CXO REvolutionaries

EXECUTIVE REPORT

Phishing and Ransomware Insights for the C-Suite

CXO REvolutionaries
QUARTERLY CYBER UPDATE

Q2/2024

SPONSORED BY: zscaler

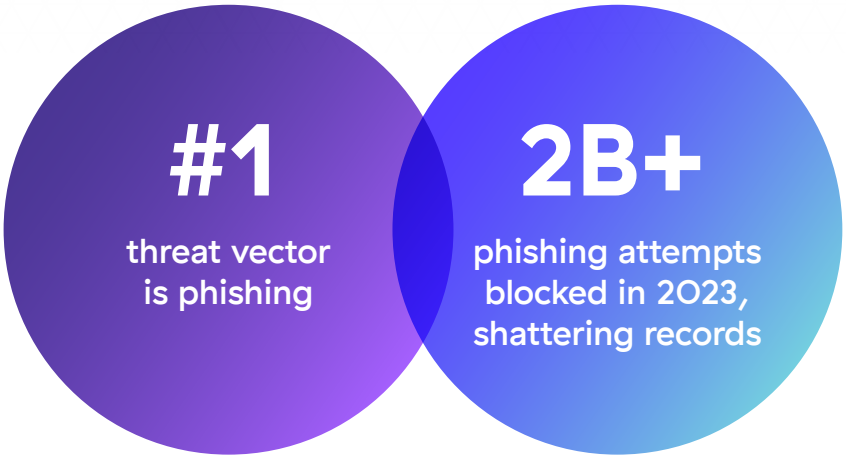
Executive Summary

Skyrocketing cybercrime costs, like the recent **$872+ million** ransomware attack on United Health, makes improving cybersecurity a business imperative for organizational leaders. The CXO REvolutionaries Quarterly Cyber Update provides executives, board members, and public officials like you a view into hot topics and trends in cybersecurity. Our goal is to keep you informed of relevant cyber issues while steering you toward optimal security strategies.

In this issue, we delve into new methods used in two of the most pervasive cybersecurity threats: phishing and ransomware. Our findings are based on data derived from Zscaler **ThreatLabz**[1] annual **ransomware** and **phishing** reports. You'll learn about:

- Three new types of phishing campaigns: brand imitation, referring domains, and job-related scams
- Ransomware variations and impact: double-extortion attacks, the latest tactics and techniques, and global statistics

The Big Picture: Phishing Ramp Up



Phishing

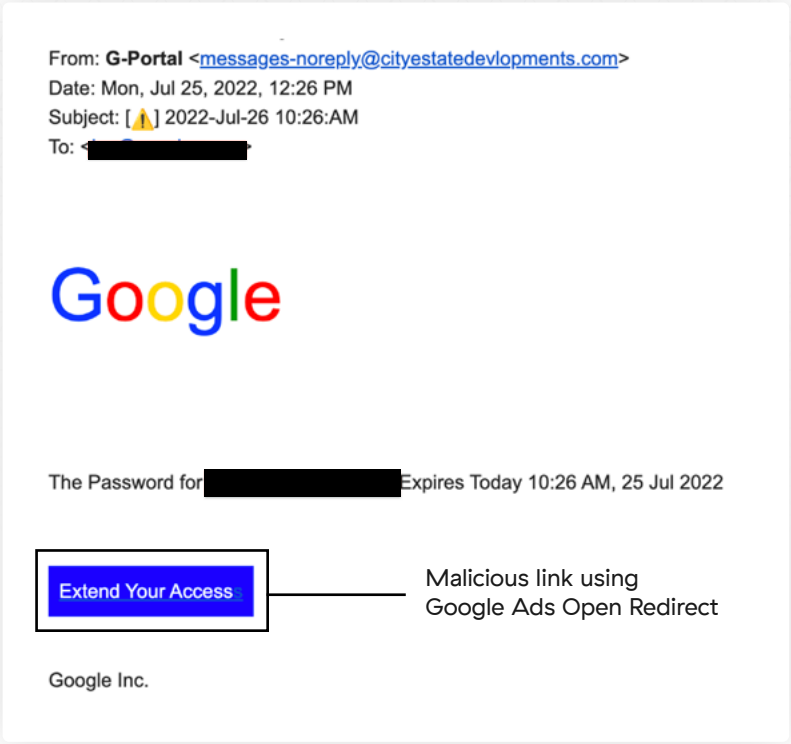
Phishing refers to fraudulent emails sent by cyber attackers to deliver malware or trick recipients into disclosing sensitive data, like credentials or credit card information. Phishing variations include SMS texts (smishing) and voice-deception (vishing) techniques.

