12 May 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?

Healthcare and Education Sectors Most Susceptible to Cyber Incidents

In total, healthcare and education made up more than a third (34%) of security incidents last year, a 1% rise compared to 2020. The data revealed a significant increase in ransomware attacks targeting the education sector, rising from 19% in 2020 to 22% in 2021. This was particularly profound in the first half of 2021 (26%).

From Behavior Analytics to Security Education: 4 Ways Organizations Should Mitigate Modern Insider Attacks

While the stakes for private sector organizations differ drastically from governments that have to protect state secrets like hacking tools or nuclear technologies, businesses do have their own needs for Data Loss Prevention measures.

Passwords: Do Actions Speak Louder Than Words?

Two-thirds of respondents (66%) in a recent password security survey conducted by Ipsos on behalf of Google said they use completely random passwords with a mix of characters, but 65% also said they reuse passwords for different online accounts.

Raspberry Robin Spreads via Removable USB Devices

Researchers discovered a new Windows malware, dubbed Raspberry Robin, with worm-like capabilities that spreads via removable USB devices.

CRITICAL VULNERABILITIES

CVE

CISA adds CVE-2022-1388 flaw in F5 BIG-IP to its Known Exploited Vulnerabilities Catalog

US Critical Infrastructure Security Agency (CISA) adds critical CVE-2022-1388 flaw in F5 BIG-IP products to its Known Exploited Vulnerabilities Catalog.

Critical Cisco NFVIS Software Flaw Let Attacker Injects Commands at The Root Level

Cisco has released an update to the Enterprise NFV Infrastructure Software (NFVIS) that addresses several security flaws found by researchers.

May 2022 Patch Tuesday forecast: Look Beyond Just Application and OS Updates

Microsoft addressed 97 vulnerabilities in Windows 10, and 67 in Windows 11. Adobe updated Reader and Acrobat to fix 62 vulnerabilities.

Microsoft Fixed RCE Flaw in a Driver Used by Azure Synapse and Data Factory

Microsoft announced to have addressed a critical remote code execution flaw, tracked as CVE-2022-29972 and named SynLapse, affecting Azure Synapse and Azure Data Factory. The vulnerability was discovered by researchers from Orca Security and resides in a third-party driver used in the above solution.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Check Point vs Palo Alto: Comparing EDR Software

Check Point prevents malware from reaching the endpoint through web browsing and email attachments without impacting user productivity. Palo Alto reduces the attack surface to improve the accuracy of malware and ransomware protection by preventing malicious executables, DLL files and Office macros.

SentinelOne vs CrowdStrike: Compare EDR Software

SentinelOne is a security platform offering endpoint detection and response, advanced threat intelligence and network defense solutions. CrowdStrike is a robust cybersecurity solution including EDR, network security and cyber-threat protection.

Microsoft Defender vs Carbon Black: EDR Software Comparison

Microsoft Defender for Endpoint, formerly known as Microsoft Defender Advanced Threat Protection, is the tech giant's enterprise endpoint security platform. It's a cloud-based solution that scales up as you add more endpoints to your network. Carbon Black's defenses recognize the need for agility in a quickly-moving cybersecurity environment. Its extensive automation features and threat discovery reduce response times to stop threats before they have a chance to cause widespread damage.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

The Main Security Challenges when Adopting Cloud Services

The popularity of cloud services has increased exponentially in recent years. The prospects of saving on capital and operational expenditures have been significant driving forces in influencing companies to adopt cloud services.

Experts Uncovered a New Wave of Attacks Conducted by Mustang Panda

China-linked Mustang Panda APT group targets entities in Asia, the European Union, Russia, and the US in a new wave of attacks.

Defending against APT Attacks

The conflict in Ukraine has highlighted the risks of cyberespionage and sabotage, which typically involve Advanced Persistent Threat (APT) groups.

VHD Ransomware Linked to North Korea's Cyber-Army Targets Financial Institutions

Experts from Trellix discovered that VHD Ransomware was linked to North Korea's cyber army. The cyber-army of North Korea has been divided into several units, all of which have different tasks and report to 'Bureau (or Lab) 121'.

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