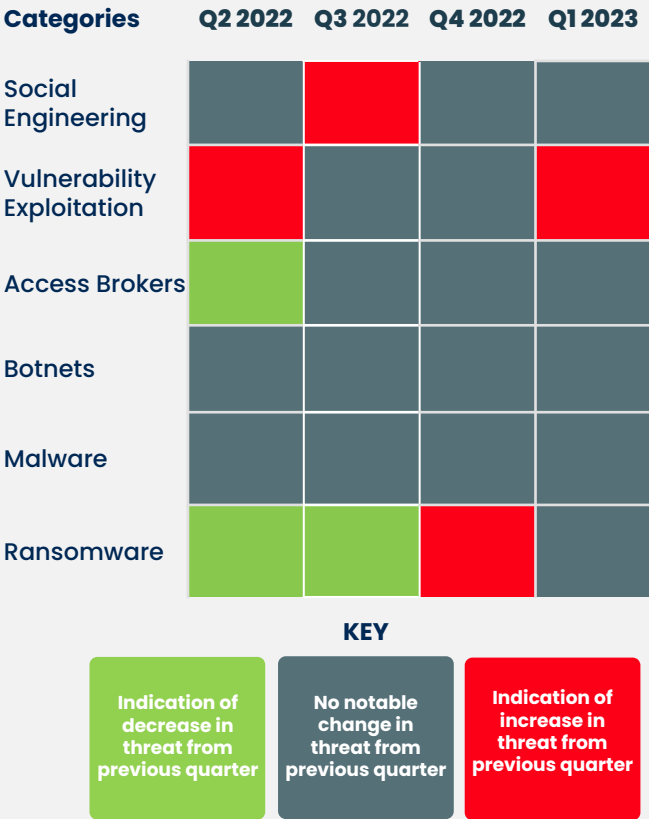


| Key Findings Q1 Manufacturing Sector

- The threat to manufacturing organizations of threat actors exploiting Common Vulnerabilities and Exposures (CVEs) likely increased in Q1 2023. Clop’s successful exploitation of CVE-2023-0669, a zero-day exploit in GoAnywhere MFT file transfer software, resulted in the most incidents in a single month by any extortion collective in ZeroFox Intelligence records. Manufacturing organizations accounted for approximately 12 percent of victims.
- The threat to the manufacturing sector of ransomware and digital extortion likely remained broadly consistent in Q1 2023, following a resurgence in threat actor activity in Q4 2022.
- ZeroFox Intelligence notes early indications of an increase in Search Engine Optimization (SEO) / Search Engine Results Pages (SERP) poisoning and the leveraging of malicious Google advertisement as a means of disseminating malware.
- The overall threat to sector entities from botnets remained broadly consistent in Q1 2023.
- Malware-as-a-service offerings sustained low barriers to entry for threat actors seeking to target manufacturing sector entities.

Manufacturing Sector Threats



| Key Cyber Threats to the Manufacturing Sector in Q1 2023

Ransomware and digital extortion outfits conducting attacks against big-game manufacturing targets and upstream supply chains	Vulnerabilities in commonly-used software modules used by manufacturing organizations leveraged to compromise multiple downstream industry targets
High threats from spear-phishing, smishing, callback phishing, and techniques to bypass Multi-Factor Authentication	Russia-aligned threat actors seeking to target manufacturing entities and disrupt global supply chains
Initial Access Brokers (IABs) selling illicit access to established buyers via private means of communication, making identification and mitigation more difficult	State-aligned threat actors leveraging custom-made malware against industrial control systems
Infostealers and botnets stealing credentials and remotely controlling infected internet-of-things devices	Saturated trojan markets sustaining low barriers to entry and high pace of new Indicators of Compromise (IOCs)

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 April 10, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.



SOCIAL ENGINEERING

ZeroFox Intelligence assesses with low confidence that the threat to manufacturing organizations from social engineering campaigns likely remained broadly consistent in Q1 2023. Sector-specific campaigns very likely remained underreported, but threat actors continued to target employees and customers with spear-phishing approaches, malicious domains, and smishing.[1,2] Industry-agnostic campaigns conducted by actors with a history of targeting manufacturers also remained prevalent.[3,4] Malware distribution via malicious email attachments remained highly prevalent, and there is some indication of an increase in Search Engine Optimization (SEO) / Search Engine Results Pages (SERP) poisoning by strains known to target the sector, including—but not limited to—GootKit, IcedID, BatLoader, RedLine, and Vidar.[5,6,7] ZeroFox Intelligence also notes an increase in malicious campaigns leveraging Google adverts as a means of distributing and delivering malware.[8,9]

Forward Look:

- Manufacturing organizations' employees and customers will very likely continue to face a high threat from spear-phishing, smishing, and malicious domains.
- It is likely the threat to the sector from SEO/SERP poisoning and Google ads will continue on an upward trajectory, particularly if it becomes more difficult to distribute malware via malicious email attachments.

