SYRIA CYBER WATCH

NOV. 25, 2012

EXECUTIVE SUMMARY

Pro-regime botnet is identified by SecDev and taken down by Twitter. SecDev analysts exposed a pro-regime botnet flooding the Twittersphere with disinformation. Researchers estimate the botnet produced millions of pro-regime tweets between July 19, when it was activated, and November 20, when Twitter shut the network down after being alerted of its operations.

A rebel-produced YouTube video declaring plans to establish an Islamic state in Syria sparked an outcry on social media this week. While most comments were critical of the group's plan, a small minority voiced support.

Social media reports show the Free Syrian Army has captured portable surface-to-air missiles in recent assaults on military installations.

Evidence suggests the Syrian regime is blocking Virtual Private Networks (VPNs), one of the main methods for bypassing online censorship, and may be trying to block another circumvention option, Secure Shell (SSH) connections. However, Open Secure Shell (OSSH) connections remain reliable, according to Psiphon 3, a main provider of circumvention tools in the region.

ANALYSTS EXPOSE PRO-REGIME BOTNET

Analysts at SecDev's Syria Operation Group (SOG) exposed a botnet designed to flood Twitter with pro-regime content relating to the conflict in Syria, in English and in Arabic.

Social media botnets, (networks of automated software robots) can be used to spread disinformation and propaganda by inundating the channels with tweets reflecting a single perspective, dominating the conversation and creating an impression of legitimacy for that point of view. Like spam in an email inbox, botnet tweets make it difficult for legitimate users to find useful information.

In this case, a network of 64 bots produced about 4 million pro-regime postings on Twitter over its four-month lifetime, SecDev researchers estimate. The botnet flooded social media by tweeting content from pro-regime news sources, and amplified its impact by continuously re-tweeting content from the bot that controlled the network, or botmaster. SecDev alerted Twitter to the botnet's activities on Nov. 20, prompting the company to shut down the botnet, which had been in operation since July 19.

The botnet focused its content on three pro-regime news agencies: the Syrian Arab News Agency (SANA), Shukumaku.com, and Syriasteps.com – a strong indication that a pro-government actor was behind the creation of this network.

The botmaster was traced to a Twitter account called @almayadeentv1, linked to a pro-regime television station. Al Maya Deen TV was created by Ghassan Bin Jiddo, a former TV presenter and producer for Al Jazeera who left the agency in protest after it aired reports critical of the Syrian government. Although the station has no official connection to the botmaster account, the editorial slant of Jiddo's station aligns with that of the botnet: Al Maya Deen TV commonly refers to the Free Syrian Army as "terrorists," and describes government actions against its opponents as "cleansing."

The legitimate Twitter account for Al Maya Deen TV is @Almayadeennews, not @almayadeentv1. However, the account profile for @almayadeentv1 on Twitter links to Al Maya Deen TV's website.

It is unlikely Al Maya Deen TV failed to notice the @almayadeentv1 botnet. Since the botnet uses the station's name, any tracking of their brand would have revealed the significant amount of content on Twitter spread by the botnet. Analytical monitoring of their website indicates large numbers of connections originating from the @almayadeentv1 profile. The network was likely created to draw attention to the pro-regime media outlets involved, while providing plausible deniability for the pro-government actors behind the botnet.

The @almayadeentv1 account was highly successful in evading detection by Twitter while it was active: it was associated with approximately167,000 tweets and re-tweets, and by mid-September was consistently topping the list of the most common re-tweets, SecDev records indicate.

While the network used 64 primary bots over its lifetime, disposable bots – automated software that is less able to evade detection – were used on occasion, but Twitter was able to spot and remove them.

In social media analyses, the botnet showed up in visualizations as a tight cluster of accounts generating the same or very similar content, all sharing a similar pattern of attributes. Examples of these include:

- shortened URLs that appeared different, but led to the same extended URLs;
- little to no interaction with other Twitter accounts;
- all posted links to Shukumaku.com, Syriasteps.com, and Sana.sy;
- the @almayadeentv1 account followed no other account;
- bot accounts followed most of the same Twitter feeds;
- bots used similar tweeting and re-tweeting patterns over 24-hour periods;
- cycling through three-letter hashtags to produce around 16,000 unique hashtags in total; and,
- identical postings from a few of the bots initially, then a cascade of re-tweets through @almayadeentv1.

The SecDev Foundation alerted Twitter to the presence of the botnet, which violates that company's policy banning users from "flooding, spamming, (or) mail-bombing" its services.

On Nov. 20, Twitter removed the 64 accounts composing the botnet.

SecDev SOG analysts are investigating who was responsible for the botnet. New information on botnet attributes and detection methods were developed during the course of this two-month investigation and will be applied to tracing social media botnets in the future.

