

Q2 Business Insurance

Quarterly Threat Landscape Scorecard

TLP: **CLEAR**

S-2022-10-03a



Business Insurance Cyber Threat Context

The insurance industry remains a lucrative target for malicious actors due to the vast amounts of policy holder information insurers possess. Cybercriminals target personally identifiable information (PII) held by insurers—including Social Security numbers, health and financial records, phone numbers, and addresses—and leverage such data to commit fraudulent activity or sell it to third parties on deep and dark web (DDW) forums. Specifically, organizations that provide business insurance are very likely to be seen as valuable targets within the broader industry. The compromise of a single business insurer could provide access to multiple downstream targets across various sectors and the opportunity to reach and exploit a wider scope of customer bases, enabling follow-on attacks. As a result, business insurance organizations face a host of potential impacts, including data corruption or data theft, business disruption, and reputational damage.

The attack surface within insurance and financial services more broadly continues to expand, as organizations increasingly adopt digital solutions to modernize infrastructure and improve product offerings. This shift, accelerated by the COVID-19 pandemic, has resulted in insurers driving investment in online services such as web and app-based agency portals, live-data tracking deployed on hybrid cloud platforms, and the adoption of automated underwriting and workflow software. While this provides new business capabilities, it also introduces new attack vectors for threat actors. Additionally, many insurance companies remain reliant on outdated and vulnerable IT systems due to the costs associated with modernizing technology and digitizing client records.

The insurance supply chain is complex, with sensitive customer data and PII often being exchanged by various third parties. Most insurers, for example, utilize independent agents to sell and write policies across various lines of business, presenting opportunities for threat actors to exploit weak security practices at multiple points. As insurers and their supply chains embrace big data and advanced analytics that require handling vast amounts of consumer information beyond current levels yet operate on outdated systems, malicious actors will almost certainly continue to view the industry as a prime target for compromising networks and gaining access to valuable data.

Key Findings

- Threat actors remain motivated to target the business insurers and the broader insurance industry to monetize access to client and network data.
- Criminal actors are most likely to use ransomware and digital extortion to extract the greatest monetary value from the data.
- The threat from saturated loader, infostealer, and trojan marketplaces filled with malware designed to target Windows or Linux-based systems remains prevalent.
- Threat actors are also turning their attention to gaps in third-party vendors' security practices to exploit stolen data.
- Social engineering remains the most frequently-reported intrusion vector across the insurance sector in 2022 and is expected to remain so for the foreseeable future.
- Cyber espionage poses a threat to the insurance industry from threat actors—typically nation-state or state-sponsored—seeking a competitive advantage or financial return.

Who is targeting Business Insurance?



Financially-motivated threat actors



Foreign governments / Nation states



Politically-motivated threat actors



Insider threats



Holds valuable data, PII, and intellectual property



Initial foothold to downstream targets



High revenues and large transactions



High level of access into multiple key sector targets

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 September 20, 2022; per cyber hygiene best practices, caution is advised when clicking on any third-party links.



Q2 Business Insurance Quarterly Threat Landscape Scorecard

TLP: CLEAR

S-2022-10-03a



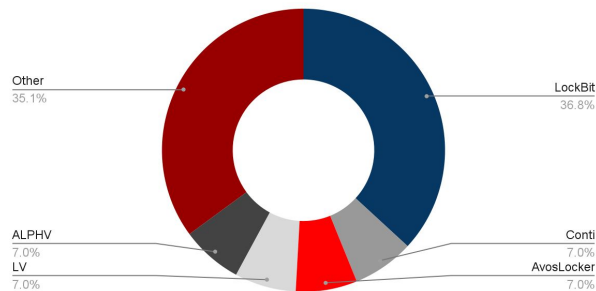
Ransomware

Ransomware and digital extortion pose some of the greatest threats to insurance organizations and their supply chains. Globally, the threat from ransomware has likely reduced in 2022, with a fall in the number of incidents when compared with 2021. However, this likely represents a temporary suppression of the threat, and ZeroFox Intelligence anticipates it will increase in the near future. Ransomware attacks against the insurance industry remain frequent; insurance organizations reportedly experienced a 13 percent increase in attacks in the first quarter of 2022.[1] Many prolific groups have been observed targeting insurance organizations, with a particular focus on firms located in Europe and the United States. Notably, LockBit is currently the most active in targeting the industry by a considerable amount and has been responsible for 36.8 percent of attacks so far in 2022.[2]

ZeroFox Intelligence has identified no evidence to suggest that business insurance is disproportionately targeted by ransomware; within the wider industry, one in five attacks was directed at business insurers in the last 12 months.[3] Nonetheless, financially- and politically-motivated extortionists very likely perceive business insurance firms—particularly those based in Europe and the United States—as attractive targets due to the wealth of PII they hold and often very high revenues of the companies.

