06 January 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?

2021 Cybersecurity Trends: Bigger Budgets, Endpoint Emphasis and Cloud

After shrinking in 2020, cybersecurity budgets in 2021 climb higher than pre-pandemic limits. Authentication, cloud data protection and application monitoring will top the list of CISO budget and cybersecurity priorities. Nearly 70 organizations surveyed by Skybox said over a third of their workforce would remain remote for at least the next 18 months.

Microsoft Ups Security of Azure AD, Identity

Microsoft's latest security announcements have focused on securing Azure AD and Identity. Updates include stronger compromise prevention for Azure AD, a zero-trust business plan, and some changes to managing user authentication in Azure Portal.

Adobe Flash Player Has Reached Its End-of-Life – Uninstall It Now If Haven't Done Already

Adobe has explicitly announced the official end-of-life of Flash Player on December 31, 2020. As stated, Flash Player will receive no security updates or bug fixes in 2021. Also, from January 12, 2021, the tech giant will block all content running Flash Player to encourage the users to avoid its use.

CRITICAL VULNERABILITIES

CVE

Secret Backdoor found Installed in Zyxel Firewall and VPN

The flaw, tracked as CVE-2020-29583 (CVSS score 7.8), affects version 4.60 present in wide-range of Zyxel devices, including USG, USG FLEX, ATP, and VPN firewall products.

Zoom 4.6.239.20200613 Meeting Connector Post-Auth Remote Root

Zoom version 4.6.239.20200613 suffers from a Meeting Connector post-authentication remote root code execution vulnerability via the proxy server functionality. The latest Zoom client has this issue patched per Zoom.

Vulnerability In Google Docs Could Allow Hijacking Feedback Screenshots

A serious vulnerability affected Google Docs that could allow anyone to steal screenshots of users' documents. Google fixed the vulnerability later.

New Zero-Day, Malware Indicate Second Group May Have Targeted SolarWinds

A piece of malware named by researchers Supernova and a zero-day vulnerability exploited to deliver this malware indicate that SolarWinds may have been targeted by a second, unrelated threat actor.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Code42 Incydr – SaaS Data Risk Detection and Response

Incydr is Code42's new SaaS data risk detection and response solution, which enables security teams to mitigate file exposure and exfiltration risk without disrupting legitimate collaboration. Code42 focuses on the problems related to the massive "work from home" shift, i.e., the fact that many different collaboration tools are being used within global enterprises.

The Scariest Thing About that GoDaddy Phishing Test Story

GoDaddy has been taking a lot of heat for a phishing test email it sent to many of its employees right before the holidays. The email told recipients that they were receiving a $650 holiday bonus and asked them to click a link in order to receive the bonus. The bonus wasn't real. It was a test to see if employees would fall for a phishing attack.

How to Fix the Vulnerabilities Targeted in the SolarWinds and FireEye Hack

This Vulcan Cyber blog post explains how to fix the vulnerabilities targeted by the red team tools used in this FireEye hack. FireEye has done the needful and specifically disclosed the vulnerabilities that their red team tools were designed to ethically exploit. All of the vulnerabilities targeted in the FireEye hack have been disclosed by their respective vendors and have a CVE assigned.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

6 Questions Attackers Ask Before Choosing an Asset to Exploit

The attacker's perspective on how an attacker evaluates assets to go after and exploit on an attack surface begins by answering six questions.

What's Next for Ransomware in 2021?

The number of ransomware attacks has jumped by 350 percent since 2018, the average ransom payment increased by more than 100 percent this year, downtime is up by 200 percent and the average cost per incident is on the rise, according to a recent report from PurpleSec.

Would You Take the Bait? Take Phishing Quiz to Find Out!

As per Google's technology incubator Jigsaw, one in every 100 emails sent today is a phishing attempt. The quiz comes complete with brief explanations about why each message is real or fake.

2020 Work-for-Home Shift: What We Learned

In an effort to have a safer 2021, have a look at the top five biggest takeaways of the remote-work shift for security teams going forward.

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