified transformer, or links to indirect reports of confirming information. As such, from a threat intelligence perspective an analyst would be encouraged to treat the claims with suspicion until supporting data was available for analysis. These pieces of information would help a threat intel analyst working for an electric entity in assessing the validity of the information and the priority of the information to reliability risks.

This Defense Use Case is in no way meant to focus on the author of the claims but will rather focus on approaches to evaluate public reports impacting entities and how to think about defending systems related to the claims. The essence of the claim is "…. Identified electronics that should not have been part of the transformer – hardware backdoors….." Unfortunately there is very little information to assess in the claim and come to any credibility score beyond a zero because no sources or data were provided in the blog. The claim notes that the Executive Order was a "Response to a real nation-state cyberattack against the US grid", this connection is one that cannot be validated directly. The authors of this DUC have researched, and monitored information being communicated to industry in regard to the Executive Order and could find no link between the EO and the claims being made in relation to hardware backdoors and the capability to cause an Aurora attack. It is likely that a wide variety of factors influenced the creation of an Executive Order that could potentially have sweeping impacts on the global electric sector.

For item 2) the reference to the intent of the hardware backdoors to cause an Aurora event, is something of reference for an analyst to research and dive deeper into in an effort to help determine credibility and prioritize reliability risk.

To provide some context, Mr. Weiss is referring to the Aurora vulnerability that was the subject of an Idaho National Labs test conducted in 2007. While a tremendous amount of information exists in relation to the Aurora vulnerability for analysis, the information is all in relation to impacts on high value rotating equipment on the generation side or on the load side. In all cases the vulnerability that is being exploited is highlighting a gap in protection that allows a cyber or physical breaker operation followed by an out of phase closure. In the years that have followed the Aurora discovery, the numerous engineering studies, industry advisories and alerts, vendor developed mitigation devices, and follow on studies of the mitigation solutions; all have focused on addressing the gap in protection with additional synchronization check capabilities and mitigating adversary capabilities to manipulate digital protection relay settings.

An additional derivative article appeared in CSO which references and quotes the Control Global claim of hardware backdoors discovered in a Chinese supplied transformer. They also point out that there are very few details provided on the matter, “Although Weiss is almost completely mum on the details of this situation, the backdoor is capable of causing a highly damaging event, he tells CSO.” They add in the article that Mr. Weiss believes there are multiple transformers with hardware backdoors installed throughout the bulk power system. The CSO article again points out the limited details available to support the claim “Although Weiss wouldn’t go into the details of what the “hardware backdoor” consists of, utility security engineer Chris Sistrunk of FireEye speculated what this might mean.” The CSO interview recognized utility industry cybersecurity expert Chris Sistrunk to speculate on what the claim of a hardware backdoor could be, specifically for a transformer. Mr. Sistrunk provided examples of transformer monitoring capabilities that may be present in some devices and added that it is plausible for those monitoring devices to be targeted with a “malicious component” capable of manipulating data.

In the CSO article they provided some additional detail around the impacted components “Weiss did confirm that one of the Chinese transformer makers who has surfaced in connection with the hardware backdoor is JiangSu HuaPeng Transformer Co., Ltd., also known as JSHP”.

The CSO article also provides details of an interview with the JSHP manager of North American Marketing & Service, who provided information of a transformer purchase that was never shipped to the installation site and never installed by JSHP. There is no additional information in regard to why JSHP was not required to perform those elements of the contract. CSO did not directly claim that this is the same transformer referenced in the claim that a “utility found the backdoor when it was installing the transformer and was "finding things that should not have been in there.”” Based on the information provided in the two articles it cannot be determined if the references in the Control Global blog to a transformer with “hardware backdoors” and the derivative CSO references to the

JSHP transformer that was reportedly not delivered to a customer are intended to be considered the same to the readers. While the CSO article provides references to the Control Global post and provides info regarding the JSHP interview detailing a customer transaction that was reportedly not completed; the CSO article does not directly assert the two transformers being discussed are one in the same.

Often times derivative reporting may provide additional information that can be leveraged from a threat intel analyst to perform additional research and determine potential scope of impact to an organization and inform risk decisions. While the CSO article did not provide any evidence to substantiate the claims contained within the Control Global post, they did provide additional research, information, independent interviews with experts, and interviews with companies who will potentially be impacted by the new EO.

