Contribution ID: **521** Type: **Paper**

Advanced Malware and Nuclear Power: Past, Present, and Future

Cybersecurity in nuclear power is difficult to manage, overall. It is expensive to implement, regardless of the regulatory regime a plant is under. Technical controls are challenging to profile in many cases, as digital failure modes can be both difficult to model and can have wider ranging consequences than typical physical failures. Furthermore, intrusion detection and prevention controls for industrial systems can be much more expensive to deploy, as well as purchase or build. As a result, insight into likely future attack approaches, goals, and techniques will be invaluable in guiding future cybersecurity investment.

In the first section of this paper, we will examine noteworthy malware campaigns released over the past decade. We will identify key trends and areas of technical and procedural convergence between individual strains. We will examine current techniques, tactics, and procedures from both operational and technical perspectives. In the second section, we will conduct the same analysis over advanced malware strains that deliberately target industrial control systems. This will include older threats like Stuxnet and Flamer, as well as new threats like Hatman and CrashOverride. Both sections will focus on the adoption of new techniques and practices of malware attack teams rather than attribution. The main thrust of these two sections is to clearly outline the evolution of today's general malware threats to establish a baseline of malware technical and procedural trending that we can compare and contrast with similar trends in advanced industrial malware strains.

Once we have been able to outline these evolving trends, highlighting both similarities and key differences between strains that target industrial systems and more general purpose strains, we will begin to hypothesize why those similarities and differences exist. For example, common initial infection vectors are radically different between advanced industrial and general purpose malware strains. Industrial strains typically rely on insider placement, while general families can take advantage of semi-commercial exploit kits. They both leverage phishing and spear-phishing approaches. In the case of industrial strains however, the phishing campaigns are much more targeted and deliberate.

We will then identify key trends in industrial malware capabilities and outline the impact of these trends on nuclear power plants, their operators, and industrial system manufacturers.

Over the past 10 years, we have seen a remarkable change in malware sophistication and the adoption of new strategies by malware authors. These kinds of approaches are beginning to appear in industrial malware strains as well. Although there are clear similarities in how malware is developed and deployed when comparing general purpose and industrial malware strains, there are distinct differences as well that are beginning to emerge. Both these differences and similarities have profound implications for nuclear power plant protection.

Gender

Male

State

United States

Author: LAMB, Christopher (Sandia National Laboratories)

Presenter: LAMB, Christopher (Sandia National Laboratories)

Track Classification: CC: Information and computer security considerations for nuclear security