27 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?

Rapid7 Admit Suffering An Impact Due To Codecov Breach
Rapid7 Disclosed Codecov Supply-Chain Attack Impact
Cybersecurity firm Rapid7 has recently confirmed a breach due to the Codecov supply-chain attack.

Air India: Supplier Breach Hit 4.5 Million Passengers
Air India has confirmed that 4.5 million passengers have had their personal data exposed in a third-party data breach first disclosed over two months ago. The incident impacted SITA, an IT provider which claims to serve around 90% of the aviation industry. Attackers compromised servers that operate passenger processing systems for airline clients.

Cloud Security Blind Spots: Where They Are and How to Protect Them
Enterprise cloud adoption brings myriad benefits, risks, challenges, and opportunities — both for organizations and attackers who target them. Even longtime users of cloud infrastructure and services could still learn a thing or two about strengthening security.

Why Password Hygiene Needs a Reboot
In today's digital world, password security is more important than ever. While biometrics, one-time passwords (OTP), and other emerging forms of authentication are often touted as replacements to the traditional password, today, this concept is more marketing hype than anything else.

CRITICAL VULNERABILITIES

CVE

ICS Vendors Assessing Impact of New OPC UA Vulnerabilities
Multiple companies that develop industrial systems are assessing the impact of two new OPC UA vulnerabilities on their products, and German automation technology firm Beckhoff is the first to release a security advisory.

Windows PoC Exploit Released for Wormable RCE
A researcher has released a proof-of-concept (PoC) exploit for CVE-2021-31166, a use-after-free, highly critical vulnerability in the HTTP protocol stack (http.sys) that could lead to wormable remote code execution (RCE).

WP Statistics Bug Allows Attackers to Lift Data from WordPress Sites
The plugin, installed on hundreds of thousands of sites, allows anyone to filch database info without having to be logged in.

ICS Advisory (ICSA-21-119-04) - Multiple RTOS (Update B)
- CVSS v3 9.8
- Integer Overflow or Wraparound

ICS Advisory (ICSA-21-138-01) - Emerson Rosemount X-STREAM
- CVSS v3 7.5
- Inadequate Encryption Strength, Cross-site Scripting

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Splunk to Acquire TruSTAR for Data Management
Splunk plans to acquire threat intelligence management provider TruSTAR to bring its intel-sharing and automation capabilities into its portfolio. TruSTAR is a cloud-native tool designed to reduce complexity and improve threat detection and response.

McAfee MVISION XDR Protects Organizations Against the Most Advanced Cyber Threats
McAfee announced significant expansion of its MVISION Extended Detection and Response (XDR) solution by correlating the extensive telemetry of McAfee's endpoint security solution, Secure Access Service Edge (SASE) solution, and threat intelligence solution powered by MVISION Insights.

Fidelis Cybersecurity Acquires CloudPassage to Enhance Its Active XDR Platform
Fidelis Cybersecurity announced the acquisition of CloudPassage. Founded in 2010, San Francisco-based CloudPassage safeguards cloud infrastructure for the world's most-recognized brands in finance, e-commerce, gaming, B2B SaaS, healthcare, biotech, and digital media. The CloudPassage Halo platform unifies security and compliance across servers, containers, and IaaS resources across any mix of public, private, hybrid, and multi-cloud environments.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Microsoft, Google Clouds Hijacked for Gobs of Phishing
Attackers sent 52M malicious messages leveraging the likes of Office 365, Azure, OneDrive, SharePoint, G-Suite and Firebase storage in Q1 2021.

Mitigate OT Security Threats with these Best Practices
The security community is continuously changing, growing, and learning from each other to better position the world against cyber threats.

Microsoft Warns of RevengeRAT Under Distribution Via Spearphishing Emails
Microsoft have recently shared details of a new threat in the wild aiming to steal users' data. Dubbed RevengeRAT or AsyncRAT, the malware currently spreads via spear phishing emails, for which, Microsoft warns users to stay cautious.

How Do I Select an eSignature Solution for My Business?
Organizations considering eSignature solutions need to be thoughtful about the eSignature technology they implement and think about a range of requirements such as technology infrastructure, scale, security, choice, and licensing models.

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