ERT Threat Alert
2018 Winter Olympics
January 30, 2018

Abstract

As the 2018 Winter Olympics approach, Radware's Emergency Response Team (ERT) is focusing on the target-rich environment high profile sporting events create. With over one million tickets for sale, the 2018 Winter Olympics will bring large crowds that will demand connectivity and technological access that pose a security risk for Olympic organizers, partners, sponsors, suppliers, service providers and attendees.

Over the last decade there have been a number of cyber security related events aimed at the Olympics, such as London in 2012[i] and Rio in 2016[ii]. The potential risk steadily increases as future games become more connected. The 2018 Winter Olympics has the potential to be one of the more vulnerable sporting events in modern history and will provide cyber criminals with numerous opportunities.

This alert outlines risks and precautions for attendees, athletes and sponsors to take before and during the 2018 Olympics in PyeongChang.

Background

With millions of global viewers, the Olympics generate a lot of excitement and demand from fans. Beyond the games, there is a variety of multimedia technologies available for streaming content, augmented reality, Internet of Things and wearables to provide viewers with more immersive and interactive experiences.

Smart stadiums and venues now offer network connectivity for fans via WiFi, Bluetooth and a number of other digital services. Along with this technology, the games are becoming more reliant on critical applications to help provide this experience to those onsite and around the world.

Reliable WiFi is always an issue at large-scale events. Korea Telecom will be delivering the first broad-scale 5G network for the games and paired with Intel 5G technologies to enable attendees to engage in a variety of experiences.[iii] In addition, NBC plans on live streaming 1,800 hours of the 2018 Winter Olympics.

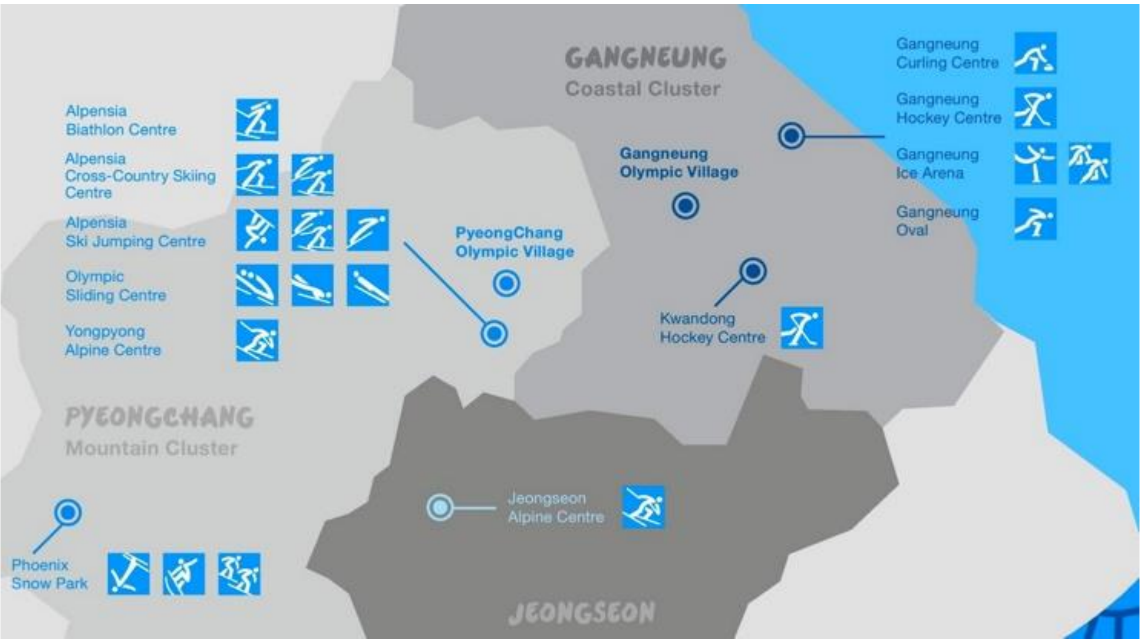


Figure 1: Olympic Venues / Source ontheworldmap.com

Venues

PyeongChang Mountain Cluster

- Alpensia Biathlon Centre - 7,500
- Alpensia Cross-Country Skiing Centre - 7,500
- Alpensia Ski Jumping Centre - 8,500
- Olympic Sliding Centre - 7000
- Phoenix Snow Park - 18000
- Jeongseon Alpine Centre - 6,500
- Yongpyong Alpine Centre - 6,000

