31 May 2022

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?

These are the Flaws that let Hackers Attack Blockchain and DeFi Projects

The number of decentralized finance (DeFi) and blockchain projects grew massively during the past year, but their increased popularity has also piqued the interest of cyberattackers – who managed to steal at least an estimated $1.8 billion in 2021.

6 Critical Areas of Cloud-Native Security That Are Influential in 2022

Cloud computing has emerged as the go-to organizational workload choice because of its innate scalability and flexibility. However, cloud computing still comes with some security risks. Examining cloud security is an important part of adopting this new technology.

Email is the Riskiest Channel for Data Security

A research from Tessian and the Ponemon Institute reveals that nearly 60% of organizations experienced data loss or exfiltration caused by an employee mistake on email in the last 12 months.

Prioritize Patching Vulnerabilities Associated with Ransomware

A threat research from Cyber Security Works (CSW) has revealed a 7.6% increase in ransomware vulnerabilities since the publication of the Ransomware Spotlight Report in January 2022.

CRITICAL VULNERABILITIES

CVE

Critical Flaws in Popular ICS Platform Can Trigger RCE

Cisco Talos discovered eight vulnerabilities in the Open Automation Software, two of them critical, that pose risk for critical infrastructure networks.

Tripwire Patch Priority Index for May 2022

First on the patch priority list this month are 2 remote code execution vulnerabilities for Excel and a security feature bypass vulnerability for Office. Up next are patches that affect components of the Windows operating systems.

Microsoft Patches the Patch Tuesday Patch that Broke Authentication

Two of the big-news vulnerabilities in this month's Patch Tuesday updates from Microsoft were CVE-2022-26923 and CVE-2022-26931, which affected the safety of authentication in Windows.

CISA Adds 75 Actively Exploited Bugs to Its Must-Patch List in Just a Week

The Cybersecurity And Infrastructure Security Agency (CISA) added three batches of must-fix bugs to its catalog of known exploited software vulnerabilities this week. The first covered 21 bugs, the second 20 known exploited bugs and the third covers a further 34.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Microsoft Defender vs Trellix: EDR Software Comparison

Looking to secure your network? Microsoft Defender and Trellix are two of the most popular endpoint detection and response software options. Compare the features of these EDR tools. With threats such as malware and ransomware becoming more complex, companies need to take caution to increase their network security. Both Microsoft Defender and Trellix Endpoint Security are top endpoint detection and response (EDR) software tools with a variety of features designed to help protect networks, devices and data.

Oracle selects Palo Alto Networks to Protect their Cloud Applications and Data Against Emerging Threats

Palo Alto Networks announced that Oracle has chosen Palo Alto Networks VM-Series Next-Generation Firewall (NGFW) as the technology to power the Oracle Cloud Infrastructure (OCI) Network Firewall.

FortiNDR Identifies Cyberattacks Based on Anomalous Network Activity and Limits Threat Exposure

Fortinet announced FortiNDR, a new network detection and response offering that leverages artificial intelligence and pragmatic analytics to enable faster incident detection and an accelerated threat response.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Voice Phishing Attacks Reach All-time High

Cases of voice phishing or vishing have been reported to have risen a whopping 550% over the past 12 months alone, according to the Quarterly Threat Trends & Intelligence Report co-authored by Agari and PhishLabs.

How to Improve Risk Management using Zero Trust Architecture

Risk management, the process of developing a strategy for addressing risk throughout its lifecycle, normally involves four phases: risk identification, assessment, response, and monitoring and reporting.

3 Key Elements to Protect a Kubernetes Cluster

With the rapid adoption of container-based technologies, organizations are increasingly concerned about the security of their Kubernetes clusters

Why are Current Cybersecurity Incident Response Efforts Failing?

This article will explore why current cybersecurity incident response efforts are failing, and how a proactive, risk-based approach enables companies to reduce exposure most effectively and to maximize the return on their limited resources.

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