How to Mitigate Risk of DDoS Attacks

2012 will be remembered as the start of massive large-scale cyber-attacks against U.S. financial institutions. Sophisticated criminal groups launched distributed denial of service (DDoS) attacks against large U.S. financial institutions, which continues throughout 2013.

One criminal group launched DDoS attacks against the nation’s largest financial institutions to garner public attention to the group’s cause. Other criminal groups launched DDoS attacks against financial institutions to divert institution resources while cyber thieves simultaneously logged into customer accounts to make unauthorized transfers to accounts at other financial institutions.

Several large U.S. banks have fallen victim to cyber-attacks since September 2012. A group known as the Izz ad-Din al-Qassam Cyber Fighters (Cyber Fighters) took credit for launching the DDoS attacks against the nation’s largest financial institutions in September and October of 2012. The group launched another round (phase 2) of DDoS attacks against mid-tier financial institutions in December 2012 and January 2013. Phase 3 was launched in March 2013 and phase 4 in July 2013. The group’s most recent DDoS attacks were not successful in taking down the sites.

While DDoS attacks are not new, Defense Secretary Leon Panetta said the scale and speed with which these attacks occurred is unprecedented. The initial DDoS attacks by Cyber Fighters targeted U.S. Bank, PNC, Wells Fargo, Chase, Capital One, SunTrust and Regions, to name a few. The attacks disrupted online banking services offered by the banks preventing customers from logging into their accounts. In December 2012, Cyber Fighters announced another round of planned attacks against five major U.S. banks - U.S. Bancorp, JPMorgan Chase, Bank of America, PNC Financial Services and SunTrust Bank. According to the group’s Pastebin post, "The wideness and the number of attacks will increase explicitly." The group made good on its threats with attacks on a number of banks including U.S. Bank, PNC, Citigroup and Wells Fargo. A Jan. 1, 2013 Pastebin posting by this group indicated no U.S. bank is safe from their attacks.

‘Project Blitzkrieg’

RSA issued a warning in October 2012 of a planned attack on 30 U.S. financial institutions shortly after the initial DDoS attacks were launched by the Izz ad-Din al-Qassam Cyber Fighters group. Monitoring an Internet forum used by cyber thieves, RSA learned of a Russian crime group’s plan to launch a Trojan-based attack against the U.S. financial institutions this spring, which it believes to be the most substantial banking Trojan operation seen to date. The Izz ad-Din al-Qassam Cyber Fighters group claims their attacks are not related to the planned Trojan-based attacks. Referred to as "Project Blitzkrieg," RSA reported the Russian crime group was actively recruiting botmasters to help launch the attack by spreading a variation of the Gozi banking Trojan, which RSA dubbed "Gozi Prinimalka." RSA believes the goal of the attack is to initiate unauthorized wire transfers and ACH transactions through online banking systems.

What You Can Do

Credit unions should not underestimate these threats and should take steps to mitigate the risk of DDoS-caused service interruptions. Although it may be impossible to prevent a DDoS attack, credit unions can implement processes to identify them. These include:

- Monitor bandwidth usage.
- Monitor firewall logs to determine what is being attacked.
- Use an intrusion detection system to identify the type of traffic.
- Conduct proper due diligence on third-party service providers, such as Internet service providers and web-hosting vendors.
- Review contingency plans to ensure they address website problems caused by DDoS attacks.
- Be prepared to provide timely and accurate information to members regarding website problems caused by DDoS attacks.

For online banking systems, credit unions should have a strong multifactor authentication method in place to comply with the Federal Financial Institution Examination Council’s (FFIEC) updated authentication guidance issued in 2011. At a minimum, the FFIEC expects all financial institutions to have a fraud monitoring system in place to detect anomalous activity related to the initial login and authentication of members requesting access to the online banking system and 2) initiating fund transfers to other parties.

This is not intended as legal advice. For more information about cyber risks, visit CUNA Mutual Group’s Credit Union Protection Resource Center at www.cunamutual.com.
What Happens To Victims

McAfee issued a report in December 2012 supporting RSA's findings stating it found evidence the Russian group piloted the Trojan by infecting a minimum of 300 to 500 computers across the U.S. In addition to stealing the victim's online banking login credentials, RSA reported the Gozi Prinimalka Trojan sends the machine's details to the botmaster. A "novel virtual-machine-synching module" installed on the botmaster's machine will purportedly duplicate the victim's computer settings, including the victim's time zone, screen resolution, cookies, browser type and version, and software product IDs.

Fraudsters can then login to the victims' accounts and successfully defeat the multifactor authentication method involving device recognition. RSA believes the group is targeting accounts held at U.S. banks due to weak authentication methods and lack of layered security controls. Cyber-thieves used DDoS attacks against financial institutions as a smoke screen to divert attention away from unauthorized transactions they initiated through account takeovers at impacted institutions. The FBI, in conjunction with the Financial Services - Information Sharing and Analysis Center (FS-ISAC), issued an alert in September warning financial institutions. The alert stated cyber thieves were distributing remote-access Trojans through phishing e-mails to compromise financial institution networks and steal customer login credentials. The stolen credentials were used to initiate unauthorized wire transfers to accounts at foreign institutions. The FBI reported DDoS attacks were launched against the financial institutions in some of the incidents, before and after the unauthorized transactions occurred. The FBI believes the DDoS attacks were launched as a smoke screen tactic to divert attention away from the unauthorized transactions. In December, the Office of the Comptroller of Currency warned financial institutions DDoS attacks may be used as a diversion to cover up unauthorized transfers initiated via online banking.

Ken Otsuka is senior consultant, risk management, with CUNA Mutual Group. He can be reached at 847-612-9653, or at kenneth.otsuka@cunamutual.com.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.