CALL FOR ISLAMIC STATE SPARKS OUTCRY

For Syrians, social media is a critical means for sharing news and discussing issues that could shape the outcome of the conflict, as debate about a video posted this week by extremist Islamist forces shows.

On Nov. 18, Liwaa Al Tawheed, one of the opposition forces in the Aleppo region, posted a video on YouTube denouncing the newly formed National Coalition of Opposition and Revolution Forces, and declaring plans to establish an Islamic state in Syria (see video). The statement purports to represent the "Armed Groups in Aleppo," although some of the listed groups, such as the Ahrar Alsham Battalions, have denied any links to it.

As of Nov. 22, the video had been watched over 100,000 times, with 1,400 likes and 858 dislikes. The video had attracted little attention when it was initially posted on Liaww Al Tawheed's Facebook page, where it scored less than 50 likes and was shared 29 times.

The video touched off a storm of controversy on Facebook, and was soon picked up by major television channels in the region. Iyad Shurbaji, a prominent Syrian journalist who has over 5,000 Facebook friends and 1,734 followers on Twitter (@eiadcharbaji), noted on Facebook that public outcry over the video has been "very reassuring. It shows that we still have the awareness needed to stand by the choices we made (in the) revolution." This post scored over 380 likes.

Most social media comments on Liwaa Al Tawheed's video were critical of the group's declaration, with many expressing the suspicion that it was part of a smear campaign staged by the regime to deter the international community from supporting the new coalition. In a typical posting, one person commented, "You are here to protect us and not to rule us." A small minority of postings showed support for the video: "You represent me," one post said. "You are the ones who will liberate Syria and Palestine, not the Free Syrian Army, which is under Western command."

ARMED REBELS SEIZE SAMS AND MANPADS

On Nov. 19, the FSA captured the base camp of one of the regime's key special-forces units, Division 46, in Aleppo. A video posted on social media shows FSA fighters seizing ammunition and some weapons, including portable surface-to-air missile launchers, known as Man-Portable Air Defence Systems, or MANPADs.

For footage of the Abnaa A'isah Battalion preparing for the attack, see this video.

Another posting shows weapons and ammunition captured in the assault.

On Nov. 20, Liwaa Asoud Alislam (part of the Damascus-based group, Liwaa Ahrar Houran, and members of the FSA) attacked a military installation in Al Hajar Al Aswad, south of Damascus (see video).

The video shows the group seizing a SAM-3 surface-to-air missile.

PSIPHON USE IN SYRIA

The Syrian regime actively blocks a range of online content, including foreign news services, opposition websites and other potentially critical sites. While circumvention methods can be used to bypass this censorship, evidence suggests the regime is blocking one of the main circumvention avenues – Virtual Private Networks (VPNs) – and may have taken steps to block another, Secure Shell (SSH) connections.

Users of Psiphon 3, a circumvention tool widely used in the region, are still able to bypass censorship using a third option (OSSH+ – an obfuscated version of the SSH protocol) that deliberately obfuscates the connection handshake rendering it more difficult to detect through deep packet inspection. Psiphon 3 is able to connect to the Internet using any one of the main cryptographic network protocols, cycling through VPN, SSH and OSSH+ connections until it succeeds (users can also manually select a preferred connection type).

OSSH+ has been the primary way Psiphon users in Syria connect to blocked sites since January 2011. Prior to January 2011, SSH was the favoured secure protocol. However, SSH connections have since dropped to between 1,200 and 2,300 a day, a sign that it is actively blocked by Syrian telecommunications operators. Psiphon reports that connections only rarely succeed via VPN (L2TP or IPSec). The online activist group, Telecomix, also reports that L2TP/IPSec connections are actively blocked.

Psiphon, enabled by OSSH+, now provides an average of 14,000 connections a day – a tenfold increase compared with the rate in December 2011.

Psiphon data shows that the Syrian regime has stepped up its censorship efforts, but has not succeeded in thwarting all circumvention efforts. In fact, citizen use of circumvention options has grown exponentially in response to the regime's efforts.

TheSecDev FOUNDATION

About Syria Cyber Watch

These reports aggregate information on events occurring in Syrian cyberspace. Analysis relies on different sources: social media, traditional media, blogs, field reports from our on-the-ground Syrian researchers, and technical network interrogation by SecDev.Cyber.

About The SecDev Foundation

The SecDev Foundation is a not-for-profit organization that seeks to broaden global public awareness and understanding in three core programme areas: cyber empowerment; the sources of security and resilience; and armed violence prevention and reduction.The SecDev Foundation supports local partners, research and advocacy in regions at risk from fragility, violence and underdevelopment in Asia, Africa, Eurasia, the Middle East and Latin America.