30 December 2020

WEEKLY CYBER THREAT LEVEL INDICATOR

SEVERE RISK

**Indicators:**
Red - Severe
Orange - High
Yellow - Elevated
Blue - Guarded
Green - Low

HAWKEYE
HUNTING CYBER ADVERSARIES

# HAWKEYE WEEKLY ROUNDUP

## CYBER THREAT LANDSCAPE

### WHAT'S TRENDING?

**VPNs, MFA & the Realities of Remote Work**

According to the 2020 Verizon "Data Breach Investigations Report," 45% of breaches featured hacking and 22% included social engineering attacks. Attacks will likely continue to occur, especially with many remote workers remaining at home, and data breaches are expected to skyrocket.

**GoDaddy Apologized for Insensitive Phishing Email Sent to Its Employees Offering a Fake Bonus**

GoDaddy sent an email to its employee that promised a Christmas bonus to help them to face economic problems caused by the ongoing COVID-19 pandemic. The web provider apologized Thursday for the cyber security test aimed at verifying the response of its personnel to a phishing campaign.

**Microsoft Warned CrowdStrike of Possible Hacking Attempt**

Microsoft warned CrowdStrike earlier this month of a failed attempt by unidentified attackers to access and read the company's emails, according to a blog post published by the security firm. While the CrowdStrike blog post did not specify the exact identities of the hackers, Reuters, citing two unnamed sources, reported that the incident is likely related to the breach of SolarWinds.

## CRITICAL VULNERABILITIES

### CVE

**Windows Zero-Day Still Circulating After Faulty Fix**

A high-severity Windows zero-day that could lead to complete desktop takeover remains dangerous after a "fix" from Microsoft failed to adequately patch it.

**Zero-Click Apple Zero-Day Uncovered in Pegasus Spy Attack**

The phones of 36 journalists were infected by four APTs, possibly linked to Saudi Arabia or the UAE. Four nation-state-backed advanced persistent threats (APTs) hacked Al Jazeera journalists, producers, anchors and executives, in an espionage attack leveraging a zero-day exploit for Apple iPhone, researchers said.

**Critical Bugs in Dell Wyse Thin Clients Allow Code Execution, Client Takeovers**

Dell has patched two critical security vulnerabilities in its Dell Wyse Thin Client Devices, which are small form-factor computers optimized for connecting to a remote desktop.

**Easy WP SMTP Security Bug Can Reveal Admin Credentials**

Easy WP SMTP, a WordPress plugin for email management that has more than 500,000 installations, has a vulnerability that could open the site up to takeover, researchers said.

## CYBER SECURITY NEWS

### WHAT'S NEW FROM VENDORS?

**Cisco Study Highlights What Works — and What Doesn't — in Security**

Cisco's global 2021 Security Outcomes Study is based on a double-blind survey of more than 4,800 active IT, security, and privacy professionals across 25 countries and multiple industries, the study correlates 25 key security practices with 11 desired outcomes.

**Restructuring of Networks Amid Pandemic Made India Vulnerable to Ransomware Attacks: Check Point**

The sudden rush to provide remote access to employees by restructuring network and security systems during the lockdown made India vulnerable to ransomware attacks in the third quarter of current year, according to cyber security firm Check Point Software Technologies.

**Google Explains the Root Cause of the 47 Minutes Global Outage of its Services**

A recent outage of Google services such as Gmail, YouTube, Google Drive, and Maps severely affected the operations of users and organizations across the globe. The search engine giant stated that the disruption was caused due to a security flaw in its global authentication system.

## SOMETHING TO THINK ABOUT

### WHAT'S NEXT?

**Third-Party APIs: How to Prevent Enumeration Attacks**

When organizations use APIs – the next frontier in cybercrime – to engage with third parties, it's crucial they understand the associated security exposure they're introducing.

**Defending Against State and State-Sponsored Threat Actors**

Security threats from states and state-sponsored actors have been around since before the field of cybersecurity was defined. They have now evolved to cyberspace, and present unique challenges for defenders.

**Telemed Poll Uncovers Biggest Risks and Best Practices**

In an exclusive Threatpost poll of 159 participants (half of whom said they've had recent telemed appointments themselves), 72 percent saw an uptick in targeted cyberattacks on telehealth devices and networks over the past nine months.

**FBI Warns of DoppelPaymer Attacks on Critical Infrastructure**

The FBI is warning businesses of DoppelPaymer ransomware attacks and a change in tactics among operators, who are now cold-calling victims to pressure them into paying the ransom.

**DUBAI:** Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
**T:** +971 4 338 3365 | **E:** info@dts-solution.com

**ABU DHABI | KUWAIT CITY | YEREVAN | LONDON**
**www.dts-solution.com**