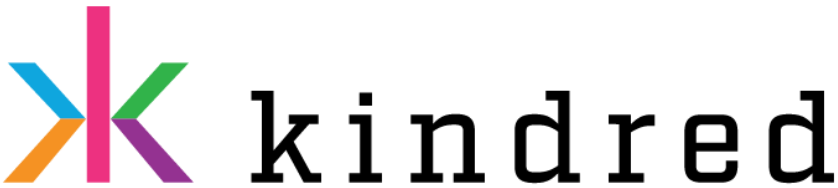

Security Newsletter

11 November 2019

Subscribe to this newsletter

Insider Threats: Trend Micro Employee Sold Consumer Data to Scammers; Feds Allege Saudi Spies Infiltrated Twitter

While companies do much to protect themselves from external threats, insiders always pose the highest risk to a company's data. Cybersecurity firm Trend Micro has disclosed a security incident this week carried out by an employee who improperly accessed the personal data of thousands of its customers with a "clear criminal intent" and then sold it to a malicious third-party tech support scammers earlier this year. According to the security company, an estimated number of customers affected by the breach is 68,000, which is less than one percent of the company's 12 million customer base. The stolen database contained Trend Micro consumer customers' names, email addresses, Trend Micro support ticket numbers, and in some instances, phone numbers.

A separate data breach incident also caused due to an insider threat, where two former Twitter employees have been charged with accessing information on thousands of Twitter user accounts on behalf of the Saudi Arabian government. According to an indictment filed on November 5 and unsealed just yesterday, one of the charged Twitter employees, American citizen Ahmad Abouammo, left the company in May 2015 and the other, Saudi citizen Ali Alzabarah, left the company in December 2015.

The information Abouammo and Alzabarah illegally accessed about Twitter users include their email addresses, devices used, browser information, user-provided biographical information, birthdates, and other info that can be used to know a user's location, like IP addresses associated with the accounts and phone numbers. Alzabarah, who joined Twitter in August 2013 as a "site reliability engineer," worked with the Saudi officials between May 21 and November 18, 2015, and allegedly accessed the private data on more than 6,000 Twitter accounts. Twitter acknowledged that the company has cooperated in this investigation and that it limits access to sensitive account information "to a limited group of trained and vetted employees."

Rogue TrendMicro Employee Sold Customer Data to Tech Support Scammers

Two Former Twitter Employees Caught Spying On Users For Saudi Arabia

More #News

- Explained: How New 'Delegated Credentials' Boosts TLS Protocol Security
- Google asks three mobile security firms to help scan Play Store apps
- Expanding Azure Active Directory support for FIDO2 preview to hybrid environments
- Amazon's Ring Video Doorbell Lets Attackers Steal Your Wi-Fi Password
- Leak of 4,000 Facebook documents heaps more trouble on internet giant
- DNS-over-HTTPS will eventually roll out in all major browsers, despite ISP opposition
- Gartner Says the Future of Network Security Lies with SASE
- Warrant let police search online DNA database
- How Do We Get to a Passwordless World? One Step at a Time.
- Facebook Portal survives Pwn2Own hacking contest, Amazon Echo got hacked
- Smartphone and speaker voice assistants can be abused using lasers
- Thinking about the balance between compliance and security
- Specially Crafted ZIP Files Used to Bypass Secure Email Gateways

#Patch Time!

- Nvidia patches severe GeForce, GPU vulnerabilities
- Microsoft Issues November 2019 Office Updates With Memory Leak Fix
- Cisco Patches Vulnerabilities in Small Business Routers, RoomOS Software
- Between 200,000 and 240,000 Magento online stores will reach EOL next year
- Libarchive vulnerability can lead to code execution on Linux, FreeBSD, NetBSD
- WordPress Admins Infect Their Sites With WP-VCD via Pirated Plugins
- Microsoft Warns of More Harmful Windows BlueKeep Attacks, Patch Now
- Watch Out IT Admins! Two Unpatched Critical RCE Flaws Disclosed in rConfig
- Apple developers – get this update to protect the rest of us

#Tech and #Tools

- The evolution of Zero Trust
- Integrating Calico and Istio to Secure Zero-Trust Networks on Kubernetes
- We built network isolation for 1,500 services to make Monzo more secure
- JWT (JSON Web Token) (in)security
- Documentation and supporting script sample for Windows Exploit Guard
- Protecting Your Malware with blockdlls and ACG
- CALDERA: automated adversary emulation system, using MITRE ATT&CK™ framework.
- Deploying honeytokens in Active Directory & How to trick attackers with deceptive BloodHound paths
- Calico: simplify, scale, and secure cloud networks
- Gitlab's red team operations documentation
- ☽amerka GUI — IoT/Industrial Control Systems reconnaissance tool
- Same-Origin Policy And Cross-Origin Resource Sharing (CORS)

- EC2 Security Strategy
- Hacking JSON Web Tokens (JWTs)
- HSTS From Top to Bottom or GTFO
- OWASP API Security Top 10 cheat sheet
- Going Keyless Everywhere

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