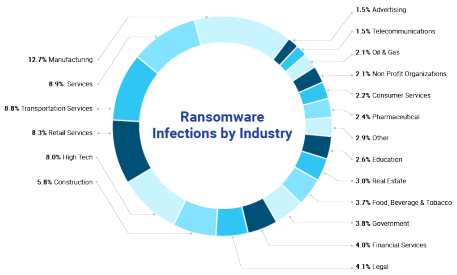
Zscaler Ransomware Report Reveals Sophisticated Double Extortion Attacks are Targeting Essential Industries Causing Significant Business Disruption

May 13, 2021

New Research Highlights the Top Vertical Industries Impacted and Tactics Used by the Most Active Ransomware Families Resulting in $1.4B in Ransom Demands

SAN JOSE, Calif., May 13, 2021 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced its new Ransomware Report featuring analysis of key ransomware trends and details about the most prolific ransomware actors, their attack tactics and the most vulnerable industries being targeted. The Zscaler™ThreatLabz embedded research team analyzed over 150 billion platform transactions and 36.5 billion blocked attacks between November 2019 and January 2021 to identify emerging ransomware variants, their origins, and how to stop them. The report also outlines a growing risk from "double-extortion" attacks, which are being increasingly used by cybercriminals to disrupt businesses and hold data hostage for ransom.

Zscaler Ransomware Roundup Chart



Percentage of ransomware attacks involving double extortion observed between November 2019 and January 2021

"Over the last few years, the ransomware threat has become increasingly dangerous, with new methods like double extortion and DDoS attacks making it easy for cybercriminals to sabotage organizations and do long-term damage to their reputation," said Deepen Desai, CISO and VP of Security Research at Zscaler. "Our team expects ransomware attacks to become increasingly targeted in nature where the cybercriminals hit organizations with a higher likelihood of ransom payout. We analyzed recent ransomware attacks where cybercriminals had the knowledge of things like the victim's cyber insurance coverage as well as critical supply-chain vendors bringing them in the crosshairs of these attacks. As such, it is critical for businesses to better understand the risk ransomware represents and take proper precautions to avoid an attack. Always patch vulnerabilities, educate employees on spotting suspicious emails, back up data regularly, implement data loss prevention strategy, and use zero trust architecture to minimize the attack surface and prevent lateral movement."

According to the World Economic Forum 2020 Global Risk Report[1], ransomware was the third most common, and second most damaging type of malware attack recorded in 2020. With payouts averaging $1.45M per incident, it's not difficult to see why cybercriminals are increasingly flocking to this new style of high-tech extortion. As the rewards that result from this type of crime increase, risks to government entities, company bottom lines, reputation, data integrity, customer confidence, and business continuity also grow. Zscaler's research supports the narrative recently established by the U.S. federal government, which classifies ransomware a national security threat; underscoring the need to prioritize mitigation and contingency measures when protecting against these ongoing threats.

Double-Extortion - the New Preferred Method

In late 2019, ThreatLabz noticed a growing preference for "double-extortion" attacks in some of the more active and impactful ransomware families. These attacks are defined by a combination of unwanted encryption of sensitive data by malicious actors and exfiltration of the most consequential files to hold for ransom. Affected organizations, even if they are able to recover the data from backups, are then threatened with public exposure of their stolen data by criminal groups demanding ransom. In late 2020, the team noticed that this tactic was further augmented with synchronized DDoS attacks, overloading victim's websites and putting additional pressure on organizations to cooperate.

According to Zscaler ThreatLabZ, many different industries have been targeted over the past two years by double-extortion ransomware attacks. The most targeted industries include the following:

1) Manufacturing (12.7%)
2) Services (8.9%)
3) Transportation (8.8%)
4) Retail & wholesale (8.3%)
5) Technology (8%)

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/087a5067-e973-42d8-be42-72e4ddcff0ce

Most Active in Ransomware

Over the last year, ThreatLabz has identified seven "families" of ransomware that were encountered more often than others. The report discusses the origins and tactics of the following top five highly active groups:

- **Maze/Egregor:** Originally encountered in May 2019, Maze was the ransomware most commonly used for double-extortion attacks (accounting for 273 incidents) until it seemingly ceased operations in November 2020. Attackers used spam email campaigns, exploit kits such as Fallout and Spelevo, and hacked RDP services to gain access to systems and successfully collected large ransoms after encrypting and stealing files from IT and technology companies. The top three industries Maze targeted were high-tech (11.9%) manufacturing (10.7%), and services (9.6%). Mase notably pledged to not target healthcare companies during the COVID-19 pandemic.
- **Conti:** First spotted in February 2020 and the second most common attack family accounting for 190 attacks, Conti shares code with the Ryuk ransomware and appears to be its successor. Conti uses the Windows restart manager API before

encrypting files, allowing it to encrypt more files as part of its double-extortion approach. Victims that won't or are unable to pay the ransom have their data regularly published on the Conti data leak website. The top three industries most impacted are manufacturing (12.4%), services (9.6%), and transportation services (9.0%).

- **Doppelpaymer:** First noticed in July 2019 and 153 documented attacks, Doppelpaymer targets a range of industries and often demands large payouts - in the six and seven figures. Initially infecting machines with a spam email that contains either a malicious link or malicious attachment, Doppelpaymer then downloads Emotet and Dridex malware into infected systems. Doppelpaymer's top three most targeted organizations were manufacturing (15.1%), retail & wholesale (9.9%) and government (8.6%).
- **Sodinokibi:** Also known as REvil and Sodin, Sodinokibi was first spotted in April 2019, and has been encountered with increasing frequency with 125 attacks. Similar to Maze, Sodinokibi uses spam emails, exploit kits, and compromised RDP accounts, as well as frequently exploiting vulnerabilities in Oracle WebLogic. Sodinokibi started using double-extortion tactics in January 2020 and had the greatest impact on transportation (11.4%), manufacturing (11.4%), and retail/wholesale (10.6%).
- **DarkSide:** DarkSide was first spotted in August 2020 after putting out a press release advertising its services. Using a "Ransomware-as-a-Service" model, DarkSide deploys double-extortion methods to steal and encrypt information. The group is public about its targeting manifesto, writing that it does not attack healthcare organizations, funeral services, education facilities, non-profit organizations, or government entities on its website. Instead, the primary targets of choice are services (16.7%), manufacturing (13.9%) and transportation services (13.9%). Similar to Conti, those that cannot pay the ransom have their data published on the DarkSide leak website.

The full Zscaler ransomware review is now available to the general public. Please see "ThreatLabZ Ransomware Review: The Advent of Double Extortion" for more information.

To hear more from the ThreatLabZ team about ransomware join the "Advances in Ransomware" session at Zenith Live, Zscaler's virtual event happening June 15th. Register for free today.

---

[1] https://www.weforum.org/reports/the-global-risks-report-2020

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 Contacts
Natalia Wodecki
Global PR Director
press@zscaler.com