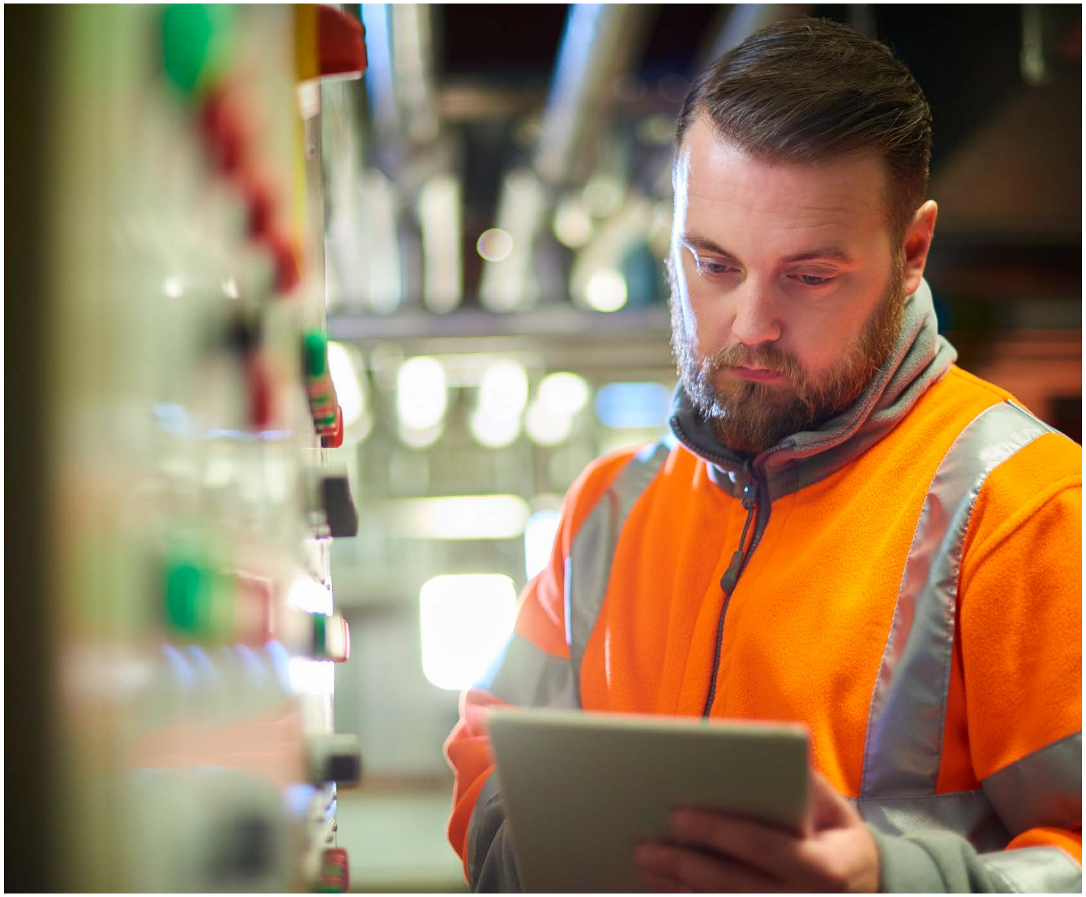
IBM

Protecting critical infrastructure

Using IBM Security QRadar EDR to track a highly sophisticated supply chain attack against a water management facility

A foreign threat actor targets a water management facility in Europe responsible for distributing water to about a million people. The facility initially assumes the new activity is legitimate. Attackers manage to compromise servers and deploy ransomware-based anti-forensic measures.



The security challenge

- Vulnerable position as a critical infrastructure in charge of regional water distribution
- No detection and hunting capabilities for fileless threats and lateral movements
- Lack of ransomware protection
- Limited resources assigned to endpoint security

Critical infrastructure sites must continually adapt to handle the growing complexity of cyber risk and increasing exposure to sophisticated threat actors. The kind of resources under management make critical infrastructure an ideal target for high-impact attacks and the exfiltration of highly sensitive data.

Aside from traditional network analysis tools, the water management facility had no endpoint monitoring in place and no response capabilities in case of an attack. Its tools didn't allow for tracking of cross-endpoint operations, such as lateral movements. Further, the general lack of IT resources meant that the operator hired external providers to manage essential services such as email, DNS, VPNs and firewalls, which created more complexity around coordinating the efforts of multiple disparate providers.

Cleaned the infected network segment in **seconds**

avoiding damage that could have blocked essential service to citizens

Successfully closed the incident within **2 days**

without loss of data, interruption of essential services or damage to endpoints

The attack involved a dozen devices before the ransomware deployment stage and several thousand after that.

