kindred

# Security Newsletter

16 September 2019

Subscribe to this newsletter

# Business Email Compromise Is a $26 Billion Scam Says the FBI

FEDERAL BUREAU OF INVESTIGATION
iC3
INTERNET CRIME COMPLAINT CENTER

FBI's Internet Crime Complaint Center (IC3) says that Business Email Compromise (BEC) scams are continuing to grow every year, with a 100% increase in the identified global exposed losses between May 2018 and July 2019. Also, between June 2016 and July 2019, IC3 received victim complaints regarding 166,349 domestic and international incidents, with a total exposed dollar loss of over $26 billion.

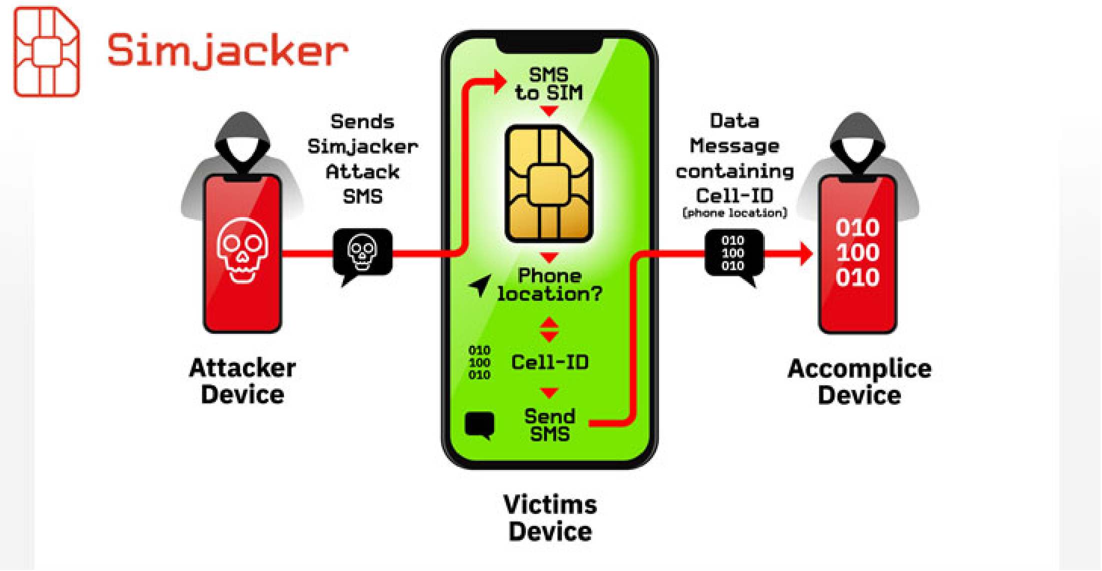
BEC aka EAC (short for Email Account Compromise) fraud schemes are scams carried out by crooks who will wire out funds without authorization to bank accounts they control via computer intrusion or after tricking key employees into doing it using social engineering. This type of attack targets small, medium, and large businesses alike, as well as individuals, and it has a high success rate due to the fraudsters' choice to pose as someone that the employees trust like a CEO or a business partner.

IC3 provides the following guidelines for employees containing both reactive measures and preventative strategies: Use secondary channels or two-factor authentication to verify requests for changes in account information. Ensure the URL in emails is associated with the business it claims to be from.Be alert to hyperlinks that may contain misspellings of the actual domain name. Refrain from supplying login credentials or PII in response to any emails. Monitor their personal financial accounts on a regular basis for irregularities, such as missing deposits. Keep all software patches on and all systems updated. Verify the email address used to send emails, especially when using a mobile or handheld device by ensuring the senders address email address appears to match who it is coming from. Ensure the settings the employees' computer are enabled to allow full email extensions to be viewed.

Read More on BleepingComputer

Even More from SecurityWeek

# New SIM Card Flaw Lets Hackers Hijack Any Phone Just By Sending SMS



Cybersecurity researchers today revealed the existence of a new and previously undetected critical vulnerability in SIM cards that could allow remote attackers to compromise targeted mobile phones and spy on victims just by sending an SMS.

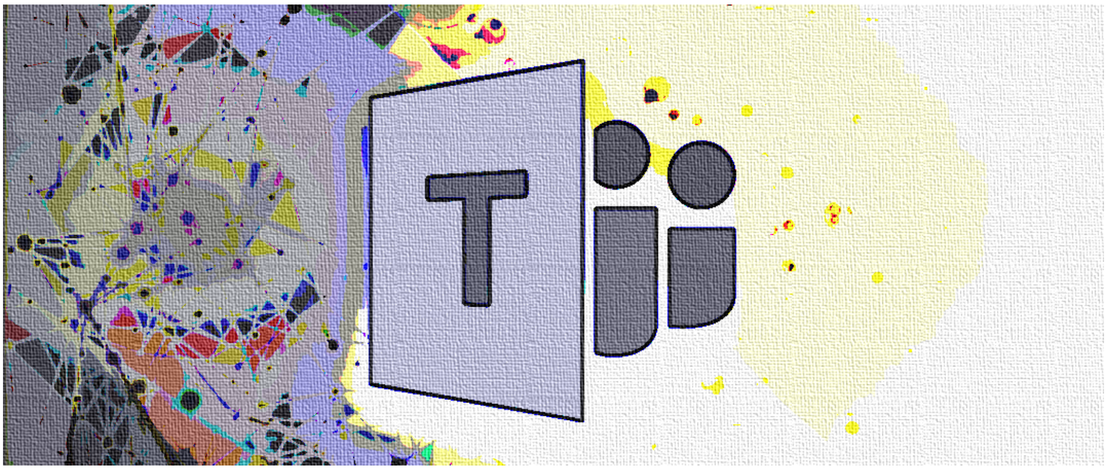
What's worrisome? A specific private company that works with governments is actively exploiting the SimJacker vulnerability from at least the last two years to conduct targeted surveillance on mobile phone users across several countries. "During the attack, the user is completely unaware that they received the attack, that information was retrieved, and that it was successfully exfiltrated," researchers explain. "The location information of thousands of devices was obtained over time without the knowledge or consent of the targeted mobile phone users. However the Simjacker attack can, and has been extended further to perform additional types of attacks." According to the researchers, all manufacturers and mobile phone models are vulnerable to the SimJacker attack as the vulnerability exploits a legacy technology embedded on SIM cards, whose specification has not been updated since 2009, potentially putting over a billion people at risk.

