NEXUSGUARD

White Paper

DDoS Protection for **Mobile Apps**

Nexusguard's Mobile SDK enables mobile app servers to distinguish legitimate traffic from malicious requests sent from hijacked mobile devices

V2.1.1

Nexusguard's Mobile SDK enables mobile app servers to distinguish legitimate traffic from malicious requests sent from hijacked mobile devices

As the Internet of Things (IoT) evolves and expands into different territories of daily life, the potential surface for DDoS attacks — sometimes combined with infiltration attempts — is growing exponentially.

According to Gartner[1], the IoT marketplace will see 26 billion units running by 2020. Additionally, IoT product and service providers will generate incremental revenue of about US$309 billion, mostly in services. Despite the lucrative market for these portable, connected devices, the growing presence of IoT exposes both the devices and the data on them tonew security vulnerabilities. In other words, the increasing ubiquity of IoT creates a greater potential for unauthorized access to personal information and can also greatly facilitate attacks — including DDoS — on other systems.

Because these gadgets are generally designed with lightweight security, largely due to a very short product life cycle and cost concerns, they have become a perfect target for cyber criminals bent on leveraging as much bandwidth as they can get their hands on. Also, the lack of data security standards governing IoT devices creates multiple vulnerabilities that hackers can exploit.

However, even though potentially compromised IoT devices present a rapidly emerging security threat, many have only limited options for firmware upgrades and other risk management features. And the fact that they are "always on" also makes them highly susceptible to intrusion and attacks.

The Challenge

DDoS attacks from smart devices are difficult to mitigate, given that IoT networks can comprise hundreds of thousands of devices. It is possible for an attacker to assign a small task to each connected device, having some send dozens of requests to the target server and others just a few spam messages. This way, small actions can easily go unnoticed by individual users. But when a huge number of devices is hijacked to orchestrate a massive, sophisticated attack, the effect can be dramatic.

While desktop and mobile botnets are now being stretched to weave gigantic botnets, it is inevitable that the average size of DDoS attacks will continue to grow at an astonishing rate in the next few years. It is already evident that botnet controllers are trying to form botnets to include desktop PCs and mobile devices, so that they can initiate more powerful and sophisticated attacks.

Several malicious apps that can compromise smartphones have already been discovered. In theory, an attacker can generate a vast amount of illegal requests to a mobile app server in attempts to bring it down or mask other fraudulent activities. More sophisticated attackers may also deploy botnets on a number of hijacked devices to fake HTTP requests as if they were being sent from individual users.

1 Forecast: The Internet of Things, Worldwide, 2014. Gartner, Inc.

In reality, due to limited mobile bandwidth, severe DDoS attacks from Trojan-infected smart devices have yet to be reported. But as mobile network bandwidth and the processing power of smart devices continue to grow, it is only a matter of time before IoT devices become a major contributor to DDoS attacks.

In light of these emerging threats, the absence or inadequacy of anti-DDoS protection in client-side apps could leave app servers susceptible to DDoS attacks. And although no significant DDoS attack from IoT devices has been detected yet, attacks that disguise themselves as legitimate requests to bypass protection are already commonplace.

The Solution

Without proper built-in protection for mobile apps, an attack can severely damage a company's reputation and result in the loss of millions due to lost revenue, brand damage, and breach of SLAs. For companies running mobile app businesses, securing DDoS protection from Nexusguard is the most viable and effective solution to protect mobile app servers. Leveraging its enormous, global cloud-scrubbing capacity, organizations can effectively mitigate DDoS attacks of all types and sizes over the cloud — regardless of the source, and without compromising user experience and speed.

Nexusguard also provides solutions for mobile app developers. During the design process, developers are encouraged to adopt a "security by design" approach whereby they are advised to carry out risk assessments, implementation of smart defaults, and security measure tests.

One very effective solution is to make the mobile app support script or verification codes, so that the app server can distinguish legitimate users from malicious traffic generated by 2 compromised devices. To that end, Nexusguard developed its Mobile SDK[2]— a tool that enables app developers to incorporate Nexusguard's Challenge-Response (C/R) code into mobile apps running on Android and iOS.

With Nexusguard's C/R code embedded in the client-end app, the app user is challenged to prove that he or she is a human being only when the app is detected sending out highly suspicious HTTP requests as determined by the Nexusguard application protection engine. Depending on an end-user's response or the authentication results, Nexusguard's application protection engine will allow the user to smoothly pass through or flag the source as malicious.

No change to the app server is required to implement Nexusguard's Mobile SDK. The developer only needs to integrate the SDK resource file into the client app. In order for the mitigation process to take effect, Nexusguard has to serve as the proxy on behalf of the app server, utilizing multi-layered filtering and mitigation techniques to effectively block all malicious traffic.

2 Prerequisite: HTTP is the application protocol used between the app client and the app server.

NEXUSGUARD

Founded in 2008, Nexusguard is the global leader in fighting malicious internet attacks. Nexusguard protects clients against a multitude of threats, including distributed denial of service (DDoS) attacks, to ensure uninterrupted internet service. Nexusguard provides comprehensive, highly customized solutions for customers of all sizes, across a range of industries, and also enables turnkey anti-DDoS solutions for service providers. Nexusguard delivers on its promise to maximize peace of mind by minimizing threats. Headquartered in San Francisco, Nexusguard's network of security experts extends globally.

Twitter twitter.com/nexusguard
Facebook facebook.com/NXG.PR
LinkedIn linkedin.com/company/nexusguard

nexusguard.com
contact@nexusguard.com

20160824-EN-A4