radware

Operation Ababil Phase 3 Wave 4
April Attack Report

radware ert

Background

The week of March 24th started the 4th wave of DDoS attacks against banks and financial institutions in the US. Qassam Cyber Fighters have launched the 4th wave of the 3rd phase of Operation Ababil and have updated their Pastebin page with new threat attacks. The targets of this attack remain the leading US banks including Bank of America, Chase Bank, PNC, Union Bank, BB&T, US Bank, Fifth Third Bank and Citibank.

Attack Information

Radware ERT is actively involved in fighting and mitigating these attacks and found that these attacks are both sophisticated and contain multiple complicated attack vectors. For the first time in the prolonged Operation Ababil campaign, the attackers are launching encrypted attacks based on SSL protocol.

The first attack vector that the ERT identified is an SSL flood attack. This flood attack is mostly generated by web servers around the world that were compromised by the attackers. The attackers exploited some well known vulnerabilities of PHP applications such as Wordpress plugins and other infamous issues with common CMS frameworks (Drupal/Joomla). Once the servers were compromised, the attackers uploaded their own attack scripts into the servers and launched the attack.

Radware's research lab has studied two main scripts (Shell Booters) that were used by the attackers during the 4th wave of operation Ababil on the banks secured online services.

The first script that was studied is designed to frequently perform an HTTP GET over SSL. Attacks that are using this script not only generates load on the HTTP server but also forces the server to handle many SSL handshakes in a very short time from many sources.

The second script that was studied generates a brute force attack on the online banking services of the victim banks. Using this attack tool, the attackers try to connect to the banks' online user accounts by guessing the user name login. The objective of the attackers is not to get access to the accounts, which is a very difficult task, but to lockout the accounts, and prevent the banks' customers from accessing their online banking services. The attackers launch thousands of requests to access the online accounts using random user names and passwords that the computer guesses. If the user name is correct and the password is wrong, the account will be locked after several attempts. In this method, the attackers manage to lockout thousands of bank accounts resulting in several angry and panicked customers calling the bank support center complaining and fearing of fraud activity on their accounts.

There are simpler attack vectors that participate in the attacks, such as download flood of heave PDF and images coming from Botnets, but the two aforementioned above are the most interesting, sophisticated ones.

Attack Mitigation

SSL based attacks are the Achilles heel of the banks cyber security defense and any other organization that utilize secured connections and secured payments. SSL based attacks are easy to launch and difficult to mitigate, making them an ideal choice for attackers while Radware observes a significant rise in the utilization of SSL based attack tools.

In order to mitigate SSL based attacks, the mitigation solution must first decrypt the encrypted SSL transaction in order to understand whether this is a malicious or a legitimate transaction. However, this operation requires the SSL keys of the bank, which cannot be given to a third party vendor or MSSP. In addition, the decryption and the encryption of the transactions require significant computing resources, which is not available on the banks servers.

Radware offers an industry unique solution for SSL based attacks that are utilizing special SSL accelerator hardware to handle the decryption of the transactions integrated with its Attack Mitigation System. Read more on the Radware solution for SSL based threats.