SPOTLIGHT ON SOCHI:
Social Media Analysis Series

BAE SYSTEMS
INSPIRED WORK

CALM BEFORE THE TWITTER STORM

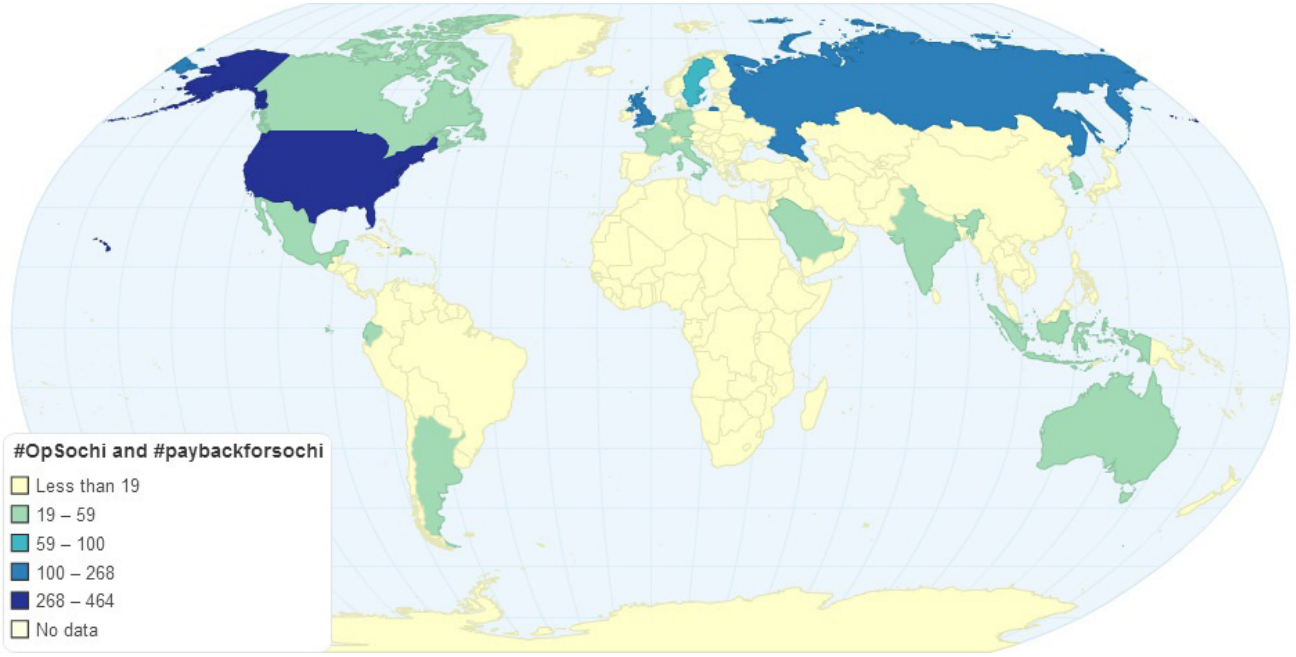
BAE Systems is partnering with Homeland Security Today magazine to produce a daily report that provides a unique perspective on the 2014 winter games in Sochi, Russia.

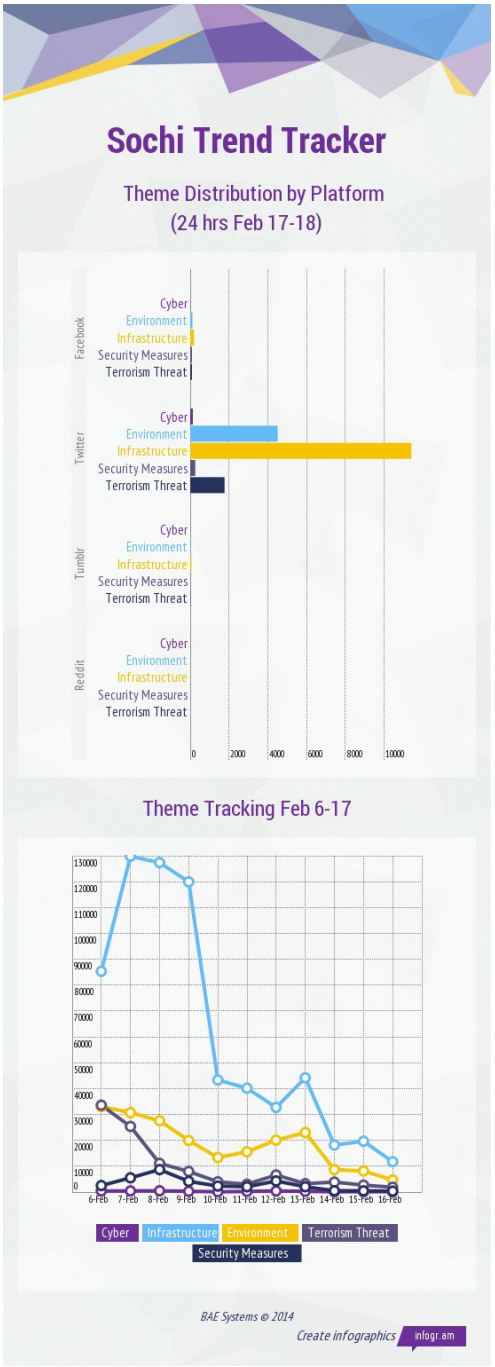
In our Feb. 7 report, "Distributed Denial of Sochi," we noted DDOS attacks against more than 1,700 websites leading up to the beginning of the winter games. The lasting impact of those attacks remains to be seen, but one thing we can be fairly certain of is that more activity from the groups involved is yet to come, especially on social media. "Twitter storms", spearheaded by at least two hacker collectives, are planned to begin on February 20 at 4pm EST.