The Control Global Blog post contains the reference to the hardware backdoor that was installed in a transformer to cause an Aurora event or other type of damaging event. In the first part of the claim there is reference to the intent to "cause an Aurora", which is a specific type of attacker objective with a robust body of knowledge and a lot of open source research available to analyze. The secondary component says, "or other type of damaging event". This is the phrase that is less clear in that the reader is uncertain of the target or type of "damage" referenced. As we consider these claims, we will examine the specifics around Aurora attacks and where it is relevant we will additionally consider the claims of "other damaging events".

It is unclear from the blog post how the hardware backdoor device was to "cause an Aurora or other type of damaging event" and if it was from the perspective of impacting the transformer or if the intended language was to indicate the hardware backdoor was to be used to conduct an Aurora attack by pivoting through a communications path to another targeted device. In either case this would be the first claim of an Aurora attack being executed from a transformer or targeting a transformer and these scenarios were not the subject of the research and tests conducted in 2007. The documents made available over the years have only considered the low probability secondary impacts to a transformer after conducting an Aurora attack against a targeted high value rotating device that is electrically connected to a transformer.

There is no publicly available information in regard to any analysis in conducting an Aurora attack from a targeted transformer or leveraging a transformer communication path to confirm what is being claimed. With no reference to external engineering studies or additional analysis this claim is currently being treated with a credibility of 0 (Cannot Be Determined).

Amount of Technical Information Available[9]: 0

For the article referenced there was very little technical information provided that would be actionable to an analyst, or a system defender responsible for securing the nations critical infrastructure. Unfortunately, in the Control Global blog post there was no technical information provided beyond the claim of a hardware backdoor in a transformer with the capability to "cause an Aurora or other type of damaging event". With no specific details provided other than a reference to a specific attack capability impacting high value rotating equipment which is typically associated with attack performance through digital protective relays and circuit breaker operations, there is a need for system defenders to connect a series of attack vector dots between the claim of a hardware backdoor in a transformer to the claimed desired intent of performing an Aurora attack or an attack with effects with no additional technical specifics being provided.

Additional derivative articles referencing the original claim provided some high-level summary technical details around why transformers utilize monitoring capabilities and provided a theoretical assertion from an industry expert that the monitoring technologies could potentially be compromised and manipulated to provide false data. For system defenders this information is helpful in trying to think about what could be manipulated within electrical transformers and would be very interesting information to pursue further (nudge for a whitepaper from Mr. Sistrunk). However, as cited in the article the information provided was not intended to validate or confirm anything in the original claim of Chinese hardware backdoors with an ability to cause an Aurora attack or other type of damaging event.

Unfortunately, there is no additional technical information found in any of the derivate reports in regard to the claim of "hardware backdoors" discovered, the communication path specifics necessary to take advantage of the vulnerability, or the transformer specifics that would lead to an Aurora attack. For these reasons the Control Global post has been issued a score of 0 (No specifics) in relation to the amount of technical information available.

The position of the SANS ICS team is that currently there is not enough information provided to validate the claims nor is there actionable steps to take for defenders who may wish to address the claims regardless of credibility or accuracy. However, the purpose of the SANS ICS DUCs is to take such claims and provide recommended actions for defenders to consider. The following sections will expand on the claims further and provide defender specific prioritized tasks to focus their efforts on if they are concerned about similar attacks to what has been discussed.

[9] 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

Attacker & TTP Description

Attacker:

In this scenario the alleged threat was the Chinese government. There is currently no technical evidence provided of this country affiliation with the claim, thus the attacker profile should be expanded for purposes of the DUC to the ICS specific threats that have been tracked in the community to date. There are four groups that have reportedly shown the capability to intentionally perform destructive attacks via cyber on ICS to date. The first two would be the United States and Israel in relation to their alleged involvement in the Stuxnet program that targeted Iranian nuclear centrifuges. The next team is XENOTIME which was responsible for the TRISIS cyber-attack on a safety instrumented system (SIS) that targeted human life at a petrochemical facility in Saudi Arabia.[10] The most relevant activity group to electric sector substation attacks is ELECTRUM which developed and deployed the CRASHOVERRIDE malware against Ukrainian transmission equipment in 2016.[11]

Another credible threat for analysts to consider, though it was not done intentionally for the purpose of destruction, is criminal teams that create counterfeit software and hardware in the ICS community. For years industry experts and researchers have been performing analysis in this area and reporting their findings out to the community.[12] It is reasonable to assume that if non-approved components were found on transformers or other grid equipment it could be the result of supply chain issues that relate to criminal activity providing counterfeit lower cost devices and not intended as dormant cyber-attack capabilities by foreign states. This is an aspect of the supply chains that asset owners, operators, and original equipment manufacturers must be concerned with.

