A Lynchpin Media PUBLICATION

intelligent CISO

security intelligence that transcends borders

Europe evolution
Understanding the growth of the region's OT threat environment

Addressing the court
How to tailor cyber defences to the legal industry

Biometric benefit
How this technology is shaping the business landscape

issue 67 | www.intelligentciso.com

TECHNOLOGICAL ODYSSEY

Massimo Vulpiani, NetWitness' EMEA Business Leader, and Karim Abillama, SE Director, International Business at NetWitness, discuss the company's mission to guard the digital safety of its valued customers, some of the most complex and security-conscious organisations on earth.

Understanding the evolution and growth of the European OT threat landscape

MAGPIE GRAHAM, INTEL CAPABILITY TECHNICAL DIRECTOR AT DRAGOS, SHARES HIS THOUGHTS ON THE GROWTH AND EVOLUTION OF THE EUROPEAN OPERATIONAL TECHNOLOGY (OT) THREAT LANDSCAPE. FROM ACTIVITIES BY THREAT GROUPS TO IDENTIFYING A THREAT LANDSCAPE, HE OUTLINES CRITICAL CONTROLS AND ESSENTIAL PILLARS FOR ORGANISATIONS BUILDING A ROBUST CYBERSECURITY STRATEGY, THE IMPORTANCE OF BUILDING DEFENSIBLE ARCHITECTURES AND STRESSES THE NEED FOR COMPREHENSIVE MONITORING TO ENHANCE OVERALL SECURITY POSTURE.

What is the history of the threat landscape in Europe and how has this evolved over the years?

Within the threat landscape, computer network operations (CNO) don't typically occur exclusively within IT or OT. Most often, it is an IT compromise that leads to an impact on the OT environment. The rise of cybercrime is probably the most notable trend we have experienced in Europe over the last decade.

Looking back on my career over the years, there has been an upward shift in the availability of tools, the ease of acquiring exploits and the motivation of cybercriminals to employ ransomware and extortion campaigns that create the most negative impacts on organisations.

In the realm of OT, we've seen an 87% increase in ransomware attacks against industrial organisations and a 35% rise in the number of threat groups in 2021.

The impact on OT is substantial due to several factors.

The first is a lack of readiness. On the IT side, we're prepared to reimage machines and remove infections, but the OT side faces different challenges like safe shutdown and start-up which are critical concerns owning to safety being paramount within industrial environments. Additional elements like cloud-based attacks and supply chain vulnerabilities have also shaped the threat landscape. OT is somewhat shielded from these as it is not as connected to the cloud although it is gradually changing, and with increasing use of ubiquitous software libraries, the software bill of materials (SBOM) is a real cause for concern – as the Log4j vulnerability demonstrated.

Supply chain attacks are always concerning owing to the lack of visibility a downstream customer has, but connectivity between supplier and industrial networks is typically limited. However, vendor control over devices and those connections home do pose risks, particularly demonstrated when engineers visit customer environments and may circumvent network egress monitoring and protection efforts using cellular modems.

Attacks against perimeter devices affect both IT and OT, but the OT space has felt the impact more so over the last few years due to the global pandemic. With remote work, external access through VPN concentrators has increased thereby exposing both environments to potential threats.

There is also a growing investment by threat groups in OT tooling, which includes reconnaissance and penetration testing tools. While some are benign, tools like COSMICENERGY and PIPEDREAM could be used in a malicious context.

For example, the information that was revealed through the Vulkan Files leaks further demonstrated that nations show interest in the OT space, to learn about diverse OT network operations and configurations may vary widely due to the historical evolution of OT networks, making it crucial to learn about these environments before conducting an offensive operation. Tools like PIPEDREAM can influence devices, the type of capability we assess many threat groups now possess or are developing. This demonstrates a shift from past OT-focused operations, when Stuxnet was probably the malware that springs to mind, a targeted, highly precise operation, versus a 'Swiss Army knife' toolset that is adaptable to many environments comprising multiple vendors' equipment.

What are some activities by threat adversaries and how can organisations identify a threat landscape?

