02 March 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?

How Russia's Invasion of Ukraine Will Affect Your Cybersecurity

Russia has invaded Ukraine, and while it may feel like a selfish time to think about it, business leaders are probably wondering if this conflict means that cyberattacks from Russia will also begin to flare up.

How to Improve Threat Detection in ICS Environments

A new report, "2021 MITRE Engenuity ATT&CK Evaluations for ICS," produced by Dragos, evaluates the ICS threat detection market and shows a realistic demonstration of an attack against an operational technology environment.

Lack of Visibility Plaguing ICS Environments

Dragos released its report on cyber threats facing industrial organizations, naming the emergence of three new threat groups targeting ICS/OT environments, including two that have gained access into the OT systems of industrial organizations.

Anonymous Hit Russian Nuclear Institute and Leak Stolen Data

Anonymous and other hacker groups that responded to the call to war against Russia continue to launch cyberattacks on gov organizations and businesses. Anonymous and numerous hacker groups linked to the popular collective continue to launch cyber-attacks against Russian and Belarussian government organizations and private businesses.

CRITICAL VULNERABILITIES

CVE

Microsoft Exchange Bugs Exploited by 'Cuba' Ransomware Gang

The ransomware gang known as Cuba is increasingly shifting to exploiting Exchange bugs – including crooks' favorites, ProxyShell and ProxyLogon – as initial infection vectors.

New Critical RCE Bug Found in Adobe Commerce, Magento

Adobe updated its recent out-of-band security advisory to add another critical bug, while researchers put out a PoC for the one its emergency-fixed last weekend.

High-Severity RCE Bug Found in Popular Apache Cassandra Database

The bug, which involves how Cassandra creates user-defined-functions (UDFs) to perform custom processing of data, is tracked as CVE-2021-44521, with a high-severity rating of 8.4.

Critical VMware Bugs Open ESXi, Fusion & Workstation to Attackers

A group of five security vulnerabilities could lead to a range of bad outcomes for virtual-machine enthusiasts, including command execution and DoS. The bugs have a range of 5.3 to 8.4 out of 10 on the CVSS vulnerability-severity scale, making them individually "important" or "moderate" issues.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Palo Alto Networks Prisma SASE Provides Network Security and SD-WAN Requirements for MSPs

Managed service providers (MSPs) have struggled to deliver SASE services cost-effectively at scale because current SD-WAN and secure access solutions for the hybrid work force lack automation, requiring manual configuration and support for disparate products and API models. Solving this challenge, Palo Alto Networks introduced new innovations for Prisma SASE specifically designed for MSPs, including a hierarchical multitenant cloud management portal and open API framework.

Zadara Partners with Seagate to Accelerate Cloud Adoption for Enterprises

Zadara announced that it is working together with Seagate to deploy zCompute, its elastic, enterprise-grade compute infrastructure, in Seagate's storage-as-a-service (STaaS) Lyve Cloud platform.

Benu Networks Collaborates with AWS to Bring Cloud-Native Networks for Service Providers

Benu Networks announced it is working with AWS to allow communication service providers (CSPs) to deploy Benu Networks' cloud-native Broadband Network Gateway (BNG) and Secure Access Service Edge (SASE) solutions on AWS.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

How Businesses Benefited from Cloud Transformation

Aptum released a report which explores the deployment of workloads on different cloud infrastructures and examines the decision-making process behind their placement.

IoT Security is Foundational, Not Optional

A PSA Certified report predicts that this year will mark a turning point in securing the Internet of Things (IoT), as the industry collectively commits to addressing the historic lag between the rate of digital transformation and the speed of securing the ecosystem.

Microsoft: Cyberattacks in Ukraine Hitting Civilian Digital Targets

Microsoft is calling attention to a surge in cyberattacks on Ukrainian civilian digital targets, warning that the new "digital war" includes destructive malware attacks on emergency response services and humanitarian aid efforts.

Protect From Cyberattacks With These 6 Steps For Cyber Resilience

The pros behind Carbonite + Webroot joined forces with researchers at IDC to develop an easy-to-understand framework for fighting back against cybercrime. The results? A 6-step plan for adopting a cyber resilience strategy meant to keep businesses safe.

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