20 January 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?

NSA Suggests Enterprises Use 'Designated' DNS-over-HTTPS' Resolvers

The U.S. National Security Agency (NSA) said DNS over HTTPS (DoH) — if configured appropriately in enterprise environments — can help prevent "numerous" initial access, command-and-control, and exfiltration techniques used by threat actors.

Joker's Stash, The Internet's Largest Carding Forum, is Shutting Down

Joker's Stash, the internet's largest marketplace for buying & selling stolen card data, announced that it was shutting down within a month.

The Popular Signal Messaging App Signal is Currently Facing Issues Around the World, Users Are Not Able to Make Calls and Send/Receive Messages

Users that attempted to send messages via the messaging app were seeing loading screen and after it displayed an error message "502". Immediately after WhatApp announced the changes to its privacy policy and obliged its users to accept it to continue using its service, a huge number of users opted to leave the Facebook-owned platform. Signal announced it is adding new servers and extra capacity at a record pace every single day this week to provide the service to a growing number of users.

CRITICAL VULNERABILITIES

CVE

Critical WordPress-Plugin Bug Found in 'Orbit Fox' Allows Site Takeover

Two vulnerabilities (one critical) in a WordPress plugin called Orbit Fox could allow attackers to inject malicious code into vulnerable websites and/or take control of a website.

Sophisticated Hacks Against Android, Windows Reveal Zero-Day Trove

Google researchers have detailed a major hacking campaign that was detected in early 2020, which mounted a series of sophisticated attacks, some using zero-day flaws, against Windows and Android platforms.

Critical Microsoft Defender Bug Actively Exploited; Patch Tuesday Offers 83 Fixes

The first Patch Tuesday security bulletin for 2021 from Microsoft includes fixes for one bug under active attack, possibly linked to the massive SolarWinds hacks.

High-Severity Cisco Flaw Found in CMX Software For Retailers

Cisco fixed high-severity flaws tied to 67 CVEs overall, including ones found in its AnyConnect Secure Mobility Client and in its RV110W, RV130, RV130W, and RV215W small business routers.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Apple Kills MacOS Feature Allowing Apps to Bypass Firewalls

Security researchers lambasted the controversial macOS Big Sur feature for exposing users' sensitive data. Apple has removed a contentious macOS feature that allowed some Apple apps to bypass content filters, VPNs and third-party firewalls.

Microsoft Implements Windows Zerologon Flaw 'Enforcement Mode'

Microsoft will enable Domain Controller "enforcement mode" by default to address CVE-2020-1472. Microsoft is taking matters into its own hands when it comes to companies that haven't yet updated their systems to address the critical Zerologon flaw. A successful exploit of the flaw allows unauthenticated attackers with network access to domain controllers to completely compromise all Active Directory identity services.

Ring Adds End-to-End Encryption to Quell Security Uproar

The optional feature was released free to users in a technical preview this week, adding a new layer of security to service, which has been plagued by privacy concerns. Smart doorbell maker Ring is giving cybersecurity critics less to gripe about with the introduction of end-to-end encryption to many of its models.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Cloud Attacks Are Bypassing MFA, Feds Warn

The Feds are warning that cybercriminals are bypassing multi-factor authentication (MFA) and successfully attacking cloud services at various U.S. organizations.

Millions of Social Profiles Leaked by Chinese Data-Scrapers

A cloud misconfig by SocialArks exposed 318 million records gleaned from Facebook, Instagram and LinkedIn.

Cisco Secure Workload Immediate Actions in Response to "SUNBURST" Trojan and Backdoor

The SUNBURST trojan and backdoor, as dubbed by FireEye researchers, that has compromised multiple U.S. Government systems recently, highlights the complexity and connectedness of the modern enterprise IT environment as a security weakness.

The Development Team Behind the Linux Mint Distro has Fixed a Security Flaw that Could have Allowed Users to Bypass the OS Screensaver

The development team of the Linux Mint project have addressed a security bug that could have allowed attackers to bypass the OS screensaver.

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