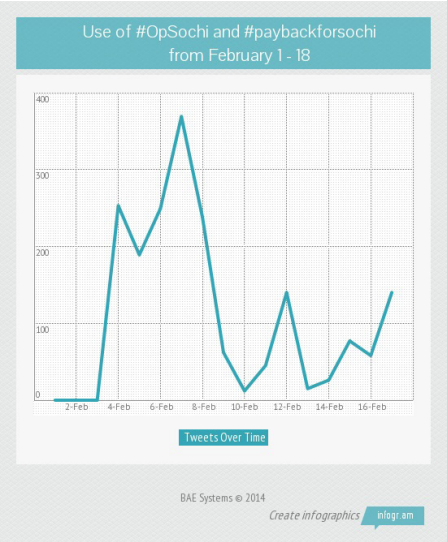
A Twitter storm is the generation of tweets and retweets using particular hashtags attempting to become a top trend on Twitter and, if the volume grows large enough, to become a mainstream media story. Often, Twitter storms occur organically, as the world observed with #SochiProblems. #SochiProblems became dominant enough that it was not only wildly successful on Twitter, but was also picked up across several media outlets. A feedback loop of tweeting, media reporting and further retweeting was established, eventually garnering #SochiProblems even more attention than the competitions themselves.

In other cases, Twitter storms are pre-planned, like the one we expect to see this week using hashtags #LegionOps and #OpSochi. These cases are generally meant to serve as a "call to arms," demonstrating a large volume of support to a cause. Unlike the hashtag hijackers we discussed in our February 14 report, who takeover already trending hashtags to redirect attention to another topic of choice, participants in a Twitter storm typically use their own original hashtags.

There are two slightly distinct collectives of hacker groups currently involved in cyber operations against Russian websites and businesses associated with the winter games. One collective is a group of hackers associated with Anonymous. This collective has labeled their activities with the hashtags #OpSochi and #LegionOps and claims its operation is driven by the mistreatment of animals in preparing Sochi for international visitors. The other collective is using the hashtag #paybackforSochi, and has tied its operations to the mass killing and deportation of Circassians in the mid-19th century. The Anonymous-affiliated collective claims the #paybackforSochi collective is affiliated with the Vilayat Dagestan branch of the Caucasus Emirate, a U.S.-designated terrorist organization. Two prominent Russian-language jihadist media outlets are supporters of the #paybackforsochi collective, which further suggests jihadist ties. We've mapped the usage of these hashtags by country in the chart below







Looking at our earlier collected data, use of the groups' associated hashtags peaked on February 7 immediately after the DDOS attacks and then saw a quick drop. Use of these hashtags is beginning to rise again and will likely continue to grow throughout the next week, culminating in the discussion that follows the storm. Dialogue regarding the Twitter storm at this point continues to be related to animal cruelty surrounding the games and talk of a "big leak" that will accompany the storm. Who or what the leaks are related to has not yet been revealed, but the success of the attacks will be determinable by the growing use of related hashtags and ultimately by the attention of any mainstream media outlets.

One should never be lulled into waving off a Twitter storm; Anonymous has proven time and again the ability to gather sensitive information and release that information to the public to the embarrassment and detriment of the targeted organization(s). Certainly, all corporate network security elements can appreciate the vigilance required in order to prevent even the slightest offense. While a Twitter storm in and of itself does not cause damage, increased media coverage and a harmful release of data it could present a physical, financial, or reputational risk to any organization.

BAE SYSTEMS
INSPIRED WORK