10 November 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?

The Ultimate SaaS Security Posture Management (SSPM) Checklist

Cloud security is the umbrella that holds within it: IaaS, PaaS and SaaS. Gartner created the SaaS Security Posture Management (SSPM) category for solutions that continuously assess security risk and manage the SaaS applications' security posture.

Proven Third-Party Risk Management Strategies

A comprehensive TPCRM strategy enables organizations to have the necessary visibility into their entire vendor ecosystem so that when a cyberattack occurs, they can mitigate risks rapidly and effectively.

International Law Enforcement Arrested REvil Ransomware Affiliates in Romania and Kuwait

Romanian police arrested two alleged Sodinokibi/REvil ransomware affiliates accused to have orchestrated attacks against thousands of victims. The operation, codenamed GoldDust, also resulted in the arrest of a third individual in Kuwait that is suspected to be a GandGrab ransomware affiliate.

Casinos of Tribal Communities are Losing Millions in Ransomware Attacks

A private industry notification issued by the FBI's Cyber Division revealed that ransomware attacks hit several tribal-owned casinos causing millions of dollar losses. Experts reported that tribal communities were hit by several ransomware gangs, including REvil/Sodinokibi, Bitpaymer, Ryuk, Conti, Snatch, and Cuba.

CRITICAL VULNERABILITIES

CVE

Robinhood Data Breach Exposes 7 Million Users' Information

Robinhood Markets, Inc. is an American commission-free stock trading and investing platform, it had 18 million accounts as of March 2021, with over $80 billion in assets. The company disclosed a data breach, a threat actor gained access to the personal information of approximately 7 million customers.

Clop Gang Exploiting CVE-2021-35211 RCE in SolarWinds Serv-U in Recent Attack

Clop ransomware gang (aka TA505, FIN11) is exploiting CVE-2021-35211 SolarWinds Serv-U vulnerability to breach businesses' infrastructures and deploy its ransomware. The flaw is a remote code execution vulnerability that allows threat actors to execute arbitrary commands on a vulnerable server with elevated privileges.

Nation-State Actors Target Critical Sectors by Exploiting the CVE-2021-40539 Flaw

Cybersecurity experts from Palo Alto Networks warn of an ongoing cyberespionage campaign that has already compromised at least nine organizations worldwide from critical sectors, including defense, healthcare, and energy. Threat actors exploited a critical vulnerability, tracked as CVE-2021-40539, in the Zoho ManageEngine ADSelfService Plus software, which is self-service password management and single sign-on solution.

CYBER SECURITY NEWS

WHAT'S NEW FROM VENDORS?

Cynamics NDR Provides Visibility and Threat Prediction Without Having to Install Appliances or Agents

Cynamics announced an NDR solution to provide visibility and threat prediction without requiring the installation of an appliance or agent in the customer's network.

IntelePeer Reputation Management Helps Prevent Calls from being Tagged and Mislabeled as Fraud or Spam

IntelePeer has launched its Reputation Management solution, an all-in-one service and system designed to protect and improve the delivery of business communications and improve call completion rates to increase overall customer engagement.

Qrypt Releases Two Solutions to Ensure Quantum-Secure Encryption for Businesses

Qrypt launched two new solutions: the Cloud Enterprise Portal, and Digital Quantum Key Distribution (Digital QKD). This expands on Qrypt's Entropy-as-a-Service (EaaS) portfolio which provides high-quality quantum random numbers and the tools to ensure Everlasting Security. Enterprises can now integrate quantum encryption into their software services with tools that are fast, easy to use, highly scalable, and don't require expensive infrastructure.

SOMETHING TO THINK ABOUT

WHAT'S NEXT?

Why Integrating SIEM Tools is Crucial to Managing Threats

SIEM tools, when integrated with other layers of security, can help flag anomalous behavior and potential issues in real time.

Surge in Cyber-Attacks Confirms the Need for Zero Trust Security

Zscaler announced the release of a report that tracked and analyzed over 20 billion threats blocked over HTTPS, a protocol originally designed for secure communication over networks.

While Businesses are Ramping up Their Risk Mitigation Efforts, They Could be Doing More

Zurich North America and Advisen have released a survey of corporate risk managers and insurance buyers revealing current views about information security and cyber risk management.

How Do I Select a DRaaS Solution for My Business?

It has become crucial nowadays, besides having all necessary protections implemented within your system, to also have a disaster recovery plan ready in case an attack occurs. A Disaster-Recovery-as-a-Service (DRaaS) solution comes in handy since it's handled by the service provider.

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