Thinking About And Preventing Botnet Activities

cyber security risk management

Summary: Botnets do have legitimate purposes, such as web indexing, but their dark side predominates. What community bankers should know.

AARP recently did some research around common smartphone activities for people ages 50Ys or older. The most common were: instant messages or emails (88%), traffic information (77%), downloading an app (69%), surfing the internet (64%), getting news and other information (62%), social networking (60%), using a voice activated assistant (45%), making a purchase (35%), and performing banking or financial transactions (35%). Now, consider the age of these customers and the fact that mobile banking ranked well behind using a voice activated assistant. It sure is something to think about.

The more people use technology, the more the bad guys target the good ones and the more potential for sneaky botnet activity. By definition, a botnet is a network of computers that has been infected with malicious software so it can be controlled as a group without the owners' knowledge.

Botnets do have legitimate purposes, such as web indexing, but their dark side predominates. Botnets have also fueled the spam industry's epic growth, vastly expanding the volume of unwanted email messages.

In the traditional transmission route, users receive emails sent from previously infected computers and open attachments that in turn infect their own networks.

But, botnets can also wriggle into your bank in other ways. Phishing emails might trick employees into visiting malicious websites, which then infect computers using a technique called drive-by downloading. Unlike a pop-up download, which asks the user for approval, drive-by downloads happen without any user participation. Or a virus might install alongside a staff-requested application, a form of attack known as a barnacle. An employee might accidentally bring a botnet virus into the office on a laptop or jump drive too.

In these instances, the end result is the same: malicious software downloads from the website to the employee's computer, turning that machine into a new part of the botnet. The virally infected computer is essentially an electronic zombie that the attacker can use to infiltrate a corporate network, send out spam, launch denial of service attacks, or harvest keystroke data, such as passwords and online banking information.

Fortunately, a lot can be done to protect against botnet attacks:

1. Start with having proper security in place
2. Add security patches to key applications
3. Control network access
4. Use strong, two-factor authentication
5. Ensure that your IT policy covers the safe use of USB thumb drives and laptops, or block them entirely.
6. Remove local administrative privileges

A complete anti-botnet security approach should also include scanning incoming and outgoing data for malicious data, safeguards against Trojan horse attacks, traffic pattern management, web application firewalls,

and products that identify and remove botnets, if you think your system is compromised.

All in all, community banks should stay on top of the latest botnet threats, warn customers and regularly review your bank safeguards to stay out of harm's way.

OUTSOURCED ALM SERVICES FOR COMMUNITY BANKS

Managing interest rate risk is both art and science. Regulators have raised the bar and community bankers have more to do than there are hours in a day. To see how easy it is to outsource & get expert help, contact us today.