19 October 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?

Enterprises Increasingly Adopting Containers, Many Turning to Providers for Support

U.S. enterprises increasingly are adopting containers to streamline their applications workflows, with many turning to container services and solutions providers to help them get full value from this cloud-native technology, according to a report by Information Services Group (ISG).

How Do I Select a SASE Solution for My Business?

Many organizations have turned to SASE adoption as a result of the pandemic, seeing it as a a security-first initiative, a recent survey has revealed. The report found that 48% of those surveyed view SASE as a security-first initiative, while 31% see it as a network-first strategy.

SaaS Adoption Growing, But So Are Security Concerns

A BetterCloud survey of more than 500 IT and security professionals reveals the latest challenges of managing SaaS at scale, particularly as digital transformation catapulted forward in 2021 — and IT kept the momentum going.

Patch Management Complexity Increased by Remote Work is Putting Organizations at Risk

71% of IT and security professionals found patching to be overly complex, cumbersome, and time consuming, an Ivanti survey reveals. In fact, 57% of respondents stated that remote work has increased the complexity and scale of patch management.

CRITICAL VULNERABILITIES

CVE

Windows Zero-Day Actively Exploited in Widespread Espionage Campaign

The cyberattacks, linked to a Chinese-speaking APT, deliver the new MysterySnail RAT malware to Windows servers. Microsoft patched the bug (CVE-2021-40449) as part of its October Patch Tuesday updates, issued this week.

Broadcom Software's Symantec Threat Hunter Team Discovers First-of-Its-Kind Ransomware

The new ransomware family, called Yanluowang, appears to still be under development and lacks some sophisticated features found in similar code. Nonetheless, Symantec said, it's dangerous.

Apache OpenOffice Users Should Upgrade to Newest Security Release!

The Apache Software Foundation (ASF) has released Apache OpenOffice 4.1.11, which fixes a handful of security vulnerabilities, including CVE-2021-33035, a recently revealed RCE vulnerability that could be triggered via a specially crafted document.

Microsoft Oct. Patch Tuesday Squashes 4 Zero-Day Bugs

Microsoft's October 2021 Patch Tuesday included security fixes for 74 vulnerabilities, one of which is an actively exploited zero-day.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Aqua Security Launches CNDR Capabilities to Detect Patterns and Respond with Granular Runtime Controls

Aqua Security adds a new detection and response capability (CNDR) to its Cloud Native Application Protection Platform (CNAPP), using real-time behavioral indicators to identify zero-day attacks from low-level eBPF events surfaced by Aqua's open source project.

Spirion Partners with HANDD Business Solutions to Help Companies with Data Privacy Regulations

Spirion and HANDD Business Solutions announced a partnership that showcases the depth of Spirion's data discovery and classification technology combined with HANDD's specialization in data protection. Spirion helps organizations comply with ever-changing data privacy regulations, avoid costly fees, protect against data breaches, and defend an organization's reputation with Spirion Sensitive Data Platform (SDP).

SentinelOne Achieves AWS Security Competency Status to Help Customers in Defending Cloud Workloads

SentinelOne announced that the company has achieved Amazon Web Services (AWS) Security Competency status. The designation recognizes SentinelOne's deep technical expertise and proven customer success protecting user endpoints and securing cloud adoption.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

The Importance of Crisis Management in the Age of Ransomware

Cybersecurity crises are becoming commonplace. With the massive surge in ransomware attacks in the last few years, businesses can't afford to ignore the increasing possibility of facing one, and should invest money and effort into crisis management.

Most Employees Believe Backing Up Company Data is Not Their Problem

Apricorn announced the findings from a Twitter poll exploring data backup and recovery processes. More than 50 percent of respondents noted that they, or their employees, have experienced a loss of data as a result of not backing up, or a failed backup.

List of IT Assets an Attacker is Most Likely to Target for Exploitation

Randori released a report that identifies the most tempting IT assets that an attacker is likely to target and exploit.

91.5% of Malware Arrived Over Encrypted Connections During Q2 2021

The latest report from the WatchGuard shows an astonishing 91.5% of malware arriving over encrypted connections during Q2 2021.

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