New Research Shows Attackers Turning to Encrypted Attacks During Pandemic

November 10, 2020

Encryption-Based Threats Grow By 260% in 2020

Healthcare, Finance and Manufacturing Under an Onslaught of Attacks

SAN JOSE, Nov. 10, 2020 (GLOBE NEWSWIRE) -- Zscaler, Inc., the leader in cloud security, today released its 2020 State of Encrypted Attacks report, published by the Zscaler ThreatLabZ team. The threat research reveals the emerging techniques and impacted industries behind a 260-percent spike in attacks using encrypted channels to bypass legacy security controls. The report provides guidance on how IT and security leaders can protect their enterprise from the rising trend of encrypted threats, based on insight sourced from over 6.6 billion encrypted threats across the Zscaler™ cloud from January through September 2020 over encrypted channels. To download and read, see the 2020 State of Encrypted Attacks.

Showing that cybercriminals will not be dissuaded by a global health crisis, they targeted the healthcare industry the most. Following healthcare, the research revealed the top industries under attack by SSL-based threats were:

1. Healthcare: 1.6 billion (25.5 percent)
2. Finance and Insurance: 1.2 billion (18.3 percent)
3. Manufacturing: 1.1 billion (17.4 percent)
4. Government: 952 million (14.3 percent)
5. Services: 730 million (13.8 percent)

Other key findings include:

- **COVID-19 is Driving a Ransomware Surge:** Zscaler researchers witnessed a 5x increase in ransomware attacks over encrypted traffic beginning in March, when the World Health Organization declared the virus a pandemic. Earlier research from Zscaler indicated a 30,000 percent spike in COVID-related threats, when cybercriminals first began preying on fears of the virus.

- **Phishing Attacks Neared 200 Million**: As one of the most commonly used attacks over SSL, phishing attempts reached more than 193 million instances during the first nine months of 2020. The manufacturing sector was the most targeted (38.6 percent) followed by services (13.8 percent), and healthcare (10.9 percent).

- **30 Percent of SSL-Based Attacks Delivered Through Trusted Cloud Providers:** Cybercriminals continue to become more sophisticated in avoiding detection, taking advantage of the reputations of trusted cloud providers such as Dropbox, Google, Microsoft, and Amazon to deliver malware over encrypted channels.

- **Microsoft Remains Most Targeted Brand for SSL-Based Phishing:** Since Microsoft technology is among the most adopted in the world, Zscaler identified Microsoft as the most frequently spoofed brand for phishing attacks, which is consistent with ThreatLabZ 2019 report. Other popular brands for spoofing included PayPal and Google. Cybercriminals are also increasingly spoofing Netflix and other streaming entertainment services during the pandemic.

“Cybercriminals are shamelessly attacking critical industries like healthcare, government and finance during the pandemic, and this research shows how risky encrypted traffic can be if not inspected,” said Deepen Desai, CISO and Vice President of Security Research at Zscaler. “Attackers have significantly advanced the methods they use to deliver ransomware, for example, inside of an organization utilizing encrypted traffic. The report shows a 500 percent increase in ransomware attacks over SSL, and this is just one example to why SSL inspection is so important to an organization’s defense.”

Inspecting encrypted traffic is mission-critical for all organizations to protect against these attacks. A multilayered defense-in-depth strategy that fully supports SSL inspection ensures that enterprises are protected from escalating threats hiding in their encrypted traffic. Processing more than 130 billion transactions per day, Zscaler performs SSL inspection at scale, helping organizations securely connect their users in a work-from-anywhere world.

To download the full report, see the 2020 State of Encrypted Attacks.

About ThreatLabZ

ThreatLabZ is the embedded research team at Zscaler. This global team includes security experts, researchers, and network engineers responsible for analyzing and eliminating threats across the Zscaler security cloud and investigating the global threat landscape. The team shares its research and cloud data with the industry at large to help promote a safer internet.

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 SASE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Media Contact:

Natalia Wodecki

press@zscaler.com

Investor Relations Contact:

Bill Choi, CFA

ir@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/94c5e9d3-ec84-44ff-9170-00108b4649ff