Capability:

As identified previously in the attacker section, the most relevant activity group with demonstrated interest and capabilities to operate within a targeted electric system is ELECTRUM. Based on analysis performed after the ELECTRUM

[10] https://www.dragos.com/resource/xenotime/
[11] https://www.dragos.com/resource/electrum/
[12] https://www.informationweek.com/government/cybersecurity/chipmaker-disables-counterfeits-with-software-update/d/d-id/1316973

attack on Ukraine in 2016, Joe Slowik authored two Dragos whitepapers "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack"[13] with the accompanying whitepaper "STUXNET to CRASHOVERRIDE to TRISIS: Evaluating the History and Future of Integrity-Based Attacks on Industrial Environments".[14] In these papers the capability of the ELECTRUM team is discussed in detail that exposes how other teams could reasonably perform similar attacks.

The summary of the analysis that is relevant to this DUC is that the capability of ELECTRUM and other similar adversaries have consistently been to leverage remote cyber operations for purposes of intelligence gathering to craft a specific attack for the target. ICS are often resilient and while it is possible to deny service through simple actions like active scanning, and tools like Nmap have likely caused more process environment downtime than Russia, China, and Iran combined, however it takes a specifically engineered and tailored capability to cause an intentional and expected outcome. For example, it's not hard to deny service to a PLC but it is incredibly difficult to cause a specific directed physical event or denial of safety especially if you want to do it in an engineered and repeatable manner.

After adversaries develop long term insights such as in the case of ELECTRUM, they were likely operating in the Ukrainian utility for well over a year and XENOTIME operated in the Saudi Arabian petrochemical facility for over three years where they developed knowledge or capabilities to achieve their attack. In the Ukraine 2015 cyber-attack it was simply the adversary's knowledge of operations that permitted them to deny power to distribution substations leveraging native functionality in the distribution management system. In Ukraine 2016 it was custom malware that leveraged native electric network protocols such as IEC-104 and OPC. Adversaries then had to deliver their capabilities to the target.

In the ICS attacks seen to date the capability has been delivered remotely while the targeted systems were in service. It is possible, and a real concern, that an adversary could learn enough to embed a capability in a technology itself before delivery to the target. This is inherently one of the concerns related to the supply chain and on the surface sounds extremely alarming. However, while technically possible the complexities surrounding this type of delivery make it highly undesirable to an adversary.

---

[13] https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf?hsCtaTracking=aa9179e5-48b0-464b-9b78-ffd6242fb635%7C30d0dd95-4a2b-4045-a7cc-c6bfa1be5e2d

[14] https://www.dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf?hsCtaTracking=5509199a-cc44-4496-ae86-bd5a409e5721%7C274ac9fc-ef44-4fa9-af5b-8e1cc83233c4

- First, mistakes are commonly made in adversary operations and the ability to have remote access enables fixing those mistakes.
- Second, compromising the supply chain in such a way would immediately jeopardize the economic value and influence that a country derives from the supply chain.
- Third, the capability would still require a trigger mechanism and simply relying on time would be highly risky as the capability could detonate in adverse conditions for the attack to be effective. If the capability required a call out to be remotely activated or utilized, then it makes even less sense to take advantage of the supply chain in the first place as the call out would be as easily detected as the intrusion to place the capability.

With just these three considerations, and there are plenty of others, such a mechanism to cause an attack is theoretically possible, and concerning, but far from the preferred choice for adversaries both historically and reasonably. This is not to dismiss the possibility that such an attack could ever exist but to call attention to the fact that there are already numerous barriers to success for the adversary in this course of action and higher confidence approaches exist to achieve similar objectives.

Motivation:

State actors have a wide variety of motivations and often in any given intelligence or cyber operations there is not a single motivation. Targeting electric sector infrastructure could reasonably serve a number of tactical and strategic requirements; it is improbable to fully understand all the motivations of strategic adversaries but there are three commonly cited scenarios in electric sector targeting.

- The mere targeting of infrastructure can cause the victim country a significant amount of tension and concern. This can help message that actions the country is undertaking are averse to the desires of the hostile nation and seek to change the targeted countries behavior. This can relate to a wide variety of economic, diplomatic, military, or social actions.

