kindred

Security Newsletter

12 August 2019

Subscribe to this newsletter

AT&T employees took bribes to plant malware on the company's network

AT&T employees took bribes to unlock millions of smartphones, and to install malware and unauthorized hardware on the company's network, the Department of Justice said yesterday. These details come from a DOJ case opened against Muhammad Fahd, a 34-year-old man from Pakistan, and his co-conspirator, Ghulam Jiwani, believed to be deceased.

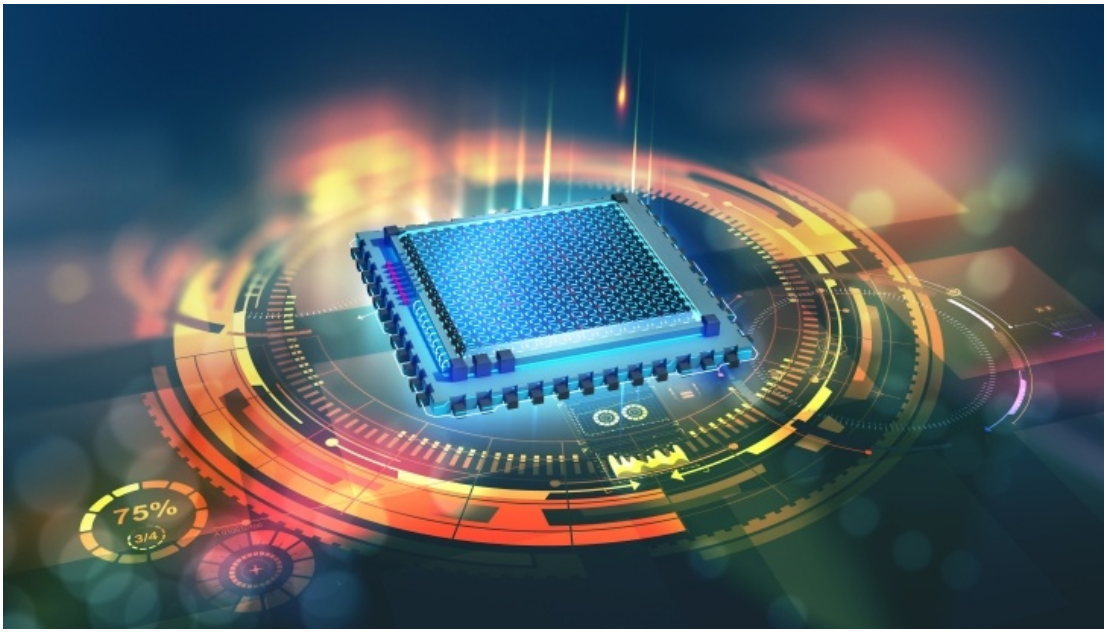
The bribery scheme lasted from at least April 2012 until September 2017. Initially, the two Pakistani men bribed AT&T employees to unlock expensive iPhones so they could be used outside AT&T's network. The two recruited AT&T employees by approaching them in private via telephone or Facebook messages. Employees who agreed, received lists of IMEI phone codes which they had to unlock for sums of money. Employees would then receive bribes in their bank accounts, in shell companies they created, or as cash, from the two Pakistani men. This initial stage of the scheme lasted for about a year, until April 2013, when several employees left or were fired by AT&T.

That's when Fahd changed tactics and bribed AT&T employees to install malware on AT&T's network at the Bothell call center. Between April and October 2013, this initial malware collected data on how AT&T infrastructure worked. In November 2014, as Fahd began having problems controlling this malware, the DOJ said he also bribed AT&T employees to install rogue wireless access points inside AT&T's Bothell call center. These devices helped Fahd with gaining access to AT&T internal apps and network, and continue the rogue phone unlocking scheme. Fahd was arrested in Hong Kong in February 2018, and extradited to the US on August 2, last week. He now faces a litany of charges that may send him behind bars for up to 20 years.

