Defending OT Environments From Ransomware

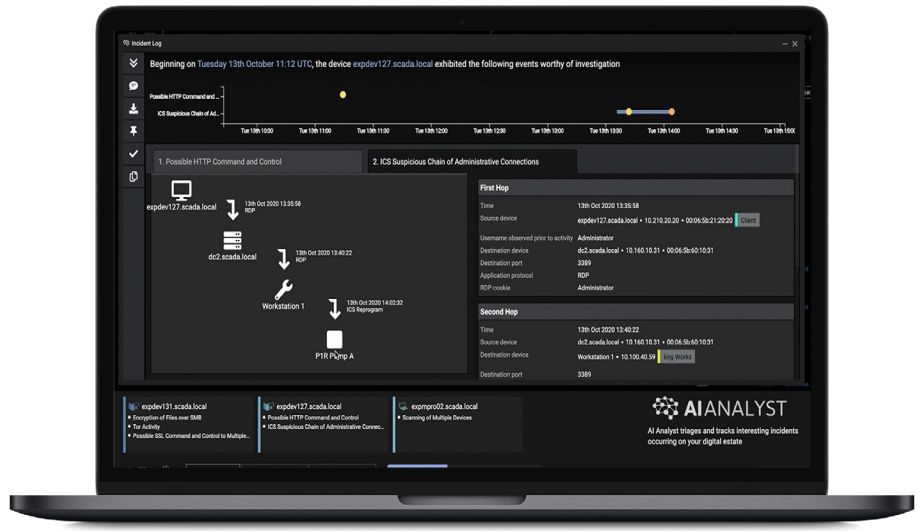
The Rise of Industrial Ransomware

Ransomware has become an increasingly prevalent threat for organizations with industrial control systems (ICS) and other forms of operational technology (OT). From EKANS to the Colonial Pipeline incident, the number and variety of ransomware strains affecting industrial organizations has sharply risen over the past few years.

Machine-speed threats like ransomware are of particular concern for several reasons. Firstly, many industrial organizations are involved in critical infrastructure, meaning that compromise can lead to broader consequences for a nation's economy and society. Secondly, disruption to OT and ICS can lead to massive financial loss and can even jeopardize human safety.

In industrial environments, ransomware can disrupt operations directly through targeting ICS mechanisms, as was seen with EKANS which included 64 ICS specific mechanisms in its kill list. It can also impact operations indirectly by disrupting IT systems that provide visibility into OT or pivoting from IT to OT by spreading laterally. Accelerating these trends is IT/OT convergence, which not only widens the attack surface but results in a loss of visibility and control. In an anonymized study, Darktrace detected over 6,500 suspected instances of ICS protocol use across 1,000 enterprise environments.

Multiple factors have compounded the risk ransomware poses. Since the outbreak of COVID-19, many organizations have relied upon remote management tools to allow operators to control ICS and OT without having to enter physical premises. Darktrace has already seen common remote management tools used in ransomware specifically targeting critical infrastructure. Moreover, ICS ransomware is often launched by lone attackers rather than state-sponsored cyber-criminal groups, meaning that the barrier of entry is drastically lowering for threat actors to compromise OT.



Darktrace's Cyber AI Analyst detecting anomalous encryption and a suspicious chain of ICS administrative credentials

"Cyber AI can detect cyber-threats before damage is done – whether they arise from an employee or from the industrial systems on our production floor."

King's Hawaiian

The Industrial Immune System: Illuminating New Threats

Darktrace's Industrial Immune System illuminates even the most complex industrial environments and cyber-physical ecosystems, identifying threats across OT, IT, and converged OT/IT in their earliest stages, before damage is done. By harnessing self-learning AI, Darktrace detects novel and never-before-seen attacks without relying on rules, signatures, threat feeds, 'knowledge packs', or lists of CVEs. Rather, it learns the normal 'patterns of life' for all devices, users, and controllers in an organization, and all the connections between them. This dynamic understanding of 'normal' enables Darktrace to autonomously detect the subtlest signals of an attack within seconds of it emerging.

Darktrace offers two powerful capabilities that are invaluable when it comes to defending against industrial ransomware in particular. Firstly, Cyber AI Analyst performs autonomous investigations, connecting the dots among disparate security events and automatically generating intuitive Incident Reports that put teams in a position to take action. Combining the skill of human analysts with the speed and scale of AI, Darktrace reduces time to triage by up to 92%.

Secondly, Darktrace Antigena provides Autonomous Response to neutralize threats in real time, taking targeted, nuanced actions to stop machine-speed threats. The scope and type of actions taken is flexible and can be controlled to reflect a risk to safety appetite as determined by the customer. For example, Darktrace Antigena can respond only to threats in IT systems or only in the higher levels of the Purdue model. Darktrace Antigena also can be deployed passively in Human Confirmation Mode, such that a member of the security team has to approve its actions.

> "We now get to see Darktrace Antigena blocking nefarious activity on the IT network that can have an impact on the OT."
>
> **Copperbelt Energy PLC**

A few common use cases for Autonomous Response in OT are:

- Engineering workstation infected with ransomware attacks application server file shares
- New device appears on the network and begins interacting with OT systems
- Engineering workstation begins performing OT reconnaissance scans
- OT application server starts beaconing to rare internet destination
- HMI infected with mining malware, drastically impacting operational performance

Threat Find: Ransomware Targets Oil Refinery

At an integrated oil refiner and supplier, Darktrace's Industrial Immune System was crucial in stopping a ransomware attack that originated in the corporate network.

Cyber AI identified the first signs of a ransomware infection in a desktop device on the network. As well as writing its own ransom note files, the device was found to be making a series of connections to rare external destinations via an internal proxy server and then downloading potentially malicious files – activities that Darktrace could detect and correlate based on its granular knowledge of 'self' for the business.

The device proceeded to make a number of SMB directory queries, more activity that Cyber AI recognized as deviant based on its understanding of the particular device, which was followed by the download of malicious files.

The Industrial Immune System flagged this activity and highlighted it as likely ransomware, alerting the customer's security team before the infection was able to spread into the OT environment.

With Cyber AI's ability to connect patterns from across diverse infrastructure, the industrial system was defended from this machine-speed attack.