Are you Prepared for a Cyber Attack?

Large-scale cyber attacks against U.S. financial institutions became commonplace in 2012. One criminal group launched distributed denial of service (DDoS) attacks against large U.S. financial institutions, including credit unions, to gain attention to their cause. Other criminal groups have launched DDoS attacks against financial institutions as diversionary tactics while fraudsters logged into customer accounts to steal funds.

Alert Details

The hacktivist group, Izz ad-Din al-Qassam Cyber Fighters, took credit for launching several distributed denial of service (DDoS) attacks against large U.S. financial institutions starting in September 2012 and continued their attacks through January. At least two credit unions were recent victims of the attacks. Defense secretary Leon Panetta said the scale and speed with which the attacks occurred is unprecedented.

However, the Izz ad-Din al-Qassam group announced on January 29th through a Pastebin posting that it will suspend the attacks after videos it deemed as offensive were taken down from a U.S. website.

Shortly after the Izz ad-Din al-Qassam group started their attacks, security firm RSA issued a warning of its discovery of a massive Trojan-based attack planned against 30 U.S. financial institutions by a Russian crime group. The Izz ad-Din Qassam group claims their attacks are not related to the planned Trojan-based attacks.

Dubbed “Project Blitzkrieg,” RSA reported the Russian group behind the planned Trojan-based attack was actively recruiting botmasters to help launch the attack. RSA believes the Russian group plans to spread a variation of the Gozi banking Trojan, which RSA referred to as Gozi Prinimalkga. The role of the botmasters would be to send spam email containing an infected attachment or a link to an infected website. It is believed the goal of the attack is to initiate fraudulent transfers through the financial institutions’ online banking systems.

McAfee issued a report in December supporting RSA’s prior findings. McAfee reported it found evidence the Russian group piloted the Trojan by infecting a minimum of 300 to 500 computers across the U.S.
Are you Prepared for a Cyber Attack?

In some prior account takeover cases at financial institutions, the cyber thieves also launched DDoS attacks before and after the unauthorized transfers were initiated. It is believed the DDoS attacks served as a smoke screen to divert attention from the thieves stealing funds from customer accounts.

Massive cyber attacks against financial institutions are becoming common. Credit unions should not underestimate these threats and should take steps to mitigate the risk of DDoS caused service interruptions and to protect members’ accounts.

Risk Mitigation Tips
Credit unions should consider the following:

1. Although it is impossible to prevent a DDoS attack, credit unions can implement processes to prepare for and identify them, including:
   - Monitor bandwidth usage;
   - Monitor firewall logs to determine what is being attacked;
   - Use an intrusion detection system to identify the type of traffic;
   - Conduct due diligence on third-party service providers, such as Internet service providers and Web-hosting vendors;
   - Ensure contingency plans are up-to-date and adequately address website problems caused by DDoS attacks;
   - Be prepared to provide timely and accurate information to members regarding website problems caused by DDoS attacks (it may be helpful to prepare a script for call center employees for this purpose); and
   - In the event an attack occurs, be sure to review transfers initiated by members through the online banking system.

2. Ensure you have deployed anti-spam software on your Internet email gateway to reduce the risk of receiving emails containing infected attachments or links to infected websites.

3. Ensure you have deployed antivirus protection with real-time capability on all servers and workstation computers. All incoming emails plus attachments as well as files downloaded from the Internet are scanned for viruses before employees are allowed to save them.

4. Ensure you have deployed content filtering software to block employees from visiting websites considered inappropriate.

5. Conduct frequent security awareness training for employees.
Are you Prepared for a Cyber Attack?

6. Ensure your credit union is in compliance with the Federal Financial Institution Examination Council’s (FFIEC) updated authentication guidance. At a minimum, the FFIEC expects all financial institutions to have a fraud monitoring system in place to detect and effectively respond to suspicious or anomalous activity related to:

- Initial login and authentication of members requesting access to the online and mobile banking systems; and
- Initiation of transfers to other parties.

Credit unions should consider additional layered security controls, including, but not limited to:

- Reasonable monetary and frequency limits;
- Out-of-band authentication; and
- Out-of-band transaction verification for large dollar transfers.

Credit unions should also provide educational material to members on the danger posed by spam email and how to protect themselves while conducting online transactions.

Subhead Related Resources

- Protection Resource Center for related RISK Alerts and white papers:
  - Massive Cyberheist Planned against U.S. Financial Institutions
  - RSA Warns of Massive Attacks on 30 U.S. Banks
  - Financial Institutions Placed on High Alert
  - Online Banking Risks and Controls white paper

- RSA FraudAction Research Labs blog – Cyber Gang Seeks Botmasters to Wage Massive Wave of Trojan Attacks Against U.S. Banks

- McAfee Report: Analyzing Project Blitzkrieg, a Credible Threat