In terms of the current activities of adversaries targeting industrial organisations, particularly of note are the attacks against power networks in support of the Russia-Ukraine conflict, a number of disruptions attributed to the threat group we track as ELECTRUM. We saw disruptive operations from it in 2015 and 2016 against Ukraine with refined and more targeted attacks in 2022.

Similarly, a group called KAMACITE has represented a long-running set of related behaviours targeting critical infrastructure and industrial verticals since at least 2014. KAMACITE facilitated ICS-specific operations including the BLACKENERGY2 campaign and the 2015 and 2016 Ukraine power events, paving the way for ELECTRUM to take action. Energy and manufacturing are their primary focus in Europe, while maritime, liquid natural gas and oil are their main focus globally. We categorise threat groups as 'Stage 1', when they display intent to operate with OT environments, but lack the full capability to do so. This activity typically involves tactics like password spraying and remote access exploitation, posing concerns for IP security. The actor's intent here is to acquire knowledge or access to the OT environment. Those threat groups with the capability to operate within the OT environment, be that for monitoring or disruptive or destructive attacks, are categorised as 'Stage 2'.

Staying with the Russia-Ukraine conflict, we have seen several wipers that were deployed, particularly during the early days of the invasion, but the destructive 'wiper' malware called AcidRain, used on Viasat modems and routers, recorded the greatest impact on industrial environments. The attack quickly erased all the data on the systems. The machines then rebooted and were permanently disabled. Thousands of terminals were effectively destroyed in this way and those organisations relying on satellite communications and without a working backup method of communication suffered loss of visibility and control, impacting various sectors including cases like wind power generation in Germany. Understanding these additional attack vectors beyond your control is crucial in threat modelling.

Back to ransomware and extortion, these tactics have had a significant impact on industrial organisations. Adversaries have adapted their strategies, even observed exploiting trust relationships between parent and subsidiary organisations across different geographies.

Virtualisation also plays an increasing role in the hosting of OT HMI systems, and in an Incident Response engagement Dragos undertook recently, the threat group gained direct access to the OT environment via a remote access system, but instead of encrypting all hosts they found, they only focused on virtual machines running the HMI systems, leaving the underlying host operational. This specificity demonstrates that criminal actors know where the actual value lies in extortion attempts, but also suggests an attempt to avoid unforeseen consequences given the dangers posed by entirely crippling an industrial environment. Perhaps this stems from lessons learned, following the backlash and requests for action from heads of state, when healthcare facilities have been severely impacted in the past. Other industry sectors such as mining and telecommunications have also been targeted. While not classified as 'critical infrastructure' from an industrial perspective, telecommunications are of the utmost importance to operations and thus necessitate consideration in any threat modelling or Business Continuity planning. Just like the Viasat incident demonstrated, crippling any critical service can be damaging even if the specific network has not been compromised.

In navigating this complex threat landscape and to aid transition into protecting your attack surface, different levels of reporting are essential. C-level executives and board members should have a broad understanding of common threats and the level of sophistication that could target their organisation's assets. Introducing industry-specific reporting will provide awareness of threats specific to your sector. In-depth reporting, ideal for SOC employees and incident responders, delves into threat groups, tools, vulnerabilities and tradecraft. Understanding attack surfaces, vulnerabilities, architecture and IT-OT network interactions becomes critical in this phase.

Architecture reviews and proactive incident response like Red Teaming are also valuable tools. Conclusively, the key foundation is monitoring of OT networks which often incorporate output from firewalls, antivirus or EDR/XD, providing a holistic view to security teams.

Based upon the work of Dragos services, in 2021, 80% of customers had no visibility into their OT environments. Even with a profound understanding of the threat landscape and potential threat groups, lacking visibility hampers response efforts. It's estimated that 95% of OT networks globally are unmonitored. The key takeaway here is

to stay informed while ensuring visibility across your infrastructure to effectively defend against evolving threats.

What are the biggest cybersecurity challenges facing ICS/OT defenders in the European markets?

