Zscaler ThreatLabz Research Shows a Nearly 50% Increase in Phishing Attacks with Education, Finance, and Government Being the Most Targeted

April 18, 2023

Annual Phishing Report Highlights New and Evolving Phishing Campaigns Resulting from the Rise of AI Platforms, like ChatGPT, Urges Organizations to Adopt a Zero Trust Architecture

Key Findings

- Phishing attacks around the world rose nearly 50% in 2022 compared to 2021
- Education was the most targeted industry, with attacks increasing by 576%, followed by finance and government, while last year's top target, retail and wholesale, dropped by 67%
- The top five most targeted countries were the United States, the United Kingdom, the Netherlands, Canada, and Russia
- Top targeted brands include Microsoft, Binance, Netflix, Facebook, and Adobe
- AI tools like ChatGPT & Phishing Kits have significantly contributed to the growth of phishing, reducing the technical barriers to entry for criminals and saving them time and resources
- SMS phishing (SMiShing) evolves to more voicemail-related phishing (Vishing), luring more victims into opening malicious attachments
- Cloud-native proxy-based Zero Trust architecture is critical for organizations to defend against evolving phishing attacks

Phishing Attacks by Industry

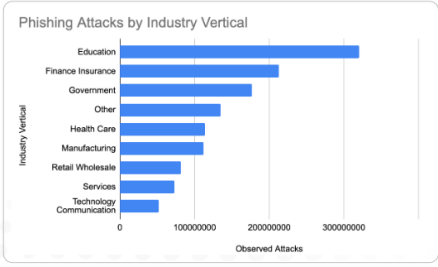

Figure 2: Phishing attacks by industry 2022

Phishing Attacks by Industry 2022

SAN JOSE, Calif., April 18, 2023 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today released the findings of its 2023 ThreatLabz Phishing Report. The report views 12 months of global phishing data from the world's largest in-line security cloud to identify the latest trends, emerging tactics, and which industries and regions are most impacted by phishing attacks. The report found that a majority of modern phishing attacks rely on stolen credentials and outlined the growing threat from Adversary-in-the-Middle (AitM) attacks, increased use of the InterPlanetary File System (IPFS), as well as reliance on phishing kits sourced from black markets and AI tools like ChatGPT.

"Phishing remains one of the most prevalent threat vectors cybercriminals utilize to breach global organizations. 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 & AI tools to launch highly effective e-mail, SMiShing, and Vishing campaigns at scale"," said Deepen Desai, Global CISO and Head of Security, Zscaler. "AitM attacks supported by growth in Phishing-as-a-Service have allowed attackers to bypass traditional security models, including multi-factor authentication. To protect their environment, organizations should adopt a Zero Trust architecture to significantly minimize the attack surface, prevent compromise, and reduce the blast radius in case of a successful attack."

The Rise in New and Evolving Threats like ChatGPT
The emergence of new AI technology and large language models like ChatGPT have made it easier for cybercriminals to generate malicious code, Business Email Compromise (BEC) attacks, and develop polymorphic malware that makes it harder for victims to identify phishing. Malicious actors are also increasingly hosting their phishing pages on the InterPlanetary File System (IPFS), a distributed peer-to-peer file system that allows users to store and share files on a decentralized network of computers. It is much more difficult to remove a phishing page hosted in IPFS because of its peer-to-peer network aspect.

ThreatLabz recently discovered a large-scale phishing campaign that involves Adversary-in-The-Middle attacks. AiTM attacks use techniques capable of bypassing conventional multi-factor authentication methods.

Vishing, or voicemail-themed phishing campaigns, have evolved from SMS or SMiShing attacks. Attackers are using real voice snippets of the executive team in these vishing attacks by leaving a voicemail of these pre-recorded messages. Then, recipients are pressured into taking action, like transferring money or providing credentials. Many US-based organizations have been targeted using Vishing attacks.

Recruitment scams on LinkedIn and other job recruiting sites are also on the rise. Unfortunately, in 2022, many big businesses in Silicon Valley made the tough decision to downsize. As a result, cybercriminals leveraged fake job postings, sites, portals, and forms to attract job seekers. Victims would often undergo an entire interview process, with some even being asked to purchase supplies to be reimbursed later.

