27 April 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?

Trends and Technologies that are Helping Supply Chains Respond, Recover and Thrive During Pandemic

Nearly half of supply chain leaders surveyed have dramatically accelerated spending on digital technologies to make their operations more responsive and forward-looking during the pandemic, according to an industry report released by MHI and Deloitte. Cloud computing, robotics and inventory/network optimization tools saw the biggest jump in terms supply chain investment, with 49% of survey respondents increasing spending.

Mount Locker Ransomware Aggressively Changes Up Tactics

The ransomware is upping its danger quotient with new features while signaling a rebranding to "AstroLocker." The Mount Locker ransomware has shaken things up in recent campaigns with more sophisticated scripting and anti-prevention features, according to researchers. And, the change in tactics appears to coincide with a rebranding for the malware into "AstroLocker." According to researchers, Mount Locker has been a swiftly moving threat.

61% of Organizations Impacted by Ransomware in 2020

Enterprises faced unprecedented cybersecurity risk in 2020 from increasing attack volume, the pandemic-driven digital transformation of work, and generally deficient cyber preparedness and training, a survey reveals. A full 79% of respondents indicated their companies had experienced a business disruption, financial loss or other setback in 2020 due to a lack of cyber preparedness.

CRITICAL VULNERABILITIES

CVE

AV Under Attack: Trend Micro Confirms Apex One Exploitation

Anti-malware vendor Trend Micro is warning that attackers are attempting to exploit a previously patched vulnerability in its Apex One, Apex One as a Service, and OfficeScan product lines.

Critical Infrastructure Implications of the Pulse Secure Multi-Factor Authentication Bypass

The FireEye Mandiant team has discovered multiple threat actors exploiting a zero-day vulnerability in Pulse Secure VPN appliances.

Password Manager Suffers 'Supply Chain' Attack

A malicious update to the Click Studios password-manager platform Passwordstate dropped malware onto its software systems this month.

Zero-Day Flaws in SonicWall Email Security Tool Under Attack

Three zero-day vulnerabilities helped an attacker install a backdoor, access files and emails, and move laterally into a target network.

DNS Vulnerabilities Expose Millions of Internet-Connected Devices to Attack

Researchers uncover a fresh set of nine vulnerabilities in four TCP/IP stacks that are widely used in everything from powerful servers and firewalls to consumer IoT products.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

CrowdStrike Security Cloud Integrates with NDR and NTA Solutions to Defend Against any Threats

CrowdStrike announced a series of integrations with CrowdStrike Security Cloud that correlates the CrowdStrike Falcon platform's enriched endpoint and workload telemetry with network telemetry for greater end-to-end visibility and contextual insights to combat threats.

Securiti Partners with Cisco to Provide Multi-Cloud Security

Securiti, a provider of AI-powered data privacy and security, is partnering with Cisco Investments to work with Cisco and help their customers solve the challenge of multi-cloud and edge security, privacy and compliance.

Kasada Partners with GreyNoise Intelligence to Provide Potential Threats Prioritization

By teaming up with Kasada, GreyNoise Intelligence will be able to provide users with an improved understanding of their security environment and more accurate information about which potential threats demand their attention. Kasada detects malicious automation and bot networks, seeing billions of bot interactions every month. GreyNoise collects, analyzes and labels data about IP addresses that scan the internet and saturate security tools with "noise".

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

5 Fundamental But Effective IoT Device Security Controls

IoT devices introduce a host of vulnerabilities into organizations' networks and are often difficult to patch. With more than 30 billion active IoT device connections estimated by 2025, it is imperative information-security professionals find an efficient framework to better monitor and protect IoT devices from being leveraged for distributed denial or service (DDoS), ransomware or even data exfiltration.

How Zero Trust Can Help Close the Cybersecurity Gaps

Using a Zero Trust model can help tackle some of the major challenges in cybersecurity today, including the skills gap.

QR Codes Popularity May Abused to Deliver Malware and Banking Heists

Threat actors might use opportunities to steal corporate data, they can also infiltrate mobile devices with the help of QR codes.

Transitioning to a SASE architecture

Juniper thinks of SASE as the embodiment of networking converged with security. It provides protection from attack, regardless of where users are located, ensuring consistent security enforcement wherever they are without having to backhaul traffic to a corporate data center.

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