26 MAY 2023 ISSUE 7

WEEKLY CYBER SECURITY BRIEFING

Armoryze Be More Secure

UK ADMINISTRATOR OF ISPOOF PHONE SPOOFING SERVICE SENTENCED TO 13 YEARS FOR FACILITATING FRAUD

Tejay Fletcher, a British citizen and administrator of the now-defunct iSpoof online phone number spoofing service, has been sentenced to 13 years and 4 months in prison for his involvement in various cyber offenses. Fletcher, based in London, pleaded guilty to charges including facilitating fraud and possessing and transferring criminal property.

iSpoof was a paid service that allowed fraudsters to hide their phone numbers and deceive victims by impersonating representatives from banks, tax offices, and other official organizations.

The scam involved tricking targets into revealing sensitive financial information or making money transfers to accounts controlled by the threat actors.

The iSpoof online phone number spoofing service, which facilitated fraud by impersonating representatives of well-known banks, resulted in substantial financial losses. Victims in the U.K. alone suffered estimated losses exceeding £48 million ($59.8 million), with global losses surpassing £100 million ($124.6 million).

Following the dismantling of iSpoof in November 2022, Tejay Fletcher and 168 others involved were arrested. Fletcher's illicit proceeds amounted to approximately £1.7 - £1.9 million ($2.1 - $2.3 million), and luxury assets were seized. Fletcher promoted iSpoof through The iSpoof Club Telegram Channel and possessed numerous mobile phones and SIM cards related to the scheme.

This case highlights the impact of cybercriminals and emphasizes the need for CEOs and CISOs to prioritize cybersecurity measures, including robust authentication protocols and employee awareness training to combat phone number spoofing and other fraudulent activities.

IMPACTFUL EU PRIVACY FINE ON META AND IMPLICATIONS FOR TRANSATLANTIC DATA TRANSFERS

In a significant development, Meta (formerly Facebook) has been fined a historic $1.3 billion by the European Union (EU) and ordered to halt the transfer of user data between the EU and the US. The fine, imposed by Ireland's Data Protection Commission, surpasses previous penalties and raises concerns over US cybersnooping. Meta intends to appeal the ruling and is seeking court action to suspend its implementation, ensuring no immediate disruption to Facebook services in Europe.

The ruling stems from a decade-long case that began when privacy activist Max Schrems lodged a complaint against Facebook's handling of his data following Edward Snowden's revelations.

The clash between Europe's strict data privacy regulations and the more lenient US regime highlights the invalidation of the Privacy Shield agreement in 2020. Standard contractual clauses were used as an alternative mechanism for EU-US data transfers. The EU's top data privacy authorities recently overruled Irish regulators' decision on Meta's use of standard contractual clauses, raising compliance concerns.

The effectiveness of the revised Privacy Shield agreement in protecting data privacy is still being reviewed. Meta is concerned about the lack of a legal framework for data transfers, potentially leading to discontinuing products and costly restructuring.

Armoryze understands the complexities of cybersecurity, privacy, and compliance challenges. Our **managed compliance services** are designed to assist organizations in navigating these issues and establishing robust privacy practices. Whether you need guidance on regulatory frameworks, data protection, or ensuring compliance, our expert team is here to help. **Contact us** today to ensure your organization maintains a secure and compliant environment amidst changing regulations.

WEEKLY
CYBER SECURITY BRIEFING

Armoryze
Be More Secure

THE IMPERATIVE NEED FOR A MODERN SECURITY OPERATIONS CENTER (SOC) IN A HYBRID CLOUD ENVIRONMENT

In today's digital landscape, organizations face sophisticated cyber threats that can compromise critical assets and disrupt operations. The adoption of hybrid cloud environments introduces unique security challenges that need to be addressed. A modern Security Operations Center (SOC) plays a crucial role in mitigating these risks and safeguarding digital assets.

A modern SOC uses AI and machine learning to detect and counter cyber threats, minimizing damage and response time. With real-time monitoring and analysis across on-premises and cloud, it ensures comprehensive visibility and control, empowering organizations to secure their digital infrastructure.

This executive summary highlights the significance of a modern SOC in a hybrid cloud setup and outlines its key features.

1. **Understanding the Hybrid Cloud Environment:** A hybrid cloud combines on-premises infrastructure with public and private cloud services, offering scalability, flexibility, and cost-efficiency. However, it also presents security challenges such as data protection, access control, and threat detection across multiple platforms. A modern SOC is essential for addressing these challenges.

2. **Comprehensive Visibility and Threat Detection:** A modern SOC provides organizations with comprehensive visibility into their hybrid cloud environment. By integrating and correlating security logs, events, and telemetry from various sources, the SOC can identify vulnerabilities and detect malicious activities in real-time. This enables proactive monitoring and response to threats across the entire infrastructure.

3. **Real-Time Monitoring and Incident Response:** A modern SOC enables real-time monitoring and incident response capabilities. Security analysts continuously monitor network traffic, user behavior, and system logs to identify anomalies and potential

security breaches. The SOC can swiftly respond, investigate, and contain threats, minimizing operational impact and staying ahead of cybercriminals.

4. **Advanced Threat Intelligence and Analytics:** Leveraging advanced threat intelligence and analytics, a modern SOC enhances threat detection and response capabilities. Machine learning algorithms and artificial intelligence analyze vast amounts of security data, identifying patterns and detecting previously unknown threats. This proactive stance enables organizations to mitigate threats before significant damage occurs.

5. **Automation and Orchestration:** Automation and orchestration are integral components of a modern SOC. Automating routine tasks and orchestrating different security tools improve efficiency, reduce the risk of human error, and facilitate a unified response to security incidents. Armoryze's Managed Threat Detection & Response service offers robust automation and orchestration capabilities.

