Incident Summary

On April 15, 2015 the New York Times released an article titled “Iran is Raising Sophistication and Frequency of Cyberattacks, Study Says.” The article focuses on the Iranian cyber threat as a whole but a significant portion of the article highlighted a report by the cybersecurity intelligence company Norse and the American Enterprise Institute (AEI). The article highlighted findings in an upcoming Norse and AEI report that was released the next day. The report stated there were significant increases in attacks on critical infrastructure and industrial control systems (ICS) by the Iranian government. The report released by AEI and Norse, titled “The Growing Cyberthreat from Iran” revealed claims of hundreds of thousands of cyber attacks on worldwide infrastructure by Iran.

The purpose of this whitepaper is to evaluate what can be learned from these claims while also taking the opportunity to educate on what constitutes a cyber attack on ICS. In our review of the data provided in the report we agree that the data could be interesting when put into proper context or analyzed along with additional data, however the data does not conclusively identify cyber attacks. As defenders, it is important to be able to use all data available including network scans which are often times numerous and not malicious. Network scans when correlated with various types of information can provide useful information. While the report was misleading in many areas, there are defense lessons that can be learned using this report as a current case study. Cross-analyzing and highlighting all the claims in the report proved to be an exhausting task therefore our focus will be limited to the ICS attack claims.

1 http://www.nytimes.com/2015/04/16/world/middleeast/iran-is-raising-sophistication-and-frequency-of-cyberattacks-study-says.html?_r=0
Credibility: 1 - The available data contained in the report is deemed as factual and credible, however the associated analysis components of the report are being evaluated as inconclusive due to non-traditional use of industry terms in the report assessments and determinations. A significant reason for this is that the report re-defines terms such as ‘attribution’ and ‘attack’ in a manner that deviates from commonly understood usage of those terms. The lower credibility ranking is specifically focused on the claims of the cyber attacks by Iran on ICS. This whitepaper will explain in detail key elements of the claims that were used to evaluate the report. Simple descriptive rating system.

Amount of Technical Information Available: 4 – Norse made a set of their data available to the public through a press release and accompanying marketing during the RSA conference. This data set was significant in size although it did not contain packet captures or flow information. Simple descriptive rating system.

---

**Attacker & TTP Description**

**Attacker:** The reports identify the Iranian government as the attacker. The Norse and AEI report notes that attributing attackers based on internet protocol (IP) addresses is usually inadequate. Therefore, they re-define how the term attribution is used. It is worth noting though that there have been a number of sources discussing a rising cyber threat in Iran however, this is outside the scope of this whitepaper as the authors evaluated the report primarily from a technical perspective.

**Capability** – The capability described in the report are scans launched from Iranian IP addresses. This capability is identified as a “sophisticated attack” although the report does not provide a definition of the term attack. Further, more data or capabilities would have to follow an automated or manual scan in order to warrant the classification of “sophisticated” to these network scans. The ability to perform network scans has been a common network capability for decades. Even massive scanning of the entirety of the Internet is an easily accessible capability that has been available in public code repositories with tools such as Masscan.\(^5\)

**Opportunity** – There were no actual ICS environments impacted in this scenario. The report discusses attacks on ICS and SCADA systems but actually means honeypots and unregistered IP addresses. However, internet connected ICS are known to be highly susceptible to real attacks, as realized by systems compromised in the Black Energy 2 campaign. This opportunity for attackers does exist in the ICS community as has been well documented in efforts such as Project Shine.\(^6\)

**Motivation** – The motivation stated in the report is Iran’s desire to be able to strike back against Western countries. The premise of the report is that the current sanctions on Iran and their geopolitical atmosphere restrict investments in traditional military capabilities and thus cyber capabilities present an alluring opportunity for them. This motivation is logical and is applicable to numerous countries around the world as cyber capabilities have become a necessary component to a nation’s defense capabilities. While this is an accurate assessment and a strong motivation for a nation state to perform cyber reconnaissance, there is nothing directly referenced in the data that provides a link to the motives of those performing the scans.

\(^5\) [http://blog.erratasec.com/2013/09/masscan-entire-internet-in-3-minutes.html#.VTcljjiFVhBc](http://blog.erratasec.com/2013/09/masscan-entire-internet-in-3-minutes.html#.VTcljjiFVhBc)

The TTPs of the adversary highlighted in the report were their ability to supposedly leverage Iranian controlled IP addresses, in Iran and abroad, to perform scans of IP addresses. The report describes this as the main attack. This paper will show that this type of activity is more properly identified as reconnaissance and is one of the first of many steps required to successfully attack an ICS (See ICS Cyber Kill Chain).

