

# Network Segmentation: The OT Standard for Industry 4.0

## TXOne Networks Inc.

Dr. Terence Liu

Mars C Cheng

Max Farrell



# TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	3
NETWORK SEGMENTATION: AS NECESSARY AS ELECTRICITY, INTERNET, AND LOCKS ON DOORS....	4
THE OT WORK SITE: DEFENSES DOWN, DOORS OPEN .....	5
THE 4 CORNERSTONES OF SHOP FLOOR PROTECTION .....	6
DEPLOYING INTERNAL SEGMENTATION WITH FLEXIBILITY, SCALABILITY, AND LOW COST .....	7
MODERNIZING WORK SITES FOR SECURITY AND CONVENIENCE WITH OPTIMIZED, COST-EFFECTIVE NETWORK SEGMENTATION.....	8
THE 3 PHASES OF INTENT-BASED NETWORK SEGMENTATION.....	9
CONCLUSION .....	10
CASE STUDY #1 - EKANS RANSOMWARE ATTACK - AUTOMOTIVE MANUFACTURING.....	11
CASE STUDY #2 - TOTAL LOGISTICAL LOCKDOWN BY LOCKERGOGA.....	14

# EXECUTIVE SUMMARY

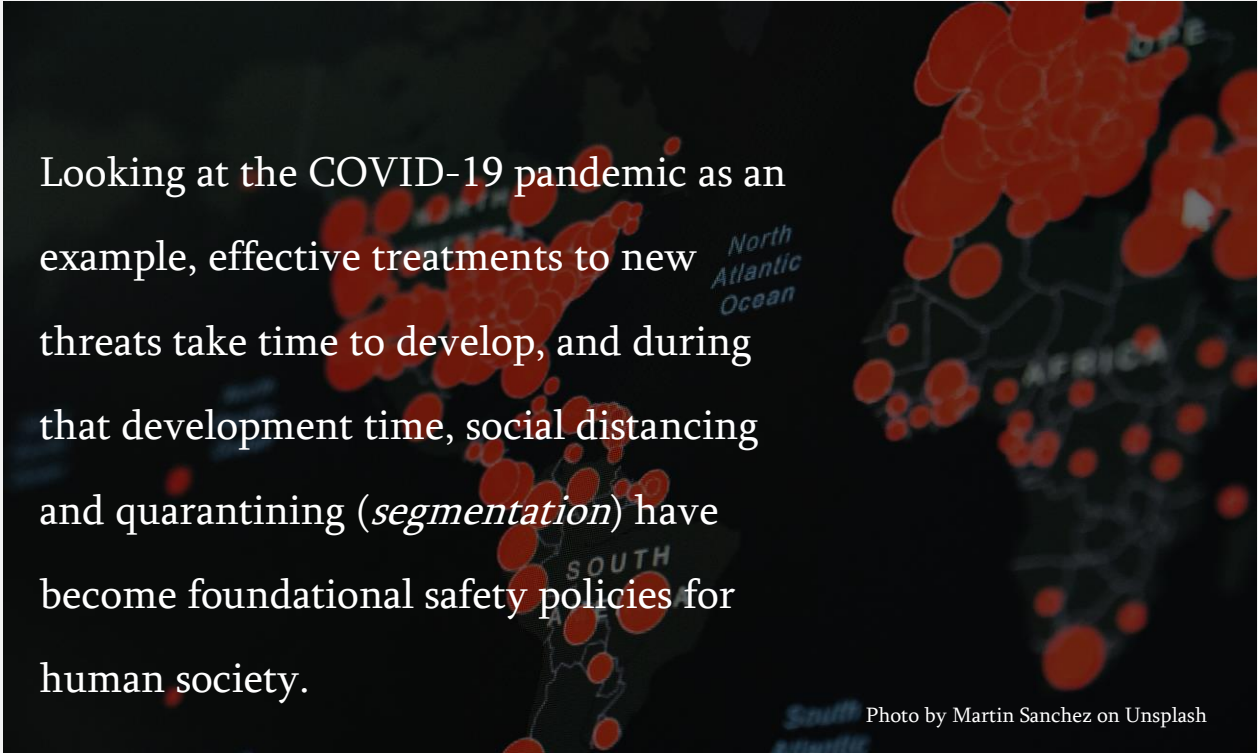
Anyone who ever created something through hard work has had to deal with bandits coming to take, by force or by cunning, the fruits of their labor. Once, the solution was to build grander and grander castles, each broken into segments and interwoven with multiple defenses to guarantee the safety of the castle's residents and resources. Any smart factory experiences daily life in much the same way: constantly targeted by hackers wanting to extort a hefty ransom, wreak havoc on the machines, compromise the safety of workers, or steal valuable intellectual property.

