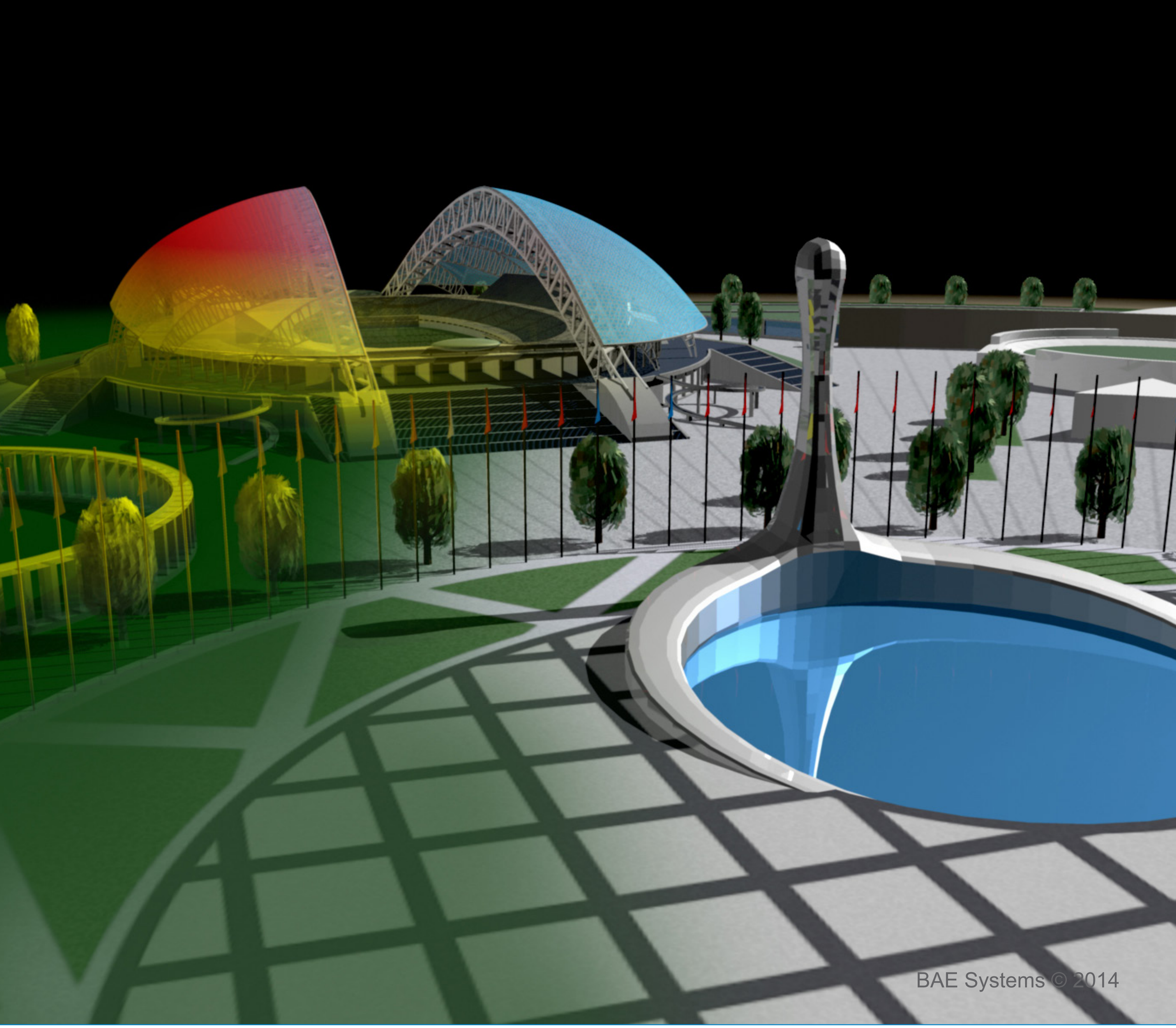
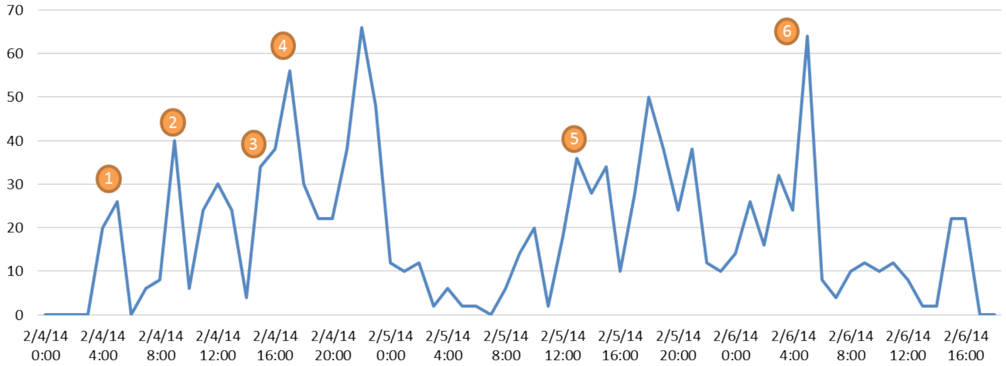


