National Cybersecurity and Communications Integration Center

BULLETIN **201205171400**

Strategic Outlook: 2012 Summer Olympic Games

Executive Overview

(U) Major social events such as the World Cup, Super Bowl, and Olympics have typically drawn the interest of cyber criminals and hacktivists. Open source reporting indicated that China was subjected to approximately 12 million online attacks per day during the 2008 Summer Olympics in Beijing. Two months after the closing ceremony for the 2008 Games, cyber criminals began launching campaigns using 2012 London Summer Olympic themes. Reporting last year indicates some groups are also preparing attacks linked to the 2014 Winter Games in Sochi, Russia.

(U) Scams, malware campaigns and attacks will continue to grow in scale and complexity as the 27 July opening ceremony in London draws near. Event organizers, sponsors and British authorities continue to increase their physical and cybersecurity awareness as the event approaches. Information systems supporting the Games, transport infrastructure, law enforcement communications, financial operations and similar will become prime targets for criminals. A collective of approximately eighty-seven UK banks exercised their ability to withstand cyber attacks last November. Olympic organizers anticipated cyber threats and began testing their cybersecurity posture during 'technical rehearsals' by running scenarios from their Technology Operations Center (TOC) situated on Canary Wharf. The TOC will be manned with over one hundred personnel continuously monitoring critical applications, such as the Commentator Information System, organizers' intranet, and a telecom infrastructure encompassing 900 servers, 1,000 network and security devices, and 9,500 computers. In addition, British law enforcement organizations have been collaborating with the U.S. Secret Service and other industry experts to understand attack vectors, detection methods and mitigation strategies to combat the threat. However, the cyber implications are more expansive than localized attacks against systems and encompass globally distributed Olympic-themed malware, spam campaigns and scams.

(U) There are eleven global sponsors of the 2012 Olympic Games: Coca-Cola, Acer, Atos, Dow, General Electric, McDonalds, Omega, Panasonic, Proctor & Gamble, Samsung, and VISA. These sponsors include a variety of companies, some of which are Critical Infrastructure Key Resources (CIKR) or Information Sharing Analysis Center (ISAC) members. The actions or creditability of the sponsors may become targets for cyber criminals or hacktivists. The purpose of this bulletin is to provide a strategic outlook for the 2012 Summer Olympic Games and similar events to assist partners in detecting and mitigating related attacks.

Technical Details

(U) **Disruption of Operations:** Protestors could choose to disrupt the Games using cyber or physical means. Typical methods of cyber disruption include a denial of service (DOS) or distributed denial of service (DDOS) attack, which may be the result of a physical or cyber action, and causes an interruption of business operations against a network, website or other resources. With an IT staff of over five thousand (approximately half are volunteers), there is

potential for insider attacks during the Olympics which could cause a DOS, this bulletin will focus on a DOS or DDOS achievable through technological means only. DDOS attacks are typically launched using a botnet and the ability to bring down a target depends on three variables:

- Type of DDOS: Certain styles of DDOS attacks are more effective than others, depending on the type of DDOS attacks. DDOS attacks typically manipulate the way systems communicate.

- Size of the botnet: A large botnet spanning multiple network blocks and geographic locations is more difficult to mitigate than a small, group of attackers concentrating on a single target.

- Resiliency of the target infrastructure: The ability of an organization to withstand a robust DDOS attack depends on the infrastructure and technology solutions in place (routers, firewalls, ISPs, etc).

(U) Attackers motivated by ideals are considered hacktivist and a wide spectrum of events may at as a flashpoint for their attacks. Criminals or hacktivists utilizing DDOS attacks or web defacements may be motivated by ideological or financial objectives. For example, in February, a group of Iranian hackers dubbed the "Cocain (sic) Warriors" took credit for defacing the official website of the National Olympic Committee of Azerbaijan and the website of Azerbaijan Airlines. The actors left an anti-Israeli political message about Azerbaijan and Israel's recent increased cooperation and arms deal. Israel recently announced that it was selling $1.6 billion in arms to Azerbaijan, a move that upset both Armenia and Iran. The text of the defacement was political, with likely intentions to reach as broad an audience as possible and amplify the message by targeting an Olympics-related national-level website. The following are examples of things which may incite hacktivists to launch attacks during the Olympics:

- Olympic organizer issued warnings about stringent enforcement of limiting photography, digital recordings and general publishing of Olympic activities. This warning included prohibition of content being posted to social media sites. It is possible that tight enforcement of copyright infringement laws during the games may also prompt cyber reactions.