In a castle, the different sections or "segments" of the layout make invasions much easier to repel - when raiders get across the moat, they still have to get through the outer wall, then the inner wall, and finally find their way into the keep, pushing against well-prepared defenders at every key position. Similarly, when a work site's network is segmented, hackers breaking into a segment will be stopped at every turn. Defenses can be well-prepared and deployed at the key positions where they are most effective, halting a hacker's movement and ability to gather information.

In today's smart factory, what are the usual factors that slow a hacker or stop their assault? Typically, they are running a perimeter firewall and maybe an air gap. Sadly we now know that these aren't enough to protect from newly-developed and unknown modern threats.

# Network Segmentation: As Necessary as Electricity, Internet, and Locks on Doors

The bottom line is that segmentation must be viewed as essential – something no work site can do without. Recent attacks have shown that, while traditional defenses can repel known attacks that are already understood, for unknown cyber threats they provide almost no defense.




Looking at the COVID-19 pandemic as an example, effective treatments to new threats take time to develop, and during that development time, social distancing and quarantining (*segmentation*) have become foundational safety policies for human society.

Photo by Martin Sanchez on Unsplash

Potentially infected laptops and USBs are carried back and forth across the firewall and air gap by unsuspecting workers every day, the industrial internet of things (IIoT) creates more and more devices reaching out for the internet, and the COVID-19 crisis forces us to use remote access to conduct day-to-day tasks. Every smart factory requires cost-effective, easily adapted security solutions that operate at a high but easily reproduced standard, and which fit transparently into existing network topology with a fast setup.

# The OT Work Site: Defenses Down, Doors Open



In 2020 July, one of the biggest GPS and wearable device manufacturers paid a \$10 million USD ransom to recover their service and production lines.\*

In the last ten years, threat actors have come to see OT factories as easy-access low-effort projects with an excellent chance of a large payout. Ransoms and lockouts are extremely high-stakes to factory owners, who will often dig deep into their pockets to pay ransoms rather than risk the loss of days of availability. Current OT security trends are based on a false sense of security created by perimeter firewalls or air gaps. They are powerless against threats brought inside by careless or malicious insiders, and unable to limit hackers with the agility to move laterally, who are willing to watch and wait for months to eventually gain access to central security credentials.

As of Sep. 17, 2020  
76% of 2020's ICS-CERT vulnerability advisories are rated severe and exploitable remotely - a 7% increase from 2019

\*<https://www.theverge.com/2020/8/4/21353842/garmin-ransomware-attack-wearables-wastedlocker-evil-corp>

Companies paying large ransoms are those which have not considered cybersecurity as part of their yearly budget, instead focusing on the historical OT standards of production lines and human resources. In the modern world, cybersecurity must interweave with company culture, as necessary as the gates and turrets of a castle.

Factories soon will implement segmentation as the foundation of their network, preserving safety for their workers and assets, but today compliance and security posture management are still challenging. The difficulty comes because technology that is well-suited to OT architecture is rare and often requires complicated changes to the factory's setup. Every layer of cybersecurity creates an increase in management effort and inconvenience to workers. Solutions that can protect against unknown threats must make it easy to scan devices as they are coming and going, simplify execution privileges on endpoints, make it almost impossible for an intruder to move laterally while logging all movement and attempted movement, and protect normal operational traffic while flagging or blocking abnormal traffic.

Such detailed systems of logging and flagging are necessary to determine the presence of and act against unknown attacks. Determining that an attack has already penetrated the environment begins with cross-referencing logs, looking for unusual actions or actions taken at unusual times, and so on. When a network is segmented, it is much easier to identify unusual movement or activity because of the border guard-like nature of each segment's boundary.

