

Q3 Manufacturing Sector

Quarterly Threat Landscape Scorecard

TLP: CLEAR

A-2022-11-09a



Q3 2022 Manufacturing Sector Threat Overview

The manufacturing sector remained a prime target for malicious actors in Q3 2022 due to its key role in critical infrastructure and the global economy. ZeroFox Intelligence assesses that the threat to the sector will increase in the coming months amidst geopolitical and economic strain, underpinned by politically-inspired targeting. In Q3 2022, manufacturers faced an increased threat from smishing, callback phishing, and threat actors leveraging techniques to bypass multi-factor authentication (MFA). ZeroFox Intelligence recommends implementing phishing-resistant MFA methods that support Fast ID Online Version 2.0 (FIDO2) and certificate-based authentication. Exploit disclosure in Information Technology and Operational Technology infrastructure continued at a high pace, with threat actors leveraging vulnerabilities in past end-of-life products. The shift to Initial Access Broker (IAB) market sales being made in private channels rather than advertising in open forums will likely continue and make identifying and mitigating access sales ahead of compromise increasingly challenging. Botnet and malware deployment remained high, including infostealers and trojans. Digital extortion attempts against manufacturing targets continued to fall, likely caused in part by difficulty eliciting victims' payments, although ZeroFox Intelligence has observed an increase in attacks against "big game" manufacturing targets. In coming months, the industry is likely to see an increase in politically-motivated extortion targeting.

Key Cyber Threats to the Manufacturing Sector in Q3 2022



Increased threats from SMS-phishing, callback phishing, and techniques to bypass MFA



Exploitation of vulnerabilities in past end-of-life products and widely used third-party software



Ransomware and digital extortion outfits conducting attacks against big-game manufacturing targets



State-aligned threat actors leveraging custom-made malware against industrial control systems



IABs moving towards private means of communication with sellers, making identification and mitigation more difficult



Changes to digital extortion tactics resulting in greater operational downtime, reputational damage, and legal ramifications



Russia-aligned threat actors seeking to target manufacturing entities and disrupt global supply chains



Saturated trojan markets sustaining low barriers to entry and high pace of new Indicators of Compromise (IOCs)

Manufacturing Sector Threats

Categories	Q1 2022	Q2 2022	Q3 2022
Social Engineering			
Vulnerability Exploitation			
Initial Access Brokers			
Botnets			
Malware			
Ransomware			

KEY

Indication of decrease in threat from previous quarter

No notable change in threat from previous quarter

Indication of increase in threat from previous quarter

Q3 Key Findings:

- Manufacturing organizations likely faced an increased threat of smishing, callback phishing (vishing), and phishing techniques that bypass MFA.
- Manufacturing organizations continued to face a high risk of threat actors leveraging exploits in products past end-of-life use.
- Advertisements for illicit access into manufacturing organizations plateaued, bucking a downward trend seen in other sectors.
- Despite a likely reduction in threat from ransomware and digital extortion, ZeroFox Intelligence observed an increase in attacks against "big game" manufacturing organizations.
- ZeroFox Intelligence assesses the threats facing the manufacturing sector will more likely than not develop significantly over the next two quarters.

SCOPE NOTE ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 12:00 PM (EDT) on October 10, 2022; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

SOCIAL ENGINEERING

ZeroFox Intelligence assesses with low confidence that aspects of the social engineering threat faced by the manufacturing sector increased in Q3 2022, although attacks are very likely underreported. It is likely emerging social engineering trends seen in campaigns against other sectors in Q3 2022 were also reflected in incidents against the manufacturing sector.

Manufacturing organizations should note that industry-agnostic social engineering campaigns increasingly leveraged smishing attacks targeting employees, either directly or via enterprise third-party providers.[1,2] Analysis indicates an increased threat of callback phishing (vishing), adding legitimacy to malicious emails by impersonating security teams and encouraging victims to return a phone call to authenticate fraudulent activity.[3] Threat actors increasingly leveraged techniques to bypass MFA, including Adversary-in-the-Middle (AiTM) now being incorporated into broader Phishing-as-a-Service (PhaaS) offerings.

Campaigns targeting customers remained evolutionary rather than revolutionary, indicating that human error remained a barrier to effective security and is still a lucrative practice for threat actors. Reports indicate the campaigns typically involve impersonation of goods manufacturers in rudimentary phishing emails, text messages, and voice calls and are often selling counterfeit products. Malware distribution via malicious email attachments targeting the sector remained highly prevalent.[4] Manufacturers should also continually monitor for, and take down, impersonating phishing domains and open redirects to avoid customers being defrauded or providing an intrusion vector for threat actors.