Business insurance organizations providing cyber coverage are also likely to be of particular interest to ransomware operators. Compromises of their networks could present threat actors a way to identify and obtain policy details and security standards for cyber insurance customers, which could be leveraged to conduct attacks or tailor ransom demands later down the line. However, only a small number of high-profile, highly-skilled ransomware operators likely have the insight and capability to identify and execute against these specific targets, with most relying on opportunistic targeting.

Groups Most Actively Targeting Insurance (Globally), 2022



Source: ZeroFox Intelligence

Recent changes to threat actor tactics in the post-exploitation stage may indicate that ransomware gangs are finding it increasingly difficult to elicit payments from victims. Threat actors have begun hacking corporate websites to display ransom notes to increase pressure on victims.[4] LockBit began testing a new process in which they gradually reduce the ransom demand, hoping victims that initially refuse to pay may decide it is financially prudent to recover stolen data at a lower price.[5] Should difficulty obtaining ransom payments remain, threat actors may resort to increasingly extreme pressure tactics.

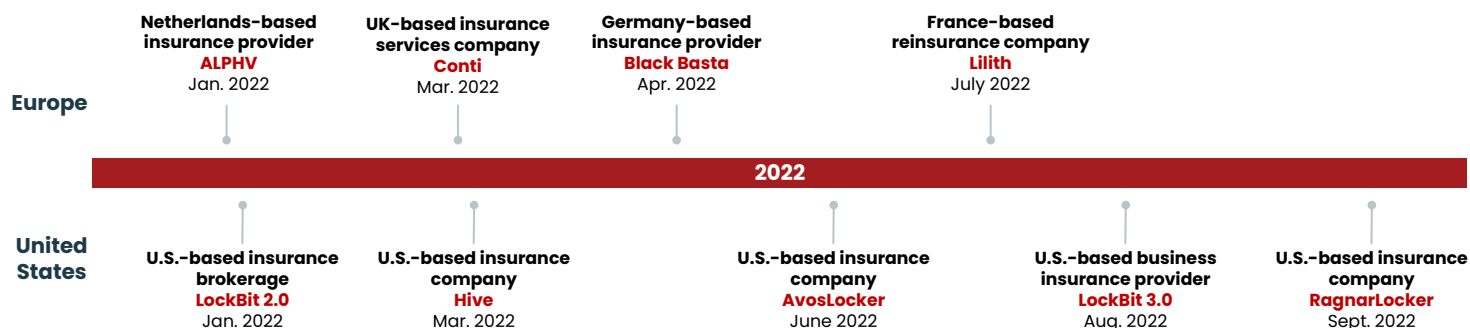
> Forward Look:

- Threat actors may resort to more extreme pressure tactics to elicit payment from victims, causing greater operational downtime, reputational damage, and legal ramifications.

> Recommendations:

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

Selected Ransomware Attacks Impacting Business Insurance, 2022



Source: ZeroFox Intelligence

FOOTNOTES

[1] <https://www.propertycasualty360.com/2022/05/20/most-industries-seeing-relief-from-ransomware-but-insurance-isnt-one/>

[2] ZeroFox Intelligence Internal Collections

[3] Ibid.

[4] <https://www.bleepingcomputer.com/news/security/ransomware-gang-now-hacks-corporate-websites-to-show-ransom-notes/>

[5] ZeroFox Intelligence Internal Collections



Initial Access Brokers

Initial access brokers (IAB) on DDW forums remain motivated to gain network access to insurance firms in a bid to cater to ransomware groups' appetite to strike what they view as a lucrative sector. The IAB ecosystem operates on reputational currency; although motivated by profit, brokers are reluctant to sell access to actors they do not trust or are not vouched for by fellow colleagues in this sphere.

- In August 2022, newer and positively-trending threat actor "69.pdf" advertised Remote Desktop Protocol (RDP) access to an unnamed U.S.-based insurance company with over 40 million clients; the advertisement was closed after only two days, indicating that the actor sold the access and further highlighting the value threat actors place on freshly-acquired customer data and network access associated with insurance companies.

6
By 69.pdf, August 25 in Auctions

69.pdf
byte

6

Paid registration
0 posts
Joined
01/24/22 (ID: 124656)
Activity
хакинг / hacking

Posted August 25
Вид доступа РДП
Insurance + app
Over 40 million clients
Revenue up 50kk
Access to 3 domains
GEO USA
START 15000\$
STEP 1000\$
BLITZ 25000\$
48 Hours

Source: ZeroFox Intelligence

- In July 2022, new and untested threat actor "endrerw" advertised Virtual Private Network (VPN) access with user rights to the internal network of a U.S.-based insurance company that specializes in real estate on the Russian language deep web forum "Exploit." The actor claims the company, which is headquartered in Johnston, Rhode Island, generates USD 5.3 billion annually in revenue.

