kindred

Security Newsletter

7 September 2020

Subscribe to this newsletter

Sendgrid Under Siege from Hacked Accounts, rushes to enforce MFA

Email service provider Sendgrid is grappling with an unusually large number of customer accounts whose passwords have been cracked, sold to spammers, and abused for sending phishing and email malware attacks. Sendgrid's parent company Twilio says it is working on a plan to require multi-factor authentication for all of its customers, but that solution may not come fast enough for organizations having trouble dealing with the fallout in the meantime.

Many companies use Sendgrid to communicate with their customers via email, or else pay marketing firms to do that on their behalf using Sendgrid's systems. Sendgrid takes steps to validate that new customers are legitimate businesses, and that emails sent through its

platform carry the proper digital signatures that other companies can use to validate that the messages have been authorized by its customers. But this also means when a Sendgrid customer account gets hacked and used to send malware or phishing scams, the threat is particularly acute because a large number of organizations allow email from Sendgrid's systems to sail through their spam-filtering systems.

In an interview with KrebsOnSecurity, Sendgrid parent firm Twilio acknowledged the company had recently seen an increase in compromised customer accounts being abused for spam. While Sendgrid does allow customers to use multi-factor authentication (also known as two-factor authentication or 2FA), this protection is not mandatory.

Neil Schwartzman, executive director of the anti-spam group CAUCE, said Sendgrid's 2FA plans are long overdue, noting that the company bought Authy back in 2015. "Single-factor authentication for a company like this in 2020 is just ludicrous given the potential damage and malicious content we're seeing," Schwartzman said. "I understand that it's a task to invoke 2FA, and given the volume of customers Sendgrid has that's something to consider because there's going to be a lot of customer overhead involved," he continued. "But it's not like your bank, social media account, email and plenty of other places online don't already insist on it."

Read More on KrebsOnSecurity

Even More on BankInfoSecurity

Morgan Stanley Hit With $5 Million Data Breach Suit

A $5 million lawsuit seeking class action status has been filed against Morgan Stanley, claiming the financial organization failed to properly safeguard personally identifiable information when the company discarded old computer equipment.

The suit is being brought by Morgan Stanley customer Timothy Smith in the U.S. District Court for the Southern District of New York on behalf of about 100 other customers affected by the data breach. The case is tied to incidents in 2016 and 2019 when the firm decommissioned several pieces of computer equipment without properly scrubbing the personal data. The data exposed may have included account names and numbers (at Morgan Stanley and any linked bank accounts), Social Security number, passport number, contact information, date of birth, asset value and holdings data. Morgan Stanley offered victims two years of prepaid credit monitoring services. The lawsuit claims that if criminals obtained access to the devices involved, they could use the customer data they contained to steal identities or sell it to other criminals or use it to make fraudulent purchases.

"In 2016, Morgan Stanley closed two data centers and decommissioned the computer equipment in both locations. As is customary, we contracted with a vendor to remove the data from the devices," the letter notes. "We subsequently learned that certain devices believed to have been wiped of all information still contained some unencrypted data."

Read More BankInfoSec

More #News

- Online Voting Startup Wants to Limit Some Security Research
- Microsoft to finally kill Adobe Flash support by January 2021
- Maximum Lifespan of SSL/TLS Certificates is 398 Days Starting Today
- Microsoft, Oracle, and Google top list of companies with most vulnerabilities disclosed in Q2
- Millions of WordPress sites are being probed & attacked with recent plugin bug
- New Attacks Allow Bypassing EMV Card PIN Verification
- Fake Android notifications – first Google, then Microsoft affected
- We Didn't Encrypt Your Password, We Hashed It. Here's What That Means:
- Firefox will add a new drive-by-download protection
- Facebook explains how it will notify third-parties about bugs in their products
- CNN-News18 allegedly hacked to deny PayTM hack claims
- Vishing scams use Amazon and Prime as lures – don't get caught!
- European ISPs report mysterious wave of DDoS attacks
- Phishing tricks – the Top Ten Treacheries of 2020

#Patch Time!

- Cisco fixes critical code execution bug in Jabber for Windows
- Magento plugin Magmi vulnerable to hijacking admin sessions
- Cisco warns of actively exploited IOS XR zero-days
- Cisco Jabber Bug Could Let Hackers Target Windows Systems Remotely

#Tech and #Tools

- ENISA Blue Team training courses
- One click forensics lab in the cloud
- Vulns - Open Source Scrapper Project - National Vulnerability Database
- Lessons Learned from SSH Credential Honeypots
- Testing docker CVE scanners. Part 2.5 — Exploiting CVE scanners
- Dive into Email Security: MTA-STS Policies
- Ciphey: Automated decoding/weak encryption cracking tool
- Lock screen/Bitlocker bypass/elevation of privilege in Bitlocker
- Detect Lateral Movement via Network File Shares
- Bulwark: asset and vulnerability management tool, with Jira integration, for app security reports

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us