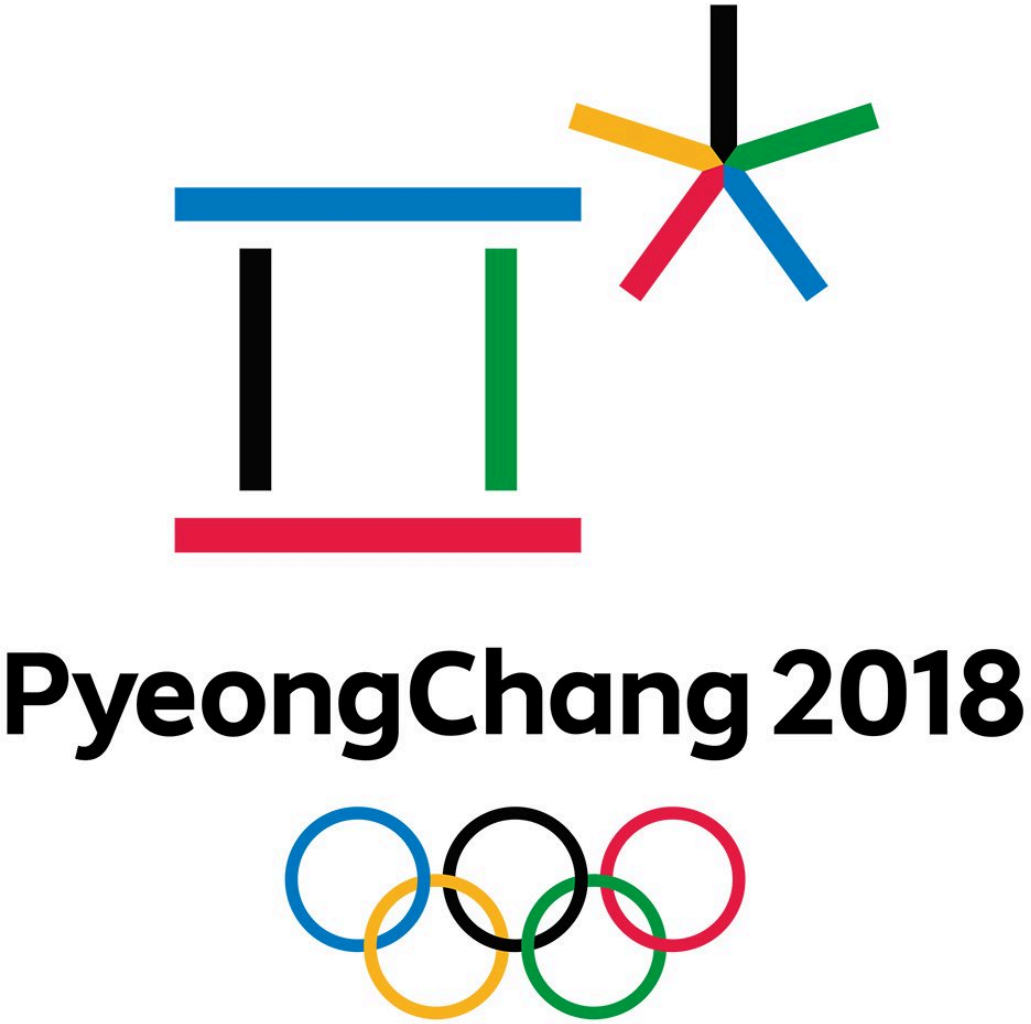
Cyber Attacks

CYBER ATTACKS AT THE 2018 PYEONGCHANG WINTER OLYMPICS

written by Nicholas Giatrelis | February 14, 2018



A cyberattack paralyzed internet networks at the opening ceremony of the 2018 Pyeongchang Winter Olympics. Several U.S. cybersecurity firms have uncovered a computer virus named **Olympic Destroyer** that was likely used in an attack.

Olympics organizers confirmed the attack affected internet (LAN and WiFi) and television services. Drones thatwere intended to be used in the opening program failed to deploy, prompting organizers to insert pre-recorded footage of the drones in global telecasts. More than 300 olympics related systems have already been compromised.

Olympic Destroyer malware was designed to knock computers offline by deleting critical system files including boot information and turning off all services, disabling the systems. The hackers knew the technical details of the Olympic Games infrastructure such as usernames, server names and passwords, Ciscos Talos threat intelligence division wrote on its blog, saying it identified 44 individual accounts in the code.

The Pyeongchang Organizing Committee for the 2018 Olympic & Paralympic Games (POCOG) was forced to shut down the servers to prevent further damage, leading to the closure of the Pyeongchang 2018 website affecting spectators who purchased tickets to 2018 Winter Games events, who were unable to print their reservations.

remote server in the Czech Republic, registered with fake credentials to a South Korean government ministry. McAfee found publicly accessible logs on that remote server that showed victim machines were in fact connecting to it from South Korea, a sign of actual infections.

Olympics is a rich target for the attackers

Olympics involve so many countries, and so many sports, each of which have their own infrastructure, that it has become a rich target environment for adversaries. Cybersecurity has been a long-standing concern for the International Olympic Committee (IOC) and host nations of the games since the early 2000s. Previous Olympic Games have had to contend with a multitude of cyber threats, from the London 2012 Olympics which experienced thousands of intrusion attempts and one false alarm threat to the power grid to the Rio 2016 Olympics, which experienced a variety of hacks including disclosures of athletes' personal data.

However, the 2018 Winter Olympics in Pyeongchang, South Korea, present further cybersecurity challenges, not just due to its location 80 kilometres from the border with North Korea and geopolitical tensions, but also due to major sporting events now becoming increasingly connected and integrated with technology.