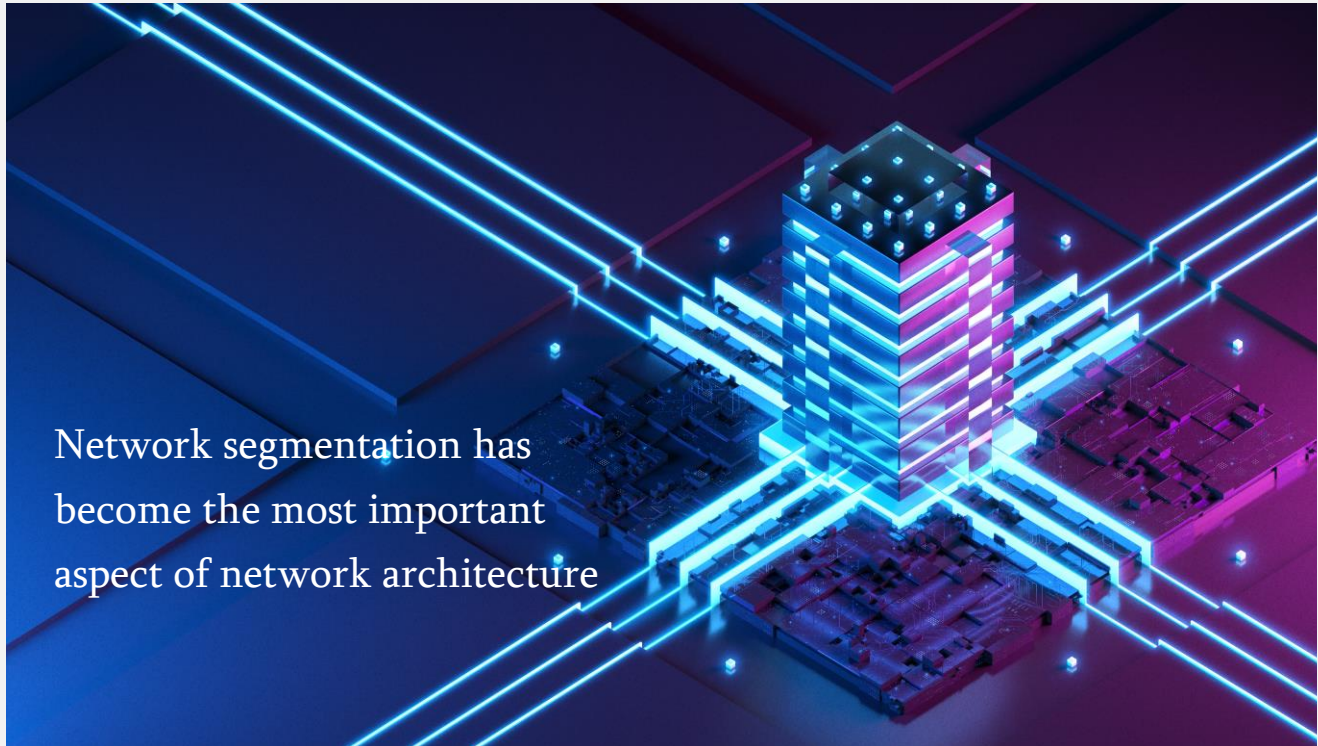
## The 4 Cornerstones of Shop Floor Protection

1. Network Segmentation - Separate the network into purpose-defined or "intent-based" zones
2. Endpoint Shielding - Apply virtual patch network technology to create a shield around legacy OS or unpatched assets or use trust list-based lockdown software on machines with defined roles
3. Checkpoint Scanning - Scan and log every asset entering or leaving the work site
4. Knowing the Business Intention - Use business intention to model routine tasks and make rules for intra- and inter-segment traffic



*To keep the operation  
running safely, check your  
**'NECK'***

# Deploying Internal Segmentation with Flexibility, Scalability, and Low Cost



Network segmentation has become the most important aspect of network architecture

Internal segmentation can be deployed flexibly, and to accommodate a variety of technologies. The two primary concerns in choosing solutions are the cost and how much change is necessary for deployment. For example, while a Software Defined Network (SDN) can create segmentation for an enterprise network, it represents a significant investment and will require the deployment of totally new network topology. Maintaining maximum utilization and availability 24/7 requires the deployment of solutions that fit quickly and transparently into the existing structure, and that have the flexibility to accommodate the factory's potentially mixed architecture of new, legacy, and unpatched assets.

