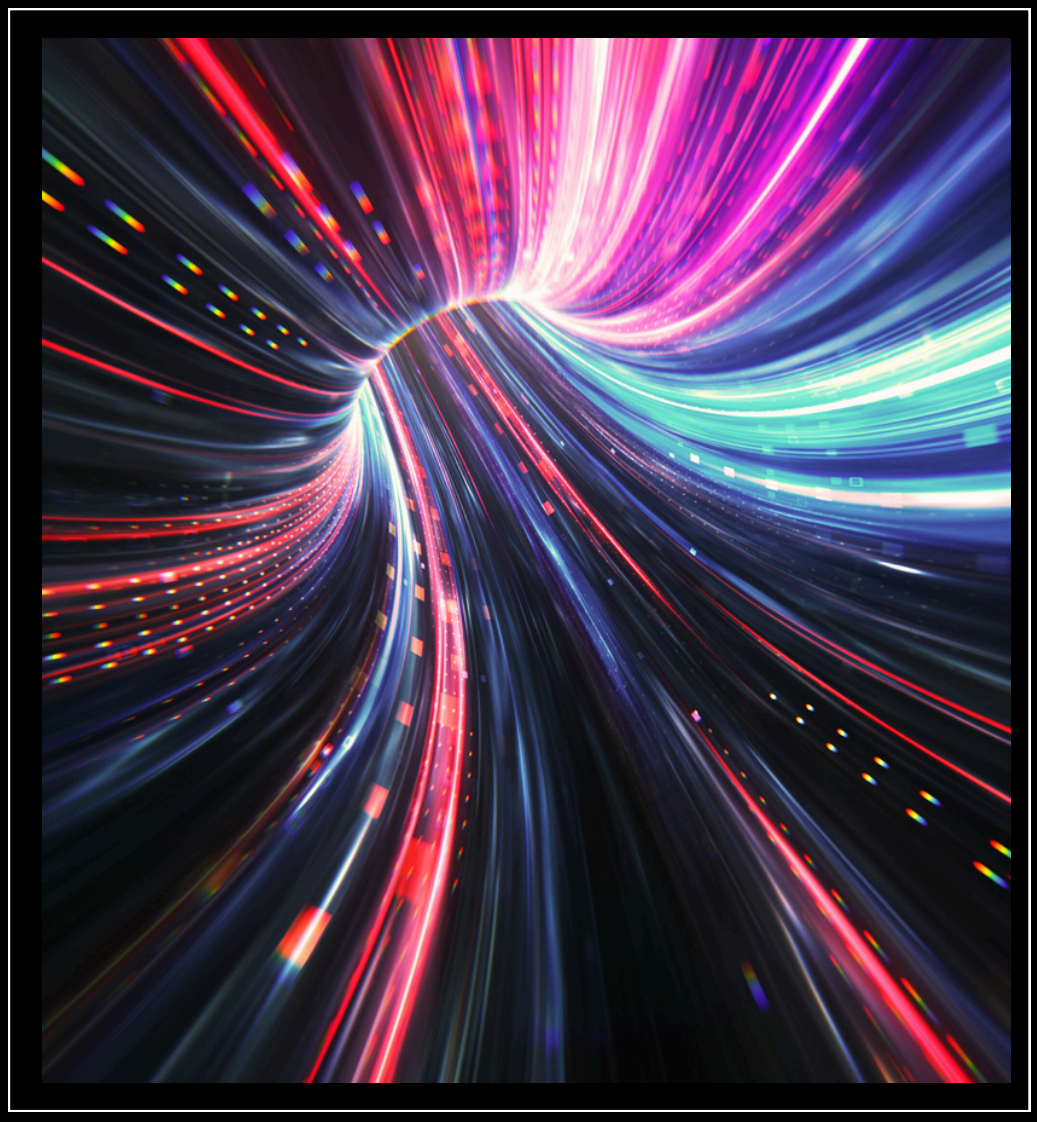

FORTUNE 500 EMPLOYEE-LINKED ACCOUNT EXPOSURE

2022 THROUGH 2024

ENZOIC

WHAT THE NUMBERS SAY ABOUT THE PAST THREE YEARS

A backbone of our economy, Fortune 500 companies employ more than 31 million people worldwide. Over the past three years of 2022, 2023, and 2024, more than three million employee-linked accounts became newly compromised by cybercriminals according to data analyzed by the Enzoic research team– that's 1 in 10 of the current total employees– and the numbers are increasing each year.