- The targeting could be a message to the populace and enhance tension between the citizens and the government of the targeted country as the populace then assesses the actions of the targeted country to be causing them risk.

- The targeting may serve the purpose of preparing the environment for future attacks wherein the adversary determines the need to use the access or capability during conflict or future scenarios.

The motivation of strategic adversaries is important to assess but is one of the most difficult intelligence requirements to achieve a high confidence assessment of, especially through intrusion analysis alone. For the purpose of this DUC the motivation of the alleged action is not taken into consideration.

ICS Cyber Kill Chain Mapping – Transformer Backdoor

The approach taken in many of the SANS Defense Use Cases focuses on the learning opportunities of reported events, independent of the credibility score and the technical detail score. The SANS author team believes there are always important educational highlights for system defenders to learn from. In the earlier portion of this DUC we provided guidance on how to assess and evaluate information in a manner that attempts to avoid biases and informs appropriate actions. In this section of the DUC we will begin to focus on actions for system defenders to take, as if the claims are true. There is value in starting from a defender point of view that an incident is true and then determining what defenders can do to mitigate the effects of a successful attack.

Assuming the claims of the Control Global and CSO reports are true, we will consider the actions of a targeted utility in defending against the reported claims of Chinese "hardware backdoors that can cause an Aurora or other type of damaging event". While we will work from an assumption that the claim is legitimate, we will need to provide various technical detail possibilities and necessary conditions to support the claim if we are going to cover defender focused actions.

Transformer

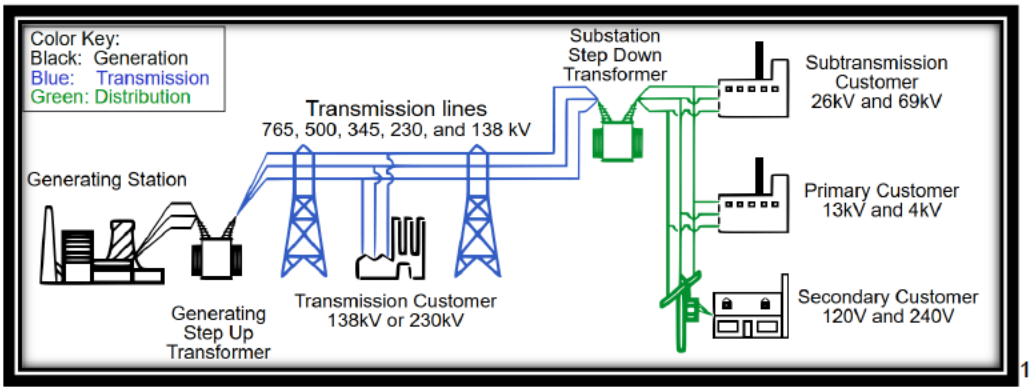
We will begin with a very brief discussion around the device being leveraged in the claimed scenario; the transformer. We will continue to focus on the two reports within this DUC, however for individuals interested in additional reading and some of the previous stakeholder efforts to assess the need for actions to ensure critical infrastructure reliability and security, there is an older 2014 Department of Energy document titled "Large Power Transformers and The U.S. Electric Grid"[15] that provides more context to the discussions occurring today in relation to the Executive Order. The DOE document provides analysis across a variety of different classes of transformers, manufacturers, materials and metals needed, and actual production data. There are several different transformer types, manufacturers, and designs. Each one has engineering specifications based on the location and purpose of the individual transformer, the surrounding electric system and the necessary features and preferences desired by the asset owner / operator. While these specifics were not provided within any of the

15 https://www.energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf

reports, we will consider the typical electric system placements of a generator step-up transformer, a step down transformer, and the additional aspects of a transformer with a load tap changer transformer installed all from the perspective of an attack with an intent to “cause an Aurora or other damaging event”.

A generator step-up transformer is the important link between a power generation resource and the transmission system. As shown in Fig. 1. This may be a target of interest in relation to the references in the claim to an Aurora attack. Currently there are no specific capabilities referenced in the public Aurora documents related to a compromise within a generator step up transformer that would directly be of interest to an adversary as a final control element of an attack with an intent of operating circuit breakers or manipulating protection relays to achieve a desired effect of causing a generator to be connected to the electric system out of synchronism. However, there could be communications paths connecting certain components of the transformer to the generator circuit breakers on the low side of the transformer. There could also be communications on the high side connecting to circuit breakers in the generation facility switchyard. These communications paths could provide connectivity to cyber components that if manipulated could achieve the desired adversary effect. In this way, it is not the actual transformer that is of interest to the adversary, but rather the electric system location of the transformer in proximity to a synchronous generation resource and the communications components and connectivity paths that may have been established by the utility.

