29 June 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?

Mercedes-Benz USA Disclosed a Data Breach that Impacted 1.6 Million Customers, Exposed Data Includes Financial Data and Social Security Numbers (SSNs)

Mercedes-Benz USA disclosed a data breach that impacted some of its customers and potential vehicle buyers.

Cloud Database Exposes 800M+ WordPress Users' Records

A misconfigured cloud database exposed over 800 million records linked to WordPress users before its owner was notified, according to Website Planet.

SolarWinds Hackers Breach Microsoft Customer Support to Target its Customers

The latest wave in a series of intrusions is said to have primarily targeted IT companies, followed by government agencies, non-governmental organizations, think tanks, and financial services, with 45% of the attacks located in the U.S., U.K., Germany, and Canada.

Hackers Trick Microsoft Into Signing Netfilter Driver Loaded With Rootkit Malware

Microsoft on Friday said it's investigating an incident wherein a driver signed by the company turned out to be a malicious Windows rootkit that was observed communicating with command-and-control (C2) servers located in China.

CRITICAL VULNERABILITIES

CVE

Cisco ASA Bug Now Actively Exploited as PoC Drops

In-the-wild XSS attacks have commenced against the security appliance (CVE-2020-3580), as researchers publish exploit code on Twitter.

Critical VMware Carbon Black Bug Allows Authentication Bypass

The 9.4-rated bug in AppC could give attackers admin rights, no authentication required, letting them attack anything from PoS to industrial control systems.

Critical Palo Alto Cyber-Defense Bug Allows Remote 'War Room' Access

Remote, unauthenticated cyberattackers can infiltrate and take over the Cortex XSOAR platform, which anchors unified threat intelligence and incident responses.

Fortinet has recently Fixed a High-Severity Vulnerability Affecting its FortiWeb Web Application Firewall (WAF)

Fortinet has recently addressed a high-severity vulnerability (CVE-2021-22123) affecting its FortiWeb web application firewall.

SonicWall 'Botches' October Patch for VPN Bug

Company finally rolls out the complete fix this week for a flaw affecting some 800,000 devices that could result in crashes or prevent users from connecting to corporate resources.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Zyxel Warns Customers of Attacks on Security Appliances

Networking device manufacturer Zyxel has issued an alert to warn customers of attacks targeting a subset of security appliances that have remote management or SSL VPN enabled.

MITRE D3FEND: Enabling cybersecurity pros to tailor defenses against specific cyber threats

D3FEND, a framework for cybersecurity professionals to tailor defenses against specific cyber threats is now available through MITRE. NSA funded MITRE's research for D3FEND to improve the cybersecurity of National Security Systems, the Department of Defense, and the Defense Industrial Base. The D3FEND technical knowledge base of defensive countermeasures for common offensive techniques is complementary to MITRE's ATT&CK, a knowledge base of cyber adversary behavior.

eSentire Acquires CyFir; Launches Cyber Investigation Services

eSentire, a managed detection and response service provider, has acquired digital forensics and investigative tools provider CyFIR, and launched an associated Cyber Investigations Portfolio.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

USB Threats Could Critically Impact Business Operations

According to a report released by Honeywell, USB threats that can severely impact business operations increased significantly during a disruptive year when the usage of removable media and network connectivity also grew.

How Do I Select a Big Data Solution for My Business?

The best customer data platform (CDPs) allow you to plug your data into whichever tools work best for you, and let you switch tools on and off as your business evolves, making them a solid long-term investment.

5 Ways To Ensure Data Security In Software Documentation

Businesses deal with different software documents every day. They contain sensitive information that involves various business transactions, processes, and systems. Hence, it's crucial to ensure data security when managing software documentation.

Your Password is Too Predictable

Password predictability is one of the most significant challenges to overall online security. Well aware of this trend, hackers often seek to exploit what they assume are the weak passwords of the average computer user.

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