CORE SECURITY

Protecting Critical Infrastructure and Industrial Networks from Advanced Threats

CORE SECURITY

Table of Contents

Introduction:

In a 'connected' age when nearly everybody has heard about 'hacktivist' groups and cyber threats, organizations still struggle to implement an effective security posture to defend against today's advanced threats. Nowhere is this more dangerous than in the "critical infrastructure" industry that runs assembly lines, provides power and controls traffic lights.

Today's cyber attackers take advantage of the incompleteness of security tools and processes to exploit weaknesses. While prevention tools are necessary, advanced malware regularly finds its way through security walls. These compromises remain hidden from detection, communicating to external actors for instructions to exfiltrate information or disrupt systems.

Due to the unique challenges associated with critical infrastructure technologies and the complex nature of attacks, early and accurate infection discovery is paramount. Through active threat discovery and automated response, the worst breaches can be avoided.

Critical Infrastructure and Industrial Networks

The Presidential Policy Directive 21 (PPD-21) of 2013 defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." This directive outlines 16 different sectors as critical infrastructure to the United States.1 This definition and the corresponding critical infrastructure sectors map fairly closely to definitions in Canada and most other countries.2 PPD-21 is an excellent outline for critical infrastructure as it relates to the national security interests. Critical infrastructures, by this definition, could be viewed as a subset of all industrial networks, which warrant the best protections available. A manufacturer of steel pipe considers their extrusion systems to be critical infrastructure in the context of their business. Though limited in terms of national security, compromise of this manufacturer's industrial network could have catastrophic results.

The infrastructure of this importance would ideally never be connected to untrusted external networks, but global organizations do have to interconnect industrial systems to run their business. A typical industrial network has the layered architecture shown in Figure 1. Each of these layers should be considered in scope for protection. Each layer has its unique attributes.

The Business Network layer requires the most freedom for users and IT assets to speak to various internal systems, as well as to the external and untrusted Internet. Found here are the email systems, intranet servers, Windows 7, and other devices associated with traditional network and device security. The Control Systems layer is nearly opposite in nature. It often includes proprietary systems, discrete and limited functions, and should never be allowed to speak directly with an untrusted network like the Internet. The Control Systems layer contains devices by manufacturers such as Rockwell Automation, General Electric, and Emerson. Security professionals may be unfamiliar with the protocols, interfaces, and security that exist at this layer.

The Supervisory Control and Data Acquisition (SCADA) layer of the industrial network architecture sits in the middle. Systems in this layer will have a combination of features from the other two.

The Supervisory layer may have proprietary Human Machine Interfaces (HMI) that are sometimes just command line terminals, but usually running legacy versions of Windows OS. These systems could have both Ethernet connections using standard TCP/IP, but also serial fieldbus. There are legitimate reasons for outbound and inbound connections into the Supervisory Network from the Business Network. For example, the SCADA network reports directly into ERP systems and dashboards for monitoring by appropriate devices/users. Users may also need to connect into these systems remotely for maintenance or diagnostics.3

Critical Infrastructure and Industrial Networks (continued...)

The eroding perimeter of the Business Network has been discussed at length in the information security community. The developing business landscape has forced this change through mobile devices, BYOD, globalized organizations, and outsourcing of all types. The same can be said of the perimeters for both the Supervisory and Control layers of industrial networks. The security best practice of isolating these layers from each other and untrusted networks with only better walls is insufficient.

Advanced Threats and Critical Infrastructure

Attacks on industrial systems are performed by threat actors with varying sophistication and goals. These attacks could be sponsored by nations for the purpose of espionage, by organized crime for infor- mation resale to other criminal actors, or by competitive foreign enterprises in order to gain advantage. According to Verizon's Data Breach Investigations Report 2013, One in five network intrusions involved manufacturing, transportation, and utilities (a greater than 10% increase), and 92% of the breaches were perpetrated by outsiders.4

Two things are known to be true. First, for valid business critical reasons, the Business Network is connected to the Supervisory Networks and consequently the Control Network via legitimate hosts and applications. Second, there is no complete and perfectly effective prevention of compromise to Business Network hosts. This means that by nature, some number of successful attacks on the Business Network can result in compromise to critical infrastructure.

Consider the following scenario:

- An attacker purchases a fairly inexpensive off-the-shelf root kit with well-established signature detection avoidance features, a command-and-control communication model, and a noise engine.
- With a bit of effort, the attacker repurposes some of the features of this kit to make it unique to their specific purposes, and unique upon each installation. The attacker establishes a new com- mand-and-control architecture using throw-away domains, dynamic DNS, and anonymous host- ing services at additional cost. Or, the attacker utilizes the criminal ecosystem to rent access to a well-maintained and well-hidden command-and-control infrastructure.
- Instead of deploying the weaponized kit on their own, the attacker pays to have yet another established partner install the kit throughout the target organization's network using a phishing campaign.
- Even a single installation of this kit within the target organization establishes a foothold from which to expand laterally to other internal systems to gather information.