Details and Controversy around the Report’s Claims

The Norse and AEI report provided data, some determinations on attribution, and the intent of the adversary. The report was cited in the New York Times and quickly became the center of controversy. The assertions focused on the sophistication and frequency of Iranian government attacks on ICS. An evaluation of every component of the report to validate or examine the findings and assumptions proved to be a difficult task and could not be completed without access to the full data set. However, based on the data available, it is in our opinion that the report’s authors made poor assumptions regarding capabilities due to incomplete technical understandings regarding basic workings of TCP/IP. To avoid saturating the reader with every critique of the report, we will focus on those items most relevant to the reports central claims. The three significant components to the reports’ claims revolved around cyber attacks, ICS targeting, and attribution:

1. Claim: Norse and AEI Claim of Cyber Attacks

   Evaluation: The Norse and AEI report claimed that there were hundreds of thousands of attacks on ICS. Additionally, the report stated:

   “Attacks launched from Iranian IP addresses increased 128 percent between January 2014 and mid-march 2015. The number of individual Norse sensors hit by Iranian IPs rose 229 percent, while the number of distinct IPs used to execute those attacks rose by 508 percent.”

---

There have been a number of undocumented cases of attacks on ICS in the past decade and there have been three pieces of publicly known malware that have specifically targeted ICS: Stuxnet, HAVEX, and BlackEnergy2. For this reason the claims of hundreds of thousands of attacks instantly stands out. Using the report’s information as well as the publicly released Norse data we determined that Norse is identifying each individual network scan as a cyber attack. There are some differing definitions on what constitutes an attack in the community but under no definition is a scan considered to be an attack. Scans are normal network activity and although their evaluation can be useful when combined with other information sources, the reports’ analysis is misleading.

2. Claim: Norse and AEI Claim of ICS targeting

Evaluation: A focus area of the AEI and Norse report was attacks on ICS. An evaluation of the data available as well as the sensors used for the company’s report identified as the “Norse Intelligence Network” reveals that the systems set up were unregistered IP addresses and honeypots. In no case were actual ICS attacked or scanned. In a significantly small portion of the data set there were ICS components connected to the Internet to act as honeypots. While data from honeypots can be extremely valuable proper data extraction and analysis of exploitation methods and after-action impacts were not used in the report. Instead, each scan against these systems was deemed to be an attack. Additionally, the Norse Intelligence Network contains websites that appear to be ICS related and unregistered IP addresses that recorded ports associated with ICS protocols. The AEI and Norse report specifically call out interactions with their “SCADA systems” which were simply IP addresses with ICS related-ports. Interestingly, they note that:

“In the course of several hundred thousand attacks, after all, ports used by SCADA systems were hit fewer than 70 times, suggesting that they are not normal elements of a scan.”

The reports’ authors would have a reader believe that outliers in their data set was proof that the activity was not normal and thus proof an attacker was specifically interested in systems hosted on that port. They also identified “62 attacks in 10 minutes against port 5051” and evaluated this as proof that an attacker was interested in OASyS DNA systems used by Telvent. Additionally, the report stated that because ICS have been discovered on remote connections before, that the Virtual Network Computer port 5900 could be related to ICS. The report appears to imply this to mean that the

---

8 Kyle Wilhoit research
2,400 attempts they observed to connect to port 5900 in their sensors could be considered an attack on ICS. Notably, the creator of Shodan, the popular search engine for finding internet connected devices, stated that many of the Norse ‘SCADA systems’ were easily identifiable as honeypots using quick searches on Shodan and were misconfigured in their attempts to look like an ICS.⁹ Again, it is worth noting that whenever the report references an attack it actually means a scan. The report’s claims of ICS attacks using the data set they contain are ambiguous. In no fair evaluation can these systems be considered a representative ICS target nor can the scans be considered an ICS attack.