A step-down transformer is the link between the higher voltage bulk power transmission system and the lower voltage distribution system for delivery to customer load. We highlight the specifics of a step down transformer for a large industrial customer in this DUC, as the industrial load may contain high value rotating equipment that is a potential target of an Aurora attack. Just as was the case with the step-up transformer, the area of adversary interest in a particular transformer would be due to its location in the electric system and the potential for communications capabilities to affect other electric system elements. The same assumed adversary target selection approach exists with a step-down transformer that is placed in the electric system near customer load of interest to an adversary and may have trusted communications to control electrical elements of interest in delivering an Aurora attack.



[16]

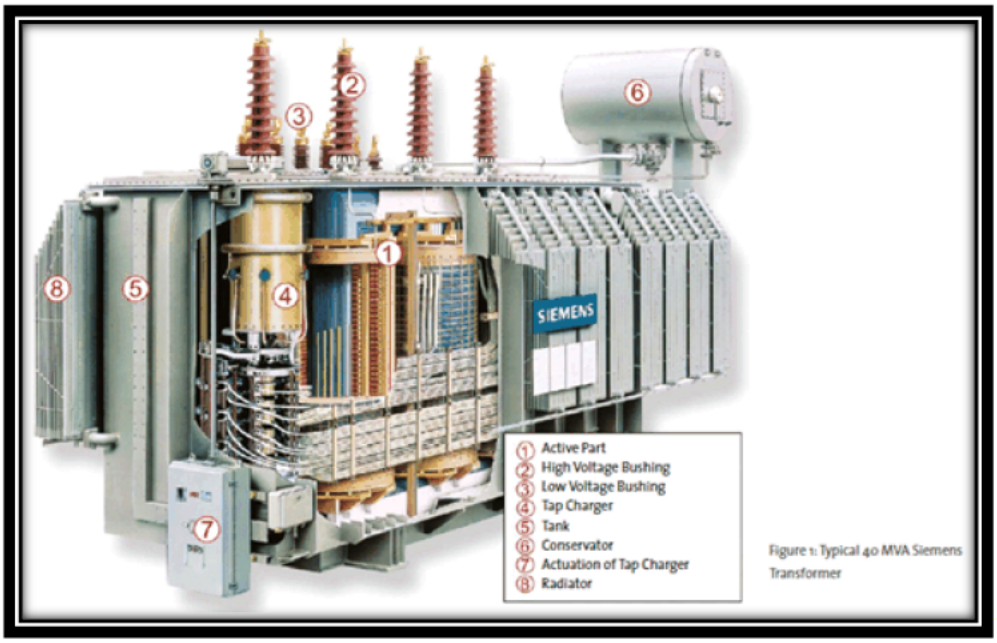
Figure 1 – Power system facilities and elements

From the perspective of the claim provided of an Aurora attack as well as the language provided regarding damaging attacks, we wanted to also discuss a particular type of transformer with a load tap changer design. See example in Fig. 2. The load tap changer capability allows for automatic or manual control to allow system operators to adjust voltage and reactive power. Unlike fixed ratio step up or step-down transformers mentioned previously, LTC transformers contain a motor operated mechanical selector that can be operated and moved to various positions on the transformer winding.

With the additional capabilities present within LTC transformers there does exist a capability to create a potential internal fault, impact ability to deliver power, or potentially create a voltage condition that impacts load by physically operating or remotely operating the LTC control. Adversaries with an active communication capability could potentially manipulate the sensor data to indirectly cause LTC operations. While these components and attack vectors do exist within an LTC transformer, there is no direct physical element that would enable an Aurora attack creating an out of synchronism issue for generation assets or industrial load.

Specific to the claim of an Aurora attack, the LTC transformer would be a target due to possible electric system location near load of interest to an adversary or due to the potential that it may have trusted communications to control electrical elements of interest in delivering an Aurora attack. Specific to the claim of other damaging effects, there are certainly attackable components within an LTC transformer if an adversary had a delivery path.

