22 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?

Cybersecurity Guide for the Hospitality Industry
A practical cybersecurity guide from the National Institute of Standards and Technology (NIST) can help hotel owners reduce the risks to a highly vulnerable and attractive target for hackers: the hotel property management system (PMS), which stores guests' personal information and credit card data.

COVID-19-Themed Cyberattack Detections Continue to Surge
McAfee released its new report, examining cybercriminal activity related to malware and the evolution of cyber threats in the third and fourth quarters of 2020.

Even Though Critical, Web Application Security is Getting Less Attention
As organizations shifted focus to support remote work and business continuity amid the challenges of 2020, web application security suffered, according to an Invicti Security report.

Guide to Automating Third-Party Cyber Risk Management
With increasing dependence on third parties in today's interconnected world, vendor security risk assessments are more essential than ever. Automation is the key to rapid and comprehensive third-party cyber risk reduction.

CRITICAL VULNERABILITIES

CVE

CVE-2021-22893: Zero-Day Vulnerability in Pulse Connect Secure Exploited in the Wild
Threat actors are leveraging a zero-day vulnerability in Pulse Connect Secure SSL VPN appliance, for which there is no immediate patch scheduled for release.

Microsoft Has Busy April Patch Tuesday with Zero-Days, Exchange Fixes
Microsoft fixes 110 vulnerabilities, with 19 classified as critical and another flaw under active attack.

Vulnerability In Juniper Networks Junos OS Could Allow Remote Code Execution
A security vulnerability directly affected Juniper Networks Junos OS allowing remote code execution attacks.

Critical Cloud Bug in VMWare Carbon Black Allows Takeover
A critical security vulnerability in the VMware Carbon Black Cloud Workload appliance would allow privilege escalation and the ability to take over the administrative rights for the solution.

NSA: 5 Security Bugs Under Active Nation-State Cyberattack
Citrix, Fortinet, Pulse Secure, Synacor and VMware are all in the crosshairs of APT29, bent on stealing credentials and more.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

VMware Announces New Anywhere Workspace Tool to Help Businesses Make Remote Work Easier
VMware announced a new remote work solution called VMware Anywhere Workspace, a zero-trust, cloud native platform that the company said is designed to eliminate friction between IT and remote employees, all while improving security and reducing overhead.

Entrust Delivers Security Management to VMware Cloud Foundation with HyTrust CloudControl
Entrust has announced its HyTrust CloudControl solution — now an Entrust business — now supports VMware Cloud Foundation, enabling unified security and compliance controls across the platform, lowering operational overhead and facilitating workload agility.

Securonix, AWS Partner on New Cloud-Native SIEM Solution
Cybersecurity firm Securonix has announced a new level to its collaboration with AWS that will allow AWS customers to use Securonix security information and event management (SIEM) software without ever leaving their current AWS hosting solutions.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Network Detection & Response: The Next Frontier in Fighting the Human Problem
NDR has adapted to not only play a major role in helping network and security teams identify threats, but it has enabled these teams to respond to them too.

Improper Cloud IAM Leaving Organizations at Risk
There is an industry-wide cloud permissions gap crisis, leaving countless organizations at risk due to improper identity and access management (IAM), a CloudKnox Security report reveals.

Open-Source Security, License Compliance, and Maintenance Issues are Pervasive in Every Industry
Synopsys released a report that examines the results of more than 1,500 audits of commercial codebases. It details the pervasive risks posed by unmanaged open source, including security vulnerabilities, outdated or abandoned components, and license compliance issues.

Protecting the Human Attack Surface from the Next Ransomware Attack
As we head into 2021, ransomware is making another resurgence, in particular targeted attacks from highly organized hacker groups.

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