Gangneung Coastal Cluster

- Kwandong Hockey Centre - 6,000
- Gangneung Curling Centre - 3,000
- Gangneung Hockey Centre - 10,000
- Gangneung Ice Arena - 12,000
- Gangneung Oval - 8,000

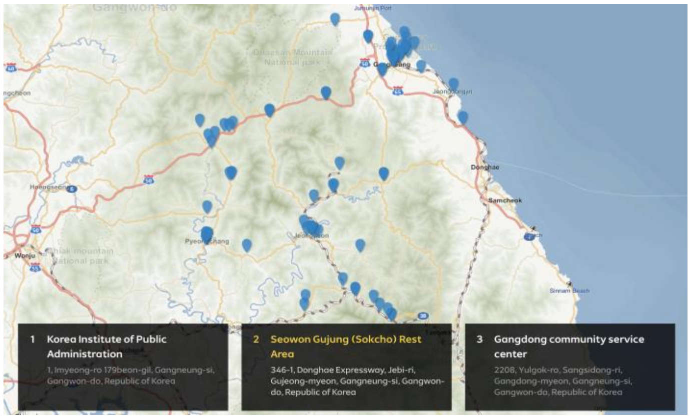
Targets

- International Olympic Committee (IOC)
- Carriers
- Service Providers
- Sponsors
- Partners
- Suppliers
- Subcontractors
- Media
- Journalist
- Hotel
- Venues
- Athletes
- Spectators

Reasons for Concern

Radware's Emergency Response Team and researchers are currently assessing the Winter Olympics in PyeongChang. The Winter Olympics creates a great platform for hacktivists and cyber criminals to spread a message, make profit or create disruption. Today, it is very easy for low-level threat actors to carry out large-scale and disruptive attacks. Toolkits and attack services are widely available for purchase on the clear and darknet.

Today, most cybercriminals and hacktivist focus on identity theft by spreading malicious software designed to harvest and steal personal information. Often it is the technologies designed to enhance the spectators' experience, such as Wi-Fi, Bluetooth and other digital services that are exploited to harvest this information from attendees.



1 Korea Institute of Public Administration
1, Imyeong-ro 179beon-gil, Gangneung-si, Gangwon-do, Republic of Korea

2 Seowon Gujung (Sokcho) Rest Area
346-1, Donghae Expressway, Jebi-ri, Gujeong-myeon, Gangneung-si, Gangwon-do, Republic of Korea

3 Gangdong community service center
2208, Yulgok-ro, Sangsidong-ri, Gangdong-myeon, Gangneung-si, Gangwon-do, Republic of Korea