Forward Look:

- Smishing of manufacturing organizations' employees and customers is likely to continue on an upward trajectory.
- Threat actors are very likely to increasingly leverage MFA-bypassing social engineering techniques.

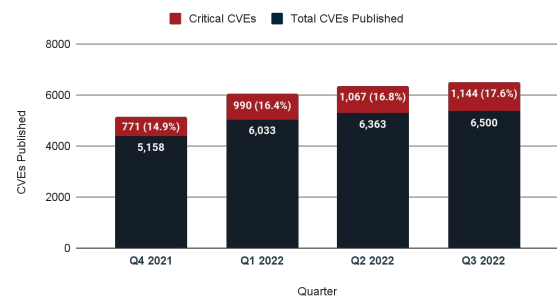
Recommendations:

- Communicate to employees about emerging trends in social engineering scams and how to conduct safe means of authentication.
- Engage ZeroFox Intelligence to conduct an Attack Surface Assessment to understand threats to your organization.

No notable change in threat from previous quarter

Indication of increase in threat from previous quarter

Total CVEs Published by Quarter



Source: [hXXps://nvd.nist.gov](https://nvd.nist.gov)

VULNERABILITY EXPLOITATION

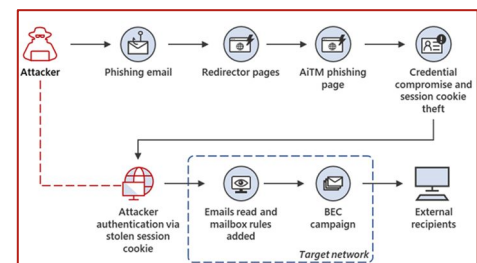
The most widely-reported examples of vulnerability exploitation in Q3 2022 targeting manufacturers remained in commonly-used software modules and network perimeter infrastructure. New disclosures this quarter impacted Apple operating systems, Atlassian Confluence, Google, Microsoft Windows and Exchange, and Whatsapp.[5] Manufacturing organizations continued to face a high risk of threat actors leveraging exploits in products past end-of-life use. This includes Industrial Control Systems, with vulnerabilities added to CISA's Known Exploited Vulnerabilities (KEV) catalog in Q3 2022 that end-users have long been advised to disconnect.[6,7] Threat actors have also attempted to exploit Zoho ManageEngine, of which multiple manufacturing organizations are stated to be customers.[8]

Forward Look:

- Vulnerabilities in commonly-used software modules and network perimeter infrastructure will likely continue to dominate the exploit landscape.

Recommendations:

- Use the ZeroFox Platform's Intelligence Search capability to investigate vulnerabilities and associated exploits.
- Ensure a thorough understanding of your technology stack and patching schedule, as well as those of operating partners.
- Leverage CISA's KEV catalog to prioritize out-of-cycle vulnerability patching.



AiTM Phishing Campaign Overview
Source: [hXXps://www.microsoft.com](https://www.microsoft.com)

FOOTNOTES

- [hXXps://www.securityweek.com/twilio-cloudflare-attacked-part-campaign-hit-over-130-organizations](https://www.securityweek.com/twilio-cloudflare-attacked-part-campaign-hit-over-130-organizations)
- [hXXps://www.bleepingcomputer.com/news/security/stealthy-hackers-target-military-and-weapons-contractors-in-recent-attack/](https://www.bleepingcomputer.com/news/security/stealthy-hackers-target-military-and-weapons-contractors-in-recent-attack/)
- [hXXps://threatpost.com/callback-phishing-security-firms/180182/](https://threatpost.com/callback-phishing-security-firms/180182/)
- [hXXps://thehacknews.com/2022/07/researchers-uncover-new-attempts-by.html](https://thehacknews.com/2022/07/researchers-uncover-new-attempts-by.html)
- [hXXps://nvd.nist.gov](https://nvd.nist.gov)
- [hXXps://thehacknews.com/technology/cve-2021-38406-cisa-kev-catalogue/#~:text=CVE%2D2021%2D38406%2C%20affecting,writes%2C%20potentially%20allowing%20code%20execution.](https://thehacknews.com/technology/cve-2021-38406-cisa-kev-catalogue/#~:text=CVE%2D2021%2D38406%2C%20affecting,writes%2C%20potentially%20allowing%20code%20execution.)
- [hXXps://www.cisa.gov/known-exploited-vulnerabilities-catalog](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
- [hXXps://www.manageengine.com/customers.html](https://www.manageengine.com/customers.html)

