HUNTRESS

2025 Cyber Threat Report

Threats Targeting the Manufacturing Industry

Overview

Last year, malicious hackers were busier than ever. They got smarter, adapting quickly and using more advanced tools and strategies to target industries like healthcare, tech, education, government, and manufacturing.

The gap between cyberattacks on big companies and small businesses is all but gone. Hackers are now using the same advanced tactics they've perfected on larger organizations to target manufacturers of all sizes, making their attacks more efficient and effective.

The following pages draw from insights from Huntress' *2025 Cyber Threat Report* to uncover the tactics of these attackers and highlight the key threats facing manufacturing today.

Attack Breakdown

Manufacturing Is a Top Target

Last year, threat actors went after various industries, hitting healthcare and education the hardest—these two sectors alone made up 38% of all attacks we tracked. But it didn't stop there: tech companies, government, and manufacturing were also heavily targeted, accounting for almost another third of the incidents.

Manufacturing in particular stood out, making up nearly 10% of the total attacks we saw.

Industries Targeted

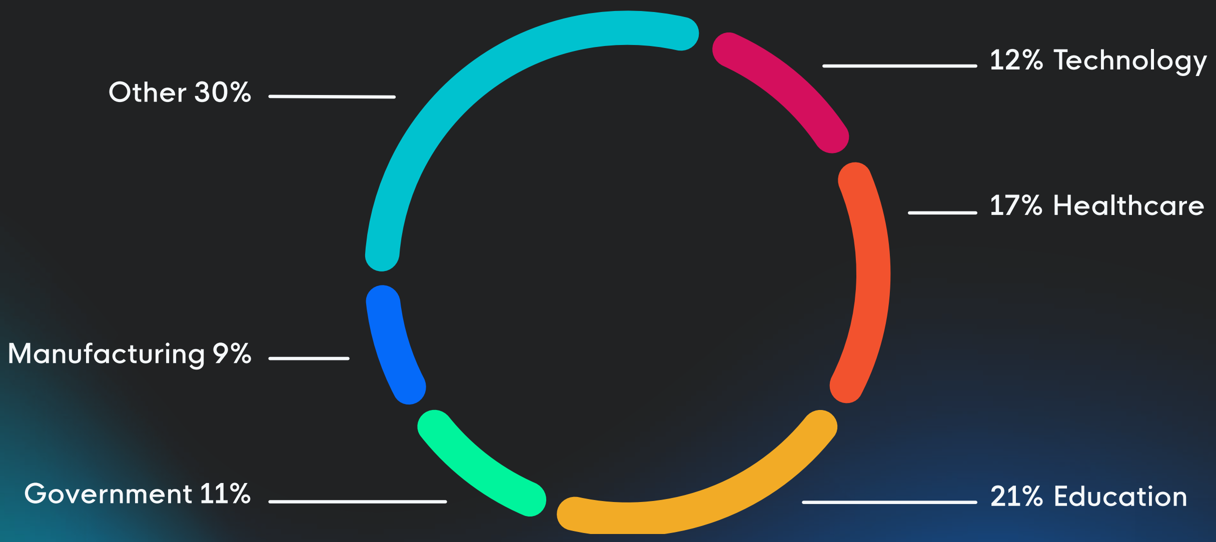

Figure 1: Industries targeted by percentage in 2024

Every industry dealt with its own set of threats, but some attack methods kept popping up, like malicious scripts, remote access trojans (RATs), and the misuse of remote monitoring and management (RMM) tools.

Ransomware was another constant issue, and manufacturing wasn't spared. As cryptocurrency prices soared later in the year, attackers got even bolder, going after smaller businesses as well as larger ones. This highlights the need for manufacturers of all sizes to have tailored defenses and proactive strategies to handle the unique risks they face.

Threats by Industry

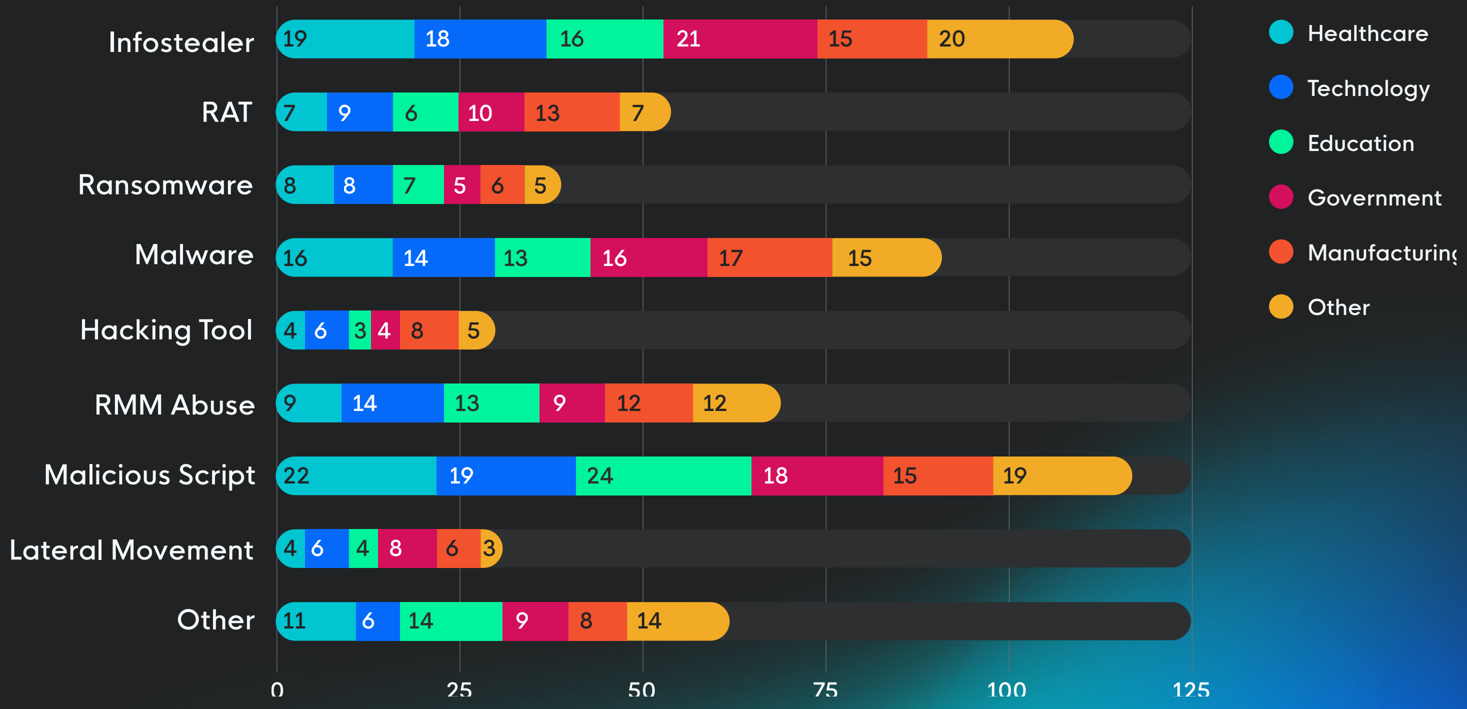

Figure 2: Threat frequency by industry in 2024

Manufacturing Sector Threats

Looking at manufacturing, the data for 2024 definitely stood out. There was a surprising number of RAT installations in these environments, with AsyncRAT, Trickbot, NetSupport, and NewCoreRAT popping up the most.

Manufacturing companies also dealt with major issues caused by malicious scripts created using various scripting languages. While PowerShell is still the go-to tool for attackers, other methods like WMI, JavaScript, and VBScript are also being used effectively. Java-based attacks have been especially successful because attackers are doing their homework and crafting strategies to target specific vulnerabilities.

We noticed an interesting trend of malware often disguising itself as Adobe components. In fact, this type of trickery made up 23% of all methods used in this area. The next most common tactic, pretending to be Windows or Defender components, was much lower at just 11%.

RMM abuse often exploited or targeted Windows Remote Desktop at a higher rate than in other environments, with attackers injecting or manipulating RDP components to steal credentials or weaken security.

In this sector, attackers focused on stealing domain passwords and quickly moving to higher-priority machines. Most lateral movement was done the old-school way using Windows LOLBins and domain tools like ADExplorer and NetAdmin Toolkits.

Threats Targeting Manufacturing

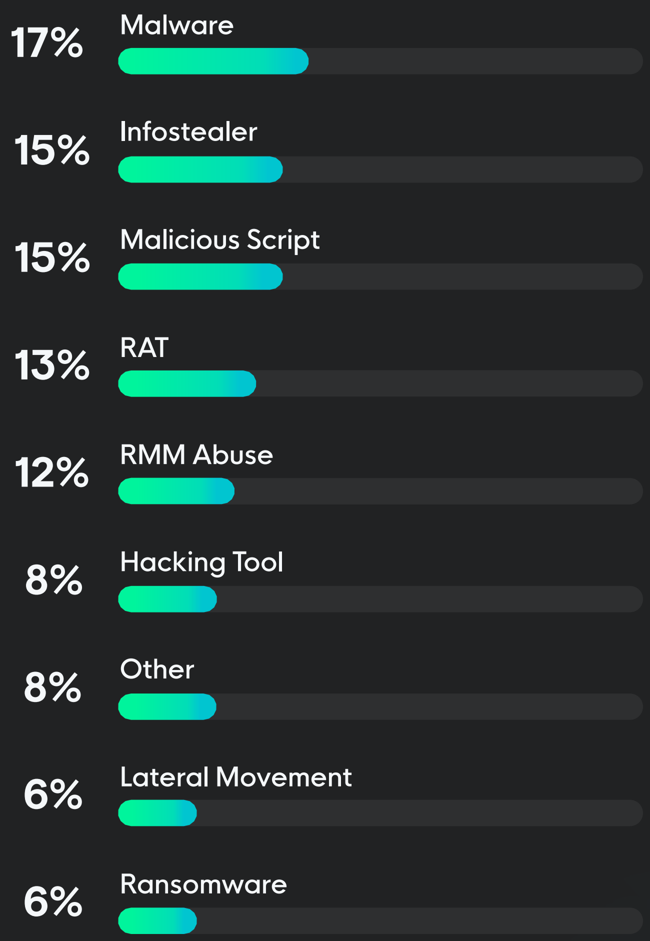

Figure 3: Manufacturing threats by type in 2024

Conclusion

Hackers are no longer focused solely on large corporations. They're now using sophisticated tactics to target manufacturers of all sizes, erasing the distinction between attacks on big enterprises and smaller businesses.

From ransomware and malicious scripts to compromised remote monitoring tools, hackers continually discover new ways to exploit vulnerabilities in the manufacturing sector. Our research highlights alarming threats, including RATs, Java-based exploits, and advanced obfuscation techniques.

All this underscores the critical need for stronger measures to protect your operations. By implementing robust cybersecurity tools and strategies, manufacturers like you can protect your systems, eliminate vulnerabilities, and stay one step ahead of evolving threats.

About Huntress

Founded in 2015 by former NSA cyber operators, Huntress protects over 3 million endpoints and 1 million identities worldwide, elevating under-resourced IT and security teams and empowering them with protection that works as hard as they do. Powered by a 24/7 team of expert security analysts and researchers, our enterprise-grade, fully owned technology is built for all businesses, not just the 1% with big budgets.

With fully managed EDR, ITDR, and SIEM solutions and Security Awareness Training, the Huntress platform helps end users quickly deploy and manage real-time protection for endpoints, email, and employees, all from a single dashboard.

Huntress exists to level the cybersecurity playing field and elevate our community through award-winning technology and world-class people. We're ethical badasses who love what we do: wrecking hackers and protecting businesses from real threats.

Huntress Protects Manufacturers

Malicious hackers target manufacturers with increasingly sophisticated tools, but you don't have to face them alone. Huntress combines advanced purpose-built technology with dedicated people-powered security to defend your systems, safeguard your operations, and protect what matters most.

Learn More

HUNTRESS®