3. *Claim*: Norse and AEI Claim of Iranian Attribution

*Evaluation:* The underlining thesis and the statement that grabbed the most headlines in news media were the claims by Norse and AEI that these ‘attacks’ could be attributed to the Iranian government. There are multiple problems with attributing activity to malicious actors based on their IP address alone. While it is the opinion of the authors that Iran is increasing their cyber capabilities and specifically targeting ICS, such as their attempt with the Shamoon malware, the report’s analysis is distorted in two significant ways.¹⁰ First and most alarmingly, the report openly states that the IP addresses in the report are not enough evidence to attribute the Iranian government in the network scans:

“It is also important to note that we use the term ‘attribution’ in an academic and policy sense, rather than a law-enforcement or military sense. We would not support using the relaxed standards of attribution we propose to target Iranian individuals or systems with military or legal response without substantial additional corroboration and evidence.”

In what may be the most concerning statement in the entirety of the report, the authors openly admit that they are re-defining the word attribution since their data does not meet the standards required for attribution. We could find no academic or policy definition of the word attribution as they imply that lowers the standard required. In fact, attribution in the academic community has recently been found to be of a significantly higher standard than what is usually presented in the technical community as can be seen in the Journal of Strategic Studies paper titled “Attributing Cyber Attacks” by Dr. Thomas Rid

---

⁹ Based on public and private interactions with John Matherly on Twitter by Robert M. Lee
and Ben Buchanan.\textsuperscript{11} Secondly, another component that was considered in the evaluation of the report is that the Norse Intelligence Network undoubtedly collects a much larger set of data than what was presented in the report. In other words, not all the scans captured would relate to Iran. However, the activity the authors thought was related to Iran was extracted and highlighted while the other data was not presented. This sort of selective data isolation can greatly skew metrics and the meaning of data.

**Breakdown of ICS Cyber Kill Chain**

The authors of this DUC utilize an understanding and definition of what constitutes a cyber attack based on commonly accepted definitions, technical understanding of what impacts ICS, and contributions in the academic community such as the Center for Strategic and International Studies’ “A Note on the Laws of War in Cyberspace”\textsuperscript{12} and the North Atlantic Trade Organization’s Cooperative Cyber Defence Center of Excellence’s “Tallinn Manual on the International Law Applicable to Cyber Warfare.”\textsuperscript{13} This understanding has been combined with known attacker patterns such as those described in Lockheed Martin’s “Intelligence-Drive Computer Network Defense Informed by Analysis of Adversary Campaign Intrusion Kill Chains” colloquially known as the cyber kill chain.\textsuperscript{14} The result is presented here as the ICS Cyber Kill Chain (Figure 1) and will be used to compare against the Norse and AEI dataset (further information on the Lockheed Martin Cyber Kill Chain \textsuperscript{15}.

\textsuperscript{11} http://www.tandfonline.com/doi/pdf/10.1080/01402390.2014.977382
\textsuperscript{12} http://csis.org/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf
\textsuperscript{13} https://ccdcoe.org/research.html
\textsuperscript{14} http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
Figure 1: ICS Cyber Kill Chain Cyber Intrusion, Preparation, and Execution

In the first stage of an ICS cyber attack the phases can be categorized for the purpose of visualization as Planning, Preparation, Cyber Intrusion, Management, and Sustainment. These phases encompass different actions such as Reconnaissance, Weaponization, Targeting, Delivery, Exploitation, Installation/Modification, Command and Control, and Actions (Figure 2).
It is in this stage that most activity targeting ICS occurs and in which the actions most directly map to what would constitute breaches in traditional information technology (IT) networks. The adversary must perform reconnaissance to find systems of interest, identify specific targets from that data set, weaponize their capability, deliver it to the victim, have it exploit an information system upon delivery or activation, install or modify files for the purpose of gaining a foothold, connect up to an external server for command and control, and perform actions on the target. These actions can include the discovery of new targets, the collection of information such as intellectual property, the exfiltration of the data, and anti-forensic techniques. It has been observed that the significant portion of malware and network intrusions in the community occur during this phase as this is where foreign intelligence and espionage operations are most likely to take place. In many cases, there is significantly more value in performing espionage than actual attack, which would include the destruction or manipulation of systems in unfavorable ways. The term “cyber attack” is sometimes applied to the exploitation phase of this stage and while in ICS this is not truly accurate it is a much more acceptable use of the term cyber attack than what was presented in the Norse and AEI report. As will be discussed later, the Norse and AEI
dataset primarily focus on the reconnaissance step and identifies it as an attack.

