Malware Thwarted MDR Manufacturing

PONDURANCE

CASE STUDY

THE CHALLENGE

An employee at a manufacturing organization accidentally visited a fraudulent site and was served a malicious download for a fake Chrome update. The download created a remote backdoor for the attacker, who was able to leverage toolsets to dump credentials and attempted to move laterally within the environment as our Security Operations Center (SOC) team stepped in.

OUR SOLUTION

As a Pondurance Managed Detection and Response (MDR) client, this manufacturer's environment is monitored 24/7 by our SOC. Our SCOPE platform ingested logs from the Endpoint Detection and Response solution, and our SOC team detected initial access and took immediate action. The team reported the malicious activity to the client's security team and isolated the compromised endpoint before the attacker could take further action. Without our preestablished processes in place with the client and our ability to act quickly, the attacker could have penetrated a lot further. The attacker would have done tremendous damage to the business had he or she been able to compromise credentials and affect more endpoints.

OUR RECOMMENDATIONS

- Monitor your infrastructure 24/7 to quickly identify suspicious activity across cloud, network, logs and endpoints.
- Have an incident response plan and playbooks in place to be able to act immediately.
- Perform user training related to downloading files from unknown or untrusted sources, as well as general cybersecurity awareness.
- Run tabletop simulations to test internal systems against potential malware downloads.
- Ensure that internal teams know how to appropriately respond to malware attacks.
- Enable multifactor authentication to make it more difficult for cybercriminals to access accounts.
- Regularly audit shared and service accounts for password strength and complexity.

Like our manufacturing client, you need to be prepared with a SOC team watching 24/7 to quickly detect bad actors in your system!

BENEFITS OF PONDURANCE MDR

- Stop security incidents through 24/7 detection and response.
- Maximize internal resources and security investments.
- Improve compliance through reporting.
- Increase visibility into alerts that require action.
- Rapidly accelerate security program maturity.
- Lower total cost of ownership.

ABOUT PONDURANCE

Pondurance delivers world-class MDR services to industries facing pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements and digital transformation.

Our advanced platform with our experienced team of analysts continuously hunts, investigates, validates and contains threats so your team can focus on what matters most.

pondurance.com

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