[16] http://www.geni.org/globalenergy/assets/svg/electricity-grid-simple-North-America.svg



[17]

Figure 2 – Typical 40 MVA Siemens Transformer with a Tap Changer

Monitoring Capabilities

Some of the technical information contained within the CSO article provided by utility subject matter expert Chris Sistrunk referenced monitoring systems installed on some transformers referenced as DGAs (dissolved gas analysis) sensors. Mr. Sistrunk stated that "It's plausible that a malicious component could send fake data to power company control system networks and the internet".

Some examples of these types of systems provided by vendors include: Sensformer[18] from Siemens, CoreSense[19] from ABB, CoreTec 4[20] from ABB, and numerous manufacturer independent transformer monitoring systems from organizations like SDMyers[21] and others. These monitoring capabilities are designed to detect and alert an asset owner and operator of equipment conditions and a need for preventative maintenance in an effort to prevent critical issues from causing reliability events. With or without these near real time monitoring systems, many asset owners have maintenance schedules for these devices and periodic checks to validate sensor data as well as device inspections. While the features of the systems vary and all are configurable, each one primarily takes inputs from sensors and makes that information available to the utility through various

[17] https://eeadda1.blogspot.com/2017/11/why-transformer-rating-in-kva-not-in-kw_30.html

[18] https://new.siemens.com/global/en/products/energy/high-voltage/transformers/sensformer.html

19 https://new abb.com/products/transformers/service/advanced-services/coresense-m10

20 https://new abb.com/products/transformers/service/advanced-services/coretec4

21 https://www.guardianmonitoring.com/

communications methods that differ for each device. It is unclear what the capabilities were for the transformer in question and it is unclear if there were any present at all, however as we proceed with the analysis from the perspective that the claims were 100% true, we can continue to consider the probability that the transformer in question had a monitoring system. If a monitoring system existed and had features similar to those identified above, it would be likely that the monitoring system supported various communication methods; serial connection, ethernet connection, optical connections, and potentially wireless connections. With a monitoring system capability there would also be local sensors connected providing data for analysis and some systems may also have capability to operate cooling fans if desired by the utility.

Communications

With the claims of hardware backdoors and the discussions earlier in this document of transformers potentially being leveraged as trusted communications paths, we wanted to spend some time on connectivity possibilities. The monitoring devices have variations in connectivity and in reference to potentially using the device to launch an attack over a trusted path to another device, we will not spend time discussing the point to point serial connections or connectivity to the 4-20mA analog interfaces available on some devices. Rather we will consider the ethernet based communications of http, modbus, dnp3, and IEC61850.

Another set of variations exist in regard to:

- The determined impact rating of the facility (High, Medium, Low),
- Where the network connection is being made in the control house,
- How the device is being used or what the device is capable of impacting if misused.

For example, these connections may very well connect into a medium impact substation control network that contains other control devices, in which case they could be subject to a wide variety of NERC CIP controls if identified as a BESCA (Bulk Electric System Cyber Asset). These controls for Medium BESCAs involve electronic perimeters, physical perimeters, remote access management, asset specific hardening, patching, logging, monitoring, alerting, change management, information protection, incident response, and recovery capabilities.

For Low impact sites with lower risk to the electric system there would only be a much smaller list of controls in place, but security controls none the less. If it was a distribution level asset not subject to CIP, then it would also likely not be subject to the Executive Order and it is beyond the scope of what was being referenced in the Control Global and CSO reports.

As mentioned, there are dozens of other examples that can be walked through, however we are looking at a connectivity example into a control network, where

an existing hardware backdoor would potentially have access to a trusted communications path to impact additional cyber assets. If for example the monitor device was instead connected to a business network and was accessed via a web interface for analytics or reporting purposes used for non-real time predictive analysis and future work management activities, with no connections into control networks, and no ability to impact the transformer, then the monitoring cyber asset would not be subject to NERC CIP.

Under these criteria it would also no longer be connected to a trusted communication control network providing access to the claimed hardware backdoor capability and it also would no longer have the ability to impact the transformer operations. In this way, the adversary who selected a particular transformer would also need to have some certainty in regard to how the asset owner was going to be connecting and managing the transformer monitoring system.

While there are numerous approaches to how the communications paths could be implemented, it should be understood that if the connections are made into a control network at a Bulk Electric System site, then the device will be subject to some level of NERC CIP requirements.

ICS Kill Chain

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.[22] 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 3.

