01 March 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?

Microsoft Releases Queries for SolarWinds Attack Detection

Microsoft is making available the CodeQL queries it used to detect malicious implants in the massive supply chain attack that affected SolarWinds, tech firms and government agencies. The CodeQL queries, written in C# language, are now available in the GitHub repository. They help in ruling out the presence of the code-level indicators of compromise.

Digital Guardian Enhances Connection with AWS Through Key Initiatives and Achievements

Digital Guardian has announced the general availability of their integration with Amazon Macie, a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and provide additional protection for customers' sensitive data in AWS.

Quantum Integration IoT Platform Allows Anyone to Build Their Own Fully Functional IoT Network

The Quantum Integration IoT platform is making the world of automation more accessible for everyone through specifically engineered hardware and software designed to allow anyone with the passion for making to build their own fully functional IoT network without any coding knowledge.

CRITICAL VULNERABILITIES

CVE

Cisco Warns of Critical Auth-Bypass Security Flaw

A critical vulnerability in Cisco Systems' intersite policy manager software could allow a remote attacker to bypass authentication..

VMWare Patches Critical RCE Flaw in vCenter Server

The vulnerability, one of three patched by the company this week, could allow threat actors to breach the external perimeter of a data center or leverage backdoors already installed to take over a system.

IBM Squashes Critical Remote Code-Execution Flaw

The flaw (CVE-2020-27221) has a CVSS base score of 9.8 out of 10, making it critical in severity.

Accellion FTA Zero-Day Attacks Show Ties to Clop Ransomware, FIN11

The threat actors stole data and used Clop's leaks site to demand money in an extortion scheme, though no ransomware was deployed.

Tax Season Ushers in Quickbooks Data-Theft Spike

Cybercriminals are ready for tax season with new malware designed to exfiltrate Quickbooks data and post it on the internet, according to a new report from ThreatLocker.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

RiskRecon Expands Cybersecurity Risk Monitoring to 3.9 Million Companies Globally

RiskRecon marked the expansion of its cybersecurity risk monitoring to 3.9 million companies globally.

Paysafe Uses Snowflake to Develop New Data Science Models for Enhanced Customer Experiences

Paysafe is leveraging technology from Snowflake to achieve meaningful data insights and deliver more informed and enhanced customer experiences by tapping into Artificial Intelligence (AI) and Machine Learning (ML) data models.

ThreatLocker Partners with Datto to Streamline Secure Business Operations for MSPs

ThreatLocker announced its partnership with Datto. This integration streamlines secure business operations for MSPs, allowing them to access their Autotask PSA account from within the ThreatLocker portal. Ransomware remains the most common cyber threat to SMBs, and MSPs have seen increased security risks for clients following the move to remote working and the accelerated adoption of cloud applications in 2020.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Data is Most at Risk on Email, with 83% of Organizations Experiencing Email Data Breaches

95% of IT leaders say that client and company data is at risk on email, an Egress report reveals.

Malicious Firefox Extension that Allows Attackers to Access and Control Users' Gmail Accounts

Proofpoint Threat Research has tracked low-volume phishing campaigns targeting Tibetan organizations globally.

Chrome Will Soon Try HTTPS First When You Type An Incomplete URL

Chrome now tries to upgrade sites from HTTP to HTTPS when HTTPS is available. Chrome also warns users when they're about to enter passwords or payment card data on unsecured HTTP pages, from where they might be sent across a network in plaintext.

One in Four People Use Work Passwords for Consumer Websites

Employees working from home on a company-provided computer are demonstrating a clear lack of cybersecurity knowledge through high-risk behavior, according to a report released by Ivanti.

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