DATASET AND METHODOLOGY

This data was collected as part of Enzoic's 24/7 threat monitoring and ingestion operations, and included in our industry-leading dataset of compromised credentials, payment card exposures, and personal identifying information (PII) assets. The credentials analyzed here represent only new, unique usernames added to the dataset during the time period; that is, we do not include or represent data compromised at any point prior to 2022. This allows us to observe a more timely and progressive aspect of the threat landscape, helping to quantify and detail the ongoing and evolving risk to businesses and individuals year-over-year. It also allows us to identify any trends that may be relevant to cybersecurity risk mitigation strategies.

CORPORATE CREDENTIALS: A MULTI-FACETED RISK

Fortune 500 companies face significant security risks from leaked employee email credentials. This risk is amplified when cybercriminals repackage and resell combined breach data from multiple sources, with Enzoic's data showing an average of 5.7 exposures per account for all compromised accounts we've seen. **While companies often lack control over these credential leaks, particularly when employees use corporate email addresses to create personal accounts on third-party services, the impact can be severe.** In addition to account take-over (ATO), fraud, and use as entry vectors for ransomware, these leaked credentials could enable spear phishing attacks, especially dangerous when employees use the same device for both personal and work purposes. The risk increases further when companies allow personal devices to access work resources, though the full extent of this vulnerability remains unknown and warrants additional forensic research from the detection side of cybersecurity data collection to better understand the prevalence of vulnerabilities.

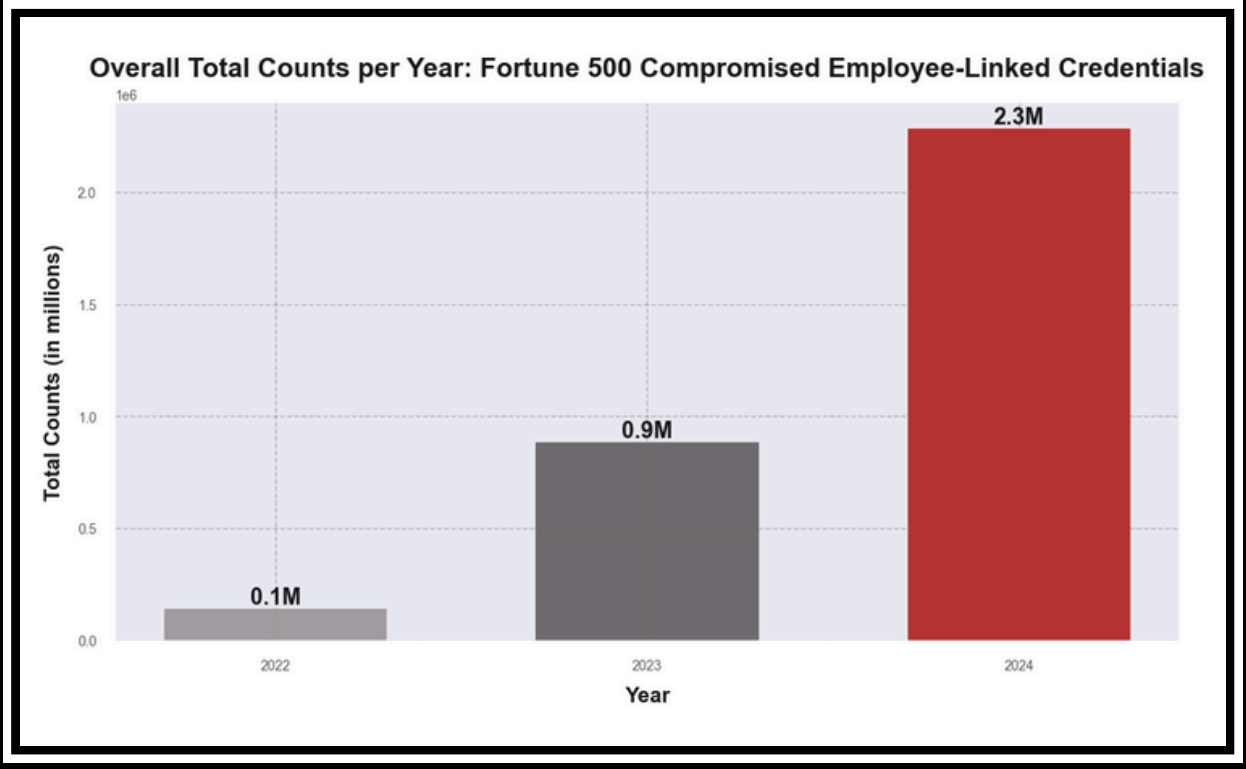

Figure 1 - Massive increases in novel corporate employee account exposure over the past three years.

