OTORIO

Pulp and Paper

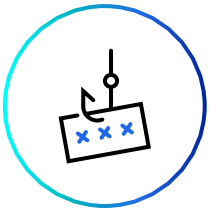
OTORIO Incident Response Team Helps Global Paper Manufacturer Resume Operations Safely

Case Study

A global pulp & paper manufacturer discovered internal phishing correspondence that has been spreading in their network and they reported it to OTORIO's Incident Response team. OTORIO's team helped identify and mitigate the phishing attack and later linked it to a larger campaign that has been targeting multiple companies around the world.

100

SITES WORLDWIDE



OVER

1000

EMPLOYEES were targeted by a phishing attack

Our Findings

OTORIO's team concluded that there were several key areas that required improvement in order to ensure that such an attack would not be successful in the future. These areas include:

- There was no central SIEM solution to collect logs from different systems
- There was no standard AV system across the network
- There was no IP logging of external connections to the network

Background

The customer operates over 100 manufacturing sites around the world. OTORIO's Incident Response team was contacted by the customer, who claimed that an internal user sent a phishing email to almost 1,000 employees. OTORIO's Incident Response team investigated the attack and concluded that there was a previous, failed attempt to perform a phishing attack on the network and that the current successful attack is part of a larger campaign that targeted different companies around the world, stealing employee credentials. OTORIO removed all threats to the network successfully, the company resumed operations, and received a clear mitigation plan to improve its security posture moving forward.

OTORIO

Pulp and Paper

OTORIO's Role

OTORIO was tasked with:

- Discovering the source of the malicious activity
- Mapping any victims on the network
- Assessing the impact on the network
- Removing any malware or attacker persistence and access
- Suggesting mitigations and future actions to be taken by the organization
- Strengthening the security posture of the organization

Moving forward

OTORIO's incident response assessment and reports gave the customer a clear picture of the steps the attacker took during the attack, with an emphasis on the security gaps that enabled their activity. OTORIO provided the company with a solid security posture plan to ensure that they are capable of taking the first steps in improving OT security immediately.

Following the successful incident response, the customer requested that OTORIO extend its services and perform Penetration Testing to assess network resilience.

Recommendations

The team provided various security control improvements that the customer can implement to ensure that its network is resilient to similar attacks in the future. Some of the suggestions included:

- Implement OWA 2-step verification
- Index defense system logs to a SIEM
- Enable safe web browsing solutions
- Assign local cybersecurity personnel with monitoring tasks
- Create incident response situation rooms, playbooks, and implementation plans

About OTORIO

OTORIO has pioneered an industrial-native OT security platform that enables its customers to achieve an integrated, holistic security strategy for industrial control systems (ICS) and cyber-physical systems (CPS).

Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. The company's platform provides automated and consolidated visibility of the entire operational network, enabling companies to take control of their security posture, eliminate critical risks, and deliver immediate business value across the organization.

OTORIO's global team combines the extensive mission-critical experience of top nation-state cyber security experts with deep operational and industrial domain expertise.

CN 300420