02 June 2021

WEEKLY CYBER THREAT LEVEL INDICATOR

ELEVATED 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?

Amazon Web Services to Open Data Centers in the UAE
The new AWS Middle East (UAE) region will consist of three availability zones (data centers) and become AWS's second region in the Middle East after Bahrain. It will enable local customers with data residency requirements to store their data in the UAE, while also providing even lower latency across the country.

OT Systems Increasingly Targeted by Unsophisticated Hackers: Mandiant
Unsophisticated threat actors — in many cases motivated by financial gain — have increasingly targeted internet-exposed operational technology (OT) systems, according to research conducted by Mandiant, FireEye's threat intelligence and incident response unit.

Bose Admits Ransomware Hit: Employee Data Accessed
The consumer-electronics stalwart was able to recover without paying a ransom, it said. High-end audio-tech specialist Bose has disclosed a ransomware attack, which it said rippled "across Bose's environment" and resulted in the possible exfiltration of employee data.

Combatting Insider Threats with Keyboard Security
As cyberattacks snowball and insider threats become an ever-larger part of the problem, it may be time to move beyond purely software-based cyber-defenses. Implementing hardware-based security, like secure keyboards, can be an important part of the mix.

CRITICAL VULNERABILITIES

CVE

A New Bug in Siemens PLCs Could Let Hackers Run Malicious Code Remotely
The memory protection bypass vulnerability, tracked as CVE-2020-15782 (CVSS score: 8.1), was discovered by operational technology security company Claroty by reverse-engineering the MC7 / MC7+ bytecode language used to execute PLC programs in the microprocessor.

VMware Sounds Ransomware Alarm Over Critical Severity Bug
VMware patched a critical bug impacting its vCenter Server platform with a severity rating of 9.8 out of 10.

SonicWall Urges Customers to Address a Post-authentication Flaw that Affects On-Premises Versions of the Network Security Manager (NSM)
SonicWall urges customers to 'immediately' address a post-authentication vulnerability, tracked as CVE-2021-20026, impacting on-premises versions of the Network Security Manager (NSM).

Pulse Secure VPNs Get Quick Fix for Critical RCECVSS v3 9.8
The company explained that this high-severity bug — identified as CVE-2021-22908 and rated CVSS 8.5 — affects Pulse Connect Secure versions 9.0Rx and 9.1Rx.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Versa SASE Delivers Secure SD-WAN Connectivity with Google Cloud NCC
Versa Networks announced its integration with Google Cloud Network Connectivity Center (NCC), allowing for secure and reliable connectivity to cloud workloads and on-premises resources in an automated, dynamic approach that reduces total costs of ownership.

3Cloud Partners with Databricks to Simplify Data and AI Workflows, Improve Collaboration
3Cloud announced they have partnered with Databricks to drive business value by unifying data and artificial intelligence (AI). Azure Databricks is one of the fastest growing Azure services and has become a key part of 3Cloud's toolset for building modern, cloud-based data and AI platforms for its clients.

Elastic Expands Partnership with Microsoft to Help Customers Consolidate and Secure their Data
Elastic announced an expanded strategic partnership with Microsoft. From directly within the Microsoft Azure portal, customers can now find, deploy, and manage Elasticsearch and accelerate their time to value with Elastic Cloud solutions, including Elastic Enterprise Search, Observability, and Security.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Newly Discovered Bugs in VSCode Extensions Could Lead to Supply Chain Attacks
Severe security flaws uncovered in popular Visual Studio Code extensions could enable attackers to compromise local machines as well as build and deployment systems through a developer's integrated development environment (IDE).

How Are Cyber Insurance Companies Assessing Ransomware Risk?
Colonial Pipeline recently shelled out $4.4 million to recover its data following a ransomware attack that forced it to shut down thousands of miles of pipeline. The decision potentially left its insurer on the hook for the bill.

The Benefits and Drawbacks of Geo-Restrictions
Microsoft have recently shared details of a new threat in the wild aiming to steal users' data. Dubbed RevengeRAT or AsyncRAT, the malware currently spreads via spear phishing emails, for which, Microsoft warns users to stay cautious.

Why is Patch Management So Difficult to Master?
According to a Ponemon Institute report, more than 40% of IT and security workers indicated they suffered a data breach in the last two years due to unpatched vulnerabilities.

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