Digital Transformation
ACADEMY



Spearphishing, ransomware remain top cybersecurity threats to manufacturing

ReliaQuest report for Aug. 1, 2024, through Jan. 31, 2025, noted a "turbulent threat landscape" with attackers ramping up their abuse of remote external services software.

Scott Achelpohl

What you'll learn:

- "Spearphishing" is an ever-popular tactic because attackers can prey on the entire supply chain.
- A chemical manufacturer lost $60 million last August after one employee fell for a business email compromise (BEC) scam.
- The report blames the rise of "smart" factories that boost productivity with automation and digitization through IIoT for the rise in ERS abuse.

Manufacturing remains a top—if not the top—target that cyberattackers are hunting, often employing the tactic of "spearphishing," according to revelations from a recent study by U.S. cybersecurity technology company ReliaQuest.

The study did not uncover much that was new (manufacturing was ranked by the IBM X-Force Threat Intelligence Report as the top targeted sector for the third year in a row last year), but the kinds and severity of threats should be eye-opening to every manufacturer seeking to reinforce their cyberdefenses in 2025.

See also: Why ransomware attackers target backups—and how to ensure your data is protected

Spearphishing, ransomware remain top cybersecurity threats to manufacturing

Some of the findings from the ReliaQuest study's Aug. 1, 2024, to Jan. 31, 2025, reporting period:

- 130% surge in abuse of external remote services (ERS)
- 24% increase in ransomware groups targeting manufacturing
- Spearphishing (the fraudulent practice of sending emails ostensibly from a known or trusted sender to induce targeted individuals to reveal confidential information) ranked as the top attack method.

As the report notes, spearphishing is an increasingly popular tactic because attackers who use this tactic can prey on the entire supply chain, "on the everyday flow of business; attackers send spearphishing emails that look routine—like a supplier requesting payment—and wait for a misstep. And when that happens, the consequences are stark."

The report cites a chemical manufacturer that lost $60 million last August after one employee fell for a business email compromise scam.

Webinar: Cybersecurity center stage in 2025 and beyond

In BEC scams, fraudsters contact employees with access to an organization's funds, often impersonating a senior executive, and ask them to transfer large sums to an account.

Such attacks cost U.S. businesses $2.9 billion in 2023, according to the FBI, and BEC attacks are among the top two events that led to cybersecurity insurance scams two years ago, according to insurance firm Coalition. Generative AI often is used to create convincing fake emails for BEC attacks.

'Smart' factories make manufacturing more vulnerable

The rise in external remote service (ERS) abuse, in particular, isn't limited to manufacturing—it's part of a broader trend, the ReliaQuest report notes, with a 70% increase across all sectors from 2023 to 2024. But why is manufacturing seeing such a big spike? The report blames the rise of smart factories that boost productivity by turning to automation and digitization through IIoT.

"In doing so, once air-gapped, locked-down factory systems have been replaced with hyper-connected OT and IT environments," the report noted. "Remote services like virtual private networks (VPNs) and remote desktop protocol (RDP), meant for real-time monitoring and remote access, have become the perfect entry points for cybercriminals."

Where OT is again shown as vulnerable

Open ports are another area of vulnerability spotlighted in the ReliaQuest report. Open ports, which the study noted are essential for communication between OT systems or remote maintenance, can become entry points for attackers if they are left unmonitored. During the August-to-January period, GreyMatter DRP alerts for open ports in the manufacturing sector rose to 12% compared to the previous period, far outpacing the increases for utilities (4%) and construction (2%).

Crystal Ball 2025: Now's the time to strengthen your company's cybersecurity compliance

OT systems also use outdated technology, according to the report, "that rely on legacy technology built for functionality, not security. Ports like 502, commonly used by Modbus devices, are often left open by default for communication and control."

It also notes: "Vendors often need remote access for maintenance, so ports are left open for convenience without adequate configurations or controls. Limited cybersecurity awareness among OT personnel can result in hesitancy to secure systems, fearing disruptions to complex, mission-critical operations."

Ransomware still surging—and manufacturing remains a prime target

In ReliaQuest's Aug. 1, 2024 to January 31, 2025, measurement window, the cybersecurity company found ransomware attacks to still be surging across all sectors with manufacturing as a prime target for this kind of attack, which is a type of malicious software designed to block access to a company's computer systems until a sum of money is paid to the perpetrators.

ReliaQuest found ransomware assailants his 2,999 organizations across all industries in that time span, a 33% increase from the previous reporting period. In manufacturing, ReliaQuest found, the number of active

ransomware groups rose from 26 in 2023 to 57 last year, a 24% increase.

Cybersecurity for operational technology: A guide for 2025

In the fourth quarter of 2024 alone, manufacturers accounted for 370 victims, trailing just behind professional, scientific, and technical services at 375.

In a separate report released this week, London-based corporate intelligence firm S-RM concluded that fully one-third of incidents its team encountered in 2024 involved ransomware, though the rate of growth in these attacks slowed from 70% in 2023 to 13% last year.

"Ransomware groups will target any company or sector where there is money to be made," S-RM's report noted. "This year, we observed an increase in attacks on health care and manufacturing companies. The costliness of business interruption and the potential access to sensitive and valuable data makes these sectors attractive targets."

"Why is manufacturing such a prime target?" the ReliaQuest report asked. "Downtime is devasting—but that's also true for sectors like health care. What sets manufacturing apart is its operational scale. One production line being compromised can disrupt entire supply chains and cause huge financial losses. And as organizations increasingly adopt IIoT devices to improve OT visibility, the risks grow exponentially. Many IIoT devices are tied to legacy OT systems that can't be updated, creating vulnerabilities that are magnets for attackers."

About the Author: Scott Achelpohl

I've come to* Smart Industry *after stints in business-to-business journalism covering U.S. trucking and transportation for* FleetOwner*, a sister website and magazine of SI's at Endeavor Business Media, and branches of the U.S. military for Navy League of the United States. I'm a graduate of the University of Kansas and the William Allen White School of Journalism with many years of media experience inside and outside B2B journalism. I'm a wordsmith by nature, and I edit* Smart Industry *and report and write all kinds of news and interactive media on the digital transformation of manufacturing.