November 2020

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?

McAfee Launches XDR, Browser Isolation, Cloud App Security Tools

McAfee today released multiple new security products during its MPOWER Digital 2020 event. Tools focus on cloud application security, remote browser isolation and extended detection and response to help defend against, and address, security threats.

Neural Networks Help Users Pick More-Secure Passwords

Neural networks trained to learn attackers' approaches to brute-force password guessing can be used as a way to enforce minimal password security without resorting to large blocklists and cumbersome combinations of letters, numbers, and special symbols, a research team at Carnegie Mellon University conclude in a new paper.

Implementing Proactive Cyber Controls in OT: Myths vs. Reality

As the frequency of cyberattacks increases — often with a higher level of sophistication in order to evade detection — it's easy to see why organizations are investing in security technologies, such as automation, that can respond more efficiently to potential attacks after certain conditions have been met.

CRITICAL VULNERABILITIES

CVE

Google Discloses Windows Zero-Day Exploited in the Wild

Security researchers from Google have disclosed today a zero-day vulnerability in the Windows operating system that is currently under active exploitation.

Cisco IOS XE Software Arbitrary Code Execution Vulnerability

A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to execute persistent code at boot time and break the chain of trust.

Oracle WebLogic Server RCE Flaw Under Active Attack

The console component of the WebLogic Server has a flaw, CVE-2020-14882, which ranks 9.8 out of 10 on the CVSS scale.

Adobe Flash Player CVE-2020-9746

Adobe Flash Player version 32.0.0.433 (and earlier) are affected by an exploitable NULL pointer dereference vulnerability that could result in a crash and arbitrary code execution.

Mitsubishi Electric MELSEC iQ-R, Q and L Series

CVSS v3 7.5
Vulnerability: Uncontrolled Resource Consumption

CYBER SECURITY NEWS

WHAT'S NEW FROM OUR VENDORS?

Municipality Leverages Secure SD-WAN for Multi-Cloud to Optimize Cloud Security (Fortinet)

Cyberattack surfaces are constantly growing as organizations upgrade their network services with digital innovations. And this is only exacerbated when these digital innovation initiatives involve migrating to multi-cloud environments.

Boldon James and Deep Secure Announce Technology Alliance to Enable Secure, Efficient Delivery of Data Across Multiple Sectors

Boldon James announced it has partnered with Deep Secure, a leading UK cybersecurity firm, delivering Malware-free, policy enforced data to protect against cyberattacks and data non-compliances.

Infoblox Added to NASPO ValuePoint Cloud Solutions Contract, Enabling State and Local Governments to Build Next Level Networks

Infoblox announced it has been added to the National Association of State Procurement Officials (NASPO) ValuePoint Cloud Solutions Contract held by Carahsoft Technology Corp. to provide Infoblox's core DDI, BloxOne DDI, and BloxOne Threat Defense products to participating states, local governments and educational institutions.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

3 Reasons Cyber Security Training is Essential

A recent Lucy Security study found that 96% of respondents agreed that a greater level of awareness over cyber security threats contributed to overall improvements in their defenses.

Nobody Gets Hacked? That's Only True in a Fantasy World

New research from Kaspersky shows that 55% of industrial organizations believe that the Internet of Things will change the state of security in industrial control systems (ICS).

Thycotic Study – What Causes a Board to Invest in Cyber Security?

Thycotic released its CISO Decisions survey, an independent global study that examines what most influences the board to invest in cyber security and the impact this has on CISO decision-making.

Ransomware is Growing: Here are Four Ways Attackers are Getting into Your Systems

More than a quarter (26%) of cases were traced back to a phishing email, and a smaller number used particular vulnerability exploits (17%), including -- but not limited to -- Citrix NetScaler CVE-2019-19781 and Pulse VPN CVE-2019-11510.

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