- The recent controversy over stadium panels provided by Dow. Critics have tried to block the installation of the panels because of the Dow links to Union Carbide, which was accused of the 1984 gas leak in Bhopal, India. These pre-game criticisms by activists may translate to physical protests or cyber actions.

- Hacktivists have consistently attacked websites and networks of countries ‘perceived’ as violating human rights, especially countries that endorse policies that limit access to digital content. As a result, countries banning or controlling Internet access to Olympic Games will also likely draw the attention of global hacktivists.

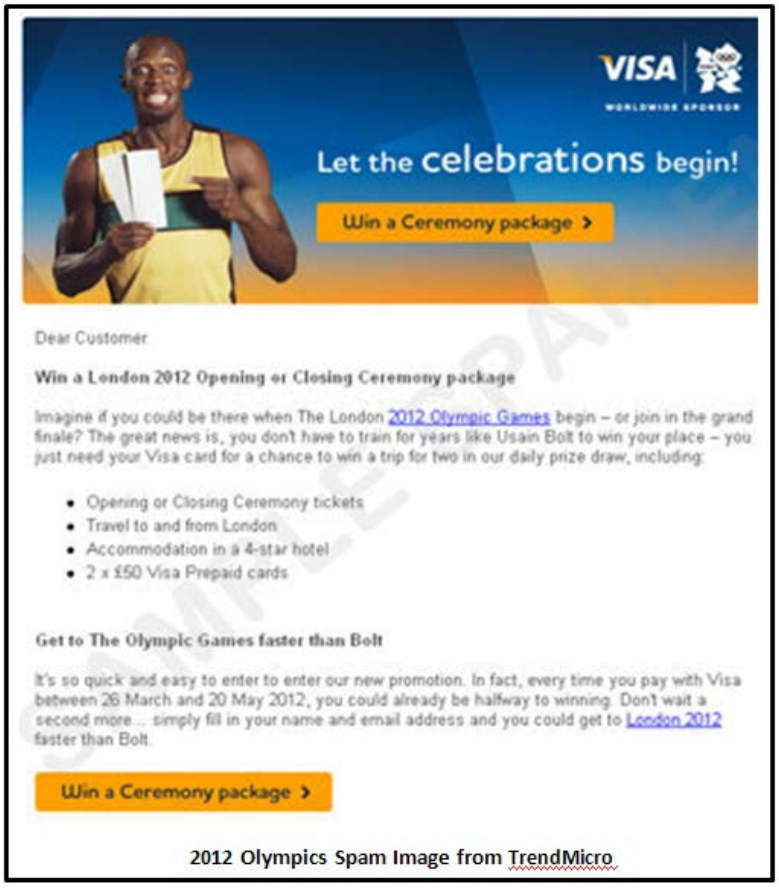
- Hacktivists may rally around an unforeseen cause, such as the emergence of a news story surrounding the Olympics or Olympics sponsors that hacktivists find offensive or

that conforms to their ideological platform (e.g. allegations of corporate malfeasance, environmental damage, corruption, etc.).

(U) **Information Theft:** The second type of attack would have a goal of information theft. This information could be used to grant a competitive edge to a company, individual or other entity. This type of attack may be facilitated by an insider or a remote attacker exfiltrating data through a system compromise. Criminals seeking competitive advantage often use spearphishing to penetrate a network. Spearphishing is an email-based attack where tailored emails containing malicious attachments or links are sent to key personnel identified during reconnaissance operations. These emails are especially convincing because they appear to be sent from a legitimate source. The highly customized nature of spearphishing emails and employment of spoofed email addresses make it extremely difficult to mitigate at the email gateway. In addition, advanced attackers understand how to bypass email filters and antivirus software so that the payload can be delivered successfully. Adversaries may target Olympic personnel to gain access to engineering schematics, scoring technologies, competitor information, ticketing systems, or similar targets.

