

Q3 Energy Sector

Quarterly Threat Landscape Scorecard

TLP: CLEAR A-2022-11-09b



Q3 2022 Energy Sector Threat Overview

ZeroFox Intelligence assesses that the energy sector saw one of the biggest increases in threat of any sector in Q3 2022, with the ongoing war in Ukraine and subsequent economic crisis continuing to shape the cyber threat landscape. ZeroFox Intelligence assesses that the threat to the sector will continue to increase in the coming months, underpinned by politically-inspired targeting. In Q3 2022, there were likely increases in particular aspects of the social engineering threat to energy organizations, including 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 v2.0 (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 Initial Access Broker (IAB) market, which is underpinning the ransomware and digital extortion threat to energy firms, is shifting towards sales being made in private channels rather than advertising in open forums. This will likely make identifying and mitigating access sales ahead of compromise increasingly challenging. Botnet and malware deployment remained high, including infostealers and trojans. ZeroFox Intelligence has identified an increase in threat from ransomware and digital extortion, bucking a trend seen in other sectors, with a rise in attacks against "big game" energy targets. In coming months, the industry is likely to see an increase in politically-motivated extortion targeting.

Energy 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

Key Cyber Threats to the Energy Sector in Q3 2022



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



IABs selling access via private means of communication, making identification and mitigation more difficult



Ransomware and digital extortion outfits conducting attacks against "big game" energy targets



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



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



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



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



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

Q3 Key Findings:

- Energy organizations likely face an increased threat of smishing, callback phishing (vishing), and phishing techniques that bypass MFA.
- Energy organizations continued to face a high risk of threat actors leveraging exploits in products past end-of-life use.
- IABs likely increasingly sold access to energy firms in the United States and Europe to ransomware operators via private channels, underpinning the increased threat the sector has faced from digital extortion.
- The ransomware and digital extortion threat to the energy sector likely increased, bucking an overall downward trend seen in other sectors.
- ZeroFox Intelligence assesses the threats facing the energy 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 energy sector increased in Q3 2022. Attacks, particularly those by state-linked entities, are very likely underreported. However, it is likely social engineering trends that emerged in campaigns against other sectors in Q3 2022 were also reflected in incidents against the energy sector. Multi-industry social engineering campaigns increasingly leveraged smishing attacks targeting employees, either directly or via enterprise third-party providers.[1] 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.[2] Threat actors increasingly leveraged techniques to bypass MFA, including Adversary-in-the-Middle (AiTM) now being incorporated into broader Phishing-as-a-Service offerings.[3] Malicious email attachments and job scams remained a prominent means of distributing malware to sector organizations.[4]

The threat from social engineering campaigns targeting customers more likely than not increased in Q3 2022, though remained evolutionary rather than revolutionary, indicating that exploiting human error remains lucrative for threat actors. ZeroFox Intelligence identified an increased threat from energy relief scams, which impersonate government programs to assist vulnerable customers with rising energy costs and the resulting strain on household finances.[5] Campaigns typically involve impersonation of energy firms or government bodies in rudimentary phishing emails, text messages, and voice calls. Energy firms should proactively monitor for campaigns targeting customers that impersonate their brand. Energy suppliers 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:

- Threat actors will likely increasingly leverage energy relief scams to target vulnerable customers.
- Smishing of energy 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.

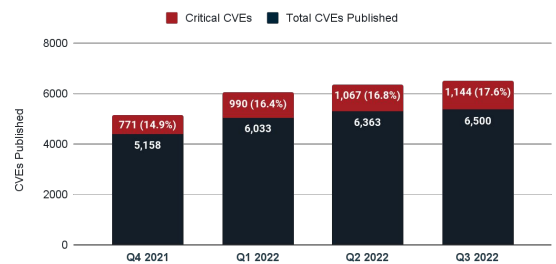
Recommendations:

- 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

Reported incidents of vulnerability exploitation against the energy sector in Q3 2022 continued to center around commonly-used software modules and network perimeter infrastructure. Sustained periods of high-vulnerability disclosures place strain on out-of-cycle patch management processes, with vulnerabilities continuing to be exploited that have long had patches available.[6] New disclosures this quarter impacted Apple operating systems, Atlassian Confluence, Google, Microsoft Windows and Exchange, and Whatsapp.[7] The threat to products past end-of-life use remained high, including in Industrial Control Systems, with vulnerabilities in products added to CISA's Known Exploited Vulnerabilities (KEV) catalog in Q3 2022 that end-users have long been advised to disconnect.[8,9] Threat actors also attempted to exploit Zoho ManageEngine, of which energy organizations are stated to be customers.[10]

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.

