Cyber Threats: Protecting Manufacturing Assets

Nina Vajda

It’s an easy, if not familiar, scene to imagine: An employee sitting at his or her computer gets a call from someone who claims to be with the company IT department. The caller warns the employee that his or her computer has been compromised, and asks for the employee’s IP address to investigate the issue.

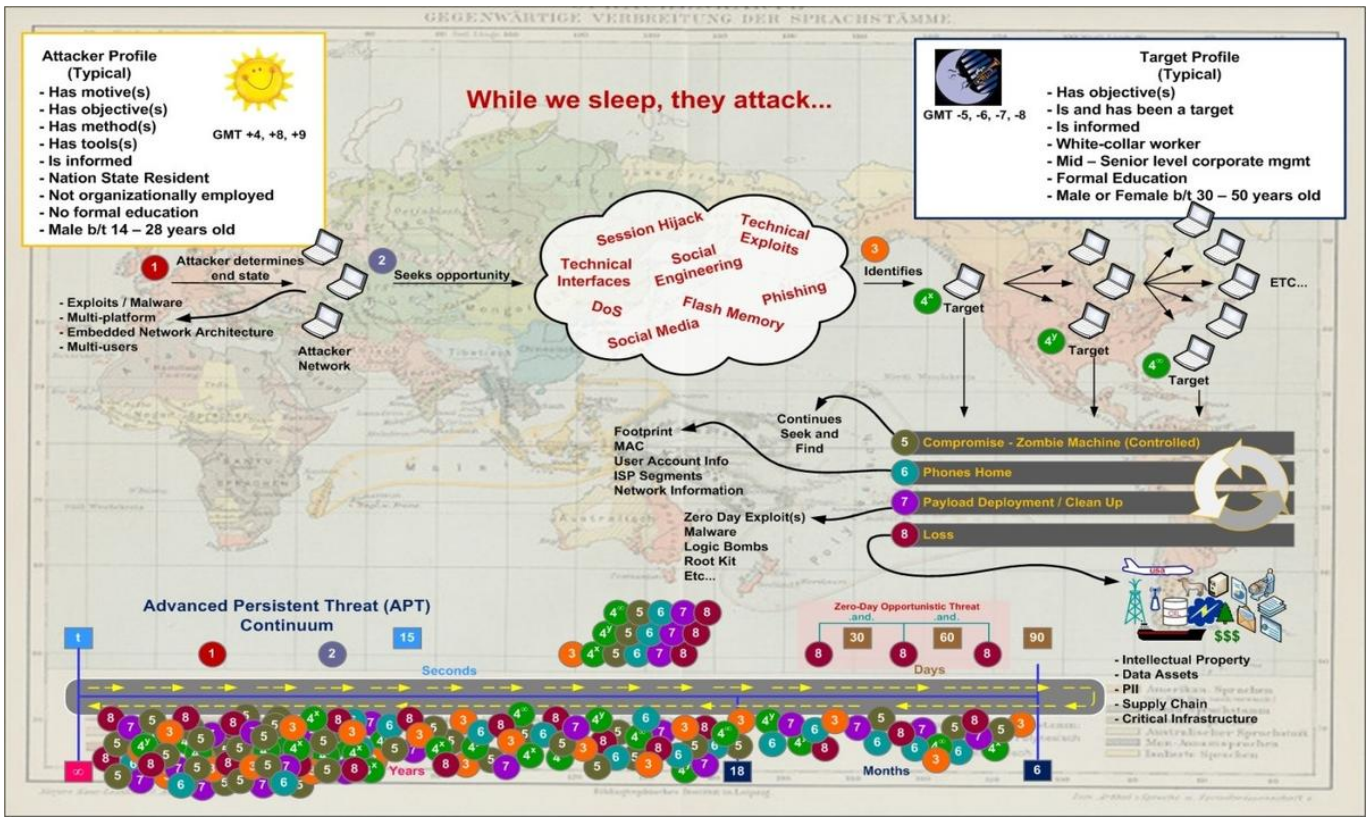
Acting with the best of intentions — and likely having little or no understanding about the complexity of cyber security — the employee provides the IP address as requested and possibly other sensitive computer information. Unwittingly, the employee hasn’t helped the company prevent a malicious cyberattack, but rather invited one.

It’s an all-too-real nightmare for IT professionals. But the fact is, the average employees sitting in front of their computers rarely are aware of the multitude of threats that exist behind seemingly innocuous sources — phone calls, social media links, email attachments, flash drives or elsewhere.

Such cyberattacks, however, are part of a larger and thriving multibillion-dollar global business. Tens of thousands of new malware (“malicious software”) variations are discovered every day. Their design, deployment and use are propelled by a range of parties, from independent opportunists and politically motivated organizations to government-sponsored entities and terrorist organizations.

Cyberattacks target everyday people as well as governments, organizations and industry. From stealing highly sensitive government data and classified military information to proprietary product information and highly valuable trade secrets, cyber threats exist anywhere an asset exists, whether that asset is personal, financial or political.

Using methods such as zero-day attacks (sometimes referred to as Advanced Persistent Threats) — which identify system vulnerabilities and strike when a user or developer is unaware of its presence — cyberattackers can use malware to retrieve and send sensitive information back to the attacker. The malware can then turn its host into a “zombie” machine to look for other target machines and compromise them.



Anatomy of a Zero-day attack

Cyber threats are so prevalent and pervasive that governments now require facilities that are considered to be critical infrastructure, such as power plants and water-treatment facilities, to achieve and demonstrate regulatory compliance to help protect from cyberattacks.

Protecting Manufacturing Assets

The threat that cyberattacks pose to manufacturers can be seen, literally, in the plethora of counterfeit products that flood the global marketplace every year, from popular automobiles to highly sophisticated military equipment. Manufacturing companies must accept that if their product has value, it’s a target for cyber criminals.

Every manufacturer has unique assets, similar to a fingerprint. Manufacturing equipment and industrial automation and controls are of varying values, as are the different technical infrastructure in place to design and produce those assets. These unique characteristics all define the different types of risks and threat sources that each manufacturer faces.

In particular, companies’ intellectual property, which is the lifeblood to their success, is a primary target in cyber espionage. This serves as an important reminder that cyber security is about much more than securing operations today — such as safeguarding success tomorrow.

It’s vital for manufacturers to conduct network-security risk assessments — including identifying the unique needs to protect their assets — and then put into place risk-mitigation processes. This includes a robust range of controls, activities,

and processes to help ensure security.

Industrial IP to the Rescue

Manufacturers and other companies previously attempted to take on cyber threats themselves, independently developing and implementing proprietary solutions to protect their assets and respond to threats.

However, the massive growth of these threats combined with the innovations being developed in the cybersecurity field has led to a change in strategy. Manufacturers cannot rely on “security through obscurity.” Instead, they increasingly are turning to industry solutions that utilize open standards, tools and best practices such as:

- **Segmentation:** This capability is at the heart of network security and should be utilized in every plant. Segmentation supports security and management efficiency by dividing a network into smaller segments, or sub networks. Through this process, security is built into the routers to limit user access to specific and defined segments.
- **IPsec:** Internet Protocol security (IPsec) is one of the most commonly used applications and another best practice for security. It authenticates and encrypts each IP data-stream packet to secure communications via virtual private networks (VPN) between hosts, such as computer users and servers, and security gateways, such as firewalls and routers.

An obvious cybersecurity solution that most manufacturers already employ is a firewall. While this is a useful security measure, it should never be used as the sole solution for cybersecurity. Just like a physical wall, a firewall can only reach so far and keep so much out.

Of course, cyber security is only part of the larger security picture. Plant physical security requires tools such as cameras and “swipe” access cards. These

Nina Vajdasecurity tools also use IP connectivity, meaning that they essentially are plug-and-play compatible when used within an Industrial IP-enabled plant.

Industrial IP enables manufacturers and their IT departments to take advantage of the vast amount of work being done by the cybersecurity experts and industry. Their job, after all, is to stay one step ahead of the threats. And the threats are growing every day.

Nina Vajda is global manager of Network & Security Services at Rockwell Automation *[1] and wrties on behalf of* Industrial IP Advantage *[2].*

Links:
[1] http://www.rockwellautomation.com/
[2] http://www.industrial-ip.org/