## The 5 Advantages of OT-Aware Operationally Intelligent Networking

- Zero configuration
- Easy deployment without changes to network topology
- Low interference with sensitive assets
- Detection and smoothing of human error
- Comprehensive visibility

# Modernizing Work Sites for Security and Convenience with Optimized, Cost-Effective Network Segmentation

Business intention is the DNA of network segmentation, completely defining its deployment. Solution acquisition and deployment are streamlined by the map of business intention. Defining the purpose of each segment by intention, conducting inspection, and then defining rulesets based on that intention is the foundation of its significant reduction in cost and increase in convenience. TXOne Networks' EdgeFire and EdgeIPS are equipped with unparalleled sensitivity to ICS protocols. They work together in tandem to securely and conveniently split the enterprise network up into easily protected, easily monitored zones, coming equipped with templates to allow quick setup with zero configuration.

The internal segmentation firewall EdgeFire divides the network into security zones while also integrating IT and OT networks as closely as possible, increasing asset visibility and eliminating 'shadow OT'. Each zone is formed by grouping assets according to intent. This makes it easy for engineers to easily monitor and know the purpose of traffic, applying consistent security policies across zones. Custom policies exist as a natural and convenient

aspect of each zone, for example if an edge computing system is running a scalable multi-cloud environment, that zone connects smoothly to cloud services while the rest of the enterprise network remains sequestered behind a honeycomb of privilege-restricted segments. The configuration process is eliminated by the use of pre-organized and prepared configuration templates that are tailor-made for the needs of any OT network.

To establish deeper segmentation of the interior of the enterprise network, the micro-segmentation Intrusion Prevention System EdgeIPS is developed specifically for micro



segmentation. Designed to be deployed either at the network edge or in front of key assets, EdgeIPS assures maximum protection and traffic monitoring. EdgeIPS is perfected to restrict and log intruders' movements while flagging or blocking unusual protocol activity to protect the factory's machines from malicious commands.

EdgeFire and EdgeIPS both come equipped with virtual patch technology, allowing special protection for vulnerable unpatched or legacy devices. Since virtual patching is a network-based behavior, it interferes minimally with sensitive assets that are unable to be updated or modified. Finally, on a larger scale, EdgeFire and EdgeIPS nodes can be centrally coordinated by TXOne Networks' OT Defense Console, or ODC, which can centrally and highly granularly manage thousands of nodes at multiple work sites.

