Pondurance Incident Response (IR) for Manufacturing

PONDURANCE

CASE STUDY

THE INCIDENT

A global manufacturing company was hit with a ransomware attack by the Egregor ransomware group. The cybercriminals gained network entry through a weaponized email attachment opened by an employee and launched a ransomware attack. The organization reached out to us shortly after they were solicited for the ransom.

OUR SOLUTION

We contained their environment and started to investigate right away. We found that their Active Directory was compromised leading to credential theft, impersonation, and data exfiltration. We were able to work with their teams to restore operations within 72 hours. We provided documentation of findings as well as recommendations to avoid incidents in the future.

Many factors contributed to this incident — lack of endpoint detection and response, lack of log services, lack of monitoring, and insufficient deployment of parent company cyber policies.

OUR RECOMMENDATIONS

- Monitor your infrastructure 24/7 to quickly identify suspicious activity across cloud, network, logs, and endpoints.
- Actively block known malicious actors and domains.
- Improve password and credential management strategies.
- Regularly conduct active directory and security group audits.
- Tighten coordination with endpoint detection and response monitoring vendors for increased awareness.
- Enable multi-factor authentication on all remote access and for privileged access to make it more difficult for cybercriminals to access accounts.
- Disable interactive login for service accounts like remote desktop protocol.

BENEFITS OF PONDURANCE INCIDENT RESPONSE

- We work closely with business and security executives to proactively reduce risk and provide timely response to urgent issues.
- Brokers and major carriers recognize us as a go-to provider for incident response and digital forensics engagements.
- We specialize in building pre-incident broker and carrier relationships to facilitate rapid on-target response and reduce the cost of incidents.
- We partner with leading law firms that specialize in cybersecurity and privacy matters.

ABOUT PONDURANCE

Our mission is to ensure that every organization is able to detect and respond to cyber threats, regardless of size, industry, or current in-house capabilities. We combine our advanced platform with decades of human intelligence to speed detection and response and quickly contain cybersecurity threats to ultimately decrease risk to your mission. Learn more about Pondurance Incident Response.

pondurance.com

500 N. Meridian St., Suite 500, Indianapolis, IN 46204