Figure 2: Access points/source: nowpyeongchang.com/wifi

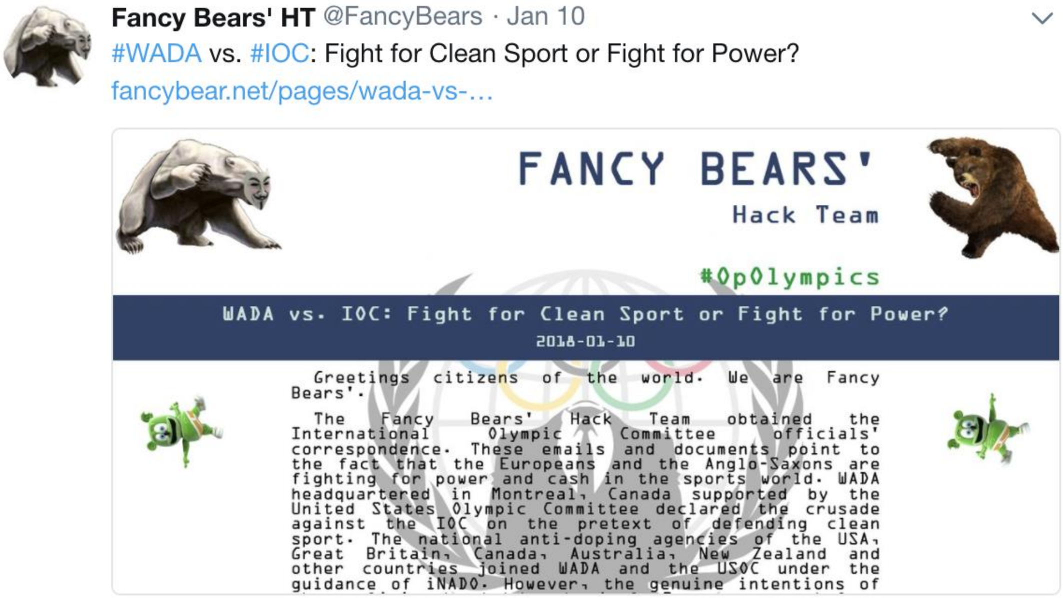
One of the biggest concerns about the Olympics is protecting critical applications and networks that support the event. Broadcast networks, industrial control systems, operational networks and other related systems are all at risk.

Mobile devices are also at risk for athletes and viewers. Athletes are targeted for espionage and spectators are targeted for personal information and financial credentials. Providing spectators and athletes with connectivity is a double-edge sword. Connected venues become a bring-your-own-device nightmare for event management and wireless network operators. Open Wi-Fi networks also present one of the biggest attack vectors for network- and malware-based attacks. Criminals know that visitors are reliant on Wi-Fi access points, making them an easy target.

Common types of attacks at the Olympics may include:

- Compromising unsecure and vulnerable access points
- Deploying evil twins or fake cell phone towers
- Spreading malware via phishing
- Data mining using fake pop ups, text messages or spoofed websites
- Denial-of-service attacks on critical applications
- Injection attacks aimed at stealing data

Several organizations associated with the games have already been targeted by spear phishing attacks. Hackers have already begun targeting the Olympics with Fancy Bear claiming to have compromised emails from the IOC.[iv] In 2016, Fancy Bear also was suspected to be behind the hack targeting WADA (World Anti-Doping Agency).



Fancy Bears' HT @FancyBears · Jan 10

#WADA vs. #IOC: Fight for Clean Sport or Fight for Power?
fancybear.net/pages/wada-vs-…

FANCY BEARS'
Hack Team
#OpOlympics

WADA vs. IOC: Fight for Clean Sport or Fight for Power?
2018-01-10

Greetings citizens of the world. We are Fancy Bears'.

The Fancy Bears' Hack Team obtained the International Olympic Committee officials' correspondence. These emails and documents point to the fact that the Europeans and the Anglo-Saxons are fighting for power and cash in the sports world. WADA headquartered in Montreal, Canada supported by the United States Olympic Committee declared the crusade against the IOC on the pretext of defending clean sport. The national anti-doping agencies of the USA, Great Britain, Canada, Australia, New Zealand and other countries joined WADA and the USOC under the guidance of iNADO. However, the genuine intentions of

