[?????????2022 ? 12 ? 29 ?]

?????????2022 ? 12 ? 29 ?

???Sanjay Bhakta



The holiday season is one of the most anticipated times of the year – for cyber criminals.

Businesses are typically understaffed and especially vulnerable during the holiday season, especially the last week of the calendar year. And everyday people are vulnerable, too. Research suggests that 75 percent of Americans experienced at least one type of holiday scam last year. So, it is essential that everyone be aware of the threats that cyber criminals pose. Here is a round-up of recent cyber security events:

The Attack and Mine Malware Botnet KmsdBot Suspected of Being Used as DDoS-for-Hire Service

A progressing analysis of the KmsdBot botnet has highlighted the possibility that it is a DDoS-for-hire service offered to other threat actors. It's the type of attack that hackers often deploy during the Christmas time period. Notable targets that include FiveM and RedM, which are game modifications for Grand Theft Auto V and Red Dead Redemption 2, and security firms and luxury brands as well. For more insight.

Microsoft Warns on Achilles macOS Gatekeeper Bypass shortly after fixing similar Windows bug

Microsoft has pointed out a security bypass bug on Macs, which is somewhat like a recent Windows 0-day. The latest bypass Achilles bug, popularly known as CVE-2022-42821 for Apple's application-safety feature, could allow the malicious takeover of Macs regardless of whether lockdown mode is

enabled. For more insight.

AWS Elastic IP Transfer Feature Gives Threat actors a way to abuse the “victims” cloud accounts

On December 20, researchers identified a new potential attack vector. In this, threat actors can take over the cloud accounts of the victims by exploiting the AWS Elastic IP Transfer (EIP) feature to steal data or use them for command-and-control for phishing attacks, denial of service, or any other cyberattacks. The potential damage to the victim is the information can be misused for malicious purposes and jeopardize other resources of the victim in other cloud providers/on-premises. For more insight.

The security events mentioned above can result in financial loss and ruin a business's reputation. According to SonicWall Cyber Threat, malware -- an ever-evolving threat -- has recorded 2.8 billion hits globally, an 11 percent increase year-to-date over 2021. Malicious breaches occurred due to technical glitches costing around $4.45 million on average as reported by IBM Security, and phishing costs for American companies alone stands at $14.8 million according to true list.

Businesses will be subject to cyber threats for the foreseeable future. Therefore, companies need to rethink and prepare to consolidate fraud, cybersecurity, and anti-money laundering under a holistic approach. At Centific, our digital safety framework mitigates various security events, preparing enterprises to become more vigilant against vulnerabilities.

Our Digital Safety Framework includes best practices such as:

- 360 Security Posture.
- Risk Score Analysis.
- Vulnerability Assessment.
- Breach and Attack Simulations.
- Security Policy Efficacies.
- Cloud and Data Security Architecture Evaluation.
- TCO Optimization.

Contact us for more information.

Learn more about the authors by visiting their LinkedIn profiles:

- Sanjay Bhakta, VP global head of solutions
- Nitanshu Upadhyay, business solutions consultant

-
-
-
-
-