Recommendations:

- Communicate to employees and customers about emerging trends in social engineering scams.
- Leverage ZeroFox Intelligence's Attack Surface Assessment to understand the threats faced.

No notable
change in
threat from
previous quarter

INITIAL ACCESS BROKERS (IABs)

ZeroFox Intelligence assesses with low confidence that there was no significant change in the threat to manufacturers from IABs in Q1 2023.[10] Brokers continued to leverage private channels for selling to well-established buyers, exercising high levels of caution to avoid law enforcement scrutiny. Advert content continued to typically focus on vulnerabilities in remote working infrastructure, including Virtual Private Networks and Remote Desktop Protocol.

Forward Look:

- Threat actors are expected to continue to sell access to manufacturing networks via private communications.
- Upstream supply chains will likely become an increasingly attractive target.

Recommendations:

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

No notable
change in
threat from
previous quarter

VULNERABILITY EXPLOITATION

The threat to manufacturing organizations from nefarious actors exploiting CVEs likely increased in Q1 2023. Exploits in commonly-used software modules and remote working infrastructure continued to dominate the landscape. Clop's January 2023 successful exploitation of CVE-2023-0669, a zero-day exploit in GoAnywhere MFT file transfer software, demonstrated the impact that targeting these CVEs can have; manufacturing organizations accounted for approximately 12 percent of victims.[11] Vulnerabilities in components of manufacturers' products, such as microchips, also remained prevalent.[12] Q1 2023 saw the highest percentage of disclosed vulnerabilities rated critical (18.4 per cent) on record, including in software for Industrial Control Systems manufactured as Contec, Sewio, and Siemens and a critical vulnerability (CVE-2023-1256) affecting human-machine interface (HMI) and SCADA products by Aveva.[13] The Cybersecurity and Infrastructure Security Agency's (CISA) updates to its Known Exploited Vulnerabilities (KEV) catalog included high and critical severity vulnerabilities that almost certainly impact manufacturing sector entities, including exploits impacting iOS operating systems, Google Chrome, Microsoft Windows, and Zoho ManageEngine.[14]

Forward Look:

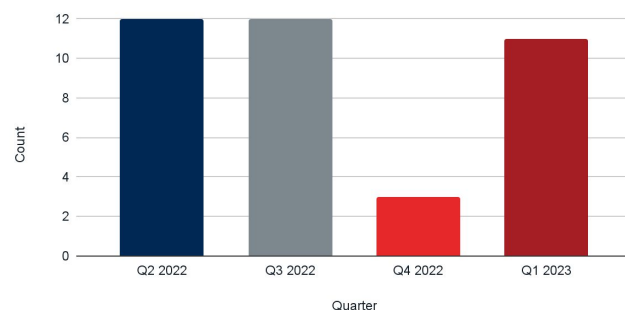
- Vulnerabilities in commonly-used software modules and remote working infrastructure will very likely continue to dominate the exploit landscape.

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.

Indication of
increase in threat
from previous
quarter

Advertised IAB Access into Manufacturing Organizations by Quarter



Source: ZeroFox Intelligence

FOOTNOTES

[1] <https://www.bleepingcomputer.com/news/security/rat-games-receives-ransom-demand-from-hackers-refuses-to-pay/>
[2] <https://techcrunch.com/2023/02/02/okta-employees-are-bought-and-targeting-tech-and-gaming-companies-says-leaked-report/>
[3] <https://securityaffairs.com/140465/malware/icedid-targets-zoom-users.html>
[4] <https://www.bleepingcomputer.com/news/security/over-1-300-fake-anydesk-sites-push-vidar-info-stealing-malware/>
[5] <https://blog.cyblej.com/2023/02/01/qakbots-evolution-continues-with-new-strategies>
[6] <https://www.bleepingcomputer.com/news/security/emotet-malware-now-distributed-in-microsoft-onenote-files-to-evade-defenses/>
[7] ZeroFox Intelligence Internal Collections

[8] <https://www.bleepingcomputer.com/news/security/ransomware-access-brokers-use-google-ads-to-breach-your-network/>
[9] <https://www.bleepingcomputer.com/news/security/bitwarden-password-vaults-targeted-in-google-ads-phishing-attack/>
[10] ZeroFox Intelligence Internal Collections
[11] ZeroFox Intelligence Internal Collections
[12] <https://thehacknews.com/2023/01/qualcomm-chipsets-and-lenovo-bios-get.html>
[13] <https://nvd.nist.gov>
[14] <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



BOTNETS

There was no significant change in the threat to manufacturing organizations from botnets in Q1 2023, which continued to pose a significant threat to both Operational Technology and Information Technology systems by stealing credentials and remotely controlling infected devices. In Q1 2023, ZeroFox Intelligence ingested almost 90 million credentials harvested by infostealer families commonly deployed by botnets, including Vidar, Racoon, Andromeda, and RedLine.[15] With increased use of internet-of- things, Distributed Denial of Service (DDoS) attacks got larger and more complex, but the impact of denial of service remained limited. As seen in Q1 2023, organizations with European operations should be wary of targeting by Russia-aligned groups that launch campaigns against countries deemed unfriendly to Russia.

