SANS ICS Industrial Control Systems

ICS Defense Use Case (DUC) Dec 20, 2014

Authors:

Robert M. Lee
Michael J. Assante
Tim Conway

ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – ***Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack***

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

Initial reports surfaced in 2009 that a state-sponsored cyber actor had successfully intruded upon servers essential to the BTC pipeline operations and caused a temporary disruption in pipeline transfers.[1] It was further reported that a team of western experts were able to assist the pipeline operator in restoring the system enabling a return to normal operations. Few details were provided other than speculation that Russian hackers through the Agency of Russian Special Services had performed the attack.

Reporting surfaced in December of 2014, indicating the "disruption" had actually involved a pipeline rupture and explosion due to an intentional over pressurization of the pipe but in 2008.[2,3] Cyber attackers were said to have gained access to the pipeline's control system and were able to suppress alarms, manipulate the process, and blind system operators.

[1] http://www.critical-intelligence.com/resources/papers/CI-BTC-Pipeline_Attacks.pdf

[2] http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

[3] http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html

The BTC pipeline event being linked to the cyber attack that occurred on August 6, 2008 inside of Turkey near the town of Refahiye. The physical rupture led to escaped product ignition and an explosion resulting in a fire that was extinguished by firefighters on August 7, 2008. The pipeline was out of commission until reopened on August 25, 2008.

The reporting relied upon four sources familiar with the incident and investigation. The pipeline operator spokesperson denied there was any tampering with computers or communications systems, but would not identify a cause of the rupture.

The incident occurred at a time when tensions between Russia and Georgia were building towards armed conflict. Russia officially deployed troops into the Russian-Georgian conflict two days after the pipeline explosion occurred. The BTC pipeline ran through Georgia and regional analyst suggest it represented a threat to Russian energy policy.

Credibility: 2- The available information and reporting is being evaluated as possibly false. The physical explosion did occur but the cyber link is not currently credible. The details of the story cannot be corroborated in publicly available information, but the general incident has been covered by multiple sources over several years. The reporting source has not responded to inquiries and the sources cited in the report were anonymous sources not involved directly with the investigation. Simple credibility rating system[4]

Amount of Technical Information Available: 2- The information available provides some insight into how the attack may have unfolded without specific details into vulnerabilities, exploits, or target architecture. Simple descriptive rating system[5]

[4] 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

[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

Attacker & TTP Description

Attacker: There is no definitive evidence attributing the attacker to specific individuals or organizations. Sources have suggested that Russian government sponsored or organized actors were to blame for the attack. We can characterize and evaluate one possible profile for the actor:

Capability - Although, the control system's in use at the BTC pipeline have not been disclosed, it is reasonable to assume an exploit may have existed or access to the ICS network could have been achieved and commands injected that did not require authentication.

Opportunity - Reporting indicated attackers included a team of two that were observed in the vicinity of the pipeline with laptop computers. BTC pipeline was also reported to have a new IP-based camera system that was networked with coverage along the right of way of the pipeline. IP-based camera systems are often misconfigured to communicate openly with the Internet and may have been an initial attack vector.

Motivation - Geopolitics at the time included Russian preparation for a limited invasion of Georgia (pipeline extended into Georgia) at the time of the incident. A Russian parliament advisor had been quoted as saying the BTC pipeline was dead. Subsequent Russian military operations included an air strike near the pipeline. These events indicate a motivation did exist at the time of the incident to disrupt the pipeline. This motivation might not be enough to offset the risk of conducting a blended attack, which includes boots on the ground, to attack the pipeline on Turkish soil.

The described Tactics Techniques and Procedures (TTPs) are lacking details, but reporting suggests the attackers might have used remote Internet connection or wireless exploitation to gain access to the security camera network. Other details indicate physical access to field controllers may have also been necessary.

Attack Surfaces & Paths

It was reported that the camera communication software had vulnerabilities that were exploited by the attackers to gain entry onto the network and move from host-to-host. The architecture of the camera system relative to the ICS network has not been disclosed, but sources suggest the attackers were able to pivot to the control network from the camera system. Sources also reported that time correlation of the observed men carrying laptops and probes recorded in system logs led investigators to connect the two events.

Sources also tell the story that attackers were able to exploit a vulnerability on the alarm server, running a Windows operating system, and placed malicious software allowing them to achieve persistent access.

The story describes the attack as targeting industrial computers (most likely Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs) at valve stations to change pressure and misreport values back to the control room. This information may point to direct physical access to control components at remote locations. The attack on the camera system may have only been used to blind the pipeline operator to physical intrusions to gain access to field ICS components.

The last component of the attack described in reporting involves possible jamming or suppression of back-up satellite communication links.