[1] All data is derived from Zscaler ThreatLabz reports unless otherwise specified.

New Brands of Phishing: Abusing Trust to Deceive

Phishing is the most common and successful way adversaries gain access into systems and networks. Research from IBM shows that [two out of five security events are initiated by phishing](). Exploiting user trust, appealing to common interests, or leveraging current events are key tactics in today's sophisticated phishing campaigns.

For example, this phishing email impersonating Google asks a user to click a link to reset their password. It suggests that failing to do so will result in the user losing access to Google resources. The "Extend Your Access" button links to an attacker-owned infrastructure that ultimately steals the user's credentials and uses their identity to promote further attacks.



Example of a phishing email with a malicious link impersonating Google

Phishing Prevails and Evolves

"Year-over-year, we continue to see an increase in the number of phishing attacks which are becoming more sophisticated in nature. Threat actors are leveraging phishing kits and AI tools to launch highly effective email, smishing, and vishing campaigns at scale."

— DEEPEN DESAI, GLOBAL CISO AND HEAD OF SECURITY, ZSCALER

With phishing kits and other malicious services sold on the dark web, amateur cybercriminals can launch an attack with minimal investment and technical know-how. Generative AI is also enabling adversaries to craft more convincing, grammatically correct emails to dupe users into surrendering sensitive data or click on malicious links.

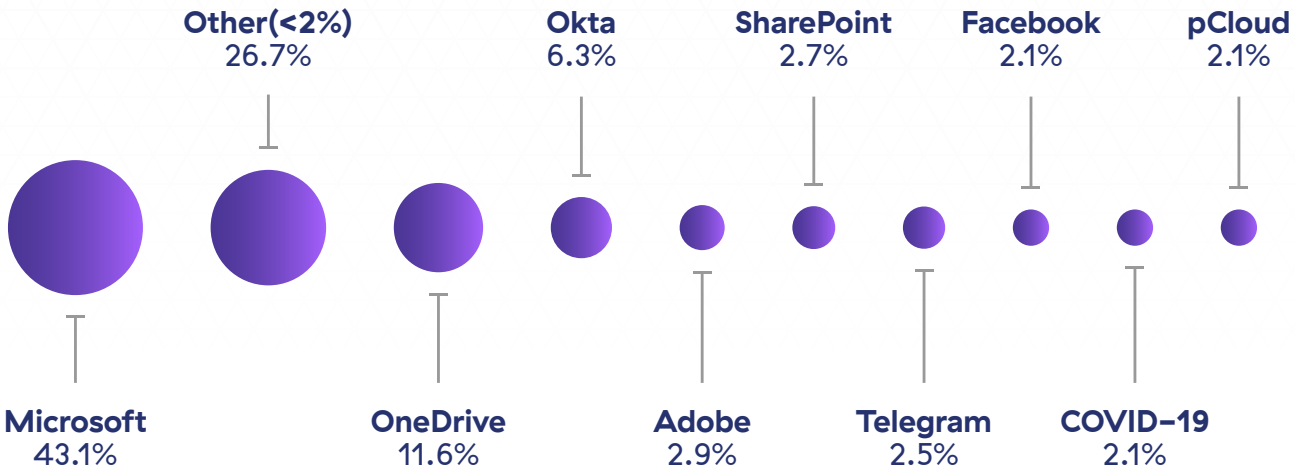
Key findings:

- Attackers are creating phishing emails that look like they come from trusted brands with Microsoft, (Microsoft) OneDrive, and Okta topping the list.
- Threat actors are making their emails appear more legitimate by taking advantage of the reputation scores of backlinked internet domains to bypass security controls.
- Adversaries are targeting job-related sites and services with phishing attacks.

Brand imitation

A popular phishing technique is impersonation of trusted brands, such as Microsoft (especially OneDrive and SharePoint), Okta, social media platforms, and illegal streaming services. Microsoft overall is the most highly impersonated brand, accounting for 43.1% of attacks, followed by OneDrive (Microsoft) and Okta.

