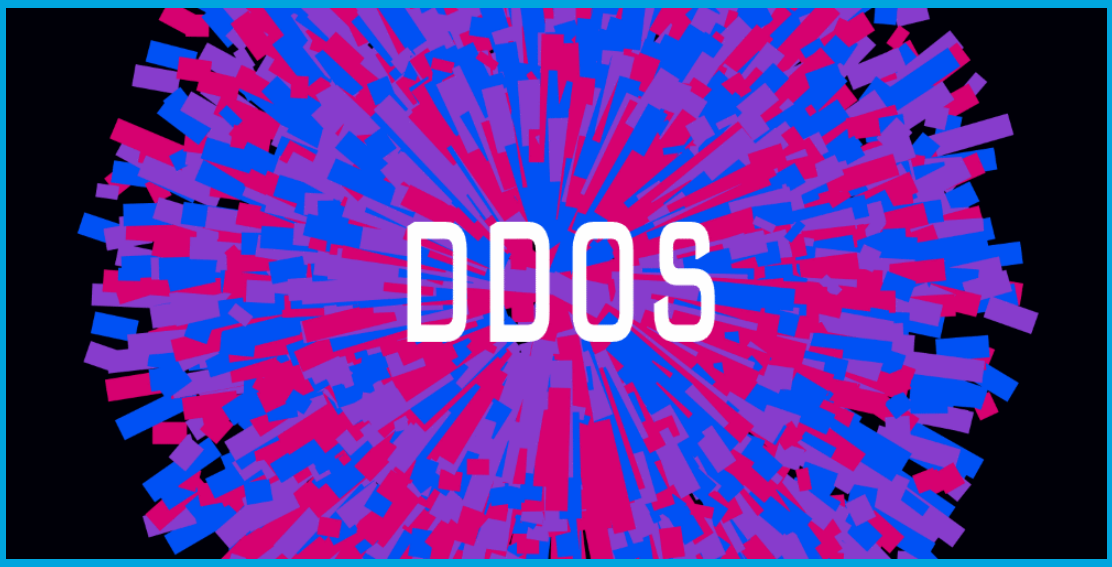
Security Newsletter

31 August 2020

Subscribe to this newsletter

Advanced DDoS extortionists target NZX, Moneygram, Braintree, and other financial services



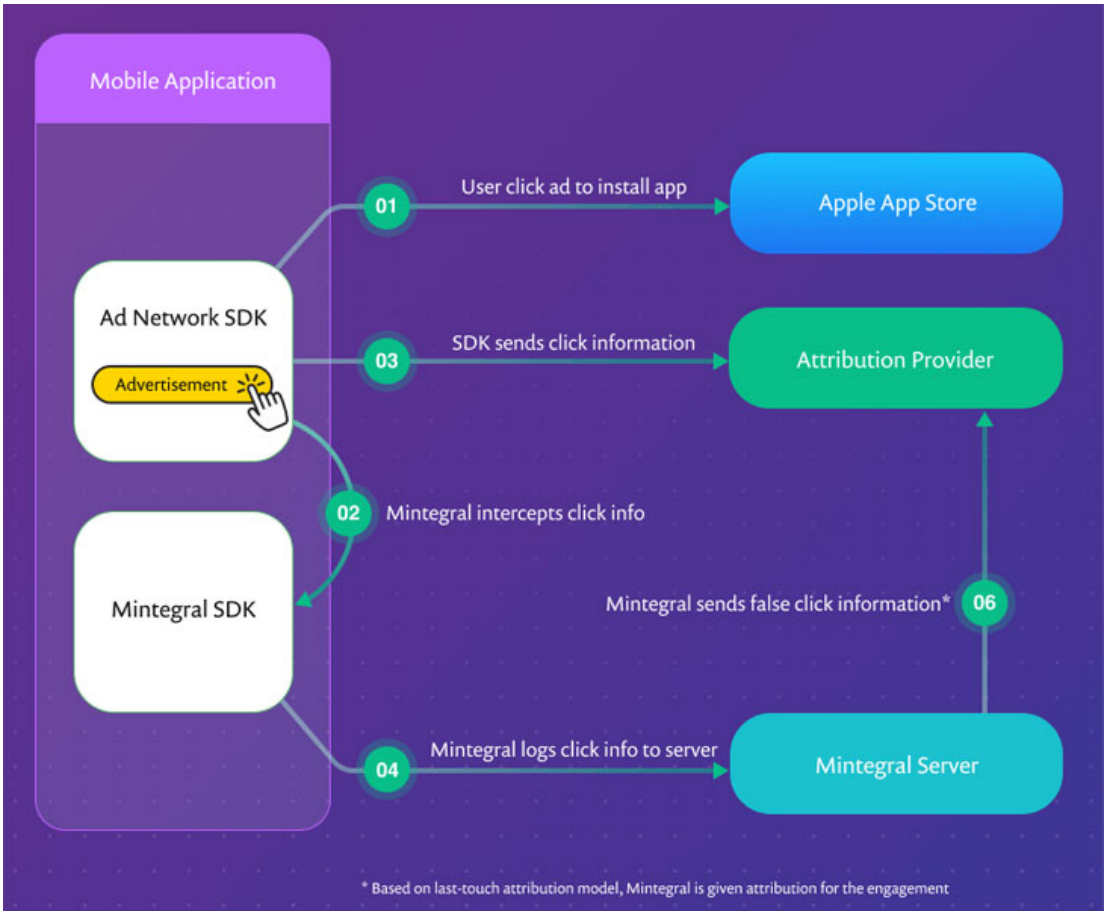
For the past weeks, a criminal gang has launched DDoS attacks against some of the world's biggest financial service providers and demanded Bitcoin payments as extortion fees to stop their attacks. One of the victims, the New Zealand stock exchange (NZX), has halted trading for the third day in a row following the attacks. Just this week, the group has attacked money transfer service MoneyGram, YesBank India, Worldpay, PayPal, Braintree, and Venmo, a source involved in the DDoS mitigation field has told ZDNet.