Researchers have responsibly disclosed details of this vulnerability to the GSM Association, the trade body representing the mobile operator community, as well as the SIM alliance that represents the main SIM Card/UICC manufacturers. Mobile operators can also immediately mitigate this threat by setting up a process to analyze and block suspicious messages that contain S@T Browser commands. As a potential victim, it appears, there is nothing much a mobile device user can do if they are using a SIM card with S@T Browser technology deployed on it, except requesting for a replacement of their SIM that has proprietary security mechanisms in place.

Read More on TheHackerNews

Even More on ZDNet

# Microsoft Teams Can Be Used To Execute Arbitrary Payloads



Attackers can use genuine binaries from Microsoft Teams to execute a malicious payload using a mock installation folder for the collaboration software. The problem affects most Windows desktop apps that use the Squirrel installation and update framework, which uses NuGet packages. A list of impacted products, as tested by the security researcher that made the discovery, includes WhatsApp, Grammarly, GitHub, Slack, and Discord.

One notable aspect of the experiment is that no resources are required on the target system other than the minimum package created by the attacker. Microsoft is aware of the problem but decided not to address it. The researcher says that the reason the company gave him was that the glitch "did not meet the bar of security issue".

Microsoft Teams is becoming a popular choice as an alternative to Slack. Microsoft announced in mid-July that its business-oriented tool for unified communications had 13 million daily active users and more than 19 million on a weekly basis, which is more than what Slack can boast.

Read More on BleepingComputer

## More #News

- Weaponized BlueKeep Exploit Released
- US city balks at paying $5.3 million ransomware demand
- WordPress 5.2.3 fixes new clutch of security vulnerabilities
- 281 Arrested in Worldwide Business Email Compromise Crackdown
- Some D-Link and Comba WiFi Routers Leak Their Passwords in Plaintext
- Wikipedia fights off huge DDoS attack
- New NetCAT Attack Can Leak Sensitive Data From Intel CPUs
- Extended Validation not so... extended? How I revoked $1,000,000 worth of EV certificates!
- Virtual Disk Attachments Can Bypass Gmail and Chrome Security
- Google experiments with DNS-over-HTTPS in Chrome

- Google hopes to protect users with open source differential privacy library
- Most consumers will refuse to work with enterprises that won't keep their data secure
- Attack Traffic Caught by Honeypots Triples Over Six Months
- Sophos open-sources Sandboxie, an utility for sandboxing any application
- Leaky database full of fake Groupon emails turns out to belong to crooks
- Phishing scams targeting Mac users on the rise with 1.6 million attacks in 2019
- DontDuo: Why you should remove phone calls from MFA options
- Firefox: What's next in making Encrypted DNS-over-HTTPS the Default
- How Sci-Fi Like 'WarGames' Led to Real Policy During the Reagan Administration

# #Patch Time!

- Facebook Patches "Memory Disclosure Using JPEG Images" Flaws in HHVM Servers
- Patch Tuesday, September 2019 Edition
- Adobe Releases Security Patches For Critical Flash Player Vulnerabilities
- Latest Microsoft Updates Patch 4 Critical Flaws In Windows RDP Client
- Chrome 77 Released with 52 Security Fixes
- Google discloses vulnerability in Chrome OS 'built-in security key' feature
- DoS Vulnerabilities Patched in NETGEAR N300 Routers

# #Tech and #Tools

- NebulousAD automated credential auditing tool using K-Anonymity
- SharpSniper: Find specific users in active directory via their username and logon IP address
- Serverless Blind XSS hunter with Cloudflare Workers
- Bypassing LinkedIn Search Limit by Playing With API
- An Accidental SSRF Honeypot in Google Calendar
- Exploiting JSONP and Bypassing Referer Check
- How to Detect Running Malware – Intro to Incident Response Triage (Part 7)
- Tips to block DoH at your org
- StringSifter: Ranks strings based on their relevance for malware analysis.
- OWASP Cheat Sheet series Project
- Initial Metasploit Exploit Module for BlueKeep (CVE-2019-0708)
- MacOS Red Teaming 208: macOS ATT&CK Techniques
- Active Directory Kill Chain Attack & Defense
- BlueSpawn: Windows-based Active Defense and EDR tool to empower Blue Teams
- Hardening Your Azure Domain Front
- AWS Security Tools curated list
- Hunting for C3
- Using PowerShell in Windows Defender

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

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 over 24 million customers across 100 markets. 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 as an innovation driven company that builds on trust.

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