EINPRESSWIRE

SaaS Alerts Exposes Rise in SMB Cyberattacks Originating from Russia-China in SaaS Application Security Insights Report

Data-Driven Analysis Reveals Top SaaS Applications and Data Targeted by Threat Actors with Detailed Insights to Support Managed Service Provider-Client Defenses

WILMINGTON, NC, UNITED STATES, March 8, 2022 /EINPresswire.com/ -- SaaS Alerts, the cybersecurity company purpose-built for MSPs to protect and monetize their customers' business SaaS applications, today unveiled the findings of its latest edition of the SaaS Application Security Insights (SASI) Report. Published semi-annually, the free downloadable report is the only one of its kind to analyze approximately 136 million SaaS security events across 2,100 small and medium businesses (SMBs) globally and identifying cyber trends negatively impacting businesses.

The statistically significant findings of the latest SASI report take into account security events occurring across more than 120,000 user accounts during the period of January 1st to December 31st, 2021 and shows that the vast majority of attacks on top SaaS platforms such as Microsoft 365, Google Workspace, Slack and Dropbox are originating from the countries of Russia and China. The data set is statistically significant and enables solution providers managing a portfolio of SaaS applications with pertinent data and trends to support defensive IT security re-alignments as required.

Additionally, over the last several weeks, SaaS Alerts has seen a sharp rise in activity from countries with consistently high levels of both attempted and successful attacks originating within their borders -- Russia and China. The vast volumes of data analyzed suggests these countries may even be coordinating attack efforts. Per analysis available from SaaS Alerts, attack trend lines that compare Russia and China show almost the exact same pattern. Juxtaposed to a chart from Germany indicates that it is not even close to the same pattern, leading to educated speculation that these countries could be coordinating efforts.

According to the Brookings Institute, “The U.S. National Security Strategy declares Russia and China the two top threats to U.S. national security. At the best of times, U.S.-Russia ties are a mixture of cooperation and competition, but today they are largely adversarial… Russia’s increasingly close relationship with China represents an ongoing challenge for the United States. While there is little that Washington can do to draw Moscow away from Beijing, it should not pursue policies that drive the two countries closer together, such as the trade war with China and rafts of sanctions against Russia.”

During the time period ranging from January 1st to December 31st, 2021, SaaS Alerts monitored more over 136 million SaaS security events, collecting and analyzing the anonymous SaaS application security data to identify a breakdown of cyberattacks on the most popular SaaS applications in use by SMBs today.

Key findings of the report reveal:

- On average, SaaS Alerts is seeing approximately 10,000 Brute Force Attacks per day against the user accounts monitored by SaaS Alerts.

- The origin of potential attacks can be traced back to specific countries with current data indicating that Attempted Unauthorized Logins are coming from actors located in China, Vietnam, Russia, Korea and Brazil.

- While Successful Unauthorized Logins are originating in Russia, China, Vietnam, Korea and Brazil. These are countries where an actor has successfully logged-in using a valid user’s credentials.

- The report finds that the Three Most Common Critical SaaS Application Security Alerts stem from:

1. Alert: “User Location Outside Approved Location” an alert which is triggered when there’s a successful login to a user account from outside of an approved location or an approved IP address range.
2. Alert: “SaaS Integration” which indicates that account credentials have been used to connect to a third-party application which may lead to data and other account information sharing between SaaS Apps. Users often establish these connections for convenience without consideration to potential security violations.
3. Alert: “Multiple Account Lockouts” which is recorded when an account is locked out 4 or more times within a 12-hour period. Often indicating that malicious actors are actively (typically programmatically) trying password combinations to gain access to the account and have succeeded in validating a correct account name.

- Other key findings from the report focus on common threat vectors that are putting SMBs at risk including a shocking ratio of Guest User Accounts (versus Licensed Accounts) being leveraged by SMBs with 42% of the over 129,000 monitored SaaS accounts being Guest User Accounts, the report also identifies the top five Third-party OAuth App Integrations being leveraged by SMB users and details a threat vector around Risky File Sharing Behavior with 19% of cloud-based file sharing activity being to external sources versus internal file-sharing. Each of these activities pose a significant threat vector as they potentially open pathways for malicious attacks if not properly monitored and managed.

“In the uncertain cyber-climate we all reside in today, detailed SaaS security oversight and robust defenses are a requirement for ensuring high resiliency and business continuity,” said Jim Lippie, CEO, SaaS Alerts. “The loss, theft or corruption of mission critical or sensitive customer data can be operationally and financially troublesome for SMBs that depend on continuous and unrestricted business operations to bolster revenues which have been the target of threat actors for years. We offer this useful threat level breakdown to assist businesses and the MSPs that support them with highly accurate insights about the security landscape they reside in.”

The security management and compliance of SaaS applications in use by SMBs today have become a greater concern for MSPs as the deployment of cyber defenses take center stage. Protection of both the SaaS application and data are critical and must receive SaaS-optimized security controls. Building a security-minded employee culture that centers on security controls, SaaS-native cyber defenses and procedural compliance can play a significant role in reducing the risk of a successful attack.

To download a free copy of the latest SASI Report by SaaS Alerts, please visit
https://saasalerts.com/sasi-report-january-2022/

About Saas Alerts
SaaS Alerts is the cyber security company purpose built for MSPs to protect and monetize customer core SaaS business applications. SaaS Alerts offers a unified, real-time monitoring platform for MSPs to protect against: data theft, data at risk and bad actors and integrates with the most popular SaaS Applications. Learn more at www.saasalerts.com.

Media Contact:
Joe Austin for SaaS Alerts, Inc.

Joe Austin
APR
+1 818-332-6166
email us here
Visit us on social media:
Facebook
Twitter

LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/564957704