Securing the Energy Sector from Advanced Threats

Reducing Risk in an Increasingly Connected World

- As a part of critical national infrastructure the energy sector is a target for Advanced Threat activity.
- Despite continued investments in new technologies to block the latest threats, attackers get through.
- Attackers leverage the human element, via social-engineering etc., to gain a foothold within our networks.
- Once inside attackers move laterally, establish resilient connectivity and have plenty of time to achieve their goals.
- Reducing the time to detect and contain incursions is key to reducing business risk.

Executive Summary

Energy businesses are increasingly attractive targets for cyber attackers given their high visibility, central role in the world economy and the politically sensitive nature of their global operations. Energy firms are being targeted every day, and many who are breached don't find out until it's too late. Attackers are leveraging social engineering and using partner organisations to gain access to high-value targets, leveraging stolen user credentials to stay under the radar. Layered perimeter security, incorporating the latest technologies, isn't stopping targeted threats. Our adversaries are people, and innovate quickly to outpace technology advances. Once inside a network attackers have a LONG time to accomplish their goals, before they are detected and stopped. Broad and deep visibility across infrastructure is becoming a necessity to identify threats more quickly. Leveraging the right threat-intelligence, and employing workflows that speed up the detection, validation and response processes are key given limited security resources. Arbor Networks has 15 year's experience securing network infrastructure and services for many of the world's largest businesses.

A Very Real Threat

Breach notifications from large organisations are now almost a weekly occurrence. Many of these organisations have invested in layered security at their network perimeter, and have the latest technologies deployed.

Unfortunately attackers are constantly innovating and have access to many of the defensive technologies used today. This allows them to develop methods to circumvent these technologies as quickly as they are being deployed, rendering many of them useless. The sophistication of attackers is variable, but in the energy sector well-resourced nation-state and terrorist organisations are a key concern.

Locking down the perimeter of the network to keep threats out is virtually impossible given modern working practices, BYOD, control applications, billing interfaces and partner connectivity. This list does not include what is often the weak-link, from a security perspective, the human element.

The energy sector has additional concerns:

- They store customer personal and financial data that is valuable to attackers motivated by financial gain.
- They occupy a unique position within critical national infrastructure and national/global economies, making them a target for ideologically and politically motivated attacks.
- Security teams within most energy sector organisations are still resource constrained.
- Proactively identifying zero-day or insider threats is becoming increasingly important.

The Human Element

Attackers continue to be successful in using social engineering techniques to gain a foothold within networks. Training and education can help reduce risk, but attackers are resourceful, and will often target low-value resources,

business partners etc., from which they can move toward their eventual target. Once inside a network, attackers often have a significant period of time to move laterally, establish resilient connectivity and accomplish their goals discretely.

Energy companies have both valuable competitive and customer data, which can make them the target of cyber-criminals, and a key position within national critical infrastructure, which makes then the target for nation-state or terrorist attack.

Preparation is Key

The energy sector has seen huge change in the recent past, with many organisations now far more reliant on the Internet for customer communications, billing and b2b activities. Significant amounts of project, personal and financial information are often stored and the protection of this data is critical. A breach can be hugely damaging from a cost, reputation and regulatory perspective.

Given the critical role many energy sector businesses posses in national infrastructure and global / national economies, they are also a target for both ideologically and politically motivated attacks that are purely aimed to cause disruption, rather than financial gain for the attacker.

The Scale of the Problem

Saudi Aramco is probably the best-known targeted attack to impact an organisation in the energy sector. This attack caused huge disruption, impacting over 30,000 computers and forcing a large, multi-national corporation to effectively do without network communications and the Internet for a significant period. All caused by a simple click on a link within a spear-phishing email. And, with Trojans specifically focused on the energy sector, such as Laziok, it is clear that attackers are active in this area.

The Way Forward

Deploying additional technologies to detect / block the latest threats as they enter our networks is the approach many organisations continue to take. This is effective at dealing with the majority of attacks, but a determined adversary will eventually get through these defences; what we need to do is detect any incursion or anomaly as quickly as possible, wherever it occurs.

The need for both broad and deep visibility of network and user activity has never been so great. All attacks make use of the network at some point, and thus should be visible if we are monitoring in the right way. Technologies to provide cost-effective, broad visibility are already built in to much of our network infrastructure. Arbor has 15 years of experience at leveraging this telemetry to detect threats and provide visibility within complex service provider and enterprise networks.

Augmenting broad visibility with deep visibility at key locations through packet capture and meta-data extraction can allow the identification of more specific threats, and access to relevant forensic data to aid investigation. But, the data produced needs to be accessible and usable by our security teams.

The Human Element (Again)

What is imperative is that security solutions maximise the effectiveness of scarce security resources and promote workflows that remain oriented around the goal—reducing business risk from cyber attack. This is an area of focus at Arbor Networks, and we provide solutions that are designed from the ground up to simplify detection, validation and response to threats.

Human security resources are the key asset in identifying unusual traffic or threat trends within our networks, and Arbor solutions are designed to maximise their capability. The concept of 'hunting' for threats is becoming increasingly well known, but the barrier to adoption is usually time / resource. Arbor solutions

use innovative visualisation techniques to allow speed-of-thought navigation through large volumes of data, reducing the time spent in the threat validation/ investigation process to free up time for more proactive, focused identification of potential problems which may otherwise have gone unnoticed.

Learn more about Arbor Pravail at: arbornetworks.com/products

New Threats Require a New Approach to Security

As an industry leader in the provision of solutions providing defence against network borne attacks, Arbor Networks is a key security partner for many businesses within the energy sector. Arbor's approach is to work with customers to deliver solutions that will ensure both service availability and security, and provide on-going advice and intelligence on threat evolution.

Arbor's Security Engineering Response Team (ASERT) specialises in researching attack campaigns targeting the energy sector. ASERT leverages the unique visibility Arbor has of around 30 percent of daily Internet traffic, together with key malware and botnet analysis capbilities, to deliver threat intelligence that can be used to accurately identify threats, with additional context around any associated campaign.

Arbor's Solution Portfolio has Three Areas of Focus

- **Always-on network perimeter protection from DDoS attacks:** Threats such as DDoS and other cyber-attacks need to be detected and blocked before they escalate into costly service outages.
- **Cost-effective internal network visibility and threat detection:** The greater your visibility across internal network operations, the better your ability to detect suspicious or malicious activities wherever they occur.
- **Security analytics:** speed up the investigation and triage of security events and augment existing threat detection processes with a more proactive 'hunting' approach. Attackers are innovating constantly; maximise the effectiveness of your security resources to counter this innovation by giving them interactive visualisations of key security data, so that threats can be identified, understood and contained more quickly.

Arbor Networks strives to be a force multiplier, maximising the effectiveness of existing network and security teams. Our goal is to provide solutions that solve problems and reduce risk.

ARBOR NETWORKS

The Security Division of NETSCOUT

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales

Toll Free +1 855 773 9200

Europe

T +44 207 127 8147

Asia Pacific

T +65 6664 3140

www.arbornetworks.com

©2016 Arbor Networks, Inc. All rights reserved. Arbor Networks, the Arbor Networks logo, ArbOS, Cloud Signaling, Arbor Cloud, ATLAS, and Arbor Networks are all trademarks of Arbor Networks, Inc. Bloomberg and Bloomberg Terminal are trademarks of Bloomberg Finance L.P. All other brands may be the trademarks of their respective owners.

SB/ENERGYSECTOR/EN/0516-LETTER