FBI FLASH

FBI LIAISON ALERT SYSTEM
#M-000001-BT

The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in **42 USC § 10607**.

The FBI is providing the following information with high confidence:

SUMMARY

(U//FOUO) As of April 10, 2013, the "Brobot" attack scripts utilized in the DDoS attacks have been modified. The FBI Cyber Division assesses that these scripts have been modified by the actors in an attempt to increase the effectiveness with which the scripts evade detection. Because the attacks have been ongoing for seven months, the actors are changing their attack methodology to circumvent mitigation efforts of the financial institutions.

(U//FOUO) Since September 2012, US financial institutions have been under coordinated and timed DDoS attacks. To date, 46 U.S. financial institutions have been targeted with DDoS attacks, with various degrees of impact, in over 200 separate DDoS attacks. These attacks have utilized high bandwidth webservers with vulnerable content management systems. Typically a customer account is compromised and attack scripts are then uploaded to a hidden directory on the customer website. To date the botnets have been identified as "Brobot" and "Kamikaze/Toxin."

TECHNICAL DETAILS

(U//FOUO) The latest version of the "Brobot" attack scripts that have been utilized to attack the login capabilities of a financial institution's website spoofs a fraudulent access cookie, user-agent string and referrer. The login script includes several random strings, but does contain one hard-coded string, '63.83.61.17-1365521883478351', in the script.

(U//FOUO) The hard-coded string does not affect the new attack scripts; however it can be used as an IDS/IPS signature to detect and block attacks from the "Brobot" botnet.

POINT OF CONTACT

Please contact the FBI with any questions related to this FLASH report at:
Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937