SPOTLIGHT ON SOCHI:
Social Media Analysis Series

BAE SYSTEMS
INSPIRED WORK

Timeline of #OpSochi and #PaybackforSochi cyber attacks

Twitter traffic from February 4-6



1 Anonymous announces #OpSochi DDoS attacks in response to Russia's culling of stray dogs

2 #OpSochi operations begin

3 Anonymous announces more than 1,700 Russian websites were taken down as part of #OpSochi

4 Anonymous announces the official Winter Games website is taken down

5 A group claiming to be affiliated with Anonymous in the Caucasus region claim the attacks were in retaliation for the mass killing and forces relocation of Circassians in the mid-19th century

6 Anonymous posts details of targeted sites to pastebin

DISTRIBUTED DENIAL OF SOCHI

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.

Throughout the duration of the winter games (February 5-23), the BAE Systems Advanced Analytics Lab will be studying social media data to convey trends in the public dialogue around security, infrastructure, transportation, cyber events, and environmental concerns.

The world’s attention is fixed firmly upon Sochi as the opening ceremonies get set to kick off. Unfortunately, this increased focus has led online activists, or “hacktivists”, to take this very public opportunity to further their political agendas, particularly through social media.

Beginning on February 4, hacktivists began leveling distributed denial-of-service attacks (DDoS) against at least 1,700 Russian websites connected to the winter games. The attacks targeted official websites of the games, as well as those owned by hotels and financial institutions connected with the event. As is the case with DDoS attacks, each of the websites was rendered temporarily unavailable.

The attacks this week have largely been launched as a form of political expression focused on one of two issues. First, websites and servers were targeted in response to Russia hosting the games in a region where the Circassian people had either been killed or forcibly moved from their land en masse in the mid-19th century. One group involved in the DDoS offensive, Anonymous Caucasus, posted a Youtube video claiming more websites and companies affiliated with the games would be targeted in the future. The United States Computer Emergency Readiness Team (US-CERT) released a Security Tip on February 4, identifying Anonymous Caucasus as a group that indeed has the capability to conduct such attacks.

Other groups associated with hacker-collective Anonymous justified their actions as retribution for the Russian government's culling of stray dogs in Sochi and use of whales and dolphins in the games. The original declaration was laid out on Twitter from user @OpSochi; as more attacks took place, other Anonymous affiliates, including Anonymous Operations and several Anonymous Caucasus Twitter pages, began tweeting on the attacks as well.

The graph above measures the use of Twitter hashtags to highlight actions as they took place during the February 4 DDoS attack. Particularly interesting is the time lag between the announcement of attacks at the first highlighted point and when activities actually began at point 2. It is also worth noting the fluctuations in the volume of chatter utilizing #OpSochi and #PaybackforSochi which typically followed peaks of mentions.

The attackers took advantage of social media by using various platforms to coordinate their actions and advertise their successes. Tweets that named specific targets included announcements when the websites had been taken down and were often tagged with specific hashtags to facilitate group action. Embedded links also provided technical details of the attacks posted primarily on the website Pastebin, a site that allows users to upload bulk text anonymously and has been used widely by hacktivists to claim credit for, and provide proof of, successful attacks. In the case of these operations, the Pastebin posts listed hundreds of websites affected, as well as contact information and passwords. The groups involved in these attacks also posted the domain names and IP addresses of other targets including www.sochi2014.com, www.sochi2014.ru, and the websites of several regional government and financial institutions.

We expect similar attacks to continue throughout the games under the auspices of various socio-political issues. Russia has been a hotbed of cyber activity by both state and non-state entities, and is a security concern that merits close attention in the coming weeks. Throughout the duration of the games, we will continue to monitor for trends in social media across a number of security themes: cyber events, crime, environmental issues, terrorism and transportation.

The BAE Systems Advanced Analytics Lab integrates analytic expertise, technology and tradecraft to make sense of big data and support critical customer missions. Much of the data analyzed in this series was processed and visualized using cutting-edge BAE Systems' Applied Intelligence solutions, such as the Open Source Intelligence Product. All geospatial images were produced using BAE Systems' enterprise solution suite of Geospatial eXploitation Products®.

Disclaimer: BAE Systems is not affiliated, associated, authorized, endorsed by, or in any way officially connected with Olympics Association or Official Sochi 2014 Olympic Winter Games.

BAE SYSTEMS
INSPIRED WORK