The attackers have been identified as the same hacker group mentioned in an Akamai report published on August 17, last week. The group uses names like Armada Collective and Fancy Bear — both borrowed from more famous hacker groups — to email companies and threaten DDoS attacks that can cripple operations and infer huge downtime and financial costs for the targets unless the victims pay a huge ransom demand in Bitcoin. Such types of attacks are called "DDoS extortions" or "DDoS-for-Bitcoin" and have first been seen in the summer of 2016.

In an update to its report added this Monday, on August 24, Akamai confirmed that the group launched complex DDoS attacks that, in some cases, peaked at almost 200 Gb/sec. The source also described the group as having "above-average DDoS skills." While previous DDoS extortionists would often target their victims' public websites, this new group has repeatedly targeted backend infrastructure, API endpoints, and DNS servers -- which explains why some of the DDoS attacks this week have resulted in severe and prolonged outages at some of their targets.

Read More on ZDNet

Popular iOS SDK Accused of Spying on Billions of Users and Committing Ad Fraud



Mintegral, popular iOS software development kit (SDK) used by over 1,200 apps—with a total of more than a billion mobile users—is said to contain malicious code with the goal of perpetrating mobile ad-click fraud and capturing sensitive information. Mintegral includes an SDK component that allows it to collect URLs, device identifiers, IP Address, operating system version, and other user sensitive data from compromised apps to a remote logging server.

Although the names of the compromised apps using the SDK have not been disclosed, the code was uncovered in the iOS version of the Mintegral SDK (6.3.5.0), with the first version of the malicious SDK dating back to July 17, 2019 (5.5.1). The Android version of the SDK, however, doesn't appear to be affected.

Stating that the SDK contains several anti-debug protection intending to hide the actual behavior of the application, Snyk uncovered evidence that Mintegral SDK not only intercepts all the ad clicks within an app but also use this information to fraudulently attribute the click to its ad network even in cases where a competing ad network has served the ad. In other words, Mintegral has been stealing ad revenues from other advertising networks by claiming the ads from a different ad network as its own, in addition to robbing developers off their revenues even when the platform isn't being used to serve ads.

Read More on TheHackerNews

More #News

- Implications for CSOs of Charges Against Joe Sullivan
- 2 ATM Manufacturers Patch Vulnerabilities
- Elon Musk confirms Russian hacking plot targeted Tesla factory
- Amazon Supplier Fraud
- Academics bypass PINs for Visa contactless payments
- Mercenary hacker group targets companies with 3Ds Max malware
- Free photos, graphics site Freepik discloses data breach impacting 8.3M users
- Microsoft Announces Public Preview of Application Guard for Office
- UltraRank Group Stole Card Data From Hundreds of Sites Using JS Sniffers

#Patch Time!

- New Chrome, Firefox versions fix security bugs, bring productivity features
- Security researcher discloses Safari bug after Apple delays patch
- WordPress Sites Targeted via Vulnerabilities in WooCommerce Discounts Plugin
- Microsoft delays Windows 10 1803 end of service due to pandemic
- Google Researcher Reported 3 Flaws in Apache Web Server Software

#Tech and #Tools

- Microsoft Zero Trust deployment guide for your applications
- How to install Infection Monkey for breach and attack simulations on your network
- Beware of O365 App Password Persistence
- Stowaway: Multi-hop proxy tool
- Red teaming with cobalt strike – not so obvious features
- Guide to Side-Channel Attacks
- Building a SIEM: combining ELK, Wazuh HIDS and Elastalert for optimal performance
- Python Basics: Packet Crafting With Scapy
- SIEM from scratch vagrant
- Evading Sysmon DNS Monitoring
- Defend the Flag: Test Microsoft Security products
- XSS: Arithmetic Operators & Optional Chaining To Bypass Filters & Sanitization
- URLSafe: Escape malicious url (or re-arm them)
- Introduction to Windows tokens for security practitioners
- MacOS Security & Privacy guide

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