08 March 2021

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?

Massive Supply-Chain Cyberattack Breaches Several Airlines

The cyberattack on SITA, a nearly ubiquitous airline service provider, has compromised frequent-flyer data across many carriers. A communications and IT vendor for 90 percent of the world's airlines, SITA, has been breached, compromising passenger data stored on the company's U.S. servers in what the company is calling a "highly sophisticated attack."

A Better Cloud Access Security Broker: Securing Your SaaS Cloud Apps and Services with Microsoft Cloud App Security

Today's business uses an average of 1,180 cloud apps, with many of those organizations securing their apps through cloud access security brokers (CASB). The organizational need for a CASB has grown alongside the use of cloud apps to enable remote work and greater user productivity.

XLM + AMSI: New Runtime Defense Against Excel 4.0 Macro Malware

This integration, an example of the many security features released for Microsoft 365 Apps on a regular basis, reflects commitment to continuously increase protection for Microsoft 365 customers against the latest threats.

CRITICAL VULNERABILITIES

CVE

Five Privilege Escalation Flaws Fixed in Linux Kernel

Experts found five vulnerabilities in the Linux kernel, tracked as CVE-2021-26708, that could lead to local privilege escalation.

Multiple Cisco Products Exposed to DoS Attack Due to a Snort Issue

The vulnerability, tracked as CVE-2021-1285, can be exploited by an unauthenticated, adjacent attacker to trigger a DoS condition by sending it specially crafted Ethernet frames.

VMware Addresses Remote Code Execution Issue in View Planner

VMware addresses Remote Code Execution issue in View Planner. VMware released a security patch for a remote code execution flaw, tracked as CVE-2021-21978, that affects the VMware View Planner.

Microsoft: These Exchange Server Zero-Day Flaws Are Being Used by Hackers, So Update Now

The four bugs are being tracked as CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. Washington DC-based security firm Volexity said in its analysis that the vulnerability CVE-2021-26855 was being used to steal the full contents of several user mailboxes.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

CrowdStrike Falcon Platform Enhancements Improve SOC Efficiency

CrowdStrike announced enhancements to the CrowdStrike Falcon platform that significantly improve Security Operations Center (SOC) efficiency and effectiveness, allowing security teams to focus on critical priorities and fortify their organizations' proactive stance against cyber threats.

Supermicro and PulseSecure Issue Advisories on Trickboot

Supermicro and Pulse Secure have each issued advisories this past week warning users that some of their products are vulnerable to the updated version of Trickbot malware that features a bootkit module, nicknamed Trickboot, which can search for UEFI/BIOS firmware vulnerabilities.

Microsoft releases IOC Detection Tool for Microsoft Exchange Server Flaws

This week Microsoft has released emergency out-of-band security updates that address four zero-day issues (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) in all supported MS Exchange versions that are actively exploited in the wild.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Check to See If You're Vulnerable to Microsoft Exchange Server Zero-Days Using this Tool

Microsoft's team has published a script on GitHub that can check the security status of Exchange servers. The script has been updated to include indicators of compromise (IOCs) linked to four zero-day vulnerabilities found in Microsoft Exchange Server.

5 Ways Social Engineers Crack Into Human Beings

Social engineers use psychological manipulation to trick human beings into divulging sensitive information that can then be used to break into systems.

How Enterprise Design Thinking Can Improve Data Security Solutions

Design must reflect the practical and aesthetic in business, but above all, good design must primarily serve people.

Cybersecurity Risks and Challenges Facing the Financial Industry

According to IBM's Cost of a Data Breach 2020 report, the average cost of a data breach in the financial services sector was US$5.85 million compared to US$3.86 million across respondents in all sectors in its survey.

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