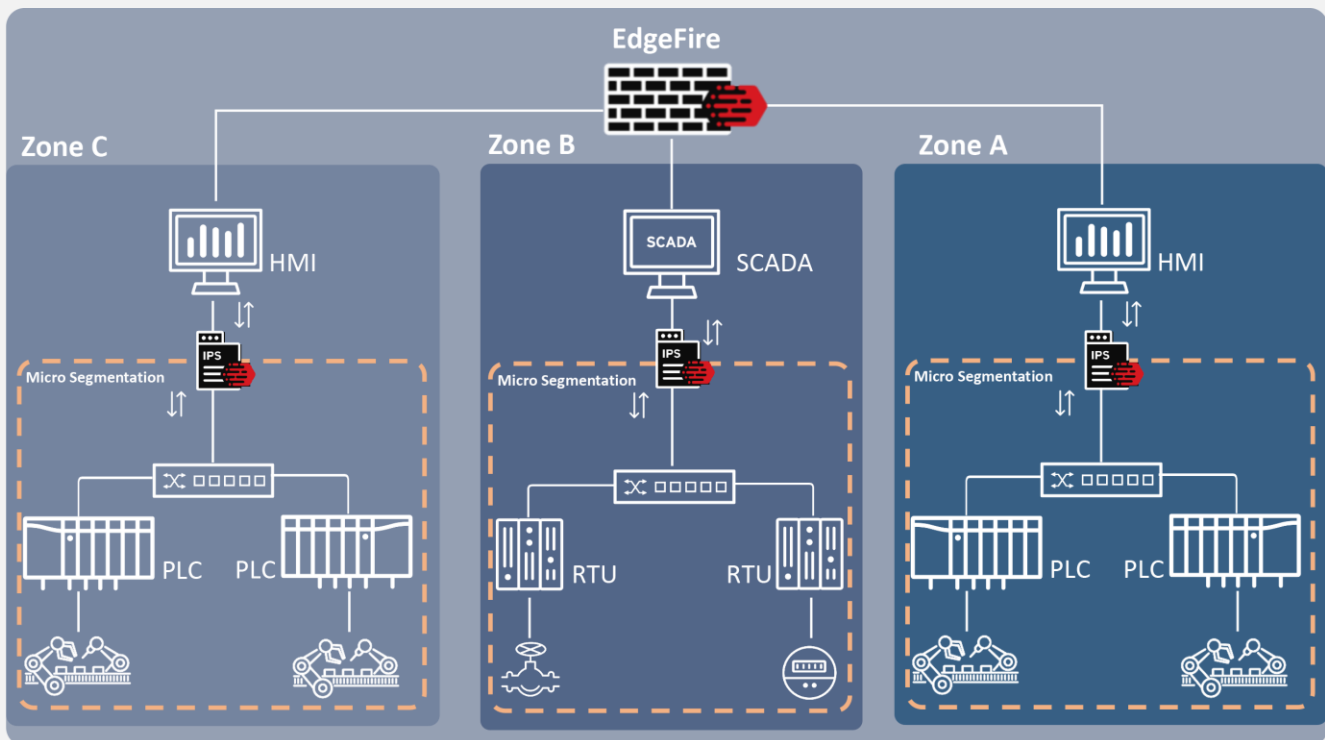
## The 3 Phases of Intent-Based Network Segmentation



1. **Design** – Design a statement of what the business is trying to do in language that applies to policy – for us, this means what protocols regularly do which tasks
2. **Deploy** – Deploy those policies through EdgeFire or EdgeIPS – if on a larger scale, use ODC to deploy to centralize management of a wider array of nodes
3. **Decide** – Use reports from integrated EdgeIPS and EdgeFire nodes to decide on maintaining or changing current routines, guaranteeing security and proper function

# Conclusion

Through deploying network segmentation via intent-based hardware, and following the 3 Ds of Design, Deploy, and Decide to create Intent-Based Segmentation, a near-perfect defense can be made against present and future cyber-attacks. Every OT work site must watch out for their NECK by always prioritizing network segmentation, endpoint security, checkpoint scanning, and knowing their business intention. Devices tailored to the needs of factories make OT network defense cost-effective, convenient, and scalable.



Picture 1: Internal Segmentation and Micro-Segmentation

# Case study #1 – EKANS Ransomware Attack - Automotive Manufacturing

*Source: Information in this case study is based on TXOne Networks' threat intelligence combined with publicly available threat resources. Based on this, we can show successful scenarios for EKANS-based attacks.*