What makes performing an ICS cyber attack so different than a traditional IT cyber attack is that the systems are designed in unique ways and configurations that require extensive knowledge by the attacker to impact them in a meaningfully and designed way. Additionally, in a properly architected ICS there are many layers of systems and detection sensors that an adversary has to traverse in the first stage to gain access to the ICS components. Unfortunately, directly connecting an ICS to the internet significantly undermines the inherent advantages that an ICS has towards security. While many ICS environments do not traditionally have security designed into them, which can be a significant problem, impacting them in a meaningful way is simply not an easy task. This problem is visualized in Stage 2 of an ICS attack (Figure 3).

![Figure 3: Stage 2 – ICS Attack Development and Execution](image)

It is in this stage that the attacker must use the knowledge gained in Stage 1 to specifically develop and test a capability that can meaningfully attack the ICS. The complexity of this task is determined by the security of the system and the intended impact. For example, a simple denial of service which disrupts the ICS is significantly easier to achieve than manipulating the process in a designed way
or being able to attack the system and have the option of re-attacking (Figure 4).

![ICS Exploit-Attack Effect Difficulty Scale](image)

**Figure 4: ICS Exploit-Attack Effect Difficulty Scale**

While there are various ways to attack an ICS environment the most common for functional impact can be identified as a Loss of View, Denial of View, Manipulation of View, Denial of Control, Loss of Control, Manipulation of Control, Activation of Safety, Denial of Safety, Manipulation of Safety, and Manipulation of Sensors and Instruments (Figure 5). There is an inherent contrast in impacts between IT and operations technology (OT) that operate an ICS. As an example, denial of service to an IT system may be extremely significant to a business process whereas in ICS the manipulation of sensors or the process is more disturbing as it could lead to the failure of safety systems designed to protect human life or induce the process to purposely injure personnel.
While ICS attacks can be classified in a number of ways, and the definition of cyber attack can be used loosely in the larger community, the Norse and AEI analysis and data do not reach any threshold appropriate for classification of an attack. The activity documented by Norse towards ICS can more appropriately be identified as reconnaissance focused on Stage 1 of the ICS cyber kill chain (Figure 6). It is worth noting that this data set would be useful for identifying and understanding patterns that could identify the eventual targeting and delivery of a weaponized exploit to a victim. Having reconnaissance data is extremely useful although often unmanageable for long periods of time due to the volume of activity on the Internet. Reconnaissance performed internal to the network though is more easily identifiable especially in more static ICS networks. This will be elaborated on in the next section.
Figure 6: Norse and AEI Data Mapped to the ICS Cyber Kill Chain
Defense Lessons Learned

1. Reconnaissance is generally the first visible stage of an adversary’s attempt to breach or attack an ICS. Reconnaissance external to the network can be observed through sensor networks such as strategically deployed honeypots, unregistered IP addresses as is the case in the Norse Intelligence Network, and in sources such as the perimeter Firewall of an organization. This data is important and when correlated with other sources of data such as advisories or timeline analysis performed during an intrusion can be extremely valuable. The report highlights adversary trends that ICS defenders should be aware of in regards to: leveraging infrastructure within target borders through organizations that may or may not be aware that they are being used as a beachhead, as well as the continued expansion of adversarial use of cloud and hosted computing environments to achieve additional capabilities. Attackers do not often use the same networked infrastructure to perform reconnaissance and to attack from but there are often correlations that can be made. However, this external network reconnaissance is very common on the Internet and the data should not be overvalued. Additionally, it must be correctly categorized to avoid alarmism and driving poor defense tactics. Lastly, this data should never be used alone to perform attribution of the true source of the reconnaissance as the data has a temporal nature and may not accurately represent the individual or organization generating the activity. Reconnaissance performed internal to the network though is more interesting as it indicates an adversary has already compromised the network. This type of scanning and information gathering is usually easily identifiable in static ICS networks through processes such as network security monitoring.\textsuperscript{16}

2. One of the inherent advantages of a properly structured ICS is that it requires multiple phases for an attacker to access the ICS while also attempting to learn its unique design and configuration. Good architecting of the network to include segmentation and separation where feasible and defense in depth practices significantly contribute to the security of the ICS. While using layered security measures are not always enough to defend the ICS from advanced and sophisticated attackers it is an essential phase of defense known as passive defense. These passive defenses build a foundation in the security posture for active measures, such as network security monitoring, to be performed. Additionally, the Norse and AEI report identified the speed, duration, makeup, and frequency of the scans observed as well as the likelihood of the scans being missed amongst all of the observable data. Defenders need to implement technologies that aid in the identification of