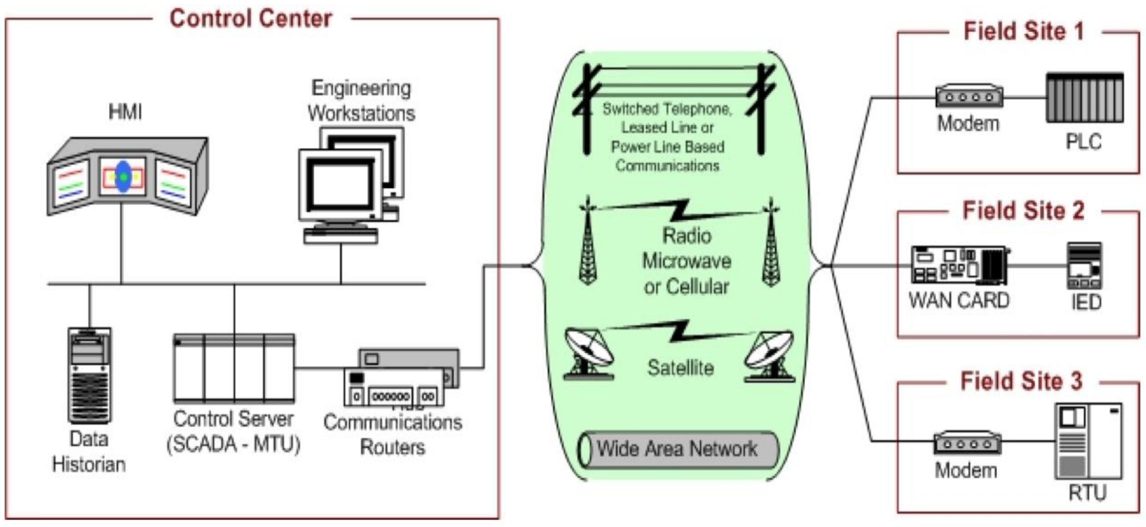

Figure (1) SCADA Diagram from NIST 800-82

Impacted Systems & Functions

The source in the Bloomberg report indicated that the control room operators did not learn about the rupture and explosion until 40 minutes after it had happened. There are two sources of information that should have been available to the control room. There was a leak detection system with alarms and the data acquisition should have been providing pressure and flow readings throughout the pipeline. A significant rupture would cause an easy to identify drop in pressure and flow. The following systems may have been compromised or impacted during the incident:

- Camera system and communication network
- Leak detection system
- Automated pressure reliefs
- Alarm server or input traffic from field devices
- Pipeline field devices found in valve or compression stations (e.g. RTUs & PLCs)
- Satellite terminals or the actual transmission of signals

The functions that appear to have been impacted include a Loss of View (LoV) or Spoofed view, possible Loss of Control (LoC), suppression of alarms, direct writing or command of control element, and camera system monitoring and storage of recordings.

Defense Lessons Learned

Regardless of the reporting's validity the scenario presented is entirely possible and presents an opportunity to extract defense lessons for the community.

#1 Defender Rule - when considering targeted cyber attacks, always assume the attacker will gain a difficult to detect foothold on any device or network that has connectivity to the Internet or an accessible wireless signal. In this scenario the pipeline operator in an attempt to provide enhanced physical security has introduced a new cyber attack surface (the IP-cameras) that should have been accounted for in system designs and cybersecurity strategies and plans.

Architecture – The IP-based camera systems served as an initial attack vector for the adversary. These systems were linked to the internal control network for field devices. A segmented network separating the IP-based camera system and utilizing a demilitarized zone (DMZ) would have added significant barriers to the adversary.

Physical Susceptibility of Control Equipment – Control equipment in the field is vulnerable to physical attacks but when combined with cyber-attacks pose a significant threat. This is not a theoretical discussion. For example, advanced attacks are said to have been originally introduced via a USB thumb drive, demonstrated the effectiveness of gaining physical access to a system in order to conduct malicious activity, and high-profile incident has proved that even logically separated or air-gapped networks are not immune to such attacks. Compromising remote facility communications or equipment is not a novel concept either. Security professionals often employ such tactics when conducting sanctioned network penetration tests for corporate clients. In this scenario the attackers used a combined attack where they used their access on the network to compromise field equipment so that it would not send malfunction alerts to the control center. This allowed the attackers to physically manipulate the systems unnoticed. This type of combined cyber-physical attack is incredibly difficult to counter but should be included in tabletop scenarios and incident response preparation. Field devices should have logging enabled whenever possible and this evidence should be combined with other sources, such as video recordings, to help defenders quickly identify the issue and confidently restore operations to normal. [6]

Those investigating a physical security breach should at least consider the possibility that a cyber-related incident may also have occurred. As a seasoned

[6] https://www.sans.org/reading-room/whitepapers/analyst/industrial-control-system-ics-cybersecurity-response-physical-breaches-unmanned-critical-in-35282

employee familiar with the site, pause for a moment and consider the location from a malicious actor's perspective. How would you do it if you wanted to compromise the local equipment or gain surreptitious upstream network access? And then inspect the site with that perspective in mind.