## **Incident:**

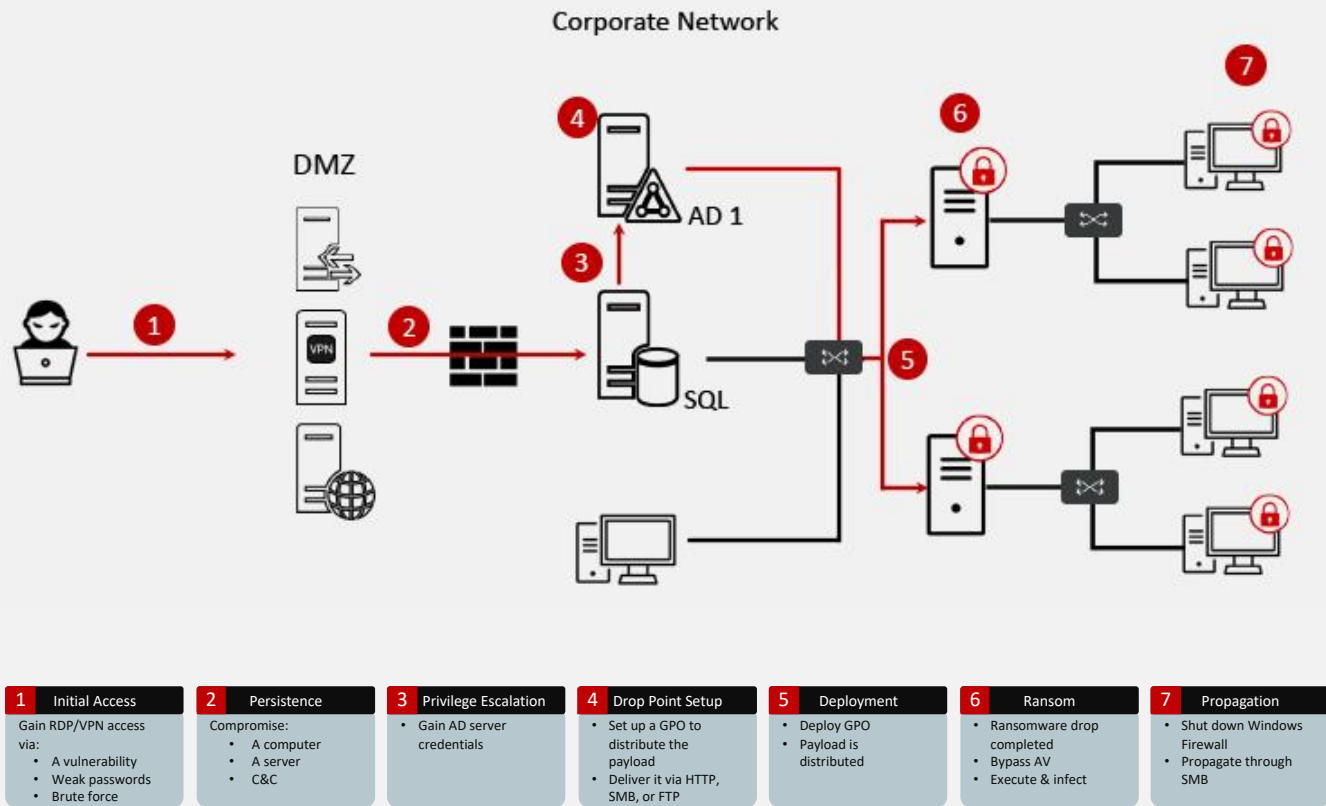
EKANS has the ability to specifically detect and target ICS applications (EXE files) and encrypt them. After the file is encrypted, each file will be appended with the EKANS marker. The applications EKANS targets have a large variety of purposes – licensing, HMI, security, historian data calculation, and more. It will encrypt other kinds of files as well, though to maximize efficiency, it will skip encrypting files that might stop the machine from operating or that its designers considered less important.

To launch an EKANS ransomware attack, threat actors will first acquire credentials in a variety of ways -- either from the darkweb, phishing, brute force, or a remote access vulnerability. Once inside, they seek the DMZ (the so-called demilitarized zone), where they will begin to look for a way to gain access to the company intranet. Often they will find this in the form of a tunnel or credentials set up for easier management of the DMZ, which they will find by use of a keylogger or the server security log.

Once gaining access to the corporate network, the network intruders need to establish their own stable communications channel by compromising a computer or server. They will implement a botnet, bot, or back door. The hard part is gaining Active Directory (AD) access credentials, and to do this they will need to use a variety of tools and will be willing to lay in wait for months. AD is the command center of the network's authentication and authorization, and once they have credentials for it, the bad actor easily takes control of processes and services that support the network.

Using AD, they will deploy malicious script, and set up a way to spread their ransomware over the network as quickly as possible -- a Global Policy Object (GPO). GPOs are normally how AD shares rule sets and updates, so in the average OT network they are considered trustworthy. When an employee logs into a workstation, that workstation will check with AD, and AD will distribute the GPO carrying the payload, which the workstation will download and execute.

The success of this action is the hacker's one chance at success after all of their hard work, so they will investigate very carefully and take a lot of time lining up their shot. Once the payload has executed, it will bypass antivirus, shut down the firewall, and begin to spread through the network using the servers' own filesharing protocols. Once the EKANS malware is in place on as many systems as possible, it will begin to target and encrypt sensitive data before locking out the system completely and delivering its ransom note.



