

Q2 Energy Sector Quarterly Threat Landscape Scorecard

TLP: CLEAR S-2022-08-19a



Q2 2022 Energy Sector Threat Overview

Threat actors continued to exchange ideas on how to maneuver within the economic and political constraints brought about by the conflict in Ukraine in Q2. Energy sector organizations and their supply chains faced a persistent threat from social engineering campaigns, with particular increases in the use of fraudulent applications, fake Windows 11 upgrades, and employment-related scams to steal credentials and deploy trojans. The threat of vulnerability exploitation grew, averaging almost 70 Common Vulnerabilities and Exposures (CVEs) disclosed per day—up from 56 per day at the end of 2021. The pace of vulnerability disclosure likely represents a new normal. The threat to the energy sector from Initial Access Brokers (IABs) showed small signs of resurgence, though this increase was not seen across all sectors. The threat from malware remained broadly consistent with previous quarters, underpinned by the high rate of new infostealers and trojans emerging and older versions launching new campaigns. Ransomware threat actors may be struggling to elicit payments from victims, driving changes to extortion tactics. Russia is the primary nation-state threat to the energy sector, particularly in Europe. Russia-linked groups will very likely continue targeting the European energy sector and wider supply chain infrastructure in an attempt to weaken their resolve to support Ukraine.

Key Cyber Threats to the Energy Sector in Q2 2022



Vulnerabilities in supply chains and third-party software used by energy organizations and the pace of exploitation



Ransomware and digital extortion outfits conducting attacks against the energy sector and its supply chains



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



Russia-backed and aligned threat actors targeting energy sector entities



Malware disguised in applications targeting employees and customers



State and state-linked actors using custom malware against industrial control systems



Saturated infostealer and trojan markets, with releases of new strains and old strains updating capabilities



State-linked and financially-motivated threat actors targeting key personnel in job-related scams

Energy Sector Threats

Categories	Q1 2022	Q2 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

Q2 Key Findings:

- Cybercriminals are increasingly concerned with challenges converting cryptocurrency to fiat currency.
- Social engineering campaigns increasingly used LNK shortcut files, fake Windows upgrades, and employment scams.
- The threat from CVEs and previously-unknown software vulnerabilities likely increased.
- The IAB marketplace showed signs of resurgence.
- ZeroFox Intelligence assesses with low confidence that the threat of malware deployment against the energy sector increased, driven by pro-Russian entities seeking to take advantage of, and exacerbate, strained supply chains.
- The threat from ransomware and digital extortion likely slightly decreased. Eliciting payment from victims may be getting more difficult.

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 5:00 PM (EDT) on July 28, 2022; per cyber hygiene best practices, caution is advised when clicking on any third-party links.



SOCIAL ENGINEERING

Social engineering campaigns continued to leverage malicious email attachments to target energy sector organizations and their customers, with increased use of LNK files. While the overall threat remained broadly consistent in Q2, ZeroFox Intelligence observed an increase in fraudulent mobile applications, fake Windows 11 upgrades, and employment-related scams to deploy banking trojans and infostealers.

Forward Look:

- Job-related scams will target desirable employees at a high pace, particularly those with elevated access levels.
- Malicious email attachments will continue to be used to disseminate malware.
- Fake mobile applications will increasingly be used to target customers.

Recommendations:

- Communicate to prospective candidates what legitimate job postings look like to get ahead of fake offers.
- Engage ZeroFox Intelligence to conduct an Attack Surface Assessment to understand the threat posed to your organization.

No notable change in threat from previous quarter

INITIAL ACCESS BROKERS (IABs)

The threat to the energy sector from IABs showed signs of a slight resurgence in Q2 2022, though this increase was not seen across all sectors. Organizations with ties to the energy sector remain an attractive target. Disruption to IAB operations is keeping supply below 2021 levels. The IAB landscape is more volatile than other cyber threats; threats often trend against particular industries for a period of time before moving on and spiking against others.

Forward Look:

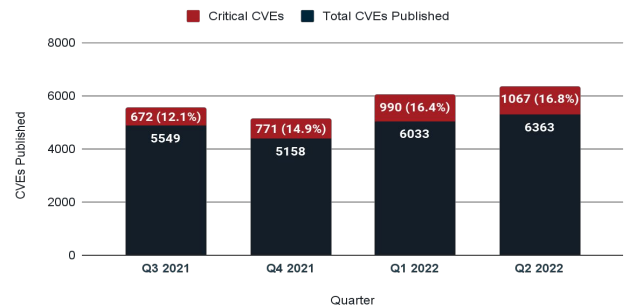
- ZeroFox anticipates a continued increase in IAB operators targeting the energy engineering industry, given the strong demand from ransomware groups. Security teams should be aware that IAB operators could target them directly or indirectly through their business partners and suppliers.