12:13



Text Message
Today 07:15

GOVUK: We have identified you as eligible for a discounted energy bill under the Energy Bills Support Scheme. Apply via:

Energy Relief Smishing Campaign

Source:

[hXXps://www.reddit.com/r/Scams/comments/xbfx5t/another_new_one_folks/](https://www.reddit.com/r/Scams/comments/xbfx5t/another_new_one_folks/)

FOOTNOTES

[1] [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)

[2] [hXXps://threatpost.com/callback-phishing-security-firms/80182/](https://threatpost.com/callback-phishing-security-firms/80182/)

[3] [hXXps://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/](https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/)

[4] [hXXps://www.securityweek.com/north-korea-lazarus-targets-energy-firms-three-rats](https://www.securityweek.com/north-korea-lazarus-targets-energy-firms-three-rats)

[5] [hXXps://news.trendmicro.com/2022/09/16/scam-alert-energy-bills-support-scheme/](https://news.trendmicro.com/2022/09/16/scam-alert-energy-bills-support-scheme/)

[6] [hXXps://www.bleepingcomputer.com/news/security/north-korean-lazarus-hackers-take-aim-at-us-energy-providers/](https://www.bleepingcomputer.com/news/security/north-korean-lazarus-hackers-take-aim-at-us-energy-providers/)

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

[8] [hXXps://nvd.nist.gov/feeds/json/cve/2021-38408-cisa-kev-catalogue/#:~:text=CVE%202022%2038408%2C%20affecting,writes%2C%20potentially%20allowing%20code%20execution.](https://nvd.nist.gov/feeds/json/cve/2021-38408-cisa-kev-catalogue/#:~:text=CVE%202022%2038408%2C%20affecting,writes%2C%20potentially%20allowing%20code%20execution.)

[9] [hXXps://www.cisa.gov/known-exploited-vulnerabilities-catalog](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

[10] [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 energy organizations from IABs increased in Q3 2022. The sustained low numbers of advertised access to energy organizations in open forums in Q3 2022 likely reflects an ongoing shift towards brokers preferring private channels to avoid law enforcement scrutiny.[11] According to threat actor chatter observed by ZeroFox Intelligence, brokers are selling to well-established buyers directly out of an abundance of caution. Brokers are likely increasingly selling access to U.S. and European energy firms to ransomware operators with whom they have established relationships via private channels, underpinning the increased threat the sector has faced from digital extortion.

Forward Look:

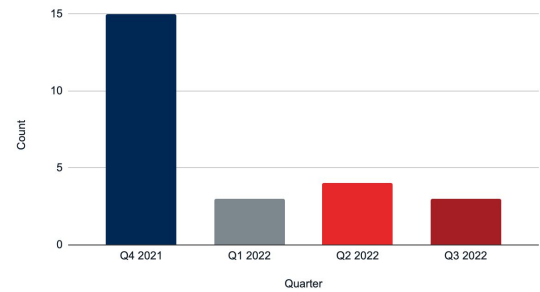
- Illicit access to large energy entities will likely increasingly be sold via private or direct communication methods.

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.

Indication of
increase in threat
from previous
quarter

Advertised IAB Access into Energy Organizations by Quarter



Source: ZeroFox Intelligence

BOTNETS

ZeroFox Intelligence observed no notable change to the botnet threat to energy organizations, which continued to impact both OT and IT systems by stealing credentials and remotely controlling infected devices.[17] In Q3 2022, ZeroFox Intelligence ingested almost 45 million credentials harvested by info-stealer families commonly deployed by botnets, of which RedLine was most active.[18] Energy organizations should be wary of being targeted directly or having their systems leveraged in politically-motivated Distributed Denial of Service (DDoS) attacks, such as those seen against Taiwan and parts of Europe.[19,20] Emotet's resurgence continued, reportedly infecting almost 1.3 million devices since the start of 2022—including energy organizations—and now pushing Quantum and BlackCat ransomware.[21]

Forward Look:

- The threat of energy 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 energy organizations in the coming months.

Recommendations:

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

No notable
change in
threat from
previous quarter

MALWARE

ZeroFox Intelligence assesses with low confidence that the threat to the energy sector from malware 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. Organizations were targeted around the world, with a particular spike against European targets.[12,13] It is not clear whether increased reporting of malware targeting OT infrastructure reflects better coverage or a change in threat.[14] For IT infrastructure, app stores and malicious attachments to emails remained two of the most prolific means of distributing malware.[15] The threat from popular loaders is assessed to have increased, with Bumblebee and Chromelader now deploying some of the most capable malware strains available.[16]

Forward Look:

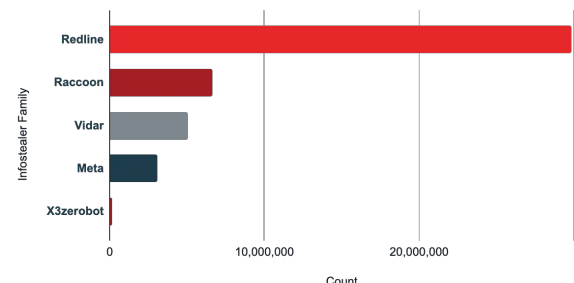
- Malware-as-a-service offerings will very likely sustain low barriers to entry for threat actors.
- Russia-linked threat actors will likely increasingly target energy entities with destructive malware.

