29 November 2021

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?

Cybercriminals Target Alibaba Cloud for Cryptomining, Malware

Cybercriminals are targeting Alibaba Elastic Computing Service (ECS) instances, disabling certain security features to further their cryptomining goals. Alibaba offers a few unique options that make it a highly attractive target for attackers, researchers noted.

Designing a Proactive Ransomware Playbook for Today's Threat Landscape

Ransomware attacks are among the most significant cyber-threats facing organizations today. According to research by Gartner, ransomware is the highest priority (78 percent) and most important emerging risk to track.

3 Top Tools for Defending Against Phishing Attacks

Even with the most sophisticated email scanning and phishing detection system available, phishing emails are still a very common intrusion vector for cybercriminals to use to introduce malware, including ransomware, to a business' network.

IKEA Hit by a Cyber Attack that Uses Stolen Internal Reply-Chain Emails

Threat actors are targeting IKEA employees in an internal phishing campaign leveraging stolen reply-chain emails. Sending the messages from the organizations allows the attackers to bypass detection. Threat actors also exploit the access to internal emails to target business partners.

CRITICAL VULNERABILITIES

CVE

Attackers Actively Target Windows Installer Zero-Day

Attackers are actively exploiting a Windows Installer zero-day vulnerability that was discovered when a patch Microsoft issued for another security hole inadequately fixed the original and unrelated problem.

Attackers Hijack Email Threads Using ProxyLogon / ProxyShell Flaws

Exploiting Microsoft Exchange ProxyLogon & ProxyShell vulnerabilities, attackers are malspamming replies in existing threads and slipping past malicious-email filters.

Exchange, Fortinet Flaws Being Exploited by Iranian APT, CISA Warns

A state-backed Iranian threat actor has been using multiple CVEs – including both serious Fortinet vulnerabilities for months and a Microsoft Exchange ProxyShell weakness for weeks – looking to gain a foothold within networks before moving laterally and launching BitLocker ransomware and other nastiness.

Critical Citrix DDoS Bug Shuts Down Network, Cloud App Access

A critical security bug in the Citrix Application Delivery Controller (ADC) and Citrix Gateway could allow cyberattackers to crash entire corporate networks without needing to authenticate. The two affected Citrix products are used for application-aware traffic management and secure remote access, respectively.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Exclusive Networks Partners with Infinipoint to Extend Zero Trust Security to Device Identity

Exclusive Networks announced its worldwide distribution agreement with Infinipoint, a provider of a pioneering Device-Identity-as-a-Service (DIaaS) security solution that enables the critical device pillar of the zero trust cybersecurity approach.

F-Secure Collaborates with CyberPeace Institute to Help Organizations Targeted by Cyberattacks

F-Secure has signed a letter of intent (LOI) with the Switzerland-based CyberPeace Institute, an independent non-governmental organization whose mission is to protect the security, dignity, and equity of people in cyberspace.

Hexaware Partners with DataRobot to Accelerate AI Initiatives for Businesses

Hexaware announced it has partnered with DataRobot to empower businesses across industries to accelerate their AI initiatives, helping drive business impact at scale. The DataRobot and Hexaware partnership enables institutions to break through this barrier with the powerful capabilities of the DataRobot AI Cloud that offers a unified platform for user personas, data types and environments, accelerating the delivery of AI to production.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Cloud Security: Don't Wait Until Your Next Bill to Find Out About an Attack!

Google's Cybersecurity Action Team just published the first ever edition of a bulletin entitled Cloud Threat Intelligence. The primary warnings are hardly surprising and boil down to two main facts.

Your Supply Chain: How and Why Network Security and Infrastructure Matter

Business leaders and organizations must prioritize securing supply chains and be aware of their vendors' security practices to mitigate critical risks that can hinder productivity, delay product delivery, or worse.

Top 5 Cloud Security Challenges, Risks and Threats

Cloud services are an integral part of modern business. They provide a cost-effective way to store data; and with the rise in hybrid workforces, they deliver a reliable way for employees to access information remotely.

More Ransomware Attacks Up to September Than Whole of 2020

Most UK business leaders expect cyber-threats to surge next year, with ransomware, business email compromise (BEC), cloud and supply chain attacks all predicted to increase, according to PwC.

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