17 May 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?

Rapid7 Source Code Accessed in Supply Chain Attack

An investigation of the Codecov attack revealed intruders accessed Rapid7 source code repositories containing internal credentials and alert-related data.

Microsoft Adds GPS Location to Identity & Access Control in Azure AD

Microsoft has announced new identity and access management capabilities to its Azure Active Directory Conditional Access feature, built to give admins more control over how resources are accessed and help them handle access policies and authentication for virtual machines (VMs).

Colonial Pipeline Shells Out $5M in Extortion Payout, Report

According to news reports, Colonial Pipeline paid the cybergang known as DarkSide the ransom it demanded in return for a decryption key. Colonial Pipeline Co., operator of the largest U.S. fuel pipeline, reportedly paid $5 million to criminals behind a ransomware attack that has sent fuel prices spiking up and down the East Coast.

200K Veterans' Medical Records May Have Been Stolen by Ransomware Gang

A database filled with the medical records of nearly 200,000 U.S. military veterans was exposed online by a vendor working for the Veterans Administration, according to an analyst.

CRITICAL VULNERABILITIES

CVE

Critical Cisco SD-WAN, HyperFlex Bugs Threaten Corporate Networks

Cisco has addressed two critical security vulnerabilities in the SD-WAN vManage Software, one of which could allow an unauthenticated attacker to carry out remote code execution (RCE) on corporate networks or steal information.

Hackers Leverage Adobe Zero-Day Bug Impacting Acrobat Reader

A patch for Adobe Acrobat, the world's leading PDF reader, fixes a vulnerability under active attack affecting both Windows and macOS systems that could lead to arbitrary code execution.

Cisco has Fixed a six-month-Old Zero-day Vulnerability Found in the Cisco AnyConnect

The Cisco Product Security Incident Response Team (PSIRT) has recently fixed a six-month-old zero-day vulnerability that is tracked as "CVE-2020-3556" in Cisco AnyConnect Security Client.

Anti-Spam WordPress Plugin Could Expose Website User Data

An SQL-injection vulnerability discovered in a WordPress plugin called "Spam protection, AntiSpam, FireWall by CleanTalk" could expose user emails, passwords, credit-card data and other sensitive information to an unauthenticated attacker.

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.

Forrester Recognizes Cisco Secure Endpoint Advancements – Promotes to Strong Performer

Secure Endpoint offers more as shown in new Forrester Wave report. At the publishing of the previous Q3 2019 Forrester Wave report for Endpoint Security Suites, Secure Endpoint was lauded as one of the least obtrusive security products to end-user productivity.

Cisco Confirms Plans to Acquire Kenna Security

Cisco confirmed plans to acquire Kenna Security, provider of vulnerability management technology, with plans to integrate its capabilities into the SecureX platform. Kenna Security's technology uses machine learning to analyze threat data and identify which risks organizations should prioritize – a useful technology to have at a time when organizations are struggling with a broader attack surface and myriad security point products.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Critical Infrastructure Remains At Risk Following Ransomware Attack

Critical infrastructure has increasingly become a top target for cybercriminals. Over the weekend, we learned of the ransomware attack against a U.S. fuel company, Colonial Pipeline, that carries nearly half the fuel consumed along the U.S. East Coast.

Cloudflare Wants to Kill the CAPTCHA

Cloudflare is testing out the possibility of security keys replacing one of the most irritating aspects of web browsing: the CAPTCHA.

Passwordless Authentication Enhances But Doesn't Replace Access Security Strategy

Passwordless has arrived. The key components enabling the new authentication technology are all in place. The quality of biometric sensors built into modern hardware has improved drastically in the past several years.

Does Multifactor Authentication Keep Your Remote Workers Safe?

A recovery phone number, a common MFA measure, stopped 100% of automated bot attacks and 99% of bulk phishing attacks. However, the multifactor authentication method prevented only 70% of targeted attacks.

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