E
By endrerw, 21 hours ago in Auctions

endrerw
byte

E

Paid registration
0 posts
Joined
07/26/22 (ID: 133938)

Posted 21 hours ago
Транснациональная страховая компания USA, штаб-квартира расположена в Джонстон (Род Айленд). Один из крупнейших страховщиков недвижимости в США. Имеют офисы по всему миру.
VPN
start 3000\$
step 500\$
blitz 10 000
24 часа рапар

Source: ZeroFox Intelligence

In early 2022, threat actors and IABs such as "endrerw" and "69.pdf" experienced renewed demand for services in Russian-language forums following a lull after the criminal space reeled from the Colonial Pipeline attack, with forum admins wanting to avoid increased scrutiny from international law enforcement and researchers.

> Forward Look:

- ZeroFox anticipates a continued increase in IAB operators targeting the insurance 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:

- Subscribe to the ZeroFox Advanced Web Search and Dark Ops Curated Intelligence for early warnings and indicators of threat actor chatter regarding your brand.
- Employ ZeroFox's 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.



Social Engineering

Social engineering remains the most frequently-reported intrusion vector across the insurance industry and is expected to remain so for the foreseeable future.[6] Campaigns are highly effective, enabling threat actors to steal credentials, deploy follow-on payloads, and conduct financial fraud. Business insurance companies likely face a higher threat than other organizations within the industry, as the compromise of a single target could enable access to downstream customers across various sectors.

Social engineering campaigns remain evolutionary rather than revolutionary. Threat actors targeting insurance are most likely to leverage topical lures, such as the war in Ukraine, and encourage employees to enter credentials in phishing domains or to execute malicious attachments to emails. Campaigns are increasingly becoming more focused in their approach rather than leveraging traditional “spray-and-pray” tactics. As long as campaigns are effective and highly cost-efficient, threat actors have little incentive to change tactics.

Trends seen across the global landscape are likely reflected across the broader insurance industry and its supply chains. Campaigns targeting hiring managers, job-seekers, and key personnel in employment-related scams are increasing in 2022, facilitating financial loss, malware deployment, and obtaining privileged access. There has also been an increase in fake Windows 11 upgrades used to deploy malware, such as remote access trojans and infostealers.

Forward Look:

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

Recommendations:

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

Cyber Espionage

Cyber espionage poses a significant threat to insurance organizations by threat actors—typically nation-state or state-sponsored—seeking a competitive advantage or financial return. Cyber espionage campaigns offer a low-risk, high-reward option for threat actors targeting PII and Intellectual Property, including research and development plans, internal processes, investment opportunities, and other forms of proprietary information.

Within the insurance industry, state-backed actors will almost certainly target the wealth of sensitive, client-company information held by insurers. Not only is this information highly valuable and easily monetized, it can also provide sophisticated threat actors the ability to target an insurer’s customers with more tailored forms of social engineering, enabling follow on attacks and allowing them to pivot into other high-value sectors to conduct further espionage.

Attacks that enable cyber espionage are often complex, involving sophisticated techniques that give threat actors the ability to maintain persistent, undetected, and long-term access in compromised environments. Threat actors will typically leverage spear phishing, exploit zero-day vulnerabilities and public-facing applications, and utilize insiders—both hostile and accidental—to deliver malicious payloads. Long dwell times within compromised systems also allows threat actors to assess a victim’s security environment to tailor a disruptive attack appropriately while also studying a target’s defensive posture and the potential for attack obfuscation.

Forward Look:

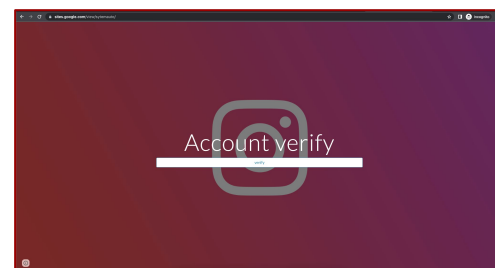
- The insurance industry will almost certainly remain attractive to state-backed actors given its role in handling vast amounts of PII and the potential for accessing multiple downstream targets.

Recommendations:

- Proactively monitor for potential network access sales to obtain critical early warning of an impending cyberattack and help identify malicious actors, including insiders, meaning to harm your network.
- Configure devices with the principle of zero-trust and least privilege.

Case Study: Phishing Campaign Targets Insurance Company Using Social Media Impersonation

In January 2022, a sophisticated phishing campaign attempted to steal login credentials from employees of a prominent U.S. insurance company via malicious emails.[7] The email body stated that the recipient had been reported for activity that violated Instagram’s copyright laws and attempted to create a sense of urgency to click the link within a time limit of 24 hours. Upon engaging the link, the user was taken to a spoofed, Instagram-branded “Account Verify” landing page, followed by an “Account Verification Form” where the user was prompted to enter credentials. To create a sense of legitimacy and trust, every stage included convincing Meta and Instagram branding. Phishing attacks are often rudimentary yet remain highly effective, and the successful targeting of a negligent insurance company employee could grant threat actors a platform through which to exploit multiple downstream targets.



Spoofed landing page containing malicious link

FOOTNOTES

[6] [hXXps://www.ibm\[.\]com/downloads/cas/ADLMYLAZ](https://www.ibm.com/downloads/cas/ADLMYLAZ)

[7] [hXXps://threatpost\[.\]com/phony-instagram-support-staff-emails-hit-insurance-company/178929/](https://threatpost[.]com/phony-instagram-support-staff-emails-hit-insurance-company/178929/)



Malware

ZeroFox Intelligence assesses with low confidence that the threat of malware deployment against the insurance industry in 2022 has increased in line with the broader financial sector. Malware deployment across the landscape has remained highly prevalent throughout 2022, and ZeroFox Intelligence expects that to continue given ease of acquisition and impact on end users. While infection rates remained high, ZeroFox Intelligence has observed no significant changes in malware capability.

IT infrastructure faces the greatest threat, with saturated loader, infostealer, and trojan marketplaces filled with malware designed to target Windows or Linux-based systems. The threat is unlikely to reduce in the near term given the ease of acquisition and potential impact, with Malware-as-a-service (MaaS) models maintaining low barriers to entry. The proliferation of mobile malware remains on an upward trajectory as a means to both steal passwords, banking information, and other sensitive user information and to intercept multi-factor authentication codes. Dissemination of malware via fake apps on application marketplaces also continues to rise, increasing the potential risk for those that use personal devices professionally.

> Forward Look:

- MaaS offerings will very likely sustain low barriers to entry for threat actors and drive down the price of acquiring highly-capable malware.
- Threat actors operating the most effective trojans will almost certainly continue to rapidly update capabilities to take advantage of vulnerabilities in widely-used software, placing increased importance on having a comprehensive and efficient patching program.

> Recommendations:

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

Botnets and Denial of Service

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 threat to insurance organizations. Insurance organizations should note Emotet's resurgence, which—at its peak—was one of the largest and most capable botnets in history.

Botnets pose a significant threat to business insurance organizations on at least two key fronts: stealing credentials and remotely controlling the infected device. Once a device is infected by malware and forced into being part of a botnet, the malware harvests credentials—including from Internet-of-Things (IoT) devices. Credentials harvested by botnet operators are often sold or traded on the DDW for a profit and reused by extortion groups to gain initial access inside a corporate network. Botnet infections that leak employee credentials are part of the initial stage before a corporation falls victim to a ransomware event.

Threat actors commonly leverage infected devices for Distributed Denial of Service (DDoS) attacks. Insurance organizations themselves are frequently targeted by such attacks; collectively, the industry experienced a 257 percent increase in DDoS attacks during the second half of 2021.[8] This includes ransom DDoS (RDDoS), in which malicious actors threaten organizations with persistent DDoS attacks unless an extortion demand is paid. Many ransomware and extortion collectives also frequently leverage DDoS attacks along with double and triple extortion tactics to increase pressure on victims to fulfil ransom demands.

> Forward Look:

- Expansion of the botnet market will continue with new botnets emerging to target web servers, modems, routers, IoT, and Android devices.
- Botnets leveraged by Russia-aligned entities could exacerbate geopolitical tensions.
- The continued resurgence of Emotet indicates it may pose a threat to insurance organizations in the coming months.

> Recommendations:

- Subscribe to the ZeroFox botnet and compromised account alerts to identify any exposure of employee or customer credentials in the wild.
- Utilize the ZeroFox Platform's Intelligence Search interface to investigate network and infrastructure IOCs of interest, including C2 Domains and Compromised Account Credentials. Proactive monitoring of botnet logs provide critical early warning of impending cyberattacks.

FOOTNOTES

[8] <https://www.netscout.com/threatreport/global-ddos-attack-trends/#vertical-industries>



Quarterly Spotlight

In Russian-language DDW 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. We expect 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
September 20, 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