Figure 3: Fancy Bear post related to IOC emails

Threat Actors

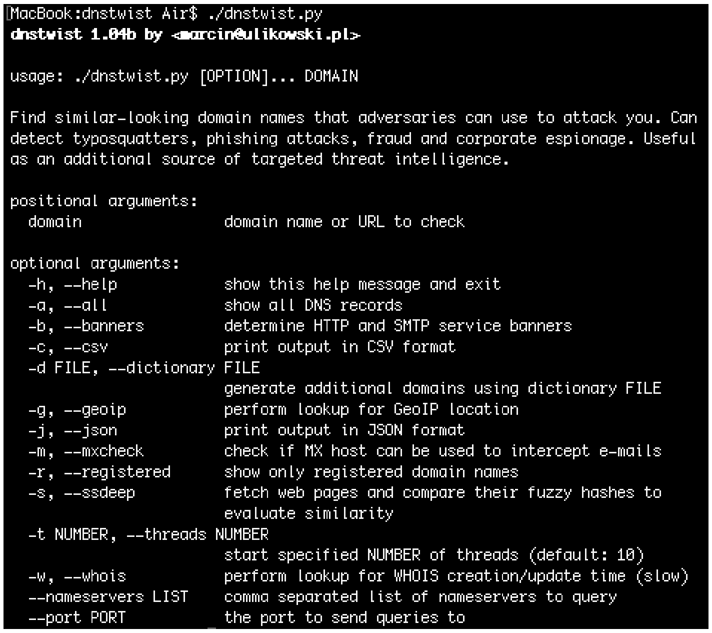
CrowdStrike[v] and McAfee[vi] both have reported a spear phishing campaign suspected of targeting those involved or supporting the 2018 Winter Olympics. The email came from a spoofed message with the senders address belonging to South Korea's National Counter-Terrorism Center but was sent from an IP address in Singapore. ThreatConnect[vii] has also reported that they have identified two domains that appear to be spoofing the UK Anti-Doping website.

Early in January, Talos also reported about malicious activities from Group 123. In several campaigns in 2017, Group 123 was seen targeting South Korean users with a spear phishing email containing a malicious document designed to install and execute ROKRAT, a remote administration tool, RAT[viii].

Attack Vectors

Phishing

A digital attempt to obtain sensitive information from a victim by using a malicious email or website. The attacker solicits personal information by posing as a trustworthy organization or the company itself. These attempts are either sent out to everyone in the company or designed to specifically target key associates. Once an associate falls victim the hacker will then have the sensitive information required to gain access to certain systems.



```
MacBook:dnstwist Air$ ./dnstwist.py
dnstwist 1.04b by <marcin@ulikowski.pl>

usage: ./dnstwist.py [OPTION]... DOMAIN

Find similar-looking domain names that adversaries can use to attack you. Can
detect typosquatters, phishing attacks, fraud and corporate espionage. Useful
as an additional source of targeted threat intelligence.

positional arguments:
  domain                domain name or URL to check

optional arguments:
  -h, --help            show this help message and exit
  -a, --all             show all DNS records
  -b, --banners         determine HTTP and SMTP service banners
  -c, --csv             print output in CSV format
  -d FILE, --dictionary FILE
                        generate additional domains using dictionary FILE
  -g, --geoip           perform lookup for GeoIP location
  -j, --json            print output in JSON format
  -m, --mxcheck         check if MX host can be used to intercept e-mails
  -r, --registered      show only registered domain names
  -s, --ssdeep          fetch web pages and compare their fuzzy hashes to
                        evaluate similarity
  -t NUMBER, --threads NUMBER
                        start specified NUMBER of threads (default: 10)
  -w, --whois           perform lookup for WHOIS creation/update time (slow)
  --nameservers LIST    comma separated list of nameservers to query
  --port PORT           the port to send queries to
```

Figure 4: Dnstwist – Source: https://github.com/elceef/dnstwist

Malicious Domains

Malicious domains are registered domains designed for malicious intent. Users are normally directed to these sites via fake giveaways for tickets promoted on social media. Bad domains look to hijack names of cities, venues or events to trick users via typo squatting into entering their credentials by spoofing the content of the original website. More advanced forms of malware contain domain-generating algorithms (DGAs) to evade solutions based on signatures or blacklisting.

