29 March 2022

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?

Extended Threat Intelligence: A New Approach to Old School Threat Intelligence

In 2021, ransomware gangs alone made at least $590 million in profits, according to U.S. Treasury Department. As threat actors leverage more targeted tactics, techniques, and procedures (TTPs) to successfully exploit vulnerable systems, security teams are increasingly looking for laser-focused solutions that would alert them with early-warning signals of cyber threats.

6 Critical Areas of Cloud-Native Security That Are Influential in 2022

Cloud computing has emerged as the go-to organizational workload choice because of its innate scalability and flexibility.

Top 3 Attack Trends in API Security

In late July 2021, online retailers got hit with a jaw-dropping 2,800 percent increase in attack takeovers. Dead-set on gift card fraud via "scrape for resale" and other types of fraud, the attacks spiraled up to the rate of 700,000 attacks per day.

FBI: 649 Ransomware Attacks Reported on Critical Infrastructure Organizations in 2021

Ransomware attacks hit 14 out of 16 critical infrastructure sectors last year, with healthcare and public health impacted the most, the IC3 notes in its 2021 Internet Crime Report.

CRITICAL VULNERABILITIES

CVE

Zero-Click Flaws in Widely Used UPS Devices Threaten Critical Infrastructure

The 'TLStorm' vulnerabilities, found in APC Smart-UPS products, could allow attackers to cause both cyber and physical damage by taking down critical infrastructure.

Microsoft Addresses 3 Zero-Days & 3 Critical Bugs for March Patch Tuesday

Microsoft has addressed 71 security vulnerabilities in its scheduled March Patch Tuesday update – only three of which are rated critical in severity. The other 68 are all rated "important."

VMware Patches Critical Vulnerabilities in Carbon Black App Control

VMware this week announced software updates that address two critical-severity vulnerabilities in its Carbon Black App Control product. An attacker looking to exploit the bug needs to be authenticated as a high-privileged user and requires network access to the App Control interface in order to execute commands on the server.

Sophos Patches Critical Remote Code Execution Vulnerability in Firewall

Tracked as CVE-2022-1040 and issued a CVSS score of 9.8 by Sophos as a CNA, the vulnerability impacts Sophos Firewall v18.5 MR3 (18.5.3) and older.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Contrast Security Works with Global Businesses to Build Overall Security Readiness and Resilience

Contrast Security announced its commitment to ally with and protect customers during the current state of heightened cybersecurity risks, as the Russia-Ukraine conflict continues. In addition to increased security controls, Contrast's dedicated DefCon and incident response teams are actively monitoring and communicating identified security vulnerabilities in relation to potential nation-state attacks.

DTEX Systems Extends Scope and Protection of Microsoft 365 E5 Modules

DTEX Systems announced new capabilities within its DTEX InTERCEPT for Behavioral DLP solution that expand the scope and protection provided by multiple Microsoft 365 E5 modules to provide wholistic behavioral data loss prevention and workforce activity intelligence capabilities across the entirety of an enterprise's application, data, and operating system architecture.

EY Collaborates with Infosys to Accelerate Digital Transformation for Organizations

EY announced a new global alliance with Infosys to support organizations in their end-to-end business transformation and growth.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Misconfigured Firebase Databases Exposing Data in Mobile Apps

Thousands of mobile apps – some of which have been downloaded tens of millions of times – are exposing sensitive data from open cloud-based databases due to misconfigured cloud implementations, new research from Check Point has found.

Here's How Fast Ransomware Encrypts Files

Forty-two minutes and 54 seconds: that's how quickly the median ransomware variant can encrypt and lock out a victim from 100,000 of their files.

What Is Multi-Factor Authentication, and What Does It Have to Do with You?

Security isn't a simple matter of caring or spending time reading manuals or being told what you can or can't do. Security is understanding how to view the world from a different perspective: instead of functional does it work, viewing it as how can I break it.

Is Next-Gen Threat Modeling Even About Threats?

The threat landscape evolves with technology, and as threats grow in sophistication, there are concerns about major events like the Colonial Pipeline ransomware attack or the Equifax breach repeating themselves elsewhere.

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