Forward Look:

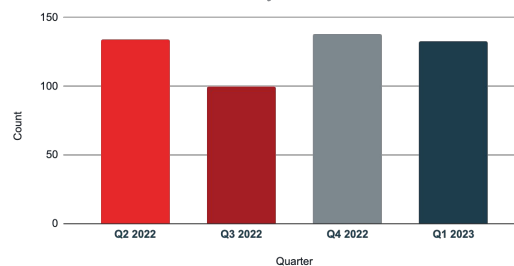
- The threat from botnets is unlikely to change considerably in the near-term. However, those with operations in countries pledging support for Ukraine are likely to face continued high threats from Russia-aligned entities.

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

Total Manufacturing Sector Ransomware and Digital Extortion Events by Quarter



Source: ZeroFox Intelligence

RANSOMWARE

The threat to the manufacturing sector from ransomware and digital extortion likely remained broadly consistent in Q1 2023, following a resurgence in threat actor activity in Q4 2022. Incidents this quarter continued to highlight the high threat of attacks against upstream third-party providers that impact downstream manufacturing customers.[19] Manufacturing supply chains remained most at risk from ransomware and digital extortion, with threat actors continuing to target chip and other component manufacturers in attacks that had a substantial impact further down the chain.[20]

LockBit remained the sector's primary digital extortion threat and was leveraged in almost 50 percent of Q1 2023 attacks. Reductions in attacks leveraging BianLian and Royal strains were offset by significant increases in ALPHV and Clop attacks. In March 2023, the Clop digital extortion collective added 102 victims to its leak site; this was the highest number of digital extortion incidents for a single month in ZeroFox Intelligence's records, and the first month in over a year LockBit has not been the most prolific strain.[21] The manufacturing sector was the third most frequently targeted in Clop's campaign, behind healthcare and technology, respectively.

No notable
change in
threat from
previous quarter

Forward Look:

- ZeroFox Intelligence anticipates a reduction in threat in Q2 2023, with Clop's campaign very likely finishing by April 2023.

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.

No notable
change in
threat from
previous quarter

MALWARE

ZeroFox Intelligence assesses with low confidence that the malware threat to manufacturers in Q3 2022 remained broadly consistent with previous quarters, with no significant change in capabilities observed. For IT systems, malware-as-a-service offerings sustained low barriers to entry, with trojans facilitating the interception of two-factor authentication codes and keystroke recording. The sector almost certainly remained an attractive target for politically-motivated threat actors seeking to steal intellectual property.[16] Prolific malware strains were upgraded with loader capabilities, and threat actors were observed offering services to upload benign applications to mobile app stores to pass security checks—and then offering to update it with malicious code, infecting new and existing installers.[17,18]

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.

FOOTNOTES

- [15] ZeroFox Intelligence Internal Collections
 [16] https://www.symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackfly-espionage-materials?web_view=true
 [17] <https://thehackernews.com/2023/02/gookit-malware-adopts-new-tactics-to.html>
 [18] <https://www.bleepingcomputer.com/news/security/new-iccid-variants-shift-from-bank-fraud-to-malware-delivery/>
 [19] <https://www.infosecurity-magazine.com/news/uk-metal-firm-vesuvius-cyberattack/>
 [20] <https://telecom.economictimes.indiatimes.com/news/chip-equipment-maker-mks-instruments-says-it-is-investigating-ransomware-attack/97660336?redirect=1>
 [21] ZeroFox Intelligence Internal Collections



OUTLOOK

ZeroFox Intelligence assesses the threats facing the manufacturing sector will develop over the next six months. The threat is expected to be heavily influenced by Russia's war in Ukraine. ZeroFox Intelligence anticipates highly capable, pro-Russian threat actors will increasingly direct aggression towards nations, organizations, and supply chains in Western countries they judge are unfriendly toward Russia. ZeroFox Intelligence also anticipates the increased targeting of Asia-based component and manufacturing organizations to disrupt global supply chains.

ZeroFox Intelligence anticipates cyber threats will increase against manufacturing supply chains, with organizations targeted via third-party providers and partners afforded trusted access within a network. While ransomware and digital extortion operations may fall in Q2 2023, incidents will likely remain above 2022 levels, as threat actors are galvanized by recent successes and demonstrate considerable impact by attacking upstream providers. ZeroFox Intelligence anticipates an increase in spear-phishing campaigns aimed at manufacturing organizations' employees, as well as a sustained high threat from smishing and vishing campaigns. Threat actors are also expected to increasingly leverage Artificial Intelligence tools to aid the credibility of their social engineering campaigns.



April 28, 2023

APPENDIX A: ZeroFox Intelligence Probability Scale

All ZeroFox Intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of the occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

APPENDIX B: 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

