08 December 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?

Why the Future Needs Passwordless Authentication
The Redmond-based tech giant noted that users could instead use its authenticator app, Windows Hello; a physical security key or a verification code sent via SMS-based text message to sign in to Outlook, OneDrive and other Microsoft services.

4 Trends Disrupting Managed Infrastructure Services
Innovations, digital transformations, cloud-based infrastructure offerings (e.g., security-as-a-service), and the emergence of hyperscalers are changing the definition of infrastructure and infrastructure managed services.

Vulnerability Scanning Frequency Best Practices
How often you should run your scans, though, isn't such a simple question. The answers aren't the same for every type of organization or every type of system you're scanning.

Ransomware – How to Stop It, and How to Survive An Attack
Ransomware attacks dominate the cybersecurity news headlines, with businesses all over the world wondering if they will be the next victim.

Nobelium Continues to Target Organizations Worldwide with Custom Malware
Russia-linked Nobelium APT group is using a new custom malware dubbed Ceeloader in attacks against organizations worldwide.

CRITICAL VULNERABILITIES

CVE

Virtual-Network Vulnerability Found in AWS, Other Clouds
A vulnerability in a library created by network virtualization firm Eltima — and used by a variety of vendors, including Amazon — has left more than a dozen cloud services vulnerable to a privilege escalation attack.

Attackers Exploit Another Zero-Day in ManageEngine Software (CVE-2021-44515)
CVE-2021-44515 is an authentication bypass vulnerability that could be triggered by attackers by sending a specially crafted request, with the goal of achieving unauthenticated remote code execution.

Unpatched Windows Zero-Day Allows Privileged File Access
A temporary fix has been issued for CVE-2021-24084, which can be exploited using the LPE exploitation approach for the HiveNightmare/SeriousSAM bug.

Windows 10 Drive-By RCE Triggered by Default URI Handler
Researchers have discovered a drive-by remote code-execution (RCE) bug in Windows 10 via Internet Explorer 11/Edge Legacy – the EdgeHTML-based browser that's currently the default browser on Windows 10 PCs – and Microsoft Teams.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Cloudflare Expands Firewall Capabilities to Help Companies Secure their Entire Corporate Network
Cloudflare announced it's expanding its Zero Trust firewall capabilities to help companies secure their entire corporate network across all of their branch offices, data centers, and clouds—no matter where their employees are working from.

Wipro Partners with Celonis to Help Enterprises Optimize their Supply Chain Management
The solution enables companies to automatically identify and fix process bottlenecks and inefficiencies, gain powerful business insights, open new growth opportunities, manage risks and maintain business continuity even in disruptive times.

SS8 Networks Partners with Ocient to Deliver High-Performance Solutions for Law Enforcement Customers
SS8 Networks announced a collaboration with Ocient to harness petabytes of data for lawful intelligence in interactive time. Together, SS8 and Ocient provide LEAs a highly scalable analytics platform and visualization engine capable of ingesting 10's of millions of records per second and returning actionable intelligence in seconds.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Cybercrime Supply Chain: Fueling the Rise in Ransomware
Trend Micro released a research detailing the murky cybercrime supply chain behind much of the recent surge in ransomware attacks.

Why the C-Suite Doesn't Need Access to All Corporate Data
The key to the zero-trust framework is the principle of least privilege, which is the notion that all users are provided with the minimum level of access required to complete a task. Likewise, users should only be granted access to a particular app, system, or network when they need access.

5 Ways GRC & Security Can Partner to Reduce Insider Risk
From an organizational perspective, taking a granular look at the new world of hybrid-remote work, the data protection needed for the 2022 world is markedly different from the data protection of 2020. How have things changed?

APT Groups Adopt New Phishing Method. Will Cybercriminals Follow?
APT groups from Russia, China, and India have adopted a new and easily implemented phishing method throughout the second and third quarters of this year that researchers say is poised for broader adoption among cybercriminals as well.

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