NEWS

The 'Great Cannon' of China enforces Internet censorship

Sophisticated DDoS attack tool can also be modified to inject malware, researchers found

By Loek Essers
Amsterdam Correspondent, IDG News Service
APR 10, 2015 8:23 AM PDT

China is deploying a tool that can be used to launch huge distributed denial-of-service (DDoS) attacks to enforce censorship. Researchers have dubbed it "the Great Cannon."

The first time the tool was seen in action was during the massive DDoS attacks that hit software development platform GitHub last month. The attack sent large amounts of traffic to the site, targeting Chinese anti-censorship projects hosted there. It was the largest attack the site has endured in its history.

That attack was first thought to have been orchestrated using China's "Great Firewall," a sophisticated ring of networking equipment and filtering software used by the government to exert strict control over Internet access in the country. The firewall is used to block sites like Facebook and Twitter as well as several media outlets.

[Related: Online privacy: Best browsers, settings, and tips]

However, while the Great Cannon infrastructure is co-located with the Great Firewall, it is a separate, offensive system, with different capabilities and design, said researchers at the University of California, Berkeley, and the University of Toronto on Friday.

The Great Cannon is not simply an extension of the Great Firewall, but rather a distinct tool that hijacks traffic to individual IP addresses, and can arbitrarily replace unencrypted content by sitting between the Web server and end user -- a method known as a man-in-the-middle attack. The system is used to manipulate the traffic of systems outside of China, silently programming browsers to create a massive DDoS attack, the researchers

said.

The attack method deployed against Github injected malicious Javascript into browsers connecting to the Chinese search engine Baidu. When the Great Cannon sees a request for certain Javascript files on one of Baidu's infrastructure servers that host commonly used analytics, social, or advertising scripts, it appears to take one of two actions. It either passes the request to Baidu's servers, which has happened over 98 percent of the time, or it drops the request before it reaches Baidu and instead sends a malicious script back to the requesting user, which has happened about 1.75 percent of the time, the report said.

In the latter case, the requesting user would be an individual outside China browsing a website making use of a Baidu infrastructure server, such as sites with ads served by Baidu's ad network. In the DDos attack against GitHub, the malicious script was used to enlist the requesting user as an unwitting participant, the report said.

These findings are in line with an analysis by the Electronic Frontier Foundation (EFF) that described the attack method used last week. According to the EFF, the attack was obviously orchestrated by people who had access to backbone routers in China and was only possible because the Baidu analytics script that is included on sites does not use encryption by default. A wider use of HTTPS could have prevented the attack, it found.

The Berkeley and Toronto researchers confirmed the suspicions about the origin of the attack, saying they believe there is compelling evidence that the Chinese government operates the cannon. They tested two international Internet links into China belonging to two different Chinese ISPs, and found that in both cases the Great Cannon was co-located with the Great Firewall. This strongly suggests a government actor, they said.

While DDoS attacks are quite crude, the Great Cannon can also be used in more sophisticated ways. A technically simple configuration change, switching the system to operating on traffic from a specific IP address rather than to a specific address, would allow Beijing to deliver malware to any computer outside of China that communicates with any Chinese server not employing cryptographic protections, they said.

A similar system used by the U.S. National Security Agency (NSA) and the U.K's GCHQ

intelligence services to deliver exploits is called QUANTUM, the researchers said.

"The operational deployment of the Great Cannon represents a significant escalation in state-level information control: the normalization of widespread use of an attack tool to enforce censorship by weaponizing users," the researchers said, adding that the findings emphasize the urgency of replacing legacy Web protocols, like HTTP, with their cryptographically strong versions, like HTTPS.

Copyright © 2015 IDG Communications, Inc.

7 inconvenient truths about the hybrid work trend

Copyright © 2022 IDG Communications, Inc.