December 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?

Misconfigured Docker Servers Under Attack by Xanthe Malware

Researchers have discovered a Monero cryptomining botnet they call Xanthe, which has been exploiting incorrectly configured Docker API installations in order to infect Linux systems.

Cybersecurity Predictions for 2021: Robot Overlords No, Connected Car Hacks Yes

In cybersecurity, the best we can do is look at trends in attack methodologies, recognize changes in the threatscape, see what new technologies are emerging and offer a best guess about where things will be going forward.

How Organizations Can Prevent Users from Using Breached Passwords

What is a breached password? How do you discover breached passwords in your environment? How can organizations effectively protect their end-users from using these types of passwords?

4 Free Online Cyber Security Testing Tools For 2021

Set of must-have online security tools that we believe may make a real difference to your cybersecurity program and improve your 2021 budget planning.

CRITICAL VULNERABILITIES

CVE

High-Severity Chrome Bugs Allow Browser Hacks

Google has updated its Chrome web browser, fixing four bugs with a severity rating of "high" and eight overall. Three are use-after-free flaws, which could allow an adversary to generate an error in the browser's memory, opening the door to a browser hack and host computer compromise.

Xerox DocuShare Bugs Allow Data Leaks

Tracked as CVE-2020-27177, Xerox said the vulnerabilities open Solaris, Linux and Windows DocuShare users up to both a server-side request forgery (SSRF) attack and an unauthenticated external XML entity injection attack (XXE).

VMware Rolls a Fix for Formerly Critical Zero-Day Bug

VMware has patched a zero-day bug that was disclosed in late November – an escalation-of-privileges flaw that impacts Workspace One and other platforms, for both Windows and Linux operating systems.

Zero-Day Vulnerabilities in Healthcare Records Application OpenClinic Could Expose Patients' Test Results

Unpatched vulnerabilities in the OpenClinic healthcare records management application could allow attackers to access confidential patient data.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Netwrix Expert Makes 7 Cybersecurity Predictions For 2021

Netwrix that makes data security easy, released predictions about key trends that will impact organizations in 2021 and beyond. Most of them arise from the digital transformation and new workflows required by the rapid transition to remote work in 2020.

Fortinet Collaborates with AWS to Deliver an Integrated Next-Generation Firewall Solution to Protect Customer Workloads on AWS

Fortinet announced new integrations with Amazon Web Services (AWS) to further provide customers with advanced security across their cloud platforms, applications, and network.

Fortinet Launches Security Consulting Services on AWS Marketplace to Protect Cloud Adoption

Fortinet announced the availability of Fortinet Consulting Services in AWS Marketplace to provide customers with a blueprint for comprehensive design and implementation best practices

Forescout Advances Industrial IoT and OT Security

Forescout announced the expansion of its partner ecosystem to create a cohesive infrastructure for monitoring and mitigating threats and emerging risks across IT and OT environments.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Protecting Critical Infrastructure From Nation-State Attacks

Enterprises should have an incident response plan with a continuous monitoring threat intelligence sharing mechanism to help protect critical infrastructure from nation-state attacks.

DNS Filtering: A Top Battle Front Against Malware and Phishing

With the proliferation of malicious websites, domain name system (DNS) filtering has been adopted as an effective method for blacklisting content and blocking out suspicious webpages.

How to Update Your Remote Access Policy – And Why You Should Now

Organizations are recognizing the severe security implications from a sudden reliance on the cloud, mobile devices and unfamiliar Wi-Fi network connections.

As Modern Mobile Enables Remote Work, It Also Demands Security

Cybercriminals are taking advantage of social uncertainty and exploiting the fact that we rely more on mobile devices to stay productive.

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