(U) **Malware and Scams:** High profile events are often used by criminals as a mechanism to make profit through malware and scams. During the 2008 Beijing Olympics, one gang made approximately $3.5 million USD selling fake tickets online to unsuspecting victims. These gang members were later arrested and prosecuted for the crimes. During the same timeframe, there was an increase in public reporting on Olympic-related spam which downloaded malware or redirected users to false websites for phishing or malware delivery. The following summarizes possible malware campaigns and scams related to upcoming London event:

1. Phishing and scams imitating official Olympic correspondence or offering tickets have already begun circulating in the wild. These scams offer ‘opening’ or ‘closing’ travel packages to the event with the goal of tricking victims into divulging personally identifiable information (PII) and financial details. Criminals have also begun distributing spam with malicious attachments (Early Check-In 2012 Olympics.doc) which exploit the RTF Stack Buffer Overflow Vulnerability and drop additional malware.



2012 Olympics Spam Image from TrendMicro

2. Criminals will promote fake Olympic-related sites by manipulating search engine optimization (SEO) technologies. Criminals will promote malicious sites with search engine results to distribute malware to victim systems. The most prevalent type of malware distributed through this type of attack is rogueware or fake antivirus, which tricks users into purchasing fake security software. Yahoo has been the top ranked global destination for Olympics coverage for the past three games and increased their support staff (and languages) to ensure that they remain a dominant source during the event. Because of Yahoo's prevalence as an Olympics resource, it is probable that criminals will target Yahoo for SEO poisoning in an effort to infect the maximum number of systems across the globe. Below is an example of SEO poisoning detected during the '2010 Winter Olympics':

3. Popular screensavers, images and icons may also be used by criminals to distribute

malware. With increased video streaming coverage of the event, criminals will likely deploy malware using fake videos and video coder-decoders (codecs). It is probable that they may imitate media tools, such as Microsoft's Azure, which will be used to stream 3,600 hours of content. Malicious actors may also utilize social media sites to augment any of their campaigns.

4. BBC, NBC, Samsung, Visa and many other companies have unveiled mobile apps specifically designed to enhance consumer experience during the Olympics. These apps may range from sporting updates to shopping or tourist information. The development and deployment of 2012 Olympics-related mobile applications will be the largest of any previous Olympics. Criminals will probably capitalize on this trend and launch fake Olympics-related applications in mobile marketplaces to steal financial and personal information.

Future Outlook

(U) The 2014 Winter Olympics to be held in Sochi, Russia, have prompted (and will likely prompt more) attention to controversial issues and Russia's role in the region. Sochi is located on the Black Sea and borders the North Caucasus region. The North Caucasus is part of the Russian Federation and is comprised of several smaller republics, many ethnic groups and a rich cultural legacy wracked by war, intermittent violence and competing claims to power. Legacies surrounding land claims and ethnic sovereignty issues in the Caucasus have been ongoing for centuries, and they continue to the current day with wars having occurred in the last few decades, particularly in the early 1990s in Chechnya and between Georgia and South Ossetia as recently as 2008. This demonstrates that political beliefs (or reactions to such speech) are often expressed via cyber means in the region.

(U) **Pro-Olympic Cyber Attacks:** The construction of the 2014 Olympics facilities near the UNESCO protected Caucasus Biosphere Reserve and Sochi National Park has drawn criticisms from global environmental groups, as well as local Sochi news organizations. These Sochi news portals came under attack in late 2010 because of their vocal opposition to the Olympic construction. It is unknown who perpetrated this series of attacks, but their choice of targets indicates the attacker was possibly attempting to subdue opposition.

(U) **Hacktivism:** Hacktivists (Anonymous Kavkaz) purporting to be part of the larger Anonymous collective vowed to attack MegaFon on May 21, 2012 as part of 'Operation BlackHole'. MegaFon is Russia's second largest mobile phone operator in Russia and one of the national sponsors for the 2014 Winter Olympics, to be held in Sochi, Russia. The Adiga actors expressed outrage about the location of the Olympics in Sochi, Russia, as they believe that the Olympic complex is being built upon mass graves from the Circassian genocide. The attack date is significant, as Circassians commemorate the Circassian-Russian War every year on May 21, the day that Circassia was annexed by the Russians and as a remembrance of the genocide that the Circassians believed occurred at the hands of the Russians.

