18 January 2022

WEEKLY CYBER THREAT LEVEL INDICATOR

HIGH 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?

The Supply Chain Needs Better Cybersecurity and Risk Management

If the supply chain is going to have any chance at recovery in the near future, organizations need to address cybersecurity and risk management. This is because cybersecurity and supply chain efficiency are closely intertwined.

Phishers are Targeting Office 365 Users by Exploiting Adobe Cloud

The attack is simple, really: the phishers create/import and host on Adobe Cloud an official-looking PDF pointing to a classic credential harvesting page hosted outside the Adobe suite (in this case, Weebly).

6 Cloud Security Trends to Watch for in 2022

There has been a lot of innovation that has sparked a new wave of technologies – from the boom in serverless technologies (allowing firms to scale and build platforms at speeds never seen before) to the evolution of cloud automation security.

AI and ML Implementation in Cybersecurity Programs Pushes for a Change in People's Mindset

AI and ML are underutilized partly because, frankly, change is hard. To adopt these new technologies, the organization must not only change its existing approaches, but also change the mindset of its people and its culture in order to really embrace them.

CRITICAL VULNERABILITIES

CVE

Oracle Critical Patch Update for January 2022 Will Fix 483 New Flaws

The pre-release announcement for Critical Patch Update (CPU) for January 2022 states that Oracle will fix 483 new flaws.

Microsoft January Patch Tuesday Addresses 96 Vulnerabilities

Microsoft January Patch Tuesday update bundle has arrived with significant security fixes. Specifically, it includes a whopping 96 different bug fixes that address some zero-days.

Critical SAP Vulnerability Allows Supply Chain Attacks

A critical vulnerability addressed recently in SAP NetWeaver AS ABAP and ABAP Platform could be abused to set up supply chain attacks, SAP security solutions provider SecurityBridge warns.

Zoho Fixes a Critical Vulnerability (CVE-2021-44757) in Desktop Central Solutions

Zoho fixed a new critical severity flaw, tracked as CVE-2021-44757, that affects its Desktop Central and Desktop Central MSP unified endpoint management (UEM) solutions.

High-Severity Flaw in 3 WordPress Plugins Impacts 84,000 websites

The vulnerability tracked as CVE-2022-0215 is a cross-site request forgery (CSRF) issue that received a CVSS score of 8.8.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Pacific Global Security Group Partners with Dragos and IronNet to Protect Sensitive OT and IT Systems

Pacific Global Security Group (Pac-Sec) is partnering with internationally recognized cybersecurity leaders Dragos and IronNet to provide specialized information technology (IT) and operational technology (OT) services for government agencies and commercial clients.

TD SYNNEX Collaborates with AWS to Help Businesses Expand Their Customer Base

The SCA provides investment in resources to help small and medium-sized businesses and public sector organizations expand their digital business offerings by leveraging an enhanced range of AWS Cloud services.

Last Week's Microsoft Outlook Outage has Some UAE Businesses Playing Catch Up

Last week's Microsoft Outlook outage did not end up having a major impact on UAE-based businesses, but it did affect some more than others. UAE users reported being unable to access their Outlook mailboxes on January 12. Later, Microsoft confirmed the outage and added that the issue was being looked into.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

How to Improve your IR Tabletop Exercises and Why You Really Should?

Incident Response (IR) tabletop exercises challenge a group of people to describe the processes by which a theoretical cybersecurity incident would be responded to and managed, from detection through remediation.

Data Security in the Age of Insider Threats: A Primer

A grand total of 94% of organizations had an insider data breach in the past year, with 84% of the data breaches resulting from human error.

5 Tips for Securing Wireless Networks

An unsecured business or home Wi-Fi network is susceptible to unauthorized access. With wireless security, you can keep unwanted users from gaining access to your network and only make it accessible to authorized persons.

New Destructive Malware Targeting Government Agencies & Organizations

The cybersecurity researchers at Microsoft have recently reported that on the websites of some Ukrainian organizations and government agencies, hackers are constantly attacking with malicious software and malware.

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

800 HACKED

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