6. **Compliance and Regulatory Requirements:** Compliance with industry standards and regulatory requirements is crucial in a hybrid cloud environment. A modern SOC ensures continuous monitoring of security controls, generates audit trails, and provides necessary documentation for compliance. Armoryze's solutions assist organizations in meeting various compliance standards such as the **Payment Card Industry Data Security Standard (PCI DSS)** and General Data Protection Regulation (GDPR).

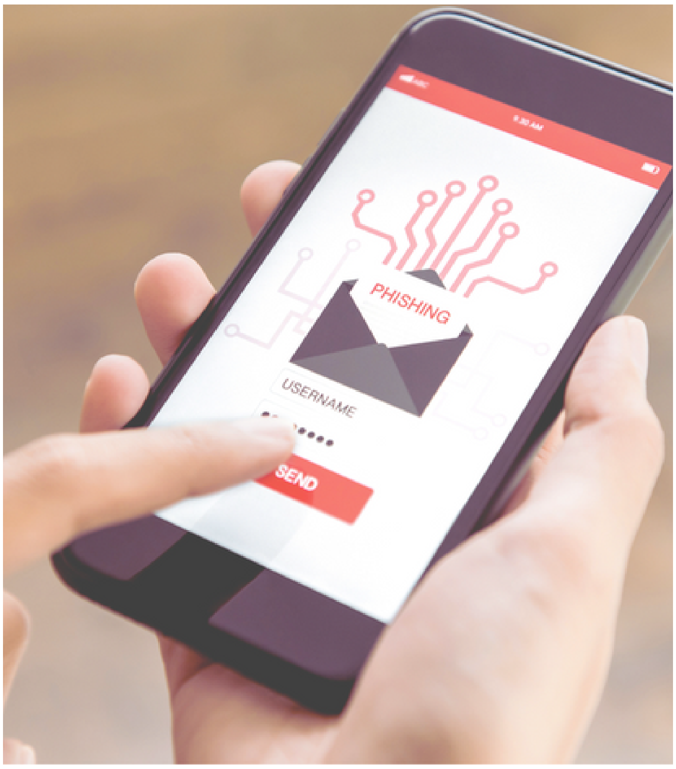
By investing in **Armoryze's SIEM** and **Managed Threat Detection & Response service**, organizations can strengthen their security posture in the hybrid cloud environment. Armoryze offers comprehensive visibility, real-time monitoring, advanced threat intelligence, automation, and orchestration capabilities.

Take a proactive step towards securing your hybrid cloud infrastructure by signing up for a free trial today. Visit our website: **https://www.armoryze.co.uk/usm-trial**

WEEKLY
CYBER SECURITY BRIEFING

Armoryze
Be More Secure

UNMASKING THE THREAT: HOW ATTACKERS CONCEAL BEC ATTACKS WITH RESIDENTIAL IPS



The ever-evolving world of cybercrime poses new challenges for businesses, as attackers find ways to bypass security measures. Microsoft recently issued a warning about a concerning trend in business email compromise (BEC) and account takeover attacks. Attackers are now using residential IP addresses to conceal the origin of their malicious activities, making it difficult to detect and prevent these attacks. This article highlights the implications of this development and emphasizes the need for heightened vigilance and countermeasures.
Attackers exploit masked IP addresses provided by platforms like BulletProftLink and residential IP services to evade detection in BEC attacks.

By using localized address space and rapidly rotatable IP addresses, cybercriminals can obfuscate their movements and launch large-scale attacks. This evasion technique is prevalent in Asia and Eastern Europe. To combat this technique globally, enhanced vigilance and countermeasures are essential.

The warning from Microsoft coincides with a surge in BEC campaigns. BEC attacks exploit email traffic manipulation to deceive victims into revealing sensitive financial information or transferring funds to fraudulent accounts. Executives, finance managers, and HR personnel are prime targets due to their access to valuable personal data.

Organizations must analyze behavior, configure mail systems, implement DMARC, block identities, and strengthen authentication to address locally generated IP addresses used by attackers. Employee training is crucial for awareness and vigilance against BEC attacks. Empowering employees to identify and report suspicious activities strengthens security. Protect your organization from BEC attacks. Schedule a **free cyber security assessment & consultation** with Armoryze experts today!

URGENT ACTION REQUIRED: BARRACUDA EMAIL SECURITY GATEWAY BREACH EXPOSES ZERO-DAY VULNERABILITY

Barracuda, a prominent cybersecurity vendor, recently disclosed a breach that affected some of its Email Security Gateway (ESG) customers. The breach exploited a zero-day vulnerability within the appliance, raising concerns about unauthorized access to email gateway appliances. This executive summary provides an overview of the incident, including the discovery of the vulnerability, patch deployment, and critical actions for affected customers.

Last week, Barracuda identified a zero-day vulnerability (CVE-2023-2868) in its Email Security Gateway (ESG) product, resulting in unauthorized access to a subset of email gateway appliances. Taking immediate action, Barracuda swiftly deployed patches worldwide to address the vulnerability. A second patch targeting Email Security Gateway appliances was released shortly after. Affected customers were promptly notified about the breach, with additional notifications sent to customers who may have been unaffected. While other Barracuda products, including their SaaS email security services, were not impacted, affected customers are advised to review their environments and take additional actions if necessary.

Barracuda's response demonstrates their commitment to promptly addressing the issue and protecting their clients' interests. Customers should remain vigilant and proactively evaluate their security posture despite the patch deployment.

Barracuda swiftly addressed a zero-day vulnerability in their email attachment screening module, minimizing potential damage to customer data and systems.

Armoryze offers **risk-based vulnerability management services** for enhanced security. Barracuda's prompt response and patch deployment prioritize customer safety, while affected customers are notified to stay vigilant and evaluate security measures.