Denial-of-Service

Considering the high volumes of traffic service providers will cope with, it would not take a sophisticated attack to take an ISP down; a massive DDoS attack via a reflective method in combination with the natural peaks of traffic may be enough to cause service degradation. Denial-of-service attacks can be generated via an IoT botnet such as Mirai. Hackers can leverage multi-vector techniques by combining network floods with various low and slow attacks and even encrypted distributed denial-of-service attacks to cause an outage. A consumption spike might appear as a DDoS attack. Many DDoS mitigation solutions are rate-based and will drop traffic above a certain threshold. Behavioral algorithms not only make an accurate distinction between attack and legitimate user traffic but also instantly detect unknown attacks at a minimal false positive rate.

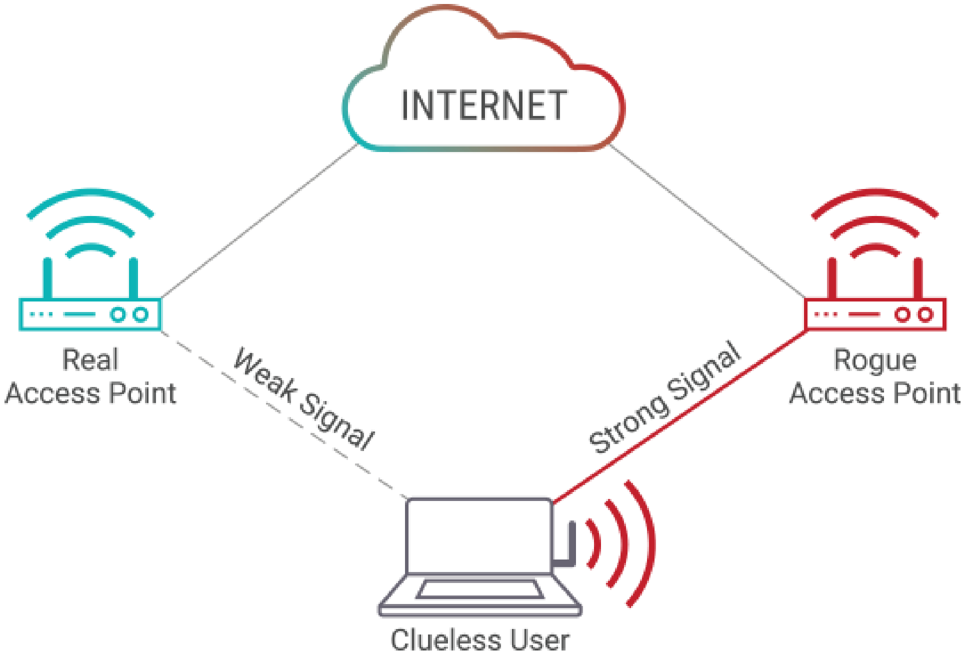
Application Attacks

Hacktivists and criminals will launch application attacks like SQL injections, password cracking, cookie poisoning, cross-site scripting*, session highjacking and others in an attempt to steal Olympic and spectator data. Information on the attendees, sponsors, or athletes can be quickly monetized or publicly used. Criminals will also use fake applications and websites to target patrons.

* Cross-site scripting against vulnerable webpages - injecting a client-side script into the user's browser.

Compromised Access Points – Risk of MITM

As part of their preparations, hacktivists and cyber criminals have likely already assessed access points and their vulnerabilities across the Olympic venues. They will set up fake access points to intercept and manipulate their victims browsing and to steal passwords, credit cards, PII and other sensitive information. A common MITM tactic using malicious access points is to name fake access point as the same name of the legitimate access points. Once a user is connected, malware can be injected onto their device.



ATM Skimmers

Criminals will be deploying skimmers on ATMs and point-of-sale systems at the 2018 Winter Olympics. It allows hackers to record the ATM user information and later sell it for profit. The larger the crowd, the higher number of potential victims.

