07 February 2021

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?

Microsoft 365 Becomes Haven for BEC Innovation

Two new phishing tactics use the platform's automated responses to evade email filters. Two fresh business email compromise (BEC) tactics have emerged onto the phishing scene, involving the manipulation of Microsoft 365 automated email responses in order to evade email security filters.

8 Top Technical Resource Providers for ICS Security

Attacks against industrial control systems (ICS) are on the rise. In its 2020 X-Force Threat Intelligence Report, for instance, IBM found that digital attacks targeting organizations' ICS had increased by more than 2,000% between 2019 and 2018.

One-Third of Businesses Have Cloud Budget Overruns of Up to 40%

More than one-third of businesses have cloud budget overruns of up to 40 percent, and one in 12 companies exceed this number, a Pepperdata survey.

Guide: How Security Consolidation Helps Small Cybersecurity Teams

The dynamic nature of cybersecurity, the changes in the threat landscape, and the expansion of the attack surface led organizations to add more security solutions.

CRITICAL VULNERABILITIES

CVE

Industrial Gear at Risk from Fuji Code-Execution Bugs

Fuji Electric's Tellus Lite V-Simulator and V-Server Lite are both affected by the vulnerabilities, which all carry a CVSS severity rating of 7.8.

SolarWinds Orion Bug Allows Easy Remote-Code Execution and Takeover

Three serious vulnerabilities have been found in SolarWinds products: Two in the Orion User Device Tracker and one in the Serv-U FTP for Windows product. The most severe of these could allow trivial remote code execution with high privileges.

Five Critical Android Bugs Patched, Part of Feb. Security Bulletin

February's security update for the mobile OS includes a Qualcomm flaw rated critical, with a CVSS score of 9.8. Google patched five critical bugs in its Android operating system as part of its February Security Bulletin.

Critical Libgcrypt Crypto Bug Opens Machines to Arbitrary Code

The Libgcrypt project has rushed out a fix for a critical bug in version 1.9.0 of the free-source cryptographic library.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Cisco Meraki and Openpath Launch New Enterprise Access, Video Security Solution

Cisco Meraki and Openpath have teamed up to provide a combined security platform designed for smart cameras and buildings access control.

Nozomi Networks Tops 100% Revenue Growth

Nozomi Networks Inc., the leader in OT and IoT security, today announced record 2020 growth and tremendous momentum moving into 2021. In 2020 Nozomi Networks' market share neared 50% among the world's top pharmaceutical, oil and gas, electric utility and mining operations. The number of devices monitored by Nozomi Networks solutions skyrocketed by more than 5,000% as the company successfully expanded its market to include IoT network cybersecurity.

Sontiq Acquires Cyberscout to Expand Its Cyber Products and Services to the Insurance Industry

Sontiq announced the signing of a definitive agreement to acquire Cyberscout. By acquiring Cyberscout, Sontiq will further build upon its world-class product platform and expand into the insurance industry with cyber solutions and forensic investigation products and services.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Mastercard Brings Cyber Education to Small Businesses

Small businesses have been disproportionately affected by hackers in recent months. To aid in countering the threat, Mastercard has launched a cybersecurity education effort targeting this market segment.

Bad Patching Practices are a Breeding Ground for Zero-Day Exploits, Google Warns

One in four "zero day" or previously unknown, software exploits that the Google team tracked in 2020 might have been avoided "if a more thorough investigation and patching effort were explored."

SolarWinds Attackers Spent Months in Corporate Email System: Report

SolarWinds' CEO says evidence indicates attackers lurked in the company's Office 365 email system for months ahead of the attack.

Know, Prevent, Fix: A Framework for Shifting the Discussion Around Vulnerabilities in Open Source

The security of open source software has rightfully garnered the industry's attention, but solutions require consensus about the challenges and cooperation in the execution.

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