Picture 2: EKANS Attack Strategy for an Automotive Network

**Prevention:**

EKANS and similar modern cyber threats can be stopped or slowed at different phases of their attack. In the case of EKANS, EdgeIPS and EdgeFire are both capable of detecting and blocking it by signature – in other words, by identifying its unique fingerprint. However, when EKANS was a brand-new threat and when other brand-new threats are developed, that's when segmentation and micro-segmentation are particularly important.

Intent-based segmentation as network architecture maximizes defensive capability in the way it is built from the ground up, making the factory network like a castle with its own walls, watchtowers, and drawbridges. EdgeFire is deployed at the front of the corporate network where it stops intruders from getting in, moving laterally, or gathering information they need to carry out their goals. At the level of key assets, EdgeIPS is deployed before mission-critical devices to apply micro-segmentation, filtering protocol traffic and giving granular access control.

While intent-based segmentation stalls attacks, it creates a precious window where abnormal and malicious behavior on the network can be identified and potentially infected nodes can be isolated and cleansed. Additionally, there are end-point based solutions that lock down key assets through the use of either allow lists or installation-free scanning – SafeLock and Portable Security 3.

Intent-based segmentation is the foundational structure that makes a network into something built to be defended. Intent-based segmentation and signature-based protection act as a double insurance to protect ICS networks even from the most adaptive cyber threats.

# Case Study #2 – Total Logistical Lockdown by LockerGoga

## Incident:

The destructive power of LockerGoga is defined by its unique ability to shut down network functionality. Because of this, the main impact of LockerGoga in major attacks hasn't been the ransomware's encryption of crucial files, it's been network interfaces completely disabled and locked across the company's entire global network. Companies hit by LockerGoga thus have not only their assets but their entire systems of logistics compromised by the attack.

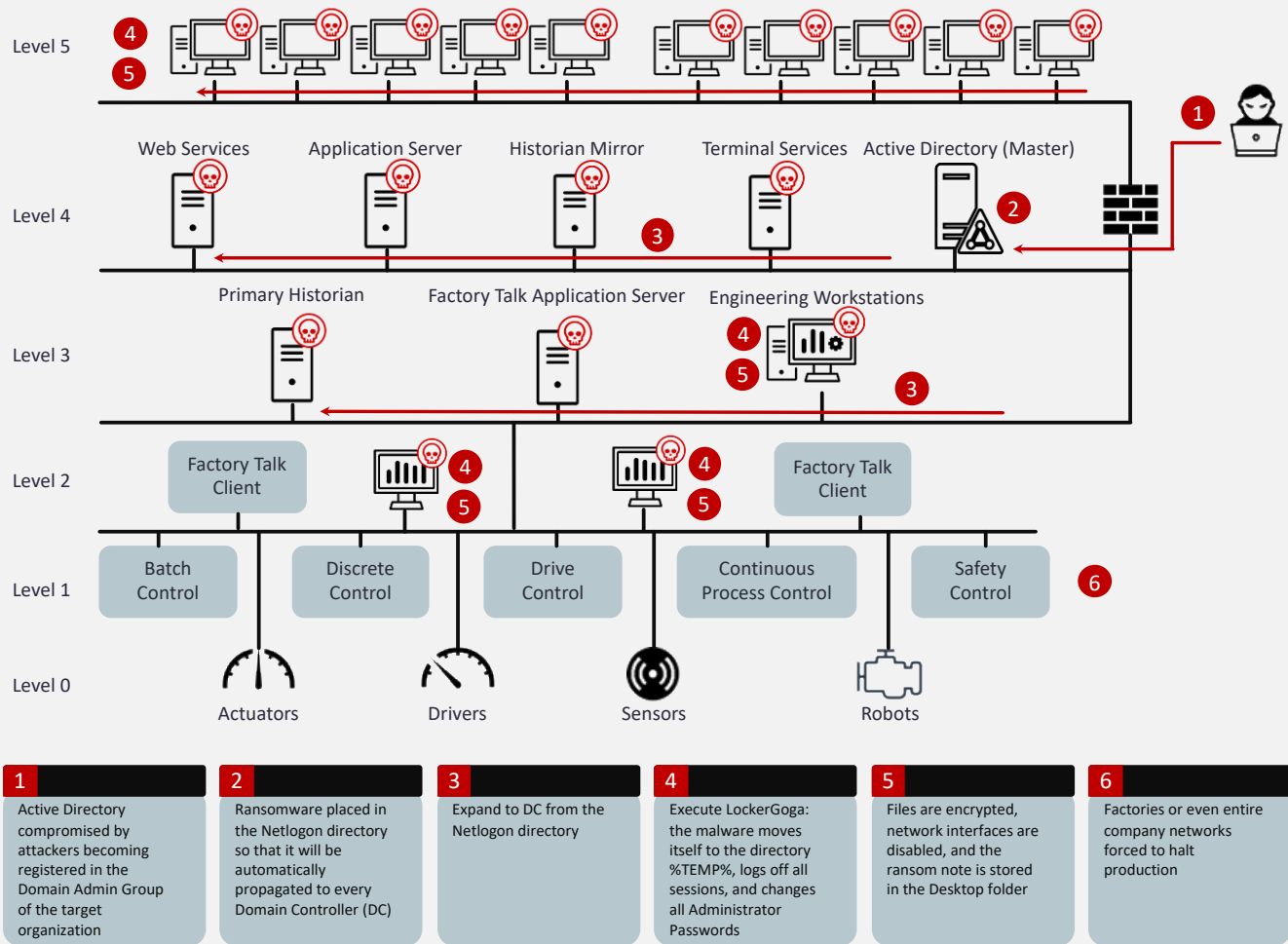
LockerGoga attacks begin with the threat actor already knowing the necessary credentials, most likely obtained via phishing or purchase over the dark web. After gaining initial access, they use hacker toolkits to move laterally on the network, as they go using the program Mimikatz to recover passwords from memory. This allows them to climb the privilege tower and reach a position with control over Active Directory.