(U) Anonymous Kavkaz (aka Adiga Hackers) started a Twitter feed on Feb. 25 and have only updated it twice, with just a handful of followers as of this writing. The true affiliation with the larger Anonymous group seems unlikely because:

- Anonymous Kavkaz does not appear to be active in the main communications channels, where they would be most likely to make connections with more capable actors.
- Anonymous Kavkaz's Facebook presence is more geared toward ethnic, religious and political grievances in the Caucasus than with traditional Anonymous causes.

(U) The group purports to have attacked and disabled (exact means unknown) the server of the Russian Commercial Bank (a subsidiary of another Russian bank, the VTB Bank) on March 29, 2012. According to a website monitoring service, the bank's website was having problems, but it is unclear what the issues were or if they were related to the alleged attack.

(U) Politically motivated actors from this region vary in ability, but the Russian e-crime underground offers advanced capabilities that could be sought out by North Caucasus hacktivists. Similarly, the Adiga hackers could seek more skilled Anonymous-associated actors for assistance, but thus far they have not been observed communicating in known Anonymous communications channels. This could be good indication that they are only peripheral, aspirational actors. It is possible the Adiga hackers only adopted the Anonymous moniker in an attempt to gain legitimacy and anchor their somewhat obscure cause in the framework of a larger movement to attract more followers or participants.

(U) This is the first time Russia has hosted the Olympics (the 1980 Olympic Games were held in the USSR) and officials are actively monitoring the region for any indication of unrest. Russia has recently deployed military forces to the North Caucasus as part of a broader effort to stabilize the region in the lead-up to the 2014 Olympics.

(U) Although each host country will face unique challenges, the majority of cyber threats will remain consistent as officials begin preparations for the 2016 (Rio de Janeiro, Brazil) and 2018 (Pyeongchang, South Korea) Olympic Games. DHS and partners should continue to coordinate with impacted CIKR partners while promoting awareness campaigns to minimize malware infections.

Mitigation

(U) The National Cybersecurity and Communications Integration Center (NCCIC) encourages the public to use safe, common sense cyber practices, such as not opening emails from unknown individuals or organizations, using spam filters and firewalls, running anti-virus and

anti-spyware software and keeping them updated regularly. Additional good email practices include:

- View emails in plaintext to disable image based malware.
- Verify the source for unsolicited emails before opening attachments.
- Never click an embedded link in an unsolicited email.

(U) The NCCIC recommends reviewing the following US-CERT products for additional security practices on safeguarding against attacks outlined in this product:

- (U) *Recognizing and Avoiding Email Scams*
- (U) *Avoiding Social Engineering and Phishing Attacks*
- (U) *Recognizing Fake Antiviruses*
- (U) *Safeguarding Your Data*
- (U) *Securing Your Web Browser*
- (U) *Understanding Denial-of-Service Attacks*

(U) Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to their security personnel for tracking and correlation against other incidents. The following mitigation strategies are intended to help our public and private partners proactively look for possible intrusions as part of a larger defense in depth strategy:

- Log unsuccessful email attempts, both incoming and outgoing. Spear phishers often have to guess the mail format (i.e. firstname.lastname@xyz.com, lastname@xyz.com, FLastname@xyz.com, etc) therefore it is likely the mail server will reject mis-formatted emails. This is probably the first sign your organization may be targeted. By reviewing logs shortly after trigger events, it is possible to learn whether attempts are being made and thus new rule sets can be created to block the sender and alert the individual they are being targeted. Also, if it is determined an attack against an individual or group is possibly occurring, notify the individual or group to be more aware of the threat.
- Log network traffic (both incoming and outgoing), especially surrounding a possible trigger event. If a successful attack occurs, network administrators will potentially see an increase in outbound traffic soon afterwards, thus indicating compromise of the network. Diligent monitoring of inbound and outbound traffic will also provide insight into new or unexplained network traffic and allow network administrators to create rule sets to block or minimize exfiltrated data.
- Notify affected parties within your organization that their contact information may be made public in some form. Prompt employees to be on the lookout for possible phishing attacks that directly relate to the trigger event.