Read More

Even More on BankInfoSecurity

SWAPGS Attack — New Speculative Execution Flaw Affects All Modern Intel CPUs



A new variant of the Spectre (Variant 1) side-channel vulnerability has been discovered that affects all modern Intel CPUs, and probably some AMD processors as well, which leverage speculative execution for high performance, Microsoft and Red Hat warned. Identified as CVE-2019-1125, the vulnerability could allow unprivileged local attackers to access sensitive information stored in the operating system privileged kernel memory, including passwords, tokens, and encryption keys, that would otherwise be inaccessible.

Speculative execution is a core component of modern microprocessor design that speculatively executes instructions based on assumptions that are considered likely to be true. If the assumptions come out to be valid, the execution continues, otherwise discarded.

Microsoft silently issued patches for the new speculative execution vulnerability in its July 2019 Patch Tuesday security update which was discovered and responsibly disclosed by researchers at security firm Bitdefender. Since the attack can not be launched remotely, it is unlikely to cause mass malware infections, like EternalBlue was used for WannaCry; instead, it can be exploited as part of an extremely targeted attack.

Read More on TheHackerNews

More #News

- Vulnerability in Kubernetes Allows Access to Custom Resources
- Package Delivery! Cybercriminals at Your Doorstep
- Baldr Credential-Stealing Malware Targets Gamers
- Three ads generate 5.5 times more revenue than a web-based cryptojacking script
- State Farm Investigates Credential-Stuffing Attack
- Microsoft To Disable VBScript by Default on August 13th

- Supply-Chain Attack against the Electron Development Platform
- New Trojan Records Your Screen When on Sex Related Sites
- Clever Amazon Phishing Scam Creates Login Prompts in PDF Docs
- Don't let the crooks 'borrow' your home router as a hacking server
- The Fundamentals of Developing Effective DevSecOps
- New Flaws in Qualcomm Chips Expose Millions of Android Devices to Hacking
- Apple expands bug bounty to macOS, raises bug rewards
- Cloudflare Introduces Certificate Transparency Monitoring
- Democratic Campaign Group Left 6 Million Emails Exposed
- Steam Zero-Day Vulnerability Affects Over 100 Million Users
- Threesome app exposes user data, locations from London to the White House
- Microsoft releases new vulnerability tracking service

#Patch Time!

- SWAPGS Vulnerability in Modern CPUs Fixed in Windows, Linux, ChromeOS
- Reverse RDP Attack Also Enables Guest-to-Host Escape in Microsoft Hyper-V
- Cisco Patches Critical Flaws in Network Switches
- WhatsApp vulnerabilities 'put words in your mouth,' lets hackers take over conversations
- Update your iPhone – remote control holes revealed by researchers
- Researchers Find Vulnerabilities in Boeing 787 Firmware
- Unpatched KDE vulnerability disclosed on Twitter
- NVIDIA patches high-severity bugs in Windows GPUs and SHIELD
- Latest Android patches fix critical 'QualPwn' Wi-Fi flaws

#Tech and #Tools

- Steam Windows Client Local Privilege Escalation 0day
- Steam Escalation of Privileges PoC
- How to Build Your Own Penetration Testing Dropbox Using a Raspberry Pi 4
- EventList: Microsoft Security Baselines with MITRE ATT&CK
- DNS investigation on Windows
- Enter Mordor: Pre-recorded Security Events from Simulated Adversarial Techniques
- Tools and Methods for Auditing Kubernetes RBAC Policies
- List of Open Source C2 Post-Exploitation Frameworks
- Profiling RDP Clients with JA3 and RDFP
- Reverse RDP Attack: The Hyper-V Connection
- 5 Encrypted Messaging Apps Doing A Better Job Than WhatsApp
- social_attacker: Multi Site Automated Social Media Phishing Framework
- HTTP Desync Attacks: Request Smuggling Reborn
- EmailRep: Free API to query email reputation and report malicious senders
- Incident: web-based case management for incident response
- Predictable, Passphrase-Derived PGP Keys
- Three (And A Half) Vulns For The Price of One!
- The Technical Side of the Capital One AWS Security Breach

- The Capital One Breach & "cloud_breach_s3" CloudGoat Scenario
- Lessons in auditing cryptocurrency wallets, systems, and infrastructures
- CTF on blockchain security
- How to Attack kerberos 101
- Kerberos Armoring (FAST)
- Event Query Language
- Atomic Red Team
- Fantastic Red Team Attacks and how to find them

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