Vulnerability Discovery and Patching – In the scenario, vulnerabilities in the camera's communication software allowed attackers to gain access to the network. Identification and patching of vulnerabilities in control system environments is always encouraged, when possible, for control systems and the infrastructure they use such as Windows and Linux systems. However, little attention is ever paid to auxiliary systems such as IP-based cameras. If a system is connected to the control system environment vulnerabilities in it must be assessed or, at a minimum, accounted for in defense preparations. When it is not possible to patch systems it is important to specifically note which systems might be vulnerable and segment or monitor the systems appropriately. Network Security Monitoring is a best-case practice to passively identify and internally monitor assets, especially those that cannot be patched, for network anomalies.

Internal ICS communication & behavior monitoring – In the attack scenario described in the Bloomberg story, the attackers were aided by a significant weaknesses shared by most ICS/SCADA systems - the lack of internal network monitoring. ICS have purposeful and thus predictable communication profiles and defenders need to leverage this important difference between an ICS and IT network. The authors of this document have developed SANS ICS515: ICS Active Defense and Response to teach deeper skills in the use of tools like Wireshark to analyze ICS network traffic and other tools to quickly detect unexpected communications. The suppression of alarms or spoofing of data from field controllers would have been an observable event that could have alerted operators to move into more conservative pipeline operations. In some processes attackers need time to accomplish their desired process effect. This is one constraint that we need to be pouring pressure on in an attempt to reduce the attacker's "free time" and respond effectively to head off process effects.

Implications / Predictions

Many system events have occurred throughout the world and are attributed to a technical failure, and some are starting to come to light many years later as something that was quite possibly done intentionally. There will likely continue to be a growing trend of re-examining or the release of accurate or in-accurate information presented in a manner that opens up these “ICS Cold Cases” for another discussion. For the asset owners and the law enforcement and intelligence, community there is great purpose in truly determining an accurate sequence of events. For the larger ICS community it is important to not look at these ICS Cold Cases with a focus on whether a specific event can be proven without a shadow of doubt, but rather from the perspective of whether it is in the realm of the possible and what can you do to protect your operation from the components that pose the greatest risk to your mission.

A continued trend may result in more and more asset owners, operators, or regulators requesting data to begin looking at their own “ICS Cold Cases” and remove the previous tunnel vision that existed in identifying a likely suspect ie. Failing PLC, mis-operating network card, human error, communication data fade, failed hard drive, VSAT Comm loss, etc. In criminal “cold cases” often times a likely suspect is identified, causing other suspects to be overlooked. Criminal cold cases are often re-examined due to improvements in forensics capabilities and based on the new evidence wrongly accused suspects are exonerated. Similarly, “ICS Cold Cases” are often closed by a technical team blaming a likely suspect and with the introduction of advanced forensics and analysis tools, likely suspects will begin to be dismissed while the evidence points to a new suspect.

The industry will continue to see a trend toward more sophisticated real-time and historical cyber events analysis as organizations pursue increased ICS specific forensics tools, ICS device level cyber security logging, and increased event correlation tools.

Conclusion

Often times in engineering intensive infrastructures, individual sectors perform an excellent job of documenting system failures and sharing the information with peers through lessons learned communications. As an emerging group of ICS cyber defenders begin to make their mark on improving system reliability in the face of cyber threats it is important to share our understanding of how systems are compromised, what threat actors were able to accomplish, and how operators were able to detect them and respond. It is also well understood that the adversary community is learning from their own success and failures.

Taking the same approach as adversaries, but from the perspective of a defender and responder is just as important. Looking at system events and lessons learned data from the perspective of an attacker is a very helpful starting point, but more focus needs to be put on how a defender could have detected and prevented an attack. Using this approach, begin by considering the data reported above and imagine it happened at your facility, what surfaces could be attacked, what defense approaches would have provided appropriate detection, and what capabilities would have been needed to respond. Even though this report has a low credibility score due to single source reporting, it is important to utilize these opportunities to develop a community approach to conduct “ICS Cyber Events Analysis”. Adversaries should not be the only ones learning from industry system events and lessons learned. The cyber incident detailed above contains plausible elements that provide a basis for defenders to tabletop by overlaying the reported capabilities and techniques against their systems. We encourage you to share defensive techniques and methods that can defeat the attack described here.

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

SANS
10TH ANNUAL
ICS SECURITY
SUMMIT & TRAINING
Orlando, FL | SUMMIT: Feb 23-24 | TRAINING: Feb 25 - Mar 2
For SCADA, Industrial Automation, and Control System Security