Brand names most commonly imitated in phishing attacks



Microsoft, (Microsoft) OneDrive, and Okta were the most imitated brands observed by ThreatLabz

Referring domains

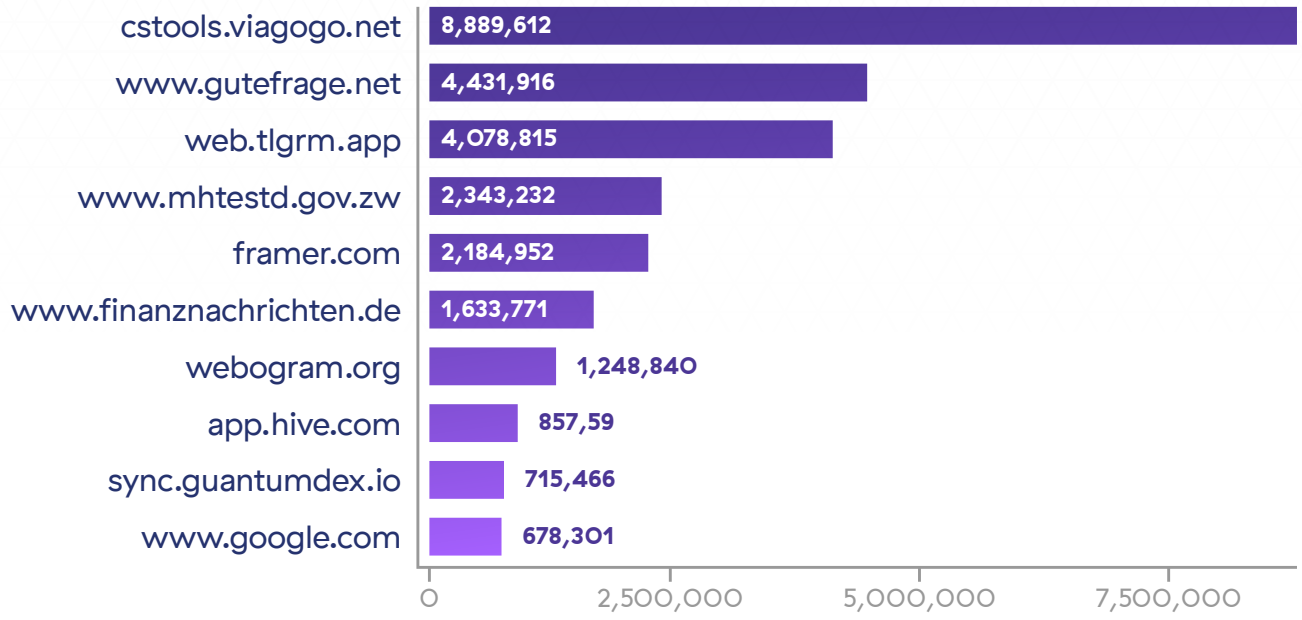
A trusted referring domain is an external website that links back to several other reputable sites to help generate traffic and improve SEO. By routing phishing emails through a trusted referring domain, attackers fly under the radar of ISPs, web service providers, and traditional security controls.

Attackers create or exploit trusted referring domains by:

- Buying ads from media outlets and/or search engines the domain
- Posting domain links in corporate forums and on online marketplaces, such as Walmart or Amazon
- Abusing sharing sites like GitHub, Dropbox, and Evernote

Every backlink a threat actor's domain obtains from an established site elevates the domain's reputation in the digital world. Once an attacker's domain is trusted, it can traffic phishing campaigns without raising red flags. ThreatLabz discovers and tracks referring domains most actively used in phishing campaigns, so you can proactively defend against this threat. In 2023 ThreatLabz blocked over two billion phishing attempts detected in the Zscaler Zero Trust Exchange, millions which came through ten referring domains.