Points of Contact

(U) This product was a collaborative effort between NCCIC components and our partners: United States Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Critical Infrastructure Cyber Protection and Awareness (CICPA), the National Communications System / National Coordinating Center for Telecommunications (NCS/NCC), and the Office of Intelligence and Analysis (I&A). We would also like to acknowledge the International partners, ISAC members and other private industry sector partners for their contributions.

(U) Please direct questions to the NCCIC Duty Officer (NDO) via email at NCCIC@hq.dhs.gov or by phone at (703) 235-8831. The NCCIC will continue to coordinate with the appropriate component organizations.

References

1. Cyber Attack Tests for Olympic Games Computer Systems, http://www.bbc.co.uk/news/technology-15244808, wesite last accessed 27 April 2012.
2. NCCIC Advisory, TARGETED PHISHING ATTACKS, April 6, 2011.
3. Warning out versus Olympics-themed cyberscams, http://www.gmanetwork.com/news/story/254154/scitech/technology/warning-out-versus-olympics-themed-cyberscams, website last accessed May 7, 2012.
4. Cybercriminals Race to the 2012 Olympics, http://blog.trendmicro.com/cybercriminals-race-to-the-2012-olympics/, website last accessed May 7, 2012.
5. London 2012 Olympics Scams Spotted, http://blog.trendmicro.com/london-2012-olympics-scams-spotted/, website last accessed May 7, 2012.
6. U.S. Secret Service agents train Scotland Yard bodyguards to fight new generation of high-tech assassins, http://www.dailymail.co.uk/news/article-2117091/U-S-Secret-Service-agents-train-Scotland-Yard-bodyguards-fight-new-generation-high-tech-assassins.html, website last accessed May 7, 2012.
7. Yahoo to double Olympics presence in London as it seeks to four-peat as top Games site, http://www.washingtonpost.com/sports/yahoo-to-double-olympics-presence-in-london-as-it-seeks-to-four-peat-as-top-games-site/2012/04/30/gIQAfyuarT_story.html, website last accessed May 7, 2012.
8. The Wrap: Dow puts its stamp on UK Olympic Stadium, http://finance.yahoo.com/news/wrap-dow-puts-stamp-uk-134106536.html, website last accessed May 7, 2012.
9. London 2012: Iran 'blocks' official Olympics website, http://www.bbc.com/news/technology-17657450, website last accessed May 7, 2012.
10. London Olympics to Visitors: Don't Share What You See, http://techcrunch.com/2012/04/26/london-olympics-to-visitors-dont-share-what-you-see/, website last accessed May 7, 2012.
11. Microsoft Sharpens Azure Media Tools Ahead of Olympics, http://www.theregister.co.uk/2012/04/16/microsoft_azure_media_services/, website last accessed May 7, 2012.
12. Search for 'Winter Olympics' and Take Your Pick-FAKEAV or Bogus Windows Media Player Updates, http://blog.trendmicro.com/search-for-%E2%80%9Cwinter-olympics%E2%80%9D-and-take-your-pick%E2%80%94fakeav-or-bogus-windows-media-player-updates, website last accessed May 7, 2012.
13. London's Olympics Plans Include Cybersecurity, http://www.pcworld.com/article/255049/londons_olympics_plans_include_cybersecurity.html, last accessed May 7, 2012.
14. Avoiding Social Engineering and Phishing Attacks, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed May 7, 2012.
15. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed May 7, 2012.
16. Securing Your Web Browser, http://www.us-cert.gov/reading_room/securing_browser/, website last accessed May 7, 2012.
17. Understanding Denial-of-Service Attacks, http://www.us-cert.gov/cas/tips/ST04-015.html, website last accessed May 7, 2012.
18. London 2012 Olympics opens Technology Operations Centre http://www.computerweekly.com/news/2240105800/London-2012-Olympics-opens-Technology-Operations-Centre, website last accessed May 14, 2012.