From that lofty position, they can easily deploy their ransomware payload into devices on the network, validating them with stolen certificates that make these actions look trustworthy. After deploying the payload, the malware kills antivirus software on the target machine and starts encrypting the system's crucial files as quickly as possible (typically within a few minutes).

Crucially, the malware totally disables network access by doing three things: first, disabling the network interface, second, modifying the user and administrator passwords, and third, logging out of the system. This locks everyone out of the system while LockerGoga does its dirty work.

Ironically, this lockout is so efficient and complete that it is difficult for operators to even retrieve the ransom message.

The disabled network interface means the company cannot control or operate HMI, cannot monitor processes, and was totally unable to tap into its OT operation for automation or otherwise. The company was also totally unable to access order records (receipts, etc.). As such, the attack disables a company’s entire global operation pending their technicians being able to recover the ransom note so they can decide if they should pay the ransom, wipe their entire setup and start from scratch, or, if their IT leadership is on the ball, restore from backups. All these choices carry a variable price tag of time and money – even restoring from backups can take days.



Picture 3: LockerGoga Ransomware Attack

**Prevention:**

As with all cyber attacks, an ounce of prevention is worth a pound of cure. No equipment can protect you from credentials being compromised by social engineering. However, the right cybersecurity solutions can protect the system when hackers begin trying to leverage those credentials. Intent-based segmentation slows down attackers, giving technicians vital extra time to react.

EdgeFire and EdgeIPS come equipped with the ability to block suspicious commands that are not likely to be sent between assets or zones, allowing them to protect the network interface from shutdown commands. While segmentation and traffic monitoring work well, to halt the progression of novel threats, signature-based threat detection that both devices come equipped with will identify and disable any known threat.





Created by

The TXOne Networks Global Threat Research and R&D Center

TXOne Networks is a joint-venture company of Trend Micro and Moxa. TXOne Networks offers cybersecurity solutions to protect industrial control systems. Trend Micro has more than 30+ years of cybersecurity threats intelligence and MOXA has more than 30+ years of OT network expertise, which gives TXOne Networks the IT and OT technology necessary to provide cutting-edge adaptive ICS cybersecurity solutions. TXOne Networks leverage those advantages to develop ICS cybersecurity products, including endpoint and network security. Both Trend Micro and Moxa are not just providing the technology and knowledge, they are also acting as the go-to market channel for both sales and support services.



Keep the Operation Running

[www.txone-networks.com](http://www.txone-networks.com)