Phishing attempts from the top ten referring domains in 2023



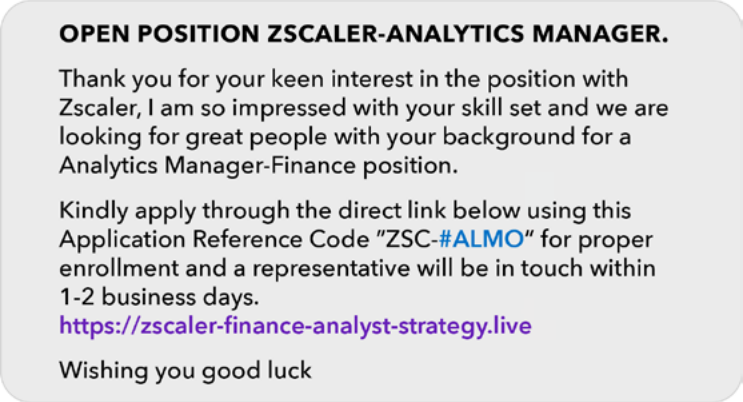
ThreatLabz observed and blocked millions of phishing attempts coming through the top 10 referring domains

Targeting job-seekers

The recent wave of layoffs in technology and other industries has prompted attackers to exploit job seekers. Adversaries are getting people to part with sensitive data through fake job postings, links to online application forms, and fraudulent employment offers.

ThreatLabz recently discovered a malicious job ad on LinkedIn featuring a photo of a recruiter from Zscaler, demonstrating that no brand is immune from phishing exploits.

Clicking on the link takes the applicant to the adversary's site where they are encouraged to fill out a job application. After completing the form, the applicant is asked to verify their identity by uploading a state ID, driver's license, passport picture, and other personally identifiable information (PII). At every step of this attack adversaries exploit the victim's trust while cloaking their malicious activities as legitimate steps in the hiring process.



OPEN POSITION ZSCALER-ANALYTICS MANAGER.

Thank you for your keen interest in the position with Zscaler, I am so impressed with your skill set and we are looking for great people with your background for a Analytics Manager-Finance position.

Kindly apply through the direct link below using this Application Reference Code "ZSC-#ALMO" for proper enrollment and a representative will be in touch within 1-2 business days.
https://zscaler-finance-analyst-strategy.live

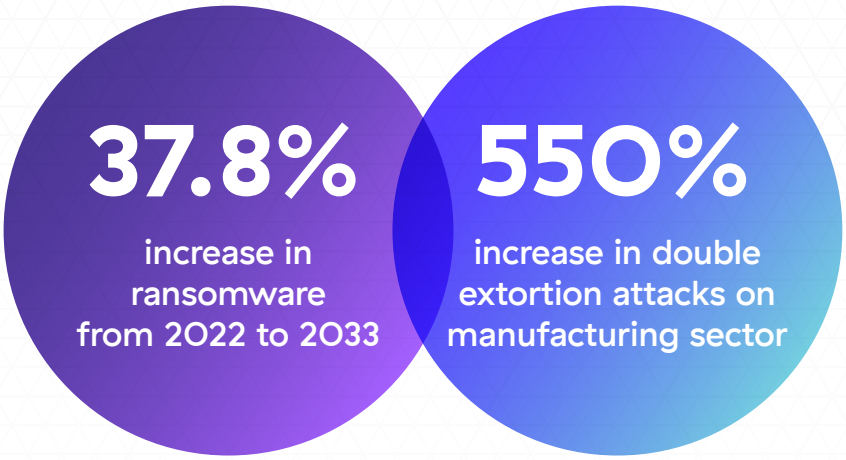
Wishing you good luck

Section Wrap Up

Preventive Measures: Fight Back Against Phishing

ATTACKER TECHNIQUES	YOUR STRATEGIES
Threat actors exploit employment uncertainty to harvest job-seekers' personal data.	• Ensure employee training includes a section on recognizing phishing attacks. • Help other leaders recognize phishing as a significant business risk, and prioritize addressing the problem.
Phishing emails abuse popular brand names and trusted referring domains to boost credibility.	• Discuss the best way to inform employees of job-seeking scams with fellow leaders. • Review the access employees have to job seeking sites and current security processes governing those.
Adversaries use high-reputation domains to traffic phishing emails.	• Discuss with security leadership viable techniques and technologies for detecting malicious traffic from trusted sources.

The Big Picture: Ransomware Ramp Up



Ransomware attacks are on the rise, and they are more ruthless and sophisticated than ever. Total attacks were up 37% in 2023 over the previous year, and the average enterprise ransom payment exceeded $100,000. Last year, several well-known brands and public agencies fell victim to damaging ransomware attacks, highlighting the need for organizations to remain vigilant in 2024.