INDUSTRY ANALYSIS: RISING ACCOUNT COMPROMISE ACROSS ALL SECTORS

A breakdown by industry shows that employee-linked account compromise is increasing in all of the top-ten sectors, with some of the overall largest numbers coming from areas where compromised credentials can seriously impact customers, corporations, and the general public. ‘Commercial Banks’ and ‘Utilities, Gas and Electric’ sectors show the most dramatic increases, with both reaching nearly 120,000 newly exposed accounts per year in 2024. The telecommunications industry's steady rise from around 20,000 to 85,000 compromised accounts per year over this period is particularly noteworthy given their integral role in digital infrastructure. Along with Telecommunications, ‘Internet Services and Retailing’ also emerges as a consistently top compromised business sector. This could be due to the nature of the businesses’ construction from and reliance on digital infrastructure inherently providing a larger attack surface, and thus lower-hanging fruit for threat actors.

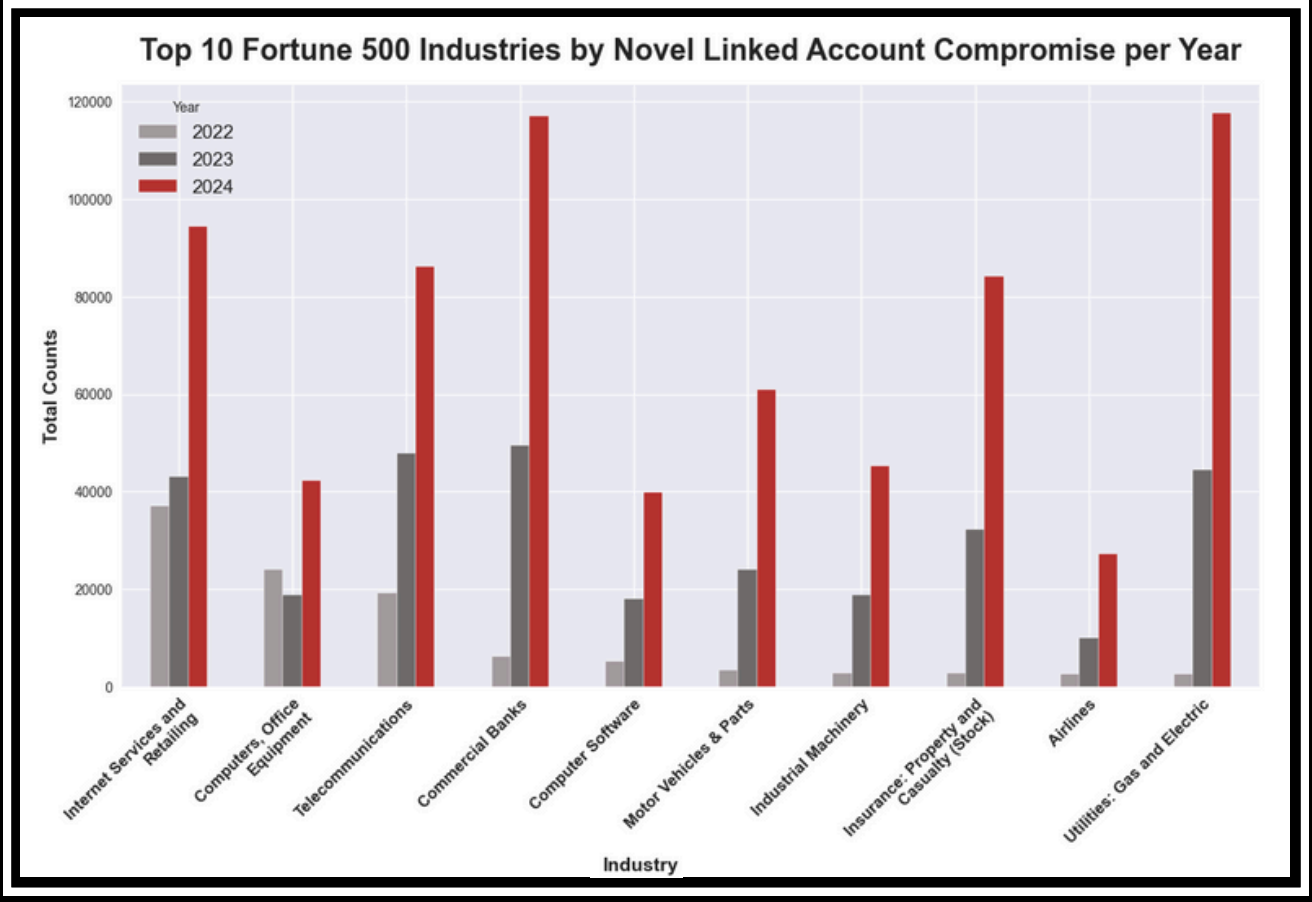

Figure 2 - Increases of account exposure across the top ten industries during the past three years.

