06 May 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?

Experts Comments on World Password Day

World Password Day has served as an annual reminder that we all need to practice better password security for nearly a decade. And yet, 80% of breaches began with brute force attacks, or lost or stolen credentials last year.

Security Expert Re: Tesla Cars Hacked Remotely by Drone

Automotive manufacturers must design resilient and safety-critical systems with an attacker's perspective in mind. Wi-Fi systems have been shown to be the weak spot when attacking infotainment and console systems, as seen in a different vulnerability found last year in a 3rd party WiFi component used by Tesla.

Scripps Health Cyberattack Causes Widespread Hospital Outages

Scripps Health, a hospital network based in San Diego, was hit by a cyberattack over the weekend, forcing some critical-care patients to be diverted, according to the San Diego Union-Tribune. Scripps acknowledged the attack in a statement but didn't specify whether it was a ransomware incident.

Ransomware Gang Exploits SonicWall Zero-Day Flaw

A cyberthreat gang that's been active since 2020 exploited a now-patched zero-day vulnerability in the SonicWall SMA 100 Series appliance to plant ransomware in attacks launched earlier this year, FireEye Mandiant researchers say.

CRITICAL VULNERABILITIES

CVE

Pulse Secure VPNs Get a Fix for Critical Zero-Day Bugs

Pulse Secure has rushed a fix for a critical zero-day security vulnerability in its Connect Secure VPN devices, which has been exploited by nation-state actors to launch cyberattacks.

Hewlett Packard Enterprise Plugs Critical Bug in Edge Platform Tool

The unpatched versions of HPE's Edgeline Infrastructure Manager are open to remote authentication-bypass attacks.

Microsoft Warns of 25 Critical Vulnerabilities in IoT, Industrial Devices

Security researchers at Microsoft are warning the industry about 25 as-yet undocumented critical memory-allocation vulnerabilities across a number of vendors' IoT and industrial devices.

F5 Big-IP Vulnerable to Security-Bypass Bug

The KDC-spoofing flaw tracked as CVE-2021-23008 can be used to bypass Kerberos security and sign into the Big-IP Access Policy Manager or admin console.

Hundreds of Millions of Dell Users at Risk from Kernel-Privilege Bugs

Five high-severity security flaws in Dell's firmware update driver are impacting potentially hundreds of millions of Dell desktops, laptops, notebooks and tablets, researchers said.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Imperva Acquires CloudVector to Provide Visibility and Security for API Traffic

Imperva announced it has entered into an agreement to acquire CloudVector. CloudVector enables customers to discover, monitor, and protect all API traffic in any environment from exploits and breaches.

Wipro Partners with Citrix and HPE to Accelerate Remote Working and Modernize Workspaces

Wipro Limited announced that it has strengthened its alliance with Citrix Systems and Hewlett Packard Enterprise (HPE). The partnership will provide enterprises a robust solution that will accelerate remote working and bring modernization into workspaces.

DigitalOcean Admits Data Breach Exposed Customers' Billing Details

DigitalOcean, the popular cloud-hosting provider, has told some of its customers that their billing details were exposed due to what it described as a "flaw." In an email sent out to affected users, DigitalOcean explained that an unauthorised party had managed to exploit the flaw to gain access to billing information.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

The Wages of Password Re-use: Your Money or Your Life

When normal computer users fall into the nasty habit of recycling passwords, the result is most often some type of financial loss. When cybercriminals develop the same habit, it can eventually cost them their freedom.

Third Parties Caused Data Breaches at 51% of Organizations

Remote access is becoming an organization's weakest attack surface, according to new research published today by the Ponemon Institute and third-party remote access provider SecureLink.

How Cost Cutting on Cybersecurity Presents an Opportunity for Hackers

Barracuda network's new research states that 41 % of businesses across the world have expense-cut on security budgets due to the economic crises of the COVID-19 epidemic.

92% Of Organizations Who Pay Ransoms Don't Get All Their Data Back

As reported by teiss, as many as 92% of organisations who paid a ransom in the past 12 months did not get all of their data back, with the average organisation getting back just 65% of its data.

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