Key findings:

- The most targeted sectors were manufacturing, services, and construction, likely because they are involved in critical infrastructure and hold highly valued intellectual property.
- Double-extortion ransomware attacks have more than tripled across multiple industries. Adversaries not only encrypt files, they first exfiltrate the non-encrypted data and threaten to release it to the dark web if the ransom is not paid on time.
- Novel ransomware techniques, such as new cryptography methods, buying Ransomware-as-a-Service (RaaS) offerings, and stealing unencrypted data, are used by criminals to increase their success rates.
- The US, Canada, and Germany are the top nations targeted by ransomware attacks.

Ransomware

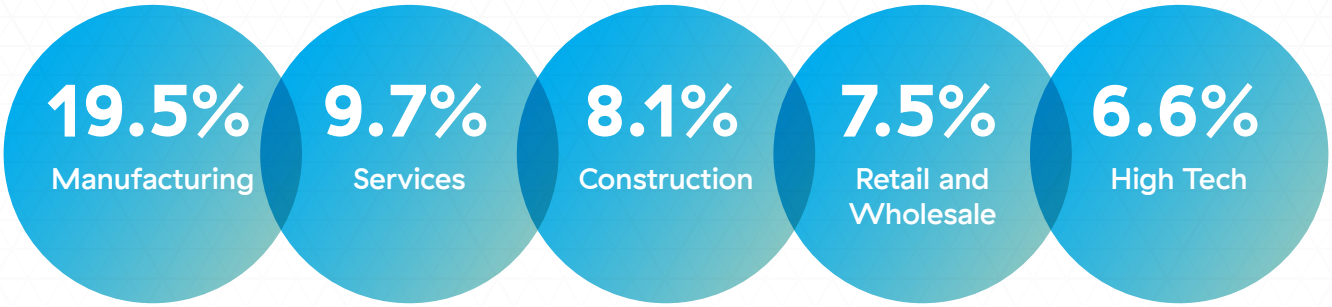
Ransomware involves encrypting an organization's data assets until a ransom is paid to the attacker in exchange for access. Extortion ransomware attacks skip the encryption process. Attackers steal the data and then threaten to release it publicly as a way of pressuring victims to pay up. Successful phishing attacks often lead to a ransomware event.

Vulnerability Used to Launch 500+ Attacks in a Month

A ransomware group known as the Clop gang exploited a vulnerability in the MOVEit Transfer application, launching a well-publicized series of ransomware attacks that aimed to steal sensitive data from organizations' databases. In July 2023, the adversaries used this vulnerability to launch over 500 ransomware attacks, the largest monthly volume on record.

Most targeted industry sectors

According to ThreatLabz, ransomware gangs have targeted the manufacturing industry more than any other sector for several years. Manufacturing companies suffered 19.5% of the observed ransomware attacks in 2023. The service industry was the second most targeted industry at 9.7%. These findings mirror the information posted on dark web data leak sites, where attackers announce companies they have breached.

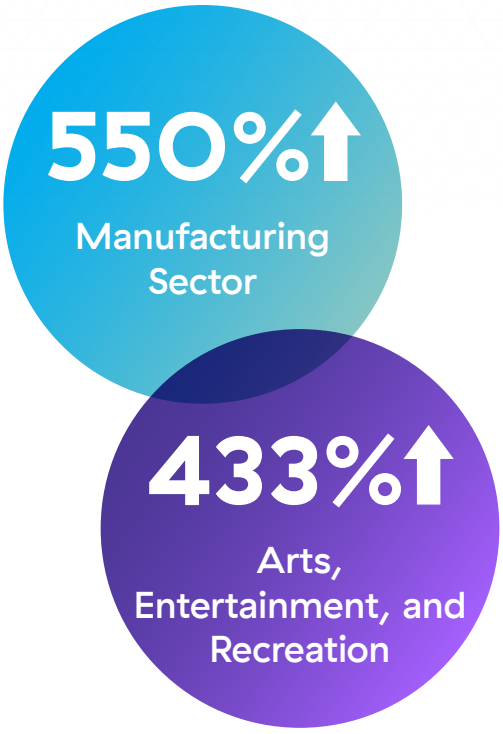


Successful ransomware attacks by industry, according to data leak sites

Ransomware sinks to new lows with double extortion attacks

Double extortion attacks, where adversaries steal data before encrypting it, is undergoing a meteoric rise. These attacks pressure victims to pay the ransom in two ways. First, organizations are told to pay a ransom for the key needed to decrypt their data. Second, if the organization refuses, attackers threaten to release the stolen data publicly on the dark web. Of course, paying the ransom is no guarantee that the attackers will honor their end of the bargain.

