27 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?

Automation and No-Code are Driving the Future of Business Operations

More than 95% of respondents indicated that business operations has become a more important function in their organization in the past year, a Tonkean survey reveals. The survey of 500 IT and business operations professionals at large and mid-sized companies also showed growing frustrations with the status quo of resources and tools to perform operations work. 86% of respondents said their projects at least occasionally get delayed because of a lack of technical resources, and only 24% believed their current toolset satisfies all their needs for optimal future of business operations.

Chipmaker Intel Corp. Blames Internal Error on Data Leak

The computer chipmaker Intel Corp. on Friday blamed an internal error for a data leak that prompted it to release a quarterly earnings report early. It said its corporate network was not compromised.

Tesla has Accused a Former Employee, a Software Engineer, of Downloading about 26,000 Sensitive Files and Transferring them on his Personal Dropbox

Tesla sued the former employee Alex Khatilov for allegedly stealing 26,000 confidential documents, including trade secrets. The software engineer transferred the sensitive files to his personal Dropbox account.

CRITICAL VULNERABILITIES

CVE

Critical Cisco SD-WAN Bugs Allow RCE Attacks

Cisco is warning of multiple, critical vulnerabilities in its software-defined networking for wide-area networks (SD-WAN) solutions for business users.

DNSpooq Flaws Allow DNS Hijacking of Millions of Devices

Researchers have uncovered a set of flaws in dnsmasq, popular open-source software used for caching Domain Name System (DNS) responses for home and commercial routers and servers. Researchers have labeled the set of vulnerabilities "DNSpooq," a combination of DNS spoofing, the concept of "a spook spying on internet traffic," and the "q" at the end of dnsmasq.

Amazon Kindle RCE Attack Starts with an Email

Three vulnerabilities in the Amazon Kindle e-reader would have allowed a remote attacker to execute code and run it as root – paving the way for siphoning money from unsuspecting users.

SonicWall Investigating Zero-Day Attacks Against Its Products

Security vendor SonicWall is investigating what the company calls a "coordinated attack" against its internal network by threat actors using a zero-day exploit within the company's remote access products.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Microsoft Edge, Google Chrome Roll Out Password Protection Tools

The new tools on Chrome and Edge will make it easier for browser users to discover – and change – compromised passwords. Two major browsers –Microsoft Edge and Google Chrome – are rolling out default features, which they say will better help notify users if their password has been compromised as part of a breach or database exposure.

Intel Confirms Unauthorized Access of Earnings-Related Data

The Financial Times Thursday quoted Intel CFO George Davis as saying an individual had accessed material pertaining to Intel's financial results from the chipmaker's corporate website before the company's scheduled earnings announcement.

The Hacker News Reported in Exclusive that the Security Firm SonicWall was Hacked as a Result of a Coordinated Attack on Its Internal Systems.

The company was targeted with a coordinated attack on its internal systems, threat actors exploited zero-day vulnerabilities in their VPN solutions, such as NetExtender VPN client version 10.x and Secure Mobile Access (SMA).

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Zero Trust: A Solution to Many Cybersecurity Problems

The SolarWinds hack and the never-ending stream of revelations about the attackers' tools, techniques and other targets has been occupying the minds of CISOs and organization's cyber defenders since mid-December.

SolarWinds Malware Arsenal Widens with Raindrop

The post-compromise backdoor installs Cobalt Strike to help attackers more laterally through victim networks. An additional piece of malware, dubbed Raindrop, has been unmasked in the sprawling SolarWinds supply-chain attacks.

Discord-Stealing Malware Invades npm Packages

Three malicious software packages have been published to npm, a code repository for JavaScript developers to share and reuse code blocks.

How Do I Select a Data Encryption Solution for My Business?

Most Fortune 1000 compliance and security teams have the ability to access employee accounts on their enterprise communications platform to monitor activity and investigate bad actors.

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

800 HACKED

ABU DHABI | KUWAIT CITY | YEREVAN | LONDON
www.dts-solution.com