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

Q3 2022: Credentials Ingested from Information Stealer Families Commonly Used by Botnets



Source: ZeroFox Intelligence

FOOTNOTES

- [11] ZeroFox Intelligence Internal Collections
 [12] <https://www.cyware.com/news/chinese-apt-targets-energy-firms-in-cyberespionage-campaigns-fe3ec488>
 [13] <https://www.reuters.com/business/energy/hackers-hit-italian-oil-company-tris-computer-networks-bloomberg-news-2022-08-31>
 [14] <https://www.infosecrity-magazine.com/news/new-attack-weapones-pls-to-hack/>
 [15] <https://www.bleepingcomputer.com/news/security/adware-on-google-play-and-apple-store-installed-13-million-times/>
 [16] <https://www.cyware.com/news/chromelader-campaign-spreads-several-malware-04593bd2>
 [17] <https://www.bleepingcomputer.com/news/security/password-recovery-tool-infects-industrial-systems-with-sality-malware/>
 [18] ZeroFox Intelligence Internal Collections
 [19] <https://www.reuters.com/world/asia-pacific/taiwan-defence-ministry-website-hit-by-cyber-attacks-amid-china-tensions-2022-08-04/>
 [20] <https://www.bankinfosecurity.com/lithuanian-energy-firm-experiences-ddos-a-18555>
 [21] <https://www.advintell.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022>

RANSOMWARE

The ransomware and digital extortion threat to the energy sector likely increased in Q3 2022, bucking an overall downward trend seen in other sectors. Attacks remained below 2021 levels, likely caused in part by ongoing difficulty eliciting payments from victims.[22] The rise in threat was underpinned by increased targeting of Europe-based energy organizations, particularly “big game” targets. [23,24] Incidents this quarter also highlight the high threat of attacks against third-party providers that could impact downstream energy customers.[25]

Energy manufacturing supply chains face a high threat, 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—one of the most prolific targeters of the energy sector—providing leaked victim data in a searchable format.[26,27] While not a novel tactic, LockBit announced a move into conducting DDoS attacks against victims as a pressure tactic, which may see other groups adopt similar methods.[28] The updating of exfiltration tool Exmatter 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.[29]

LockBit remained the sector’s primary digital extortion threat, responsible for more than one third of attacks in Q3 2022. Security teams should also be wary of updated versions of other ransomware 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.[30]

In coming months, the sector is likely to see an increase in politically-motivated targeting by extortion collectives and state-backed entities. If or when Russia’s focus shifts towards political opponents, destructive extortion attacks will likely increase against European energy supply chains.

Forward Look:

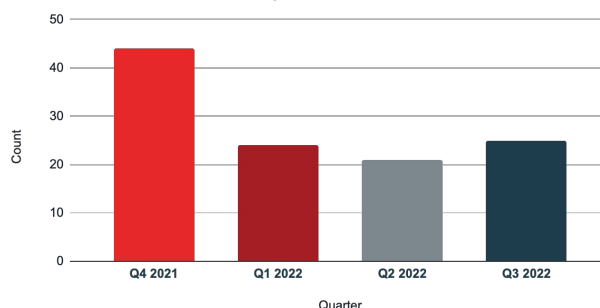
- The threat of digital extortion to energy organizations will most likely increase.
- Threat actors may resort to more extreme pressure tactics to elicit payment from victims that cause greater operational downtime, reputational damage, and legal ramifications.

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 increase in threat from previous quarter

Total Energy 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.[31] 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.[32]

FOOTNOTES

[22] ZeroFox Intelligence Internal Collections

[23] <https://www.securityweek.com/ransomware-gang-leaks-data-allegedly-stolen-greek-gas-supplier>

[24] <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-european-gas-pipeline/>

[25] <https://www.cpmagazine.com/cyber-security/identity-management-firm-enruster-suffers-a-security-breach-ransomware-gang-obtains-files/>

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

[27] <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-italian-energy-agency/>

[28] <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/>

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

[30] New ransomware strains identified in Q3 2022 include Lilith, Cheers, Yanluowang, Omega, RedAlert, BianLian, Royal, Monster, Agenda, and PlayCrypt.

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

[32] 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 threat to the energy sector will likely increase significantly over the next two quarters. The landscape will almost certainly be shaped by Russia's war in Ukraine and worsening global economic conditions. As the Northern Hemisphere enters winter, Russia and state-aligned entities will likely increasingly seek to target Western energy supply chains, including the renewables sector. 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 energy organizations in countries attempting to shift dependence away from Russian energy supply.

Social engineering scams targeting customers will almost certainly remain evolutionary rather than revolutionary, and an increase in energy relief scams is anticipated. Energy 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 infrastructure and commonly-used software modules will likely continue to dominate the exploit landscape. Energy organizations should prioritize replacing end-of-life products, including in OT infrastructure.

ZeroFox Intelligence anticipates the IAB market will continue to sustain a high threat to the energy sector from ransomware and digital extortion. IABs are anticipated to continue increasingly 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.


ZEROFOX INTELLIGENCE
November 4, 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