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.

Indication of increase in threat from previous quarter

Total CVEs Published by Quarter



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

VULNERABILITY EXPLOITATION

Energy sector organizations faced an unprecedented threat from disclosed vulnerabilities, particularly in cloud and network perimeter infrastructure—including routers, firewalls, and commonly-used software modules. The importance of efficient patching was magnified by widespread reporting of vulnerabilities, enabling threat actors to rapidly target vulnerable systems.

Forward Look:

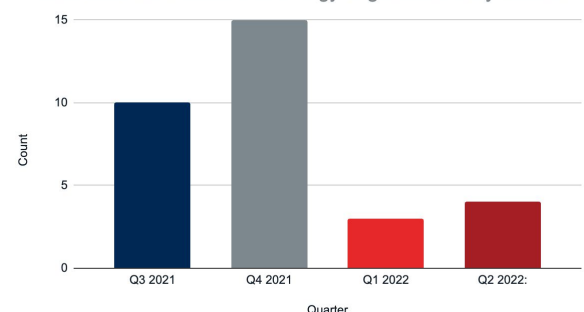
- Vulnerabilities in the cloud and network perimeter infrastructure will likely continue to dominate the exploit landscape.
- The scale and pace of exploit disclosures likely represent a new normal for the vulnerability landscape.

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.

Indication of increase in threat from previous quarter

Advertised IAB Access into Energy Organizations by Quarter



Source: ZeroFox Intelligence

FOOTNOTES

[hXXps://www.bleepingcomputer.com/news/security/cyber-espionage-campaign-targets-renewable-energy-companies/](https://www.bleepingcomputer.com/news/security/cyber-espionage-campaign-targets-renewable-energy-companies/)
[hXXps://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-link-shortcut-files-malware/](https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-link-shortcut-files-malware/)
[hXXps://www.cert.gov.ng/advisories/hackers-using-fake-windows-11-upgrade-to-install-malware-steals-information](https://www.cert.gov.ng/advisories/hackers-using-fake-windows-11-upgrade-to-install-malware-steals-information)
[hXXps://www.bleepingcomputer.com/news/security/microsoft-365-credentials-targeted-in-new-fake-voicemail-campaign/](https://www.bleepingcomputer.com/news/security/microsoft-365-credentials-targeted-in-new-fake-voicemail-campaign/)
[hXXps://www.infosecurity-magazine.com/news/linkedin-impersonated-brand/](https://www.infosecurity-magazine.com/news/linkedin-impersonated-brand/)
[hXXps://nvd.nist.gov](https://nvd.nist.gov)
 ZeroFox Intelligence Internal Collections



BOTNETS

Most organizations around the world saw a negligible change in the threat from botnets in Q2 2022. Russia-aligned groups began targeting entities that vocally opposed the war in Ukraine with botnet attacks, though not at the scale or breadth expected. Botnets deploying infostealers continued to pose a high threat to energy organizations. Organizations in the energy sector should note the resurgence of Emotet, which—at its peak—was one of the largest and most capable botnets in history.

Forward Look:

- Botnets leveraged by Russia-aligned entities could exacerbate geopolitical tensions.
- The resurgence of Emotet indicates it may pose a significant threat to energy organizations and their supply chains in the coming months.

Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate network and infrastructure Indicators of Compromise (IOCs) of interest, including C2 Domains and Compromised Account Credentials. Proactive monitoring of botnet logs provides critical early warning of impending cyberattacks.

No notable change in threat from previous quarter

RANSOMWARE

The threat to the energy sector from ransomware and digital extortion likely slightly reduced in Q2 2022, though attacks appear to have hit harder than those that took place in Q1 2022, particularly against energy equipment manufacturers and supply chains. Despite a fall in the number of attacks, energy remains a frequently targeted sector. However, other sectors saw a resurgence in the frequency of attacks. Threat actors may be struggling to elicit payments from victims, driving changes to extortion tactics.