In contrast to the US and some East Asian countries, there is a noticeable lack of government drive and initiative in this region. This absence of proactive efforts from government organisations such as regulatory bodies or national security agencies has resulted in limited awareness of cybersecurity risks, inadequate monitoring and insufficient preparedness for potential cyberattacks.

Although these issues extend globally, the absence of mandatory standards and the accompanying lack of mitigation measures or timely software patches are still a problem and will cause organisations to struggle in prioritising their cybersecurity efforts effectively.

Also, the diversity of vendors and protocols used in Europe and other regions complicates matters. Reports and recommendations from the US may not apply to widely used vendors or protocols in Europe, leading to a lack of awareness regarding specific vulnerabilities. Consequently, organisations face a multitude of threats without comprehensive guidance.

So, while enhancing a cybersecurity posture requires organisations to take various measures, the main challenge also lies in the limited drive from government authorities to implement cybersecurity regulations effectively. What is needed is a more concerted effort to promote the adoption of practical strategies for complying with regulations. Providing step-by-step guides and architectural examples, especially regarding patch management solutions, can significantly assist organisations in transitioning from a vulnerable state to an effective cybersecurity stance. Ideally, such guidance should come from trusted bodies at either the European or national levels to ensure comprehensive support.

Cybersecurity adversaries have consistently challenged European ICS/OT cybersecurity defences which is a defining reason for their continued effectiveness. What is a more effective approach for organisations to handle these defences?

Dragos CEO, Rob Lee, together with Tim Conway, released the SANS Five Critical Controls which organisations can use to focus their efforts in protecting OT networks and bolster a stronger security posture.

One of these controls is having a specialised incident response plan for Industrial Control Systems (ICS). While many organisations understand how to respond to typical enterprise IT-specific network incidents, the same cannot be said for ICS incidents, making it an area where preparedness often falls short.

Ransomware is a prevalent threat especially in the OT environment and understanding the tactics employed by ransomware actors is vital. Defending against the most prolific of these actors gets you a long way towards securing your systems. However, it is also essential to consider low-probability and high-impact scenarios. This necessitates a comprehensive understanding of your assets where predictive analysis can play a pivotal role. Visualising your network, especially in segmented environments, is invaluable as it allows you to maintain critical functions. Without this knowledge, organisations tend to resort to shutting down everything in response to a potential ICS incident, which can have devastating consequences. For example, say a water treatment plant was targeted in a cyberattack, with confirmed intrusion activity within the enterprise IT network. It is all too often the case that the response would be to shut down the OT environment in a safe manner, given the absence of a dedicated OT/ICS incident response plan, the lack of monitoring in the OT environment to provide assurances that the actor had not traversed the boundary, and the subsequent inability to accept the risk to continue operations in lieu of those assurances, which may also include doubts around the true depth of segregation between IT and OT networks. All too often, given constrained budgets and non-existent guidelines (or ones that are simply not followed) do we see issues such as credential reuse between environments, or sharing of switching infrastructure undermine the security that is thought to be in place.

Another critical control is building a defensible architecture. While many organisations have long-standing network infrastructures that may have existed since the 60s and 70s, adding new elements provides opportunities to enhance defence and security. In emerging sectors like renewables and nuclear power, greenfield sites offer a chance to establish highly defensible networks. Thus, conducting parameter analysis and architecture reviews is essential to identifying and implementing these security enhancements. Thinking about conduits and zones is one great approach, that you can read more about in our blog series on ISA/IEC 62443.

The next control revolves around specific monitoring. Effective defence hinges on visibility as you can't defend against what you can't see. Regardless of how much you know about potential threats, if you can't see them or their actions, your ability to prevent or mitigate incidents is compromised. This is particularly critical in the OT environment where detecting intrusions in their early stages is challenging without proper visibility. While we have improved in stopping the initial stages of attacks, achieving this in the OT realm is impossible without adequate visibility.

So, these critical controls are essential pillars of every organisation building a robust cybersecurity strategy. They address the unique challenges presented by ICS incidents, emphasise the importance of building defensible architectures and stress the need for comprehensive monitoring to enhance overall security posture. ◆