How the Idealized Downloader Lifecycle Works

- While directed by the controlling attacker, the compromise jumps from host to host, using new variants upon each new installation, new command-and-control domains, erasing records of its existence, and exfiltrating interesting data.
- The attacker finally lands on a host with a copy of a "SCADA_Network_Diagram" file. This host also appears to be running a read-only SCADA Dashboard application.

The above example demonstrates a few characteristics that are typical of many advanced threat attacks:

Advanced threat malware doesn't need to be written from scratch. There are inexpensive kits that work fairly well at avoiding signature and anomaly detection tools that can be repurposed with little effort. DIY malware kits such as SpyEye and Remote Access Trojan (RAT) kits can be had for under $200.5

The services of the advanced threat ecosystem can be bought and sold or rented on an as needed basis.

Attacks on industrial networks can and do initiate from within the Business Network, or a compromise of the Business Network is used as reconnaissance for a follow up attack directed at the Supervisory or Control layers.

Industrial Network Vulnerabilities

Industrial Networks are particularly difficult for the traditional information security professional to protect. Users, platforms, and operational function are starkly different for the technologies in the SCADA and Control layers, and it isn't surprising there is such a chasm between information security and industrial network security. Does the security operations center have a procedure for patching unique systems such as specific fixed-function devices? Does anybody in information security know how to access one? How frequently are turbine maintenance supervisors given information security awareness training?

Industrial networks come with an entirely different set of users. Maybe operator is a more appropriate term. Within their work functions, these operators may never open an .exe file, visit the intranet site, or use instant messaging. It's also very possible that their interface with networked technology is limited to knobs, levers, joysticks or toggle buttons. These operators become vulnerable in different ways to the advanced attack, whether of Internet origin or not.

Industrial Network Vulnerabilities (continued...)

Enterprises are very familiar with platforms on the IT side of security. There are only a handful of devices and OSs: Windows, Mac, and Linux. Experience with these platforms is in ready supply.

Operational process around backup, restoration, patching, high availability, monitoring, hardening, and vulnerability management are well documented. Operating systems also use ubiquitous standards for communication: TCP/IP, HTTP, FTP, SSH. While there is some overlap with industrial networks have a lengthy list of proprietary operating systems, firmware, device drivers, hardware, and communication protocols. Modbus for example has both TCP/IP and serial RS-232/485 versions. Installing vulnerability patches on these types of live industrial networks is time consuming and extremely difficult because the system has to keep running. The architecture of Windows allows it to be patched easily when compared to firmware vulnerabilities in a proprietary control system.

Improved Posture Against Critical Infrastructure Attacks

Balance is necessary to weigh the risks associated with interconnectivity of the layers outlined in Figure 1. National critical infrastructure and industrial network both derive benefit from this connectivity, but can also suffer from its vulnerabilities. The attacker in the example above will take the path of least resistance to achieve the necessary goal, whether industrial network reconnaissance, or further compromise. In order to improve the security posture for any of these organizations, it is paramount that industrial network security and traditional information security teams integrate controls, policy and process.

An effective way to reduce exposure of industrial networks to advanced Internet-based attacks is to integrate the tools used to secure each of the layers; Business, Supervisory, and Control. Best practices exist but are rarely explored, usually because of the lack of oversight across these layers. Consider the following two examples:

- When a SCADA IPS detects TCP traffic from a device in the Supervisory layer directed at a Business layer host coming from a new network, an alert should be sent to the SIEM such that security opera- tions can validate this is a valid user performing a valid action. In the meantime, packet capture can be initiated for Internet-bound activity from the potentially nefarious user. Network admission control could even quarantine this device for a short period to avoid attack progression. This precautionary response could assist in detecting and thwarting data exfiltration.
- If a Business layer network security device determines that a network host is compromised, and under some sort of criminal control, this network device should immediately take action to prevent the attack from escalating. When an infection is confirmed, this network device can alert a perimeter firewall protecting the industrial network to actively block inbound connection attempts to read-only or read/write SCADA systems.

Only a coordinated detection and response effort between traditional security and industrial security controls could mitigate the exposure to an Industrial network. Most importantly it requires a willingness of both the industrial security team and information security team to cross train and learn about the capabilities of both systems.