\textsuperscript{16} Network security monitoring is one of the four phases of the Active Cyber Defense Cycle which is the subject of the SANS ICS 515 – Active Defense class.
malicious activity, in addition to the need for event logging and alerting. These defense in depth and proper architecture methods provide multiple opportunities for defenders to detect the adversary. For example, internal network reconnaissance can often be detected by intrusion and anomaly detection systems and reviews of internal firewall logs.\(^{17}\)

3. The Norse and AEI report did not present any actual cyber attacks against real ICS environments however it did highlight a discussion on threat intelligence and provide a good opportunity for the ICS community to evaluate one of the downsides of threat intelligence. Cyber threat intelligence is an incredibly important component of a mature security posture when incorporated on top of an ICS with good architecture, passive defenses, and active defenses. Cyber threat intelligence though must always be evaluated to determine its applicability to any given organization. Additionally, a critical eye should be given to cyber threat intelligence reports making claims that do not seem realistic, such as hundreds of thousands of attacks on ICS. Organizations looking to incorporate threat intelligence into their security postures should make sure that the vendor has the appropriate and demonstrated ICS experience required to produce this type of threat intelligence and that the vendor has taken every method to reduce confirmation bias. Confirmation bias is a quick way for analysts to disrupt the value of an intelligence product. As an example, the report makes numerous references to political sanctions and existing framework agreements. These politically aligned statements contained within the scope of data set analysis can be concerning. Regardless of the validity of the final conclusion, the politically aligned statements are generally not supported in the evidence presented in the report. Potential confirmation bias must always be watched for when evaluating threat intelligence reports.

\(^{17}\) Proper ICS architecture as well as passive defense mechanisms that provide the foundation for ICS defense are taught in SANS ICS 410 – ICS/SCADA Security Essentials.
Implications / Predictions

- Adversaries will continue to perform reconnaissance against systems on the Internet to identify systems worth targeting and continuing operations against.

- Policy recommendations based off of threat intelligence reports will continue to emerge as parties find value in technical data that appears comprehensive and convincing although missteps in analysis are hard to counter.

- Mislabeled terms such as ‘cyber attack’ will ultimately result in confusion, alarmism, and hype regarding the number and type of attacks observed in the community; this poses a threat to the trust bestowed in the security community and stands to impact relationships with asset owners.

- The community will continue to see the rise of some cybersecurity companies attempting to grab national headlines by making bold statements regarding ICS and international tension. Sharing data with the community is helpful, but evidence should be cited to support analytical judgments and author opinions should be clearly stated. This is not to say that this was the intent of Norse as their intent is unknown and cannot be fairly evaluated.

- As the security community and the ICS community continue to mature and create bridges between the two communities there will be a better understanding of what constitutes a real threat and what actions are taken. In recognizing this it can be stated that the formed relationships will result in a push back against hype and alarmism that will ultimately yield a more nuanced and mature discussion.
Conclusion

The claims in the Norse and AEI report released on Apr 17, 2015 are evaluated as misleading. The intent of the report was to highlight attacks by the Iranian government against ICS. This whitepaper evaluated these claims and concluded that the reports and their data set showed that attribution to the Iranian government was not obtainable from the data, the activity identified by the report authors as attacks were network scans, and no real ICS environments were impacted. ICS components did make up a subset of the data as honeypots but this subset of data was a significant minority of the data reported. Available information showed these were likely misconfigured systems, and the systems were directly connected to the Internet in a way that network scans could not be considered substantial data.

This whitepaper attempted to remain objective in its analysis of the data provided in the Norse report. However, under technical and analytical review, the report failed to meet the quality of analysis required to support the author’s claims and often used terms in a manner that appeared to support a political objective rather than in a manner that is common within the defense or intelligence community. Continued reports that blend technical data analysis with political positioning can damage sensitive relationships and trust in the ICS security community as well as contribute to alarmism that may drive misappropriation of resources and attention in the broader community. Items that ICS defenders should take note of from the report and from this whitepaper include:

- the ever-present reconnaissance activity on the Internet searching for ports associated with ICS,
- the growing use of cloud or hosted environments for scanning purposes,
- the need for asset owners to implement appropriate event logging, correlation and routine reviews of data sets to identify activity of interest
- improved understanding of attribution concerns and how to evaluate threat intelligence reports
- reference models to improve understanding of cyber attack phases in ICS environments

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