Businesses dealing in household and personal products saw a 550% increase in double extortion attacks, while the arts, entertainment, and recreation sector saw double extortion attacks rise by 433%. Several other industries also experienced triple-digit increases in double extortion attacks including energy, aerospace and defense, utilities, healthcare, and education.



Ransomware gets more sophisticated and devious

Threat actors are upping their game with crafty new ransomware techniques that make their job easier. Here are some of the latest that every executive should know about.

- **Encryptionless extortion:** This method makes attacks faster and simpler. As the name implies, encryptionless attacks do not encrypt the data on target systems. Instead, adversaries steal sensitive data and threaten to release it publicly if the organization does not pay, so it works much like blackmail. Targets are typically organizations that prize their brand reputation. By skipping the encryption process, adversaries allow victim organizations to function as usual without drawing the attention of media or law enforcement. This method also allows attackers extra time to focus on stealing massive amounts of data. For example, Zscaler ThreatLabz has observed an encryptionless attack where the targeted organization lost more than 24TB of data.

Hydro Adopts Zero Trust After Ransomware Attack

When a ransomware attack locked down thousands of systems in a single day, Norwegian manufacturing and hydropower provider Hydro transitioned to zero trust architecture, which makes applications, users, and the internal network invisible to malicious actors.

- **Ransomware-as-a-Service (RaaS):** These services offer a subscription-based model for accessing ransomware tools to launch attacks. Operators sell affiliates access to ransomware, cybercrime tools, leak sites, and other services in return for a significant share of profits. After affiliates attack the targeted organizations, operators collect their gains and often expand their businesses. Affiliates make enough to justify the investment in RaaS and continue to launch more attacks. This self-perpetuating economic cycle leads to a growth in ransomware attacks.
- **Elliptic curve cryptography (ECC):** Technology is an alternative to RSA encryption commonly used by ransomware groups. Using ECC allows adversaries to encrypt and decrypt data more swiftly and use fewer system resources. Zscaler ThreatLabz has witnessed several high-profile ransomware families adopting ECC, which include encryption schemes Curve25519, NIST B-233, NIST P-521, and NIST K-571.

> "Attackers tend to lose interest because it's just too much work for them to go further. They typically prefer easier targets."
>
> — DANIEL REMARC BOGNAR, HEAD OF NETWORK ARCHITECTURE, HYDRO[6]

