FEATURE

Bad bots on the rise: A look at mobile, social, porn, and spam bots

Bad bots create untold security nightmares for the enterprise. Today, we're taking a look at the trouble they lead to, and what companies can do about it.

By David Geer

CSO |

APR 30, 2014 10:15 AM PDT

From 2012 to 2013, Incapsula, a website security firm focusing on CDN solutions as load balancing, found that bot traffic went from consisting of 51 percent to 61.5 percent of all Internet traffic, a 10.5-percent increase. Thirty-one percent of those bots are malicious, according to data from the report.

The word “bot” means different things. For this story, a bot is a malicious mobile, social, porn, or spam robot that lives on the Internet and unsuspecting users’ devices.

People errantly install mobile bots on smartphones as hidden elements of software bundles or free apps from third-party app stores. Since phone vendors do not authorize these downloads, users typically jailbreak or root their devices in order to enable a wider selection of free apps.

[Keep up with 8 hot cybersecurity trends (and 4 going cold). Give your career a boost with top security certifications: Who they're for, what they cost, and which you need. | Sign up for CSO newsletters.]

However, rooting disables the fundamental security that is present when it is impossible to download or install other than screened approved apps from the phone vendor’s app store.

Social bots invade user accounts, infecting social media when someone installs an application or API add-on in their Facebook or Twitter account, explains Richard Henderson, Security Strategist, FortiGuard Labs, Fortinet.

Installation grants the program permission to post to that person's Facebook or Twitter content. Sometimes the user doesn't have to grant permission for the infection to occur. It can happen automatically, says Henderson.

Social bots and malware use permissions to post and message the user's contacts with links to more malware or to counterfeit merchandise. Again, users don't realize when they install these apps that hackers have deceived them. Infected accounts can spam contact lists with thousands of messages and links to additional infections, says Henderson.

Porn bots include chat room spammers and bots that pop up on adult websites. Chat room spammers crawl the Internet looking for chat forums that use technologies such as Internet Relay Chat (IRC) and web-based chat. Porn bots invade these sites, messaging offers of free adult images via links.

Porn chat bots live on free adult websites where they pop up chat windows with pictures of attractive people saying, "I see you are from [your town here]. I live in your area. Would you like to chat?"

The chat bot determines the user's location based on their IP address.

"There's some rudimentary intelligence in those bots," says Henderson, "designed to build familiarity with the user to entice them to click to another porn site, which will require them to pay for premium content."

Spam bots are a sub-category of any of these other types of bots. “They’re designed to entice people to click on a link directing them to a malware delivery site or someplace selling counterfeit goods such as fake watches, Louie Vuitton handbags, and pharmaceuticals,” he adds.

Bot Threats

Mobile bots hide under the device’s operating system, sending premium text messages in secret. The associated messaging services end up costing the user thousands in phone bills.

“There’s no way to see that you’ve been sending these texts until you get your phone bill,” says Henderson.

Other mobile bots quietly collect user data, sending it back to the hacker. “These bots can send the entire phone book, the contents of your text messages, and anything you type in,” Henderson adds.

Still other mobile bots intercept and replace Internet-based ads with malicious forgeries. The intent is to get users to click on a bogus ad and attempt to make a purchase, according to Henderson, so the hacker can steal credit card data.

Social bots use social engineering, taking control of Facebook or Twitter user accounts and sending posts, tweets, and messages that appear to come from the user to everyone in the contact list.

People are likely to trust and click the associated links, making social bots attractive for delivering viruses, malware, and phishing attacks that collect account information. Hackers profit through ID theft and most any scheme that uses social engineering.

Porn bots generate income through a bait and switch, up-selling approach. Users who believe they are paying to communicate with someone local, receive access to premium adult content instead. Porn bots expose the enterprise to potentially damaging content such as child pornography, which causes legal entanglements, according to James Brown, Chief Experience Officer for JumpCloud

Spam bots leave people with faulty merchandise and all sorts of link-based, secretly insinuated malware from ransomware to rootkits.

Solutions for the Enterprise

These bottom-feeding Internet robots are responsible for a variety of enterprise losses including brand damage and lost revenues from unsatisfactory, counterfeit products. Bots increase the impact of malware, and social engineering through the sheer number of people they can reach almost instantaneously.

Through drive-by threats, bundled malware, and secretly-manifested financial charges, bad bots increase the financial gains of gangsters and hackers in attacks that frustrate consumers and enterprise employees.

Enterprises should monitor network traffic for all uncharacteristic, unexpected, and suspicious network behavior. In particular, traffic leaving servers for anomalous locations such as countries where the enterprise does not do business or to an Internet address that a server does not typically contact should raise red flags, according to Brown.

“Deploy intrusion detection and prevention systems preventing unauthorized outbound connections through corporate firewalls. Ensure that you roll out anti-virus software on all servers,” says Brown. Block future outbound connections to complicity IP addresses. Reimage infected servers entirely.

With the BYOD craze comes a balancing act between corporate security and employee usability. The organization should develop a thorough BYOD strategy in response. Saying no to BYOD is no longer an option.

“Our studies say that 50-percent or more of employees, especially younger employees, will ignore a policy that does not permit BYOD. They will try to connect their devices to the corporate network,” says Henderson.

It’s better to develop a proper BYOD policy and enforce it. It’s easier to work with most employees, keeping them happy, and regulating what they can do while addressing a much smaller number of infractions. Then when someone doesn’t agree to the policy or abide by it, the enterprise can block the device or sanction the user.

A typical BYOD policy that eases employee, device, and bad bot management permits a limited number of specified devices while requiring some combination of a suite of security software, NAC, and monitoring software. Many enterprises use containerization on the device or technologies that permit access only to a virtual image or representation of corporate data such that actual data never leaves the enterprise perimeter.

The enterprise should be able to satisfy employees who are concerned about data monitoring and privacy.

“Companies need to make it clear that while they have the ability to monitor personal Internet behavior, they don’t collect that information or take any action unless there is a breach of corporate data,” says Henderson.

Next read this

- *The 10 most powerful cybersecurity companies*
- *CISOs’ 15 top strategic priorities for 2021*
- *7 tenets of zero trust explained*