The process

Solution overview

- IBM Security® QRadar® EDR uses NanoOS, which is designed to be undetectable and provide an exceptional level of visibility across endpoints and infrastructure
- Natively tracks lateral movements and anomalous login attempts
- Provides native protection against ransomware attacks
- Offers a powerful threat hunting interface to allow the tracking and reconstruction of highly complex incidents

The water management facility ran IBM Security QRadar EDR software on all the facility's servers, desktops and laptops to continuously monitor every asset and promptly track and investigate potential security breaches. Employing the solution's built-in dual AI engines and detailed behavioral analysis, the client gained full visibility over the infrastructure, allowing real-time queries to the endpoints and extended searches for both indicators of compromise (IOCs) and indicators of behavior (IOBs), together with advanced data mining to discover dormant threats.

Six months after deployment, the QRadar EDR agent detected initial anomalous activity and tracked the attackers on their journey to access a specific set of data. The client's existing traditional antivirus software and intrusion detection system (IDS) didn't detect any activity until the very last stage of the attack. Had the client not deployed QRadar EDR, the attackers would have managed to acquire and exfiltrate the data.

Supply chain attack

On the day of the initial breach, QRadar EDR flagged a suspicious login from a VPN server toward an endpoint in the unprivileged network segment. The security team assumed the login was due to maintenance work by an external security provider and thus assigned a low priority to the incident. The attackers deployed initial malware, mainly used to map the network segment looking for direct paths to the privileged network. After finding no such paths available, the attackers deployed a second in-memory malware for collecting credentials to reuse in subsequent lateral movements. With credentials obtained, the attackers moved on to the domain controller and soon after to a file server containing internal documents.

Root cause analysis

The initial anomalous login happened outside shift hours, from an endpoint that usually interacts with servers but not with workstations. The VPN channel was managed by an external provider that was also in charge of maintaining the mail server and firewalls in addition to the VPN itself. Because of the nature of the access, the alert was maintained active to track every operation, but at that point, the internal security team assigned a low priority to the event, assuming the provider was running maintenance on the infrastructure.

> The client automated the cleanup process using QRadar EDR’s remediation module, and it used the solution’s anti-ransomware protection to prevent data loss and operational disruption.

The next day, QRadar EDR raised a second alert, showing the activity of a lightweight malware used to scan the internal network, soon followed by another alert signaling the presence of an in-memory vector with keylogging and credential harvesting capabilities. At that point, the security team focused on these events, initiating a threat hunting session while the attackers finally managed, through a series of lateral movements, to access one of the domain controllers. The team decided to take advantage of NanoOS technology's invisibility to keep tracking the attackers for as long as possible to understand the modus operandi and their objectives.

As the attackers tried to reach the file server containing highly sensitive information, the team decided to stop them and initiate the eradication plan. While the various devices were being remediated, the attackers realized that, despite the high level of access, they couldn't access the information they were looking for. Figuring that they were discovered, they deployed a ransomware on the entire infrastructure to cover their tracks.

Attack and reconstruction

Once the motivations for the attack were clear, the operator needed to understand the whole attack to reinforce the weak points in the infrastructure. The attack involved a dozen devices before the ransomware deployment stage (Phase 1) and several thousand after that (Phase 2).

The attackers managed to obtain access to the VPN and mail server provider and used them as the initial entry point to the internal network. The attackers reused the provider's credentials to move into different machines, finally settling on a specific workstation. At that point, they used a chain of tools to scan the internal network and identify targets for lateral movements. On the final stage, they used the domain controller itself to spread ransomware on every device.

Disaster averted: response and remediation

The water management facility secured VPN access and conducted a threat hunting session that identified every machine the attackers managed to access. The QRadar EDR remediation module automated the cleanup process, and the segment was cleaned up in a matter of seconds. The facility obtained all tools used during the reconnaissance and lateral movement stage and immediately propagated a policy including IOC and behaviors across the entire infrastructure. No additional compromised hosts were identified after the policy deployment. Credentials were immediately reset for all users, and the ransomware attack required no further intervention because the client enabled QRadar EDR anti-ransomware protection for all devices, preventing the loss of important information and interruption of normal activities.

The facility successfully closed the incident on the second day, without any loss of data, interruption of essential services, or damage to the endpoints.

Had the facility not employed QRadar EDR, the attackers would certainly have exfiltrated sensitive information and might have remained active for an extended period, with the entire infrastructure eventually disabled by the final ransomware attack. Such an attack would have had an enormous impact on the facility’s ability to keep delivering essential services to citizens in the region, potentially blocking them altogether. Given the difficulty in identifying supply chain attacks, the facility might have been breached again through the same channel if no forensic information had been available to pinpoint the root cause of the breach.

About the water management facility

This water management facility in Europe is responsible for handling and distributing water to about a million people. The facility is classified as critical infrastructure and essential services.

Solution component

- IBM Security® QRadar® EDR

Produced in the United States of America, June 2023.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. Generally expected results cannot be provided as each client's results will depend entirely on the client's systems and services ordered. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.