ANATOMY OF A DEVASTATING ICS CYBER ATTACK

How Phishing, Unpatched Systems, and Poor Segmentation Enabled Disruption of a Critical Facility

DEFENTOS
cyber security

CASE STUDY

TABLE OF CONTENT

INTRODUCTION

This study explores a severe ICS cyber-attack on a key industrial facility, initiated through spear phishing and exacerbated by unpatched systems and insufficient network segmentation, leading to significant disruption.

This paper investigates a sophisticated cyber-attack on an essential industrial infrastructure, focusing on the attacker's methods and the system vulnerabilities exploited.

The incident began with a spear phishing attack that compromised a plant engineer's credentials. Subsequently, the assailant took advantage of critical weaknesses within the Industrial Control Systems (ICS) network, notably the use of obsolete, unpatched Windows platforms, and poor firewall policies that failed to adequately separate the ICS environment from the broader corporate network.

The exploration of these elements sheds light on the multi-faceted nature of security lapses that can lead to profound operational consequences in critical facilities.

ATTACK LIFECYCLE

Despite having a highly innovative product, Wardiere Inc. struggled to reach their target audience. Their website had low traffic, and their conversion rate was not meeting their expectations.

Phase 1: Reconnaissance and Target Selection

The attacker conducted thorough reconnaissance to identify potential targets within the industrial sector. The attacker focused on critical infrastructure facilities with ICS networks that showed signs of weak security practices. They used various techniques, such as scanning, phishing, and social engineering, to gather information about the industrial sector and its network infrastructure.

They looked for potential targets that had critical infrastructure facilities, such as power plants, water treatment plants, or oil refineries, that used industrial control systems (ICS) to monitor and control physical processes. The attacker also assessed the security posture of these targets and focused on on the one which showed signs of weak security practice, such as outdated software, default passwords, or lack of encryption.

By doing so, the attacker aimed to exploit the vulnerabilities in the ICS networks and cause damage or disruption to the physical operations of the facilities.

Phase 2: Phishing and Initial Compromise

The attacker did not stop at reconnaissance but proceeded to launch a phishing campaign to gain access to the ICS network. They created fake emails that looked like they came from trusted sources, such as vendors, partners, or colleagues, and addressed them to plant engineers who worked at the facility. These emails contained attachments that pretended to be relevant documents, such as manuals, reports, or invoices, related to the ICS system maintenance.

The attachments had malicious code embedded in them, which would execute when opened. One plant engineer fell for the trap and opened the attachment, without realizing that it was a malicious file. This triggered the installation of a sophisticated remote access Trojan (RAT) onto the engineer's workstation. A RAT is a type of malware that allows the attacker to remotely control the infected device and perform various actions, such as stealing data, installing other malware, or manipulating system settings. The RAT gave the attacker a foothold in the ICS network and enabled them to carry out further attacks on the facility.

Phase 3: Lateral Movement and Escalation of Privileges

The RAT was not the only malware that the attacker used to compromise the facility. The RAT also harvested the engineer's corporate credentials, which were stored on the workstation. These credentials gave the attacker a foothold within the corporate network, which was connected to the ICS network. The attacker used various techniques, such as scanning, enumeration, and credential dumping, to move laterally within the network and identify potential targets. One of these targets was an unpatched Windows server within the ICS network, which had a known vulnerability that could be exploited remotely. The attacker exploited this vulnerability to gain access to the server and execute commands on it. The server had default passwords and weak access controls, which allowed the attacker to escalate privileges and gain administrative rights on the server. The attacker then installed a backdoor on the server, which enabled them to establish a persistent presence within the ICS network and communicate with a command and control (C2) server outside the network. The backdoor also gave the attacker access to other devices and systems within the ICS network, such as programmable logic controllers (PLCs), human-machine interfaces (HMIs), and sensors. The attacker was now ready to launch the final stage of their attack on the facility.

Phase 4: Exploration and Data Exfiltration

The attacker did not only aim to disrupt the facility's operations, but also to steal its secrets. The attacker navigated the ICS network, mapping its architecture and identifying critical systems responsible for process control. These systems included PLCs, HMIs, and sensors that regulated the physical parameters of the industrial processes, such as temperature, pressure, and flow. The attacker also discovered that the ICS network was inadequately segregated from the corporate network, allowing lateral movement between the two environments. This meant that the attacker could access not only the ICS devices, but also the corporate servers, databases, and workstations that stored valuable intellectual property related to the facility's industrial processes. This intellectual property included design documents, engineering drawings, process specifications, and trade secrets. The attacker exfiltrated this data to their C2 server outside the network, using encryption and obfuscation techniques to evade detection. The attacker not only caused physical damage to the facility, but also compromised its competitive advantage and reputation.

Phase 5: Impact and Evasion

The attacker's activities disrupted the facility's operational processes, leading to production downtime and financial losses. The attacker manipulated the PLCs, HMIs, and sensors within the ICS network, causing them to malfunction or display false readings. This resulted in abnormal fluctuations in the physical parameters of the industrial processes, such as temperature, pressure, and flow. These fluctuations could damage the equipment, compromise the product quality, or even cause safety hazards. The facility's incident response team detected anomalies within the ICS network but struggled to identify the source and scope of the attack due to the lack of proper network monitoring and segmentation. The facility did not have adequate visibility into the network traffic and activity, making it difficult to trace the attacker's actions and determine the impact of the attack. The facility also did not have proper network segmentation, which would have isolated the ICS network from the corporate network and prevented lateral movement between the two environments.

The attacker employed various evasion techniques to maintain persistence and evade detection. These techniques included encryption, obfuscation, anti-forensics, and data wiping. The attacker encrypted their communication with the C2 server and their exfiltrated data, making it harder to intercept and analyze. The attacker also obfuscated their malware code and used legitimate tools and processes to blend in with normal network activity. The attacker used anti-forensics tools to delete or modify logs, files, and registry entries that could reveal their presence or actions. The attacker also wiped their malware and backdoors from the compromised devices after completing their attack, leaving no traces behind

VULNERABILITIES EXPLOITED:

PHISHING AND SOCIAL ENGINEERING

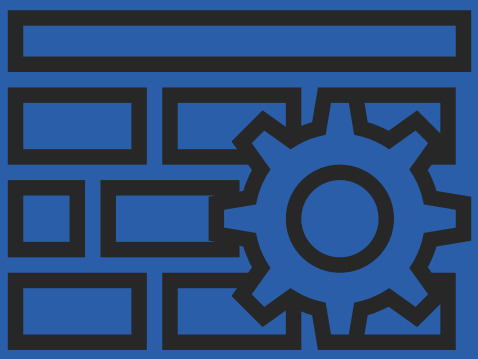
The attacker leveraged sophisticated phishing techniques to deceive plant engineers and obtain their corporate credentials. The lack of adequate security awareness training and email filtering solutions contributed to the success of this attack vector.

OUTDATED AND UNPATCHED WINDOWS SYSTEMS

The ICS network's reliance on outdated and unpatched Windows systems provided the attacker with a readily exploitable entry point. Known vulnerabilities that were not patched allowed the attacker to gain unauthorized access.

INADEQUATE FIREWALL SEGREGATION

Insufficient firewall segregation between the ICS and corporate networks facilitated lateral movement. The attacker was able to traverse between the two environments, expanding their reach and compromising critical systems.



CONCLUSION

The ramifications of such breaches extend far beyond the immediate disruption, potentially impacting societal trust, economic stability, and even national security. In environments where precision and uninterrupted operation are paramount, the infiltration of malware or other forms of cyberattacks can result in catastrophic failures, environmental disasters, and loss of life. These potential outcomes necessitate a paradigm shift in how industrial organizations perceive and address cybersecurity, acknowledging it not just as a technical issue but as a fundamental component of their operational integrity.

Addressing these vulnerabilities requires a holistic approach that transcends the conventional IT security framework.Enhanced collaboration across departments, ensuring that security measures are ingrained in the organizational culture, is crucial. This involves regular training and awareness programs that empower employees to recognize and respond to cyber threats proactively, thereby acting as the first line of defense.

In conjunction with technological measures, there must be an emphasis on regulatory compliance and the establishment of industry-wide cybersecurity standards. These standards should encourage or mandate regular security audits, vulnerability assessments, and the sharing of threat intelligence among entities within the industry. By fostering a culture of continuous improvement and adaptability in the face of new threats, industrial entities can fortify their cyber defenses, ensuring the resilience and continuity of critical global infrastructure.

THANK YOU!

Defentos is your trusted cyber security partner supporting you with security advice, testing and awareness training.

CONTACT

DEFENTOS B.V.
+31 (0) 33 – 202 6728
INFO@DEFENTOS.COM