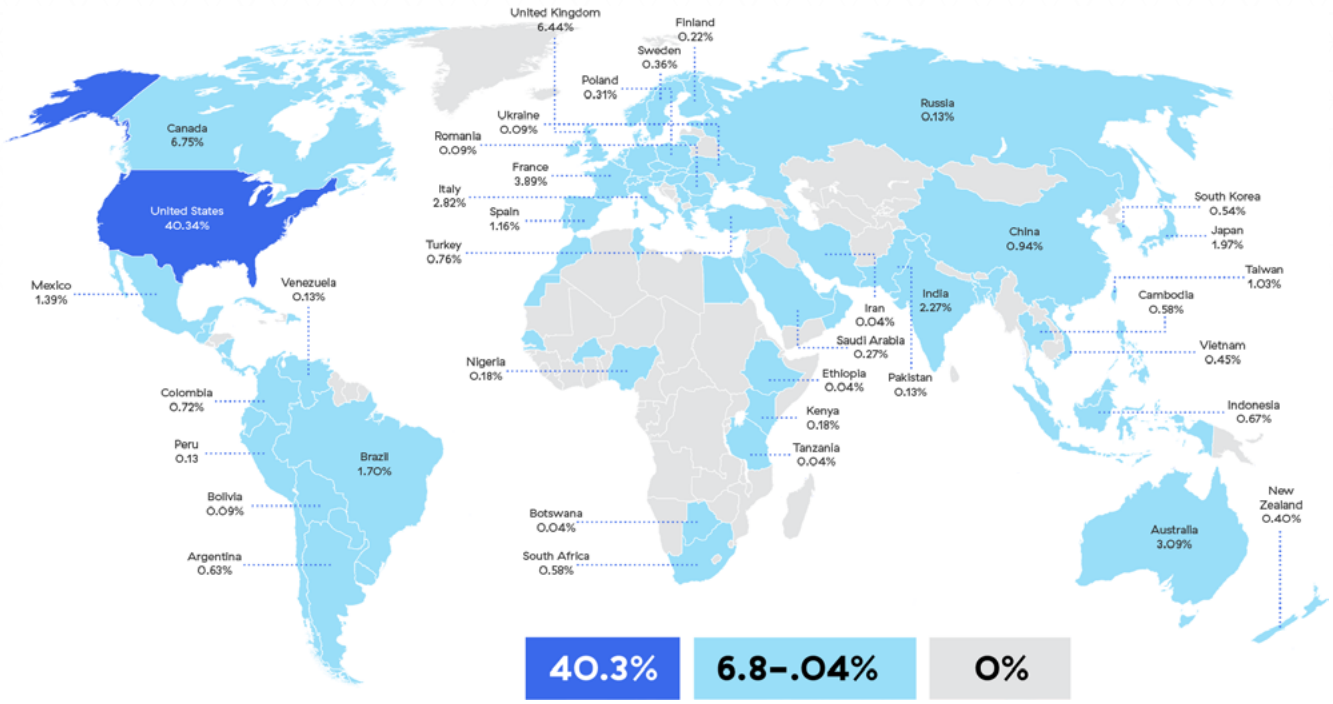
Ransomware

- Money Message
- BlackBasta 2.0
- Nokoyawa 1.0 & 1.1
- Nokoyawa 2.0 & 2.1
- REvil variants (e.g. RansomCartel)
- BlackByte
- Babuk variants

Ransomware families ThreatLabz observed using elliptic curve cryptography schemes

Where ransomware strikes most often

ThreatLabz reports that the United States is targeted most frequently by ransomware attacks, accounting for 40% of all activity. Canada places a distant second, attracting 6.75% of global ransomware activity. Germany is third with 4.92%.



Ransomware activity global heatmap

Section Wrap Up

Preventive Measures: Defend Against Ransomware

ATTACKER TECHNIQUES	YOUR STRATEGIES
Double extortion ransomware attacks are surging.	• Review the latest cybersecurity risk audits, and examine how critical data is protected. • Ensure your organization maintains scheduled data backups that are tested regularly.
Encryptionless ransomware attacks, where adversaries steal data and threaten to publish, is on an uptick.	• Discuss how data usage and movement is governed with the risk team or CISO. • Determine if your organization has a recovery plan, and review your processes. • Prepare policies and PR firm–approved language for communicating about cyberattacks.
Ransomware–as–a–service makes launching ransomware attacks easier and “lowers the bar” for cybercriminals.	• Ensure your organization uses zero trust principles to deprive ransomware attacks of critical resources.

The Good Fight

For years, CISOs have been briefing fellow CXOs and boards that it's not a matter of if they will be attacked, but when. Accepting the risks of conducting business and connecting to the internet is a fact of life, along with death and taxes. It implies engaging in the relentless battle against digital adversaries. The quality of your perseverance in the face of ever-evolving threats speaks volumes about your integrity and resilience, far more than any single cyber event victory or defeat.

> "There is a risk to conducting business and connecting to the internet... If you are not protecting your organization, you are accepting the risk and gambling that today is not the day that ransomware knocks on the door much like the big bad wolf and threatens to blow down their straw house."
>
> — BENJAMIN CORLL, ZSCALER CISO IN RESIDENCE

Here are a few quick suggestions for mitigating or preventing negative impacts from a cyber event:

- Have a response plan
- Implement common preventative measures (MFA, regular software updates, etc)
- Train users to identify and avoid socially engineered threats
- Invest in the resources your security team needs to identify, respond, and remediate incidents

For in-depth advice on how CXOs can improve their organization's security, read **Seven Questions Every CXO Must Ask About Zero Trust**.

Additional Resources

CXO REvolutionaries

An executive-level resource for actionable, practical, and real-world examples for creating enterprise change through digital transformation initiatives.

Podcasts

Executive-oriented technology podcasts including "The CISO's Gambit," "The CIO Evolution," and "Cloudy with a Chance of Trust."

LinkedIn

Social media updates related to executive events, insights, and content releases.

CXO REvolutionaries

SPONSORED BY: zscaler

About CXO REvolutionaries

CXO REvolutionaries drive zero trust and digital transformation thought leadership for the global CXO community. Explore our educational and informational resources for insights on successfully transforming your organization's IT and cybersecurity.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform.