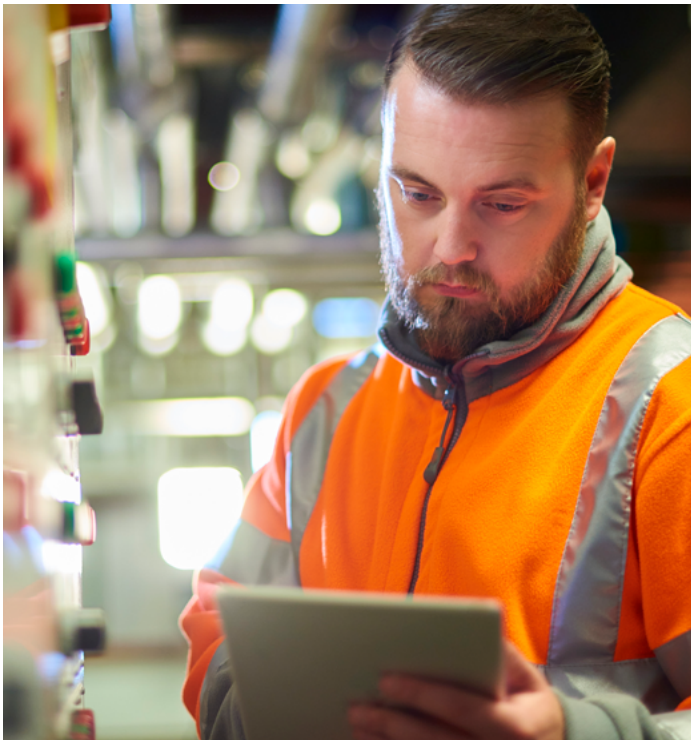
REAQTA
an IBM Company

IBM

Case study: critical infrastructure

Tracking a highly sophisticated supply chain attack against a water management facility



Case

A foreign threat actor targets a water management facility through a supplier. The operator notices suspicious activity but assumes it's just maintenance work by an external security services provider. Attackers manage to obtain access and traverse the operator's network by lateral movement. They compromise high-level servers and deploy ransomware-based anti-forensic measures after attempting to exfiltrate internal information about the water management facility.

Challenges

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

Solution

- IBM® Security ReaQta uses NanoOS, which is designed to be undetectable, to 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

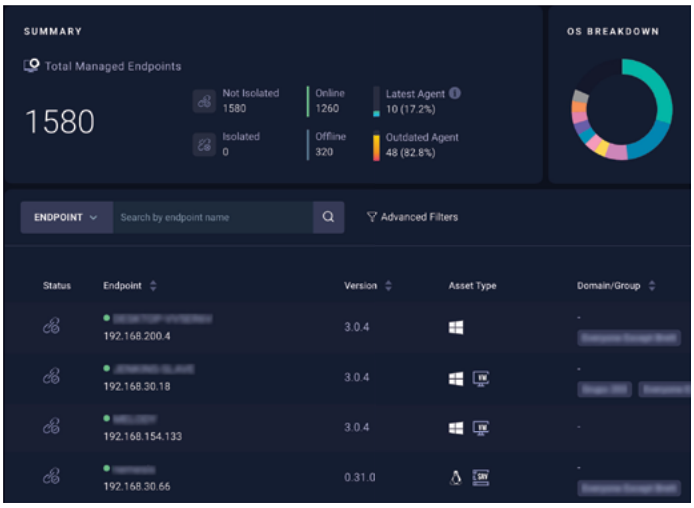
The company

This water management facility in Europe is responsible for handling and distributing water to about 1 million people. The facility is classified as critical infrastructure and essential services.

The security challenge

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.



NanoOS, a unique hypervisor-based approach, works outside the operating system and provides deep visibility into processes and applications running on endpoints.

The process

ReaQta, an IBM Company, was commissioned to run its solution on all the facility's servers, desktops and laptops to continuously monitor every asset and promptly track and investigate potential security breaches. Using built-in dual AI engines and detailed behavioral analysis, ReaQta NanoOS technology provided 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 agent detected initial anomalous activity and tracked the attackers toward their journey to access a specific set of data. The solutions in use, a traditional antivirus and an intrusion detection system (IDS), didn't detect any activity until the very last stage of the attack. Without ReaQta, the attackers would have managed to acquire and exfiltrate the data, successfully wiping the entire infrastructure to cover their tracks.

Supply chain attack

On the day of the initial breach, ReaQta flags a suspicious login from a VPN server toward an endpoint in the unprivileged network segment. The security team assumes the login was due to maintenance work by an external security provider and thus assigns a low priority to the incident. The attackers manage to deploy initial malware, mainly used to map the network segment looking for direct paths to the privileged network. After finding that no such paths are available, the attackers decide to deploy a second in-memory malware, used for collecting credentials to reuse in subsequent lateral movements. When such credentials are obtained, the attackers move on to reach the domain controller, and soon after to a file server containing internal documents. On the last stage of the attack, they deploy a ransomware on the entire infrastructure to cover their own tracks.

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 next day, ReaQta 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.

Response and remediation
VPN access was secured, and a threat hunting session identified every machine that the attackers managed to access. The ReaQta remediation module automated the cleanup process, and the segment was cleaned up in a matter of seconds. All tools used during the reconnaissance and lateral movement stage were obtained and a policy including IOC and behaviors was immediately propagated 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 ReaQta anti-ransomware protection was enabled for all devices, preventing the loss of important information and interruption of normal activities.

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

The result

IBM Security ReaQta invisibly tracked the attackers' movements until the security team shut down access, and the ReaQta solution was later deployed to clean up compromised devices without downtime. Without ReaQta, sensitive information would have certainly been exfiltrated, and attackers might have remained active for an extended period, with the entire infrastructure eventually disabled by the final ransomware attack. Such a devastating 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.

For more information, visit:
ibm.com/products/reaqta

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
May 2022