INITIAL ACCESS BROKERS

ZeroFox Intelligence assesses with low confidence that the threat to manufacturers in Q3 2022 from IABs remained broadly consistent with Q2 2022. Advertisements for illicit access into manufacturers plateaued, bucking a downward trend seen in other sectors. There has likely been a shift towards brokers preferring private channels rather than advertising in forums to avoid law enforcement scrutiny; according to threat actor chatter, brokers are selling to well-established buyers out of an abundance of caution.[9] It is too early to ascertain whether manufacturing will continue to be an outlier in advertisements posted in open forums, though it is very unlikely to be due to difficulty selling to buyers in private channels.

> Forward Look:

- Illicit access to large manufacturing entities will likely increasingly be sold via private or direct communication methods.

> Recommendations:

- Employ ZeroFox Threat Intelligence feeds to get ahead of threat actor activity.
- Proactively monitor for potential network access sales to obtain critical early warnings of impending cyberattacks.

No notable
change in
threat from
previous quarter

MALWARE

ZeroFox Intelligence assesses with low confidence that the threat to the manufacturing sector from malware deployment in Q3 2022 remained broadly consistent with previous quarters, with the landscape continuing to be largely shaped by Russia's ongoing war in Ukraine. Low barriers to entry and the pace of trojan updates continued to sustain a high threat, with manufacturers targeted globally.[10] It is not clear whether increased reporting of malware targeting OT infrastructure reflects better coverage or a change in threat.[11] For IT infrastructure, app stores and malicious attachments to emails remained two of the most prolific means of distributing malware.[12] The threat from popular loaders is assessed to have increased, with Bumblebee and ChromeLoader now deploying some of the most capable malware strains available.[13]

> Forward Look:

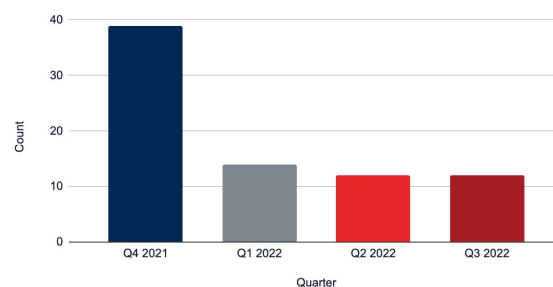
- Malware-as-a-service offerings will very likely sustain low barriers to entry for threat actors.
- Russia-linked threat actors will likely increasingly target manufacturing entities with destructive malware.

> Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to Malware and Ransomware.

No notable
change in
threat from
previous quarter

Advertised IAB Access into Manufacturing Organizations by Quarter



Source: ZeroFox Intelligence

BOTNETS

The botnet threat to manufacturing companies remained consistent with previous quarters, continuing to pose a significant threat to both Operational Technology and Information Technology systems by stealing credentials and remotely controlling the infected device.[14] In Q3 2022, ZeroFox Intelligence ingested almost 45 million credentials harvested by infostealer families commonly deployed by botnets, of which RedLine was most active.[15] Manufacturing organizations should be wary of being targeted directly or having systems leveraged in politically-motivated Distributed Denial of Service (DDoS) attacks, such as those seen against Taiwan and much of Europe.[16,17] Emotet's continued resurgence should be of considerable concern; it has reportedly infected almost 1.3 million devices since the start of 2022, including manufacturing organizations, and is now pushing Quantum and BlackCat ransomware.[18]

> Forward Look:

- The threat of manufacturing organizations' systems being targeted or leveraged in botnet attacks by Russia-aligned entities is likely to increase.
- Emotet is expected to pose an increasing threat to manufacturing organizations in the coming months given its resurgence.

> Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate network and infrastructure IOCs of interest, including C2 Domains and Compromised Account Credentials.