Forward Look:

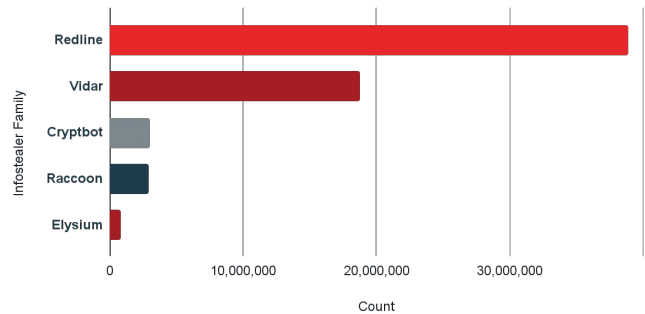
- ZeroFox Intelligence anticipates the threat to energy sector organizations will likely increase.
- Threat actors may resort to more extreme pressure tactics to elicit payment from victims that cause greater operational downtime, reputational damage, and legal ramifications.

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 extortion event, engage ZeroFox Intelligence for support.

Indication of decrease in threat from previous quarter

Q2 2022: Credentials Ingested from Information Stealer Families Commonly Used by Botnets



Source: ZeroFox Intelligence

MALWARE

ZeroFox Intelligence assesses with low confidence that the threat of malware deployment against the energy sector increased in Q2, driven by pro-Russia and Russia-backed entities seeking to take advantage of, and exacerbate, strained supply chains. State and state-linked threat actors continued to leverage custom-made malware to pose a significant threat to industrial control systems (ICS).

Forward Look:

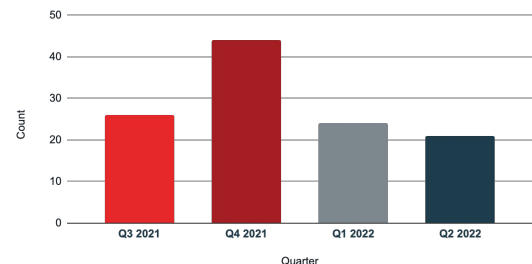
- Energy sector organizations will likely face an increased threat from wipers leveraged by Russia-backed entities.
- Modification to trojans to exploit newly-disclosed vulnerabilities will place greater importance on having a robust patching program.

Recommendations:

- Integrate ZeroFox tactical threat intelligence into your supply chain management and actively engage in third-party monitoring.
- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to malware and ransomware.

Indication of increase in threat from previous quarter

Total Energy Sector Ransomware and Digital Extortion Events by Quarter



Source: ZeroFox Intelligence

FOOTNOTES

ZeroFox Intelligence Internal Collections

[hXXps://www.politico.eu/article/russia-hackers-killnet-attack-lithuania-over-kaliningrad-sanction/](https://www.politico.eu/article/russia-hackers-killnet-attack-lithuania-over-kaliningrad-sanction/)

[hXXps://www.theregister.com/2022/06/10/emotet-malware-chrome-credit-cards/](https://www.theregister.com/2022/06/10/emotet-malware-chrome-credit-cards/)

[hXXps://www.cisa.gov/uscert/ncas/alerts/aa22-103a](https://www.cisa.gov/uscert/ncas/alerts/aa22-103a)

[hXXps://portswigger.net/daily-swig/ransomware-attack-on-montrose-environmental-group-disrupts-lab-testing-services](https://portswigger.net/daily-swig/ransomware-attack-on-montrose-environmental-group-disrupts-lab-testing-services)

[hXXps://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack/](https://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack/)



Quarterly Spotlight

In Russian-language Deep and Dark Web forums, the fate of cryptocurrency and strategies to exchange crypto for fiat currency are increasing concerns, particularly because many cybercriminals see cryptocurrencies as the only means of transferring financial support to Russia. ZeroFox expects cyber actors to pivot and adapt in near real-time to offset temporary disruptions to their financial gains, likely relying on institutions in geopolitically indifferent or supportive countries. They will also very likely continue to seek methods that use stable financial institutions, exchanging rubles for cryptocurrency that can then be converted to hard currency—most likely U.S. dollars—and offshored to non-Russian banks for safety.

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.

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 & 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.

Outlook

Russia's invasion of Ukraine will likely continue to heavily influence the cyber threat landscape. The conflict and resulting humanitarian and economic crises will almost certainly continue to be leveraged by threat actors in social engineering lures. Vulnerabilities in cloud infrastructures, perimeter security devices, and commonly-used software modules will also likely continue to dominate the exploit landscape. ZeroFox Intelligence anticipates pro-Russia threat actors and state-linked entities will likely increasingly target countries and organizations with malware in retaliation for perceived stances taken during the war. If ransomware operators struggle to elicit payments from victims, it is likely they will resort to more extreme pressure tactics, threatening to cause greater operational downtime, reputational damage, and legal ramifications.

ZEROFOX INTELLIGENCE
August 19, 2022

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