The increased connectivity and use of technology has opened the games up to more vulnerabilities and potential cyberattacks. While most of the previous attacks have focused on ticket scams, availability of IT services and personal data, there are now more substantial cyber threats to stadium operations, infrastructure, broadcasting and participants and visitors to the games.

There might also be cyber attacks that compromise devices to spread propaganda or misinformation. The worst case scenario would be attacks in which hackers tried to shut off lights in a stadium during an event, says the executive director at the center for long term cybersecurity at the University of California, Berkeley.

In response to these threats, the South Korean government and Pyeongchang organising committee have invested around 850,000 into cybersecurity measures, as well as hiring a number of external cybersecurity firms during the games. However, these investments are dwarfed by the overall investment into the Games and its associated infrastructure, which has exceeded 7 billion. The cyber threat has also prompted organisations such as Discovery Communications, the European broadcaster for the Games, to take out cyber insurance to cover in case of a cyberattack.

Whos behind the attacks?

The hacks appeared to be well organized and backed by substantial resources with the hallmarks of a nation state. Olympic Destroyer's disruptive tactics and spreading methods resemble **NotPetya** and **BadRabbit** , two pieces of Ukraine-targeting malware seen in the last year that the Ukrainian government, the CIA, and other security firms have all tied to Russian hackers.

A Russia-linked cyber attack has already stolen and leaked documents from other Olympic organizations. The so-called Fancy Bear group, or APT28, began its operations in late 2017 — according to Trend Micro and Threat Connect, two private cybersecurity firms — eventually publishing documents in 2018 outlining the political tensions between IOC officials and World Anti-Doping Agency (WADA) officials who are policing Olympic athletes.

The incident underscores the threat of hacking even as South Korea organized a team of experts well before the event started. Due to the ad hoc nature of cyber operations at the Olympics, the event is more vulnerable to hackers who exploit the lack of security discipline among personnel brought together from different organizations.

A senior analyst at McAfee warned that the Olympics may experience more cyber attacks before closing ceremonies. A researcher at ThreatConnect asserted that organizations like Fancy Bear have no reason to stop operations just because they've already stolen and released documents. Even the United States Department of Homeland Security has issued a notice to those traveling to South Korea to remind them to protect themselves against cyber risks.

What can you do to stay secure?

As employees are likely to view Olympics related content at work, these activities will have direct implications for all organizations.

End User Awareness: Use this opportunity to warn users of the threats associated with scams, phishing, and malware associated with the Olympics and train users about social engineering attempts. Consider conducting a

Wh
SO
Wh
Wh
Sca
NIS
Cor
Wh
Cor
Priv
A D
Cor
Do
app
be
DS
Wh
Crit
Do
ons
ass
Ho
Cer
Bra
RECEN

Email Security: Flag emails from external sources with a warning banner. Implement filters at your email gateway to filter out emails with known phishing attempt indicators. Implement filtering on email servers.

Mobile Device Security: Remind employees to only install apps on in accordance with the agencies mobile device policy and to thoroughly screen app permissions before downloading. Users should be wary of apps that request permissions outside of what is expected and pay close attention to the publisher to ensure the app originates from a trusted or official organization. If permissible, within the confines of organizational Internet use policies, consider providing employees with guest wireless access.

Travel to the Olympics: Restrict employees from bringing corporate devices to the Olympics and do not allow remote connections. Do not connect a device or transfer data from a device to your networks until the device has been scanned and preferably reimaged. Direct employees to the State Departments travel recommendations for general security information before traveling to the Olympics and urge them to consult the MS-ISAC Security Primer on Cybersecurity While Traveling.

Schedule a Consultation

Sources:

https://www.schneier.com/
https://www.talosintelligence.com/
https://securingtomorrow.mcafee.com/
https://www.nytimes.com/2018/02/08/technology/winter-olympics-hackers.html
http://www.wired.co.uk/article/winter-olympics-cybersecurity
https://www.cisecurity.org/wp-content/uploads/2018/02/Olympics-Related-Malicious-Activity.pdf

About RSI Security

RSI is the nation's premier information security and compliance provider dedicated to helping organizations achieve risk-management success. We work with some of the world's leading companies, institution and governments to ensure the safety of their information and their compliance with applicable regulation. We also are a security and compliance software ISV and stay at the forefront of innovative tools to save assessment time, increase compliance and provide additional safeguard assurance. With a unique blend of software based automation and managed services, RSI can assist all sizes of organizations in managing IT governance, Risk management and compliance efforts (GRC).

PCI Security Standards Council™ APPROVED SCANNING VENDOR

PCI Security Standards Council® QUALIFIED SECURITY ASSESSOR™

Get A Free Cyber Risk Report

Hackers don't rest, neither should you. Identify your organization's cybersecurity weaknesses before hackers do. Upon filling out this brief form you will be contacted by one of our representatives to generate a tailored report.

Sept

Wh
bet
ISO

Sept

Un
HIT
Fac
Cyb

Sept

Un
Cor
Cor

Sept

Ber
Cer

Sept

CATE

- Client Features
- Compliance Checkli
- Compliance Standar
  - ADA Compliance
  - California's Cyber
    - California Con (CCPA)
    - California Onli Act (CalOPPA)
  - CIS CSC
  - CMMC
  - CryptoCurrency S (CCSS) / Blockchair
  - Cybersecurity Tec
  - EI3PA

Company *

Job Title *

Phone *

Business Email *

Notes

I'm not a robot

reCAPTCHA
Privacy - Terms

Submit

0 comment 0

NICHOLAS GIATRELIS

previous post
PIN ON GLASS – INTRO, BENEFITS, OBSTACLES

next post
TAKING THE PULSE OF HEALTHCARE CYBERSECURITY IN 2018

YOU MAY ALSO LIKE

TAILORED SOCIAL ENGINEERING
January 30, 2024

ARE YOUR WEB APