09 June 2021

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 Future of Threat Hunting and Zero Trust: 8 Innovations to Watch at RSA

Here are eight trends shaping our industry that'll be getting some airtime, from artificial intelligence (AI) to zero trust.

$280 Million Stolen Per Month from Crypto Transactions

CyberNews researchers found that front-runners are abusing decentralized cryptocurrency exchanges by draining hundreds of millions in crypto from trader transactions on the Ethereum network. Unsuspecting traders can lose as much as $280 million to front-runners each month.

China-linked Attackers Breached Metropolitan Transportation Authority (MTA) using Pulse Secure Zero-Day

China-linked threat actors breached the network of the New York City's Metropolitan Transportation Authority (MTA) network exploiting a Pulse Secure zero-day.

Google Tool Reveals Dependencies for Open Source Projects

Google has been working on a new, experimental tool to help developers discover the dependencies of the open source packages/libraries they use and known security vulnerabilities they are currently sporting.

CRITICAL VULNERABILITIES

CVE

10 Critical Flaws Found in CODESYS Industrial Automation Software

Cybersecurity researchers on Thursday disclosed as many as ten critical vulnerabilities impacting CODESYS automation software that could be exploited to remote code execution on PLCs.

HPE Fixes Critical Zero-Day in Server Management Software

Hewlett Packard Enterprise (HPE) has fixed a critical zero-day remote code execution (RCE) flaw in its HPE Systems Insight Manager (SIM) software for Windows.

Cisco Fixes High-Severity Issues in Webex, SD-WAN, ASR 5000 Software

Cisco has addressed multiple vulnerabilities in its products, including high-risk flaws in Webex Player, SD-WAN software, and ASR 5000 series software. The IT giant fixed three high-severity vulnerabilities (CVE-2021-1503, CVE-2021-1526, CVE-2021-1502) affecting Webex Player for Windows and macOS.

Industrial Switches From Several Vendors Affected by Same Vulnerabilities

Industrial switches provided by several vendors are affected by the same vulnerabilities due to the fact that they share firmware made by Taiwan-based industrial networking solutions provider Korenix Technology.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

FireEye, Mandiant Split Apart in $1.2B Private Equity Deal

FireEye announced plans to sell its products business, including the FireEye name, as part of a $1.2 billion transaction that splits off the Mandiant Solutions unit from the company's endpoint protection and cloud security products.

Snow Software and BMC Expand Partnership to Support IT Leaders with DX and Hybrid Work Initiatives

Snow Software announced an expanded partnership and enhanced product integration with BMC Software. With the combination of Snow's comprehensive data visibility and the BMC Helix Platform, the two companies will help IT teams create agility, maintain stability and foster growth.

VMware and Zoom Enable Secure Collaboration Experience for Hybrid Work Environments

VMware announced its work with Zoom to enable a better and more secure collaboration experience for hybrid work environments. The effort delivers interoperability between the recently announced VMware Anywhere Workspace and the Zoom collaboration platform to further improve ease of use, application and network performance, and security.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Then and Now: Securing Privileged Access Within Healthcare Orgs

Healthcare organizations have always been high-value targets for cybercriminals, as their networks store large volumes of personally identifiable information (PII) including Social Security numbers, dates of birth, addresses and very sensitive personal health data.

Microsoft 365: Most Common Threat Vectors & Defensive Tips

As more organizations have grown reliant on Microsoft 365, Google Cloud, and Amazon Web Services, cybercriminals have begun to realize that the shift benefits them and are consequently tailoring their attacks to take advantage of the major cloud platforms in use by organizations.

Six Million Players' Profiles Leaked Following Cloud Misconfiguration

AMT Games has accidentally exposed almost six million players profiles due to a misconfigured cloud database.

How Do I Select a Unified Endpoint Management Solution for My Business?

To select a suitable UEM solution for your business, you need to think about a variety of factors.

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

800 HACKED