Not far behind, we see ‘Commercial Banks’ and ‘Utilities.’ It’s no secret that cybercriminals go where the money is, which makes banking a perennially attractive target. Utilities as a sector has exhibited some of the most rapid growth in compromised employee credentials, corroborating reports of surges in cyberattacks against US-based utilities reported in 2023. The US government has released bulletins and reports for both Water and Energy utilities that discuss how the adoption of internet-connected infrastructure has increased the attack surfaces of utilities[2], and how they are a particularly attractive target due to the critical nature of the services they provide.

‘Utilities’ also emerges as the most highly compromised sector by ratio of compromised accounts to employees; with over 300,000 accounts compromised in the last three years, this exceeds 50% of the total number of employees for Fortune 500 companies in the industry. This suggests grave weaknesses in current cybersecurity postures. Other sectors are not absolved though, with many having more total compromised accounts– and no percentage is an acceptable level of risk, as it only takes one account for a threat actor to gain a foothold.

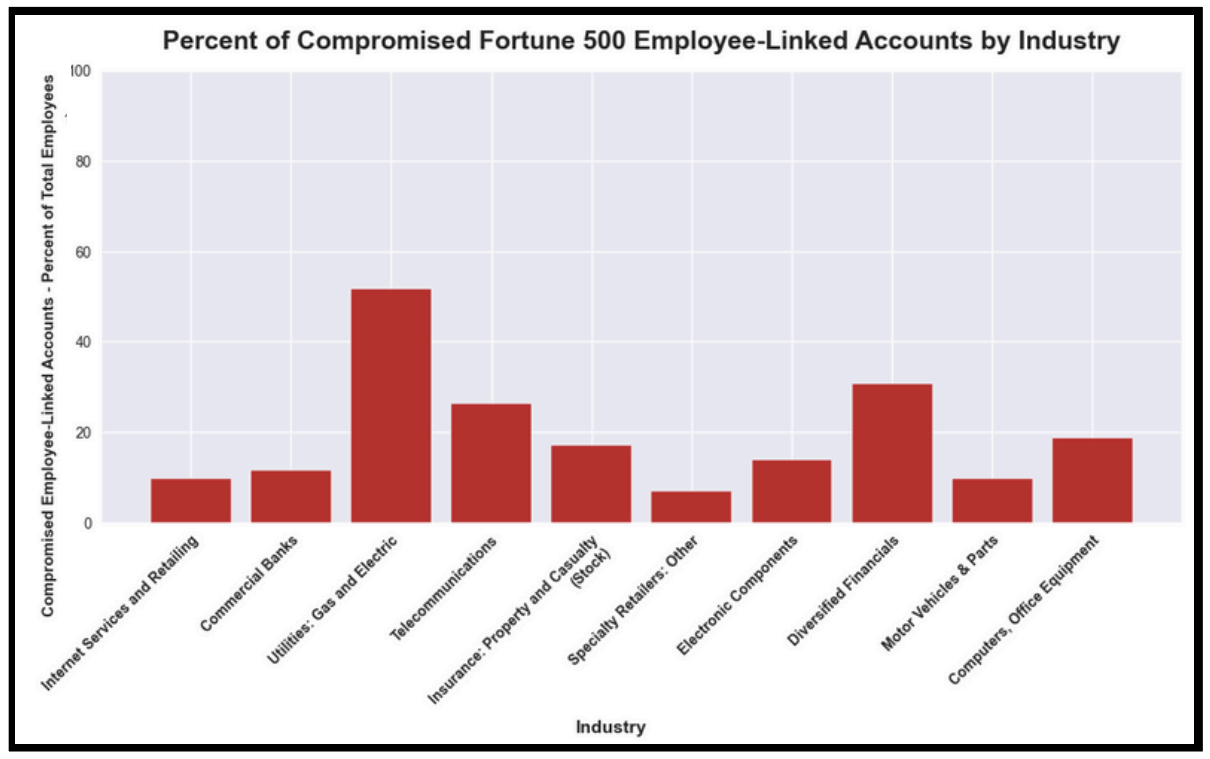

Figure 3 - Some sectors may be more prone to linked account compromise, as the percentages of compromised accounts per total sector employees indicate.

