22 February 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?

Microsoft Rolls Out "Kids Mode" For Safe Browsing In Edge Browser

In a recent blog post, Microsoft has announced the launch of a new feature with its Edge browser – the "Kids Mode".

International Law Firm Jones Day Hacked with Data Posted on Dark Web

This week, it was confirmed that international law firm Jones Day had data stolen from cybercriminals and is a direct result of the wider data breach suffered by file-sharing service Accellion. The hacker, which goes by the name Clop, had uploaded much of the sensitive information on the dark web which may have included data on prominent clients like Donald Trump.

Kia Outage May be the Result of Ransomware

Kia Motors America may have been hit by a ransomware attack that has taken down some of its key customer-facing services. In a story published, website BleepingComputer reported that Kia Motors USA was suffering a nationwide outage that was impacting IT servers, self-payment phone services, dealer platforms, phone support, and mobile apps.

CRITICAL VULNERABILITIES

CVE

Privacy Bug in Brave Browser Exposes Dark-Web Browsing History of Its Users

Brave has fixed a privacy issue in its browser that sent queries for .onion domains to public internet DNS resolvers rather than routing them through Tor nodes, thus exposing users' visits to dark web websites.

Now-Patched Telegram Vulnerabilities Could Allow Spying On Chats Via Animated Stickers

Telegram Vulnerabilities Exposing Chats Via Stickers An Italian security firm Shielder shared details of some Telegram vulnerabilities that anyone could exploit by sending malicious animated stickers.

Unpatched SHAREit Flaw Let Attackers Execute Remote Code

Experts from Trend Micro discovered vulnerabilities in the SHAREit application, which has over 1 billion downloads in Google Play.

Microsoft Pulls Bad Windows Update After Patch Tuesday Headaches

Microsoft released a new servicing stack update (KB5001078) after an older one caused problems for Windows users installing Patch Tuesday security updates.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

CrowdStrike to Acquire Humio for $400 Million

Crowdstrike announced on Thursday a deal to acquire the cloud log management and observability technology firm Humio for $400 million. CrowdStrike says its acquisition of 5-year-old Danish firm Humio will enable it to further expand its eXtended Detection and Response capabilities by taking in and correlating data from any log, application or feed to deliver actionable insights and real-time protection.

Palo Alto Networks Buys Bridgecrew in 'Shift Left' Cloud Security Push

Palo Alto Networks on Tuesday snapped up early-stage startup Bridgecrew, adding a cloud security platform for developers to its $3.4 billion-a-year enterprise product portfolio. For Palo Alto, the deal is part of a strategy to spend big to snap up early-stage companies in the cloud security and DevOps workflow space.

Microsoft's Power BI Gets New Tools to Prevent Leakage of Confidential Data

Information protection makes sure that only people with permissions see data in Power BI, while retaining the ability to share top-level trends, balancing productivity and security.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

2020 Middle East Encryption Trends Study

The Middle East Encryption Trends Study highlights how leading organizations are applying their encryption strategies and the challenges they are facing.

Microsoft Starts Removing Flash from Windows Devices via New KB4577586 Update

Microsoft has begun deploying this week KB4577586, a Windows update that permanently removes the Adobe Flash Player software from Windows devices.

SolarWinds Hackers Stole Some Source Code for Microsoft Azure, Exchange, Intune

Microsoft on Thursday said it concluded its probe into the SolarWinds hack, finding that the attackers stole some source code but confirmed there's no evidence that they abused its internal systems to target other companies or gained access to production services or customer data.

5 Security & Productivity Hacks for Home Businesses

The five security and productivity hacks that can help SMBs be effective and efficient in the months and years ahead.

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