Name Brands Used To Lure Victims
Cybercriminals often find success when impersonating popular consumer and technology brands. Microsoft was once again the most imitated brand of the year, accounting for nearly 31% of attacks as the attackers phished for access to various Microsoft corporate applications of the victim organizations. Cryptocurrency exchange Binance accounted for 17% of imitated brand attacks, with phishers posing as fake customer representatives from banks or P2P companies. Big brands like Netflix, Facebook, and Adobe rounded out the top 20 most imitated and phished brands.

North America Continues To Be A Top Target For Phishing Attacks
The U.S., once again, keeps its top spot as the most targeted country for phishing attacks. Data indicated that more than 65% of all phishing attempts

occurred in the U.S., an increase from last year's 60%.

While the U.S. continues to lead the way, the research revealed staggering year-over-year increases in phishing attempts targeting Canada (718%), the U.K. (269%), Russia (199%), and Japan (92%). Conversely, Hungary and Singapore both decreased by 90% and 48%. ThreatLabz believes the decrease in Singapore may be due to the government's efforts toward investing in cybersecurity, including initiatives by the country's Cyber Security Agency (CSA).

Phishing Attacks on Education and Healthcare Industries Surge
The education industry experienced the most significant surge in 2022 phishing attempts, jumping from the eighth spot to number one, with an increase of 576%. ThreatLabz believes the 2022 application process for student loan repayments and debt relief played a role in this surge. Rounding out the top five industries under attack are finance, insurance, government, and healthcare, which saw just under 31 million attempts in 2021 to over 114 million in 2022.

Retail and wholesale industries, which topped the list as most targeted last year, saw a decrease of 67%. The service industry also saw a decline of 38% from attempts in 2021.

Countering Phishing Attacks
With the average organization receiving phishing emails daily, financial losses incurred from malware and ransomware attacks can quickly drive up year-over-year IT costs. Facing all the threats outlined in this report is a big job, and while the risk of phishing threats can not be eliminated entirely, IT and security teams can learn from observed incidents. Zscaler recommends the following best practices to manage phishing risk better:

- Understand the risks to better inform policy and strategy
- Leverage automated tools and threat intel to reduce phishing incidents
- Implement Zero Trust architectures to limit the blast radius of successful attacks
- Deliver timely training to build security awareness and promote user reporting
- Simulate phishing attacks to identify gaps in your program

The Zscaler Zero Trust Exchange ™Protects Systems from Phishing
Industry statistics reveal that the average organization receives a high volume of phishing emails daily, and user compromise is one of the most complex security challenges to defend against. The Zscaler Zero Trust Exchange platform is built on a holistic zero trust architecture to minimize the attack surface, prevent compromise, eliminate lateral movement, and stop data loss. Zscaler helps stop phishing in the following ways:

- **Prevents compromise**: Full SSL inspection at scale, browser isolation, and policy-driven access control to prevent access to suspicious websites.
- **Eliminates lateral movement**: By connecting users directly to apps, not the network, to limit the blast radius of a potential incident.
- **Shuts down compromised users and insider threats**: If an attacker gains access to your identity system, Zscaler can prevent private app exploit attempts with in-line inspection and detect the most sophisticated attackers with integrated deception.
- **Stops data loss**: Inspect data-in-motion and data-at-rest to prevent potential data theft from an active attacker.

To view the full report, download the 2023 ThreatLabz Phishing Report. Global CISO and Head of Security Research, Deepen Desai, will present the report findings at RSAC 2023 on Thursday, April 27th, from 8:30 AM - 9:20 AM PT. Additional details can be found here.

Methodology
a ThreatLabz evaluated data from the Zscaler security cloud, which monitors over 280 billion transactions daily across the globe. ThreatLabz analyzed year's worth of global phishing data from the Zscaler cloud from January 2022 through December 2022 to identify key trends, industries and geographies at risk, and emerging tactics.

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.

Media Contact:
Natalia Wodecki
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/0710b412-baba-4f1d-91d7-7529ed5b3578