AN ONGOING THREAT: STATISTICS AND TRENDS

The persistent threat of credential compromise poses a noteworthy and measurable risk to Fortune 500 companies, with data suggesting this is not a sporadic issue but rather a steady, ongoing challenge. Our own research over several years with a large mass-market B2B SaaS customer handling hundreds of thousands of logins per month shows 1.48% of the logins each month using credentials known to be compromised- which aligns remarkably well with the 2019 Google/Stanford findings that 1.5% of web-based login attempts involved breached credentials[3], indicating this is a steadfast and systemic vulnerability. This may bear repeating: despite remediation of the exposed credentials, the number of compromised logins remains roughly static. This shows that credential compromise is a dynamic and continuous threat. When combined with the dramatic year-over-year increases in breached email counts across major industries - particularly in sensitive sectors like Commercial Banking and Utilities - this creates a compounding security challenge. The steady drip of new compromise, coupled with the recycling and repackaging of existing breach data by access brokers and data brokers, creates a large and ever-growing circulating corpus of corporate account data that presents a large, continuous source of risk for fraud, ATO, and system intrusion.

→ RISK FOR FRAUD, ATO, AND SYSTEM INTRUSION

AN EPIDEMIC OF INFOSTEALER MALWARE RESHAPES THE THREAT LANDSCAPE

The dramatic surge in compromised accounts across Fortune 500 industries from 2022 to 2024 indicates we may be seeing a fundamental shift in the credential compromise landscape, possibly driven by the rapid proliferation of infostealer malware. The data reveals a particularly stark escalation between 2023 and 2024, with Commercial Banks and Utilities each seeing individual employee account compromise soar to nearly 120,000 emails - roughly triple their 2023 levels. This sharp acceleration aligns with the documented rise of highly efficient infostealer families like Redline, Raccoon, and Vidar[4], which can automatically harvest credentials from infected devices. These malware families have proven highly effective, capturing not just login details but also digital fingerprints and session cookies that can help bypass traditional multi-factor authentication.

THE CONSISTENT PATTERN OF STEEP INCREASES ACROSS ALL TEN TOP SECTORS, RATHER THAN ISOLATED SPIKES IN SPECIFIC INDUSTRIES, SUGGESTS A SYSTEMATIC EXPLOITATION OF CORPORATE CREDENTIALS THAT MATCHES THE WIDESPREAD, DIVERSE, AND INDISCRIMINATE NATURE OF INFOSTEALER ATTACKS.

NOTES ON METHODS AND LIMITATIONS

We do not make any assertion or claim that these companies or their systems have been actively compromised or hacked in any way. Our data indicates only that an account has been seen as part of a compromised credential pair (username and password) that was found in purported breach data or published by threat actors in lists of what they claim are valid accounts. We cannot independently confirm the validity of any given account as an employee account. We used publicly available domain data to indicate which email domains are most highly associated with employees (i.e. instead of customers); for instance, ‘gmail.com’ is a customer domain, and was removed from the dataset prior to analysis, while ‘google.com’ is known to be used by Google employees. Notably, although ‘att.com’ is indicated to be for AT&T employee use, it was also removed from this data as the counts were over 4 times the reported number of AT&T employees, suggesting that the domain was used for other purposes than employee accounts alone (or some other issue, such as threat actors fabricating data).

Our dataset for this study does not include duplicate entries, or instances where an account was found in multiple breaches. For example, if the email address test@company.com was found in 6 datasets, 2 of which had multiple entries for that account (e.g. duplicated lines, or different passwords for the account), it would still be counted only once during this analysis.

Additionally, Enzoic ingests billions of credentials that include usernames that are not email addresses, as some services allow the user to select any string they wish as a login name. As these do not include domains or a verifiable consistent format, we cannot assume them to be linked to any particular company or organization. Thus, any Fortune 500 organization that allows non-email usernames for employees is not represented in this data, and the numbers overall should generally be considered a minimum low-bound of the possible compromised account totals.

[1] https://www.reuters.com/technology/cybersecurity/cyberattacks-us-utilities-surged-70-this-year-says-check-point-2024-09-11/

[2] Water and Wastewater Cybersecurity, US CISA, https://www.cisa.gov/water
Energy Sector, US CISA, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector

[3] Water and Wastewater Cybersecurity, US CISA, https://www.cisa.gov/water Energy Sector, US CISA, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector

[4] For more information: https://www.forbes.com/councils/forbestechcouncil/2023/10/11/unraveling-the-infostealer-threat/