No notable
change in
threat from
previous quarter

FOOTNOTES

- [9] ZeroFox Intelligence Internal Collections
 [10] <https://www.bleepingcomputer.com/news/security/attack-weapons-pls-to-hack/>
 [11] <https://www.bleepingcomputer.com/news/security/adware-on-google-play-and-apple-store-installed-13-million-times/>
 [12] <https://www.bleepingcomputer.com/news/security/password-recovery-tool-infects-industrial-systems-with-sality-malware/>
 [13] ZeroFox Intelligence Internal Collections
 [14] <https://www.reuters.com/world/asia-pacific/taiwan-defence-ministry-website-hit-by-cyber-attacks-amid-china-tensions-2022-08-04/>
 [15] <https://www.bleepingcomputer.com/news/security/password-recovery-tool-infects-industrial-systems-with-sality-malware/>
 [16] <https://www.bleepingcomputer.com/news/security/password-recovery-tool-infects-industrial-systems-with-sality-malware/>
 [17] <https://www.bleepingcomputer.com/news/security/password-recovery-tool-infects-industrial-systems-with-sality-malware/>
 [18] <https://www.bleepingcomputer.com/news/security/password-recovery-tool-infects-industrial-systems-with-sality-malware/>

RANSOMWARE

The threat to the manufacturing sector in Q3 2022 from ransomware and digital extortion likely slightly reduced in Q3 2022. Attacks continued on a downward trajectory and remained below 2021 levels, likely caused in part by difficulty eliciting payments from victims.[19] However, ZeroFox Intelligence observed an increase in attacks against “big game” manufacturing organizations, which were notably conducted by a broad range of threat actors[20,21]. Incidents this quarter also highlight the high threat of attacks against third-party providers that could impact downstream manufacturing customers.[22] Manufacturing supply chains are most at risk from ransomware and digital extortion, with threat actors very likely believing that the pressure from downstream dependents will make targets more susceptible to paying ransoms. The supply chain threat is compounded by developments in extortion tactics, with ALPHV/BlackCat providing leaked victim data in a searchable format.[23] The updating of exfiltration tool Exmattered with data corruption functionality indicates a possible move towards ransomware gangs destroying data rather than encrypting it, using the exfiltrated copies as the means of recovering data.[24]

LockBit remained the sector’s primary digital extortion threat; it was responsible for over 40 percent of Q3 2022 attacks. Black Basta, flagged as a Q2 2022 emerging actor, continued its upward trajectory with successful, high-profile attacks. Security teams should be wary of updated versions of strains that frequently target the sector and their associated IOCs, including Hive—as well as the unusually high number of new strains identified this quarter.[25] In coming months, the industry is likely to see an increase in politically-motivated targeting by extortion collectives. If or when Russia’s focus shifts towards political opponents, destructive extortion attacks will likely increase against European-centric manufacturing supply chains, particularly relating to energy, defense, and other critical sectors.

Forward Look:

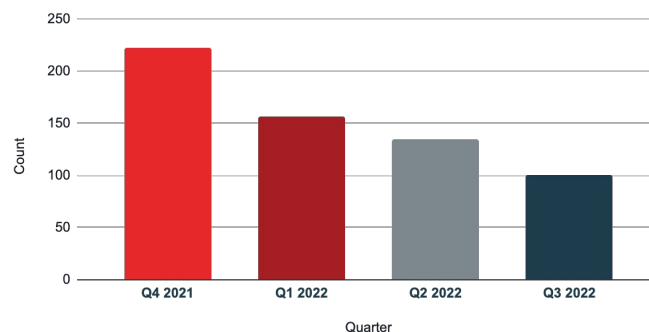
- The threat of digital extortion to manufacturing organizations will most likely increase.
- Threat actors may resort to more extreme pressure tactics to elicit payment from victims that cause greater operational downtime, reputational damage, and legal ramifications.

Recommendations:

- Utilize the ZeroFox Platform’s Intelligence Search interface to investigate IOCs and metadata related to Malware and Ransomware.
- Should an organization be impacted by a ransomware event, engage ZeroFox Intelligence for support.

Indication of decrease in threat from previous quarter

Total Manufacturing Sector Ransomware and Digital Extortion Events by Quarter



Source: ZeroFox Intelligence

QUARTERLY SPOTLIGHT

Organizations must adapt their approach to security as threat actors pivot to circumvent or intercept MFA. Weak MFA methods such as SMS verification codes have long been exploited by threat actors to compromise enterprise systems. However, analysis indicates an increase in recent months of threat actors leveraging phishing techniques where traditionally-strong MFA gives little or no protection. These techniques include AiTM phishing, MFA fatigue, or spamming—as encouraged by Lapsus\$—and OAuth Consent phishing attempts, which are all techniques that are included in widely-distributed phishing kits.

Phishing-resistant MFA attempts to limit a corporation’s risk of social engineering attacks and should be implemented in conjunction with a broader Zero Trust initiative.

ZeroFox Intelligence recommends implementing phishing-resistant MFA methods that support Fast ID Online v2.0 (FIDO2) and certificate-based authentication.[26] FIDO2 aims to maximize security with minimal impact on user experience. It supports passwordless, two-factor, and multi-factor user authentication with embedded or external authenticators. All FIDO protocols are based on Public Key Infrastructure.

While phishing-resistant MFA will not protect against all attacks, ZeroFox Intelligence has yet to observe threat actors on the deep and dark web publishing or brokering exploits related to phishing-resistant MFA.[27]

FOOTNOTES

[19] ZeroFox Intelligence Internal Collections

[20] <https://www.bleepingcomputer.com/news/security/building-materials-giant-knauf-hit-by-black-basta-ransomware-gang/>

[21] <https://www.securityweek.com/power-electronics-manufacturer-semikron-targeted-ransomware-attack>

[22] <https://www.cpomagazine.com/cyber-security/identity-management-firm-entrust-suffers-a-security-breach-ransomware-gang-obtains-files/>

[23] <https://blog.cyble.com/2022/07/06/alphv-ransomware-expands-its-arsenal-of-extortion-techniques/>

[24] <https://securityaffairs.co/wordpress/136226/cyber-crime/exmattered-tool-shift-extortion-tactics.html>

[25] New strains identified include Lilith, Cheers, Yanluowang, Omega, RedAlert, BianLian, Royal, Monster, Agenda, and PlayCrypt.

[26] <https://fidoalliance.org/specifications/>

[27] ZeroFox Intelligence identified an academic paper that describes a potential weakness in FIDO UAF that could allow threat actors to bypass verification if they have a malware implant.

OUTLOOK

ZeroFox Intelligence assesses the threats facing the manufacturing sector will more likely than not develop significantly over the next two quarters. The landscape will almost certainly be shaped by Russia's war in Ukraine, the trade dispute between China and the United States, and worsening global economic conditions. Attacks in Q3 2022 highlighted the fragility of manufacturing supply chains. As the Northern Hemisphere enters winter, Russia will likely increasingly seek to target Western manufacturing supply chains, including supply to the Energy sector and other critical industries.

Manufacturing organizations should expect to be increasingly targeted via third-party providers, particularly those afforded trusted access within a network. Threat actors will very likely increasingly seek to bypass MFA to compromise corporate environments, including targeting authentication providers. Vulnerabilities in cloud infrastructures and commonly-used software modules will likely continue to dominate the exploit landscape. Manufacturing organizations should prioritize replacing end-of-life products, including in OT infrastructure.

ZeroFox Intelligence anticipates a continued increase in IABs leveraging private means of communication to sell access, as well as leveraging trusted relationships with specific buyers. There is no indication the threat will decrease, with buyers still seeking to obtain access via brokers. However, the ability to identify and mitigate access sales ahead of compromise will very likely become increasingly challenging, amplifying the importance of partnerships with third-party security vendors that have access to private channels.

Pro-Russia threat actors and state-linked entities have begun targeting countries and organizations with malware in retaliation for perceived stances taken during the war in Ukraine. ZeroFox Intelligence expects this trend to continue, likely impacting manufacturing organizations in countries perceived as being unsupportive of—or opposed to,—Russia.


ZEROFOX INTELLIGENCE
October 28, 2022

APPENDIX: Traffic Light Protocol for Information Dissemination

TLP: RED

HOW IT IS USED

Sources may use **TLP: RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share **TLP: RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP: AMBER

HOW IT IS USED

Sources may use **TLP: AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share **TLP: AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP: AMBER+STRICT restricts sharing to the organization only.

TLP: GREEN

HOW IT IS USED

Sources may use **TLP: GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share **TLP: GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP: CLEAR

HOW IT IS USED

Sources may use **TLP: CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share **TLP: CLEAR** information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox provides enterprises protection, intelligence, and disruption to dismantle external threats to brands, people, assets, and data across the public attack surface in one comprehensive platform.

With complete global coverage across the surface, deep, and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats, and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages, and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email, and more.

Ready to See for Yourself?

> Request a Demo:

Sign up on zerofox.com/request-a-demo

> Learn More:

Visit zerofox.com

Contact us at sales@zerofox.com / 855.736.1400