New Zscaler Research Shows Over 400% Increase in Phishing Attacks with Retail and Wholesale Industries at Greatest Risk

April 20, 2022

Annual ThreatLabz Report Reveals Phishing-as-a-Service as the Key Source of Attacks Across Critical Industries and Consumers Globally; Underscores Urgency to Adopt a Zero Trust Security Model

Key Findings

- Phishing attacks rose 29% globally to a new record of 873.9M attacks observed in the Zscaler™ cloud last year
- Retail and wholesale were the most targeted industries, experiencing over a 400% increase in phishing attacks over the last 12 months
- The United States, Singapore, Germany, Netherlands, and the United Kingdom were the most frequently targeted by phishing scams
- Emerging phishing vectors, such as SMS phishing, are increasing faster than other methods as end users become more wary of suspicious emails
- Rising phishing activity is directly linked to “phishing- as-a-service” options, which provide a marketplace of pre-built attack tools that reduce technical barriers to entry for criminals

SAN JOSE, Calif., April 20, 2022 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today released the findings of its 2022 ThreatLabz Phishing Report that reviews 12 months of global phishing data from the Zscaler security cloud to identify key trends, industries and geographies at risk, and emerging tactics. According to the FBI Internet Crime Complaint Center (IC3), phishing attempts are the most frequently-reported cyberattack. Zscaler’s ThreatLabz research team analyzed data from more than 200 billion daily transactions, and 150 million daily blocked attacks in order to identify emerging threats and track malicious actors from across the globe. This year’s report showed dramatic 29% growth in overall phishing attacks compared to previous years, with retail and wholesale companies bearing the brunt of the increase. The report also showed an emerging reliance on phishing-as-a-service methods, as well as new attack vectors, such as SMS phishing, becoming one of the more prevalent methods of intrusion.

“Phishing attacks are impacting businesses and consumers with alarming frequency, complexity, and scope - with the rise in phishing-as-a-service making it easier than ever for non-sophisticated actors to launch successful attacks. Our annual report highlights how cybercriminals continue to escalate their usage of phishing as a starting point to breach organizations to deliver ransomware or steal sensitive data,” said Deepen Desai, CISO and VP of Security Research and Operations at Zscaler. “To defend against advanced phishing attacks, organizations must leverage a multi-pronged defensive strategy anchored on a cloud native zero trust platform that unifies full SSL inspection with AI/ML-powered detection to stop the most sophisticated phishing attempts and phishing kits, lateral movement prevention and integrated deception to limit the blast radius of a compromised user, proactive controls to block high risk destinations such as newly registered domains that are often abused by threat actors, and in-line DLP to safeguard against data theft.”

Phishing has always been one of the most pervasive cyberthreats, with various methods used to steal private information. One of the reasons this type of attack grows in prevalence every year is its low barrier to entry. Cybercriminals use current events, such as the COVID-19 pandemic or cryptocurrency, to convince unwitting victims to hand over confidential data, such as passwords, credit card information, and login credentials.

The 2022 ThreatLabz Phishing Report found that phishing attacks lure victims by posing as top brands or promoting topical events. The top phishing themes in 2021 included categories such as productivity tools, illegal streaming sites, shopping sites, social media platforms, financial institutions, and logistical services.

A Global Problem
In 2021, the U.S. was the most-targeted country globally, accounting for over 60% of all phishing attacks blocked by the Zscaler security cloud. The next most frequently attacked countries include Singapore, Germany, the Netherlands, and the United Kingdom.

Not all countries experienced the same attention from phishing attacks. For example, the Netherlands experienced a decrease of 38 %, which may have resulted from recently-passed legislation that increased the penalties for online fraud.

Phishing attacks were also not evenly distributed across different industries. Retail and wholesale businesses experienced an increase of over 400% in phishing attempts - the most out of all tracked industries. These businesses were followed by financial and government sectors, with organizations in these industries seeing over 100% increases in attacks on average. However, some industries experienced partial relief from phishing attacks last year. Healthcare saw a notable drop of 59 %, while the services industry saw a decline of 33 %.

Phishing-as-a-Service - The Growing Threat
While phishing has long been one of the most common tactics used in cyberattacks by sophisticated threat actors, it's becoming more accessible to non-technical cybercriminals due to a maturing underground marketplace for attack frameworks and services. By selling their pre-built phishing tools and services on the dark web, cybercriminals are making it easier to deploy phishing scams at scale, creating a greater chance for more phishing activity in 2022.

Countering Phishing Attacks

According to the Zscaler ThreatLabz research team, an average-sized organization receives dozens of phishing emails every day. This means that employees at all levels must be aware of the most common phishing tactics and empowered to spot phishing attempts that can result in financial losses and damage to the business' brand.

Facing the threats outlined in the 2022 ThreatLabz Phishing Report can be daunting, and while it's impossible to eliminate phishing risk, effective management can prevent business-critical information from falling into the hands of cybercriminals. Among other recommendations, Zscaler suggests the following tactics for countering phishing growth:

- Learning and understanding the risks posed by phishing to better inform policy and technology decisions
- Leveraging automated tools and actionable intelligence to empower employees with the tools needed to reduce phishing incidents
- Delivering timely employee training to build security awareness and promote user reporting
- Simulating phishing attacks to identify gaps in security policies and procedures
- Evaluating security infrastructure to ensure access to the latest research and system capabilities

How the Zscaler Zero Trust Exchange™ Can Mitigate Phishing Attacks

User compromise is one of the most difficult security challenges to defend against. The Zscaler Zero Trust Exchange incorporates phishing prevention controls into a holistic zero trust architecture that disrupts every stage of attacks and minimizes damages. Capabilities include:

- **Preventing compromise** with full SSL inspection at scale, threat analysis using natively integrated threat intel and IPS signature detection, AI/ML phishing detection, and policy-defined high-risk URL categories commonly used for phishing such as newly observed and newly registered domains.
- **Eliminating lateral movement** by connecting users directly to apps, not the network, to limit the blast radius of a potential incident.
- **Shutting down compromised users and insider threats** with in-line application inspection and integrated deception capabilities to trick and detect attackers.
- **Stopping data loss** by inspecting data both in motion and at rest to prevent theft by an active attacker.

To download the full report, see the ThreatLabz 2022 Phishing Report.

Methodology
The ThreatLabz team evaluated data from the Zscaler security cloud, which monitors over 200 billion transactions daily across the globe. ThreatLabz analyzed a year's worth of global phishing data from the Zscaler cloud from January 2021 through December 2021 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 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 Contacts
Natalia Wodecki
Global PR Director
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/ee00f0a5-1f7f-4e77-8b4f-d178075ec1c7