The FireEye Approach to Operational Technology Security

December 11, 2019 | by [Steve Miller](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/cap-steve-miller), [Nathan Brubaker](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/nathan-brubaker), [Daniel Kapellmann Zafra](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/daniel-kapellmann-zafra), [Neal Gay](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/neal-gay), [Rob Caldwell](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/rob-caldwell)

[**OPERATIONAL TECHNOLOGY**](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-tags/operational-technology) [**CYBER PHYSICAL**](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-tags/cyber-physical) [**THREAT INTELLIGENCE**](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-tags/threat-intelligence) [**INFORMATION TECHNOLOGY**](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-tags/information-technology) [**ICS SECURITY**](https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-tags/ics-security)

Today FireEye launches the Cyber Physical Threat Intelligence subscription, which provides cyber security professionals with unmatched context, data and actionable analysis on threats and risk to cyber physical systems. In light of this release, we thought it would be helpful to explain FireEye’s philosophy and broader approach to operational technology (OT) security. In summary, combined visibility into both the IT and OT environments is critical for detecting malicious activity at any stage of an OT intrusion. The FireEye approach to OT security is to:

*Detect threats early using full situational awareness of* *IT and OT networks.*

The surface area for most intrusions transcend architectural layers because at almost every level along the way there are computers (servers and workstations) and networks using the same or similar operating systems and protocols as used in IT, which serve as an avenue of approach for impacting physical assets or control of a physical process. The oft touted airgap is in many cases a myth.

There is often a singular focus from the security community on industrial control system (ICS) malware largely due to its novel nature and the fact that there have been very few examples found. This attention is useful for a variety of reasons, but disproportionate to the actual methods of the intrusions where ICS-tailored malware is used. In the attacks utilizing Industroyer and [TRITON](https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html), the attackers moved from the IT network to the OT network through systems that were accessible to both environments. Traditional malware backdoors, Mimikatz extracts, remote desktop sessions and other well-documented, easily detected attack methods were used throughout these intrusions and found at every level of the IT, IT DMZ, OT DMZ and OT environments.

We believe that defenders and incident responders should focus much more attention on intrusion methods, or TTPs, across the attack lifecycle, most of which are present on what we call “intermediary systems”—predominately networked workstations and servers using operating systems and protocols that are similar to or the same as those used in IT, which are used as stepping-stones to gain access to OT assets. This approach is effective because almost all sophisticated OT attacks leverage these systems as stepping stones to their ultimate target.

To illustrate this philosophy, we present some new concepts for approaching OT threats, including the Funnel of Opportunity for OT Threat Detection and the Theory of 99, as well as practical examples derived from our analysis and incident response work. We hope these ideas challenge others in the security community to put forward new ideas and drive discussion and collaboration. We strive for a world where attacking or disrupting ICS operations costs the threat actor their cover, their toolkits, their time and their freedom.

The "Funnel of Opportunity" Highlights the Value of Detecting OT Attacks In "Intermediary Systems"

Over the past 15 years of responding to and analyzing many of the most important threats in IT and OT, FireEye observed a consistent pattern across almost all OT security incidents: There is an inverse relationship between the presence of an attacker’s activities and the severity of consequence to physical assets or processes. The attack lifecycle when viewed like this begins to take on a “funnel” shape, representing both the breadth of attacker footprint and the breadth of detection opportunity for any given level. Similarly, from top to bottom we represent the timeline of the intrusion and its proximity to the physical world. The bottom is the cross-over of impact from the cyber world to the physical world.

Diagram

Description automatically generated  
Figure 1: The Funnel of Opportunity for OT Threat Detection

In the early stages of the attack lifecycle, the intruder spends prolonged periods of time targeting components such as servers and workstations across IT and the IT DMZ. Identifying threat activity at this architectural level is relatively straightforward given that dwell time is high, threat actors often leave visible traces, and there are many mature security tools, services and other capabilities designed to detect this activity. While it is difficult to anticipate or associate this early intrusion activity in IT layers with more complex OT targeted attacks, IT networks remain the best zone to detect attacks.

In addition to being relatively easy to detect, early attacker activity also presents a very low risk of negative impact to OT networks. This is primarily because OT networks are commonly segmented, often with an OT DMZ separating them from IT, limiting attacker access to the industrial process. Also, targeted OT attacks commonly require threat actors to acquire abundant process documentation to determine how to cause a desired outcome. While some of this information may be available in IT networks, planning this type of attack would almost certainly require further process visibility only available in the OT network. This is why, as the intrusion progresses and the attacker gets closer or gains access to OT networks, the severity of possible negative outcomes becomes proportionally higher. However, the activity becomes more difficult to detect as the attacker’s footprint grows smaller and there are fewer security tools available to defenders.

The TRITON and Industroyer Attacks Exemplify This Phenomenon

Figure 2 shows an approximate representation of endpoints that were compromised across the architecture of victim organizations during the TRITON and [Industroyer](https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf) attacks. The Funnel of Opportunity is located in the intersection between the two triangles. It is here where the balance between attacker presence and operational consequence of an intrusion makes it easier and more meaningful for security organizations to identify threat activity. As a result, threat hunting close to the OT DMZ and DCS represents the most efficient approach as the detectable features of the intrusion are still present and the severity of potential consequences of the intrusion is high, but still not critical.

Chart, funnel chart

Description automatically generated  
Figure 2: Approximate representation of endpoints compromised during the TRITON and Industroyer attacks

In both the TRITON and Industroyer incidents, the threat actor followed a consistent pattern traversing the victims’ architecture from IT networks, through the OT network, and ultimately reaching the physical process controls. In both incidents, we observed that the actor moved through segmented architectures using computers located in different zones. While we only illustrated two incidents in this blog post, we highlight that movement across zones leveraging computers has also been observed in *every* public OT security incident to date.

The Theory of 99: Almost All Threat Activity Happens in Windows and Linux Systems

FireEye’s unique visibility into the full attack lifecycle of thousands of intrusions from both independent research and first-hand incident response experience has enabled us to support this theory with real-world data, some of which we share here. FireEye has consistently identified similar TTPs leveraged by threat actors regardless of their target industry or ultimate goals. We believe that visibility into network traffic and endpoint behaviors are some of the most important components for IT security. These components are also critical in preventing pivots to key assets in the OT network and detecting threat activity once it does reach OT.

Our observations can be summarized in what we call the Theory of 99, which states that in intrusions that go deep enough to impact OT:

* 99% of compromised systems will be computer workstations and servers
* 99% of malware will be designed for computer workstations and servers
* 99% of forensics will be performed on computer workstations and servers
* 99% of detection opportunities will be for activity connected to computer workstations and servers
* 99% of intrusion dwell time happens in commercial off-the-shelf (COTS) computer equipment before any Purdue level 0-1 devices are impacted

As a result, there is often a significant overlap across TTPs utilized by threat actors targeting both IT and OT networks.

Table

Description automatically generated  
Figure 3: TTPs seen across both IT and OT incidents

Figure 3 presents a summary of TTP overlaps between TRITON, Industroyer, and some relatively common activity from cybercrime group [FIN6](https://www.fireeye.com/solutions/financial-services/rpt-fin6.html). FIN6 is a group of intrusion operators who have compromised multiple point-of-sale (POS) environments to steal payment card data and sell it in on the dark web. While the motivations and ultimate goal of the threat actors that developed TRITON and Industroyer differ significantly from FIN6, the three actors share common TTPs, including the use of Meterpreter, compromising dual-homed systems, leveraging RDP to establish remote connections and so forth. The overlap in tools and TTPs across actors interested in IT and OT should be of no surprise. The use of IT tools for OT compromises directly corresponds to a trend best known as IT/OT convergence. As IT equipment increasingly becomes integrated in OT systems and networks to improve efficiency and manageability, we can expect threat actors to be able to leverage networked computers as a conduit to reach industrial controls.

Drawing parallels between intrusions into high security environments, we can gain insight into actor behaviors and identify detection opportunities earlier in the attack lifecycle. Intelligence on intrusions across various sectors can be useful in highlighting which common and emerging adversary tools and TTPs are likely to be used in tailored attacks against organizations with OT assets.

FireEye Services, Intelligence, and Technology Provide Unparalleled Protection In IT and OT

While the FireEye approach to OT security detailed in this blog post emphasizes the criticality of “intermediary systems” when defending OT, we do not want to downplay the importance of the OT expertise and technology needed to respond to the most critical 1% of threat activity that does impact control systems. OT is in our DNA at FireEye: FireEye Mandiant’s OT practice has been one of the leading industry voices over the past six years, and the FireEye Cyber Physical Intelligence offering is the most recent evolution of the heritage of Critical Intelligence—the first commercial OT threat intelligence company founded in 2009.

Table, timeline

Description automatically generated  
Figure 4: FireEye OT-specific offerings

We believe that sharing our philosophy for OT security and highlighting FireEye’s comprehensive OT security capabilities will help organizations look at this security challenge from a different angle and take tangible steps forward to build a robust, all-encompassing security program. Figure 4 maps FireEye’s OT security offerings against the [NIST Cybersecurity Framework’s Five Functions](https://www.nist.gov/cyberframework/online-learning/five-functions), matching FireEye services to the lifecycle of an organization’s cyber security risk management.

If you are interested in learning more or purchasing FireEye OT-focused solutions, you can reach out here: [FireEye OT Solutions](https://www.fireeye.com/solutions/industrial-systems-and-critical-infrastructure-security.html).