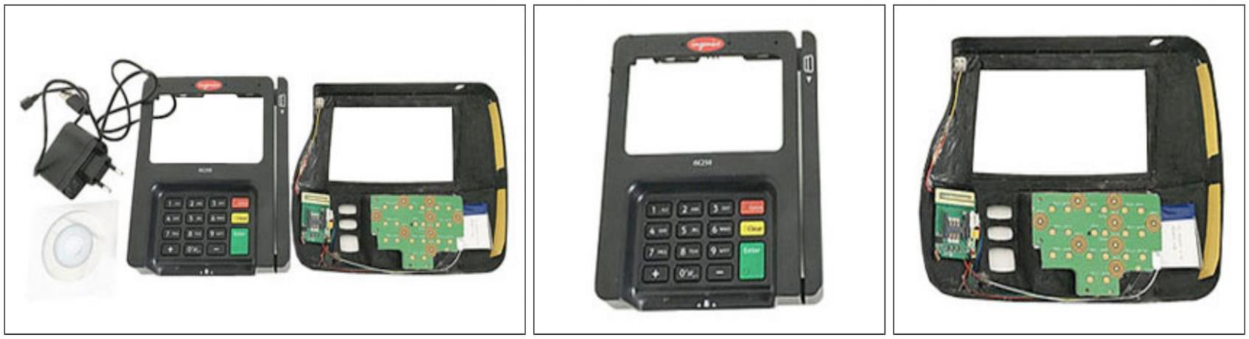


Figure 5: ATM Skimmers

Mobile Phones

There is a high risk for targeted attacks against high profile visitors at the 2018 Winter Olympics. Visitor devices could be easily targeted by cyber criminals at the games. Fake charging stations or compromised access points can allow an attacker to gain root access into a device. Once infected, devices can perform tasks like record audio and video, take photos, send text messages, open webpages, steal user data, delete files, launch denial-of-service attacks via HTTP floods and perform web injections.

How to Prepare

Technology can provide a more immersive and rewarding experience for fans but also creates problems and security risks for those managing the event. Those that sponsor, support or supply the Olympics should understand the risk and their exposure. Here are suggestions for both attendees and those hosting the 2018 Winter Olympics.

Attendees/Users: How to Prepare for the Winter Olympics

- Ensure your phone is updated with the latest operating system
- Disable Bluetooth when not in use
- Disable Wi-Fi when not in use
- Use the official event Wi-Fi when device is in use
- Always use a VPN
- Have RFID shields to protect RFID cards
- Be careful when using ATMs – Understand how to spot and avoid card skimmers gathering data.
- Exercise caution when presented with pop ups while browsing
- Avoid Olympic related scams delivered via email.

Event Operators: How to Prepare for the Winter Olympics

We recommend that operators review their network between events and inspect networks as necessary in order to defend the threats presented during the Olympics.

- Ensure hardware is up to date
- Conduct audits of the network between games
- Access Control List (ACL) – Filtering network traffic
- Use load balancing for traffic distribution
- Have network and application protection to detect, mitigate and report attacks

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort

- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Under Attack and in Need of Expert Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

[i] http://www.computerweekly.com/news/2240168945/Cyber-attacks-launched-at-London-2012-Olympic-Games-every-day
[ii] http://www.silicon.co.uk/security/rio-olympics-ddos-attacks-196998?inf_by=5a68339b671db85b2d8b4a7b
[iii] https://newsroom.intel.com/editorials/intel-power-5g-network-2018-olympic-games/
[iv] https://fancybear.net/pages/wada-vs-ioc.html
[v] https://www.crowdstrike.com/blog/malicious-spear-phishing-campaign-targets-upcoming-winter-olympics-in-south-korea/
[vi] https://securingtomorrow.mcafee.com/mcafee-labs/malicious-document-targets-pyeongchang-olympics/
[vii] https://www.threatconnect.com/blog/duping-doping-domains/
[viii] http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html