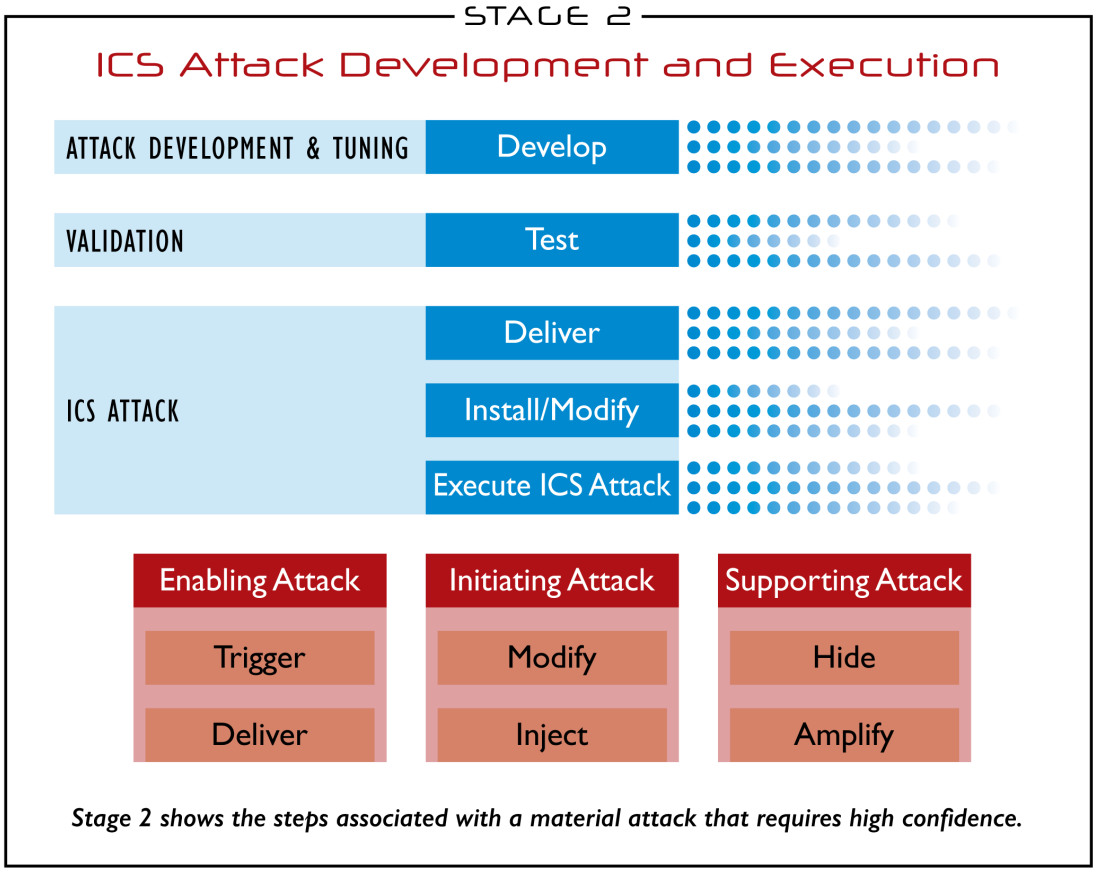


Figure 3: The ICS Cyber Kill Chain with Stage 2 Highlighted

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.

As indicated previously, without technical details provided regarding the hardware backdoor, the type of transformer, or the communications in place, we will walk an adversary kill chain example for purposes of discussion.

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

Three potential options can be introduced for discussion purposes:

1) The hardware backdoor provided remote wireless communications capabilities as an adversary path to then pivot from the transformer into the connected communications network. From an out of band wireless established position the adversary could begin the Stage 2 steps of Attack development, validation, and attack.

2) The hardware backdoor provided a phone home feature through the connected communications network providing an adversary C2 path. With a persistent maintained path through the Stage 1 corporate environment and an established persistent position into the Stage 2 environment an adversary could begin the Stage 2 steps of Attack development, validation, and attack.

3) The hardware backdoor contained malicious capabilities to be triggered and communicate over the connected communications network based on some logic triggered event. This would require the malicious capability to have perfect knowledge of the control environment or auto discovery capabilities within the target environment to operate autonomously and then deliver a predeveloped and validated attack.

Option 1 and 2 mentioned above provide an adversary access to the OT environment if the utility has connected the communications to a control network.

Option 3 provides capabilities to execute malicious commands only if the utility has connected the communications to a control network. In all cases the ability to “cause an Aurora” is reliant on the hardware backdoor having communications capabilities to the substation control network.

Defense Lessons Learned

The SANS Defense Use Cases try to avoid listing non specific mitigations regarding best practice ICS defenses like architecture, patching, backups, etc. Those items are all essential and solid recommendations however, we try to focus on the mitigations that will assist in addressing an attack based on the specific attack methods or vulnerabilities addressed in the DUC.

Based on the items addressed in this DUC we would identify the following steps for defenders in three groups:

1) Actions to prioritize a response across a large footprint:
   a) Work with substation engineering teams to obtain an accurate fixed asset list or unit of property list to ensure an accurate field inventory data set
   b) Evaluate that list and identify the various transformer asset manufacturers of concern and purchase dates

c) Working with transmission operations and planning teams obtain a list of priority substations based on power system analysis studies, load flow data, and system restoration cranking paths
d) Working with CIP Compliance teams obtain the list of Medium and Low substations based on CIP-002 and the physical site determinations of CIP-014
e) Overlay the lists to identify the highest priority sites based on system reliability, system restoration, customer load, age of transformer, manufacturers of concern, and compare that to the existing physical and cyber protections at those highest priority sites.
f) Identify areas of gaps and consider adding security controls at or beyond what is required based on risk.

2) Actions to mitigate an Aurora attack on high value rotating equipment;

a) If the primary concern of an entity reading this DUC is an Aurora impact, it would be of highest priority within your utility to begin discussions with Transmission operations teams, field engineers, system planners, system protection engineers, and OT cybersecurity experts within your organization to review previous action plans or assessments taken in response to the Aurora mitigation reports made available. For those entities located in North America, we recommend a review of the NERC Aurora recommendation that occurred in 2010 and ensure your organizations response action plans were sufficient and remain sufficient.

b) If the action plans are no longer relevant or up to date based on current system design, then a review would need to be performed. For entities in all geographies, a review of the applicability and potential consideration of Aurora mitigation devices may be a valuable discussion to have with your protection system vendors as well.

3) Actions to mitigate impact of an attack. The most likely scenario for the delivery or detonation of such an attack would be performed remotely as it significantly reduces the risk to the adversary:

a) Deploy proper segmentation of networks and ideally enforce multi factor authentication for remote connections. For entities subject to NERC CIP, review ESP egress rules that are required for operations, if any rules exist relevant to the transformer monitoring communications verify communications are as intended and verify all CIP-005 Interactive Remote Access controls.
b) Deploy network monitoring technology for visibility and detection use cases that are safe to operate in ICS networks and understands ICS/OT communications and protocols. For entities subject to NERC CIP this is an area where we are encouraging organizations go beyond existing CIP-007 logging and alerting requirements

c) Ensure incident response plans take into consideration the ICS and site personnel with rehearsal of the scenario of concern in the form of a table-top exercise. For NERC CIP organizations, begin working toward future CIP-008-6 incident response plans
d) Perform routine assessments for any wireless communications at the sites of highest concern and work to identify any unknown activity
e) Pursuit of additional controls specific to sensor security. Based on the technical details discussed across a variety of scenarios this would not be the highest priority actions recommended based on the attack paths and realities of the manner in which these attacks would likely be orchestrated. Such security can have limited but important use-cases when considered as part of a larger security effort and should be pursued based on individual entity risk priorities and available resources.

Conclusion

The authors of this DUC believe there are many lessons learned for defenders that can be identified within the claim of hardware backdoors in transformers regardless of the information available to support the statement. Lessons include those specific to cyber threat intel analysts in regard to assessing information sources and claims, lessons for leaders in regard to how you consume information and prioritize actions, and lessons for the practitioners operating, maintaining, and defending systems potentially being targeted. As in every case, there is much more that could be learned with additional details and discussion from the targeted organization. Throughout the ICS community there are appropriate ways to share information safely through sector specific Information Sharing and Analysis Centers (ISACs), directly with sector specific agencies, local FBI, DHS, DOE, or even with trusted vendors who can anonymize and share the information in ways that are actionable. Actionable information is being shared now more than ever in trusted channels, enabling organizations to better defend and respond to credible threats. The days of keeping cyber security near misses to yourself should be over, as the industry understands cybersecurity is a direct component of functional safety programs, we need to learn from and perform root cause analysis on ICS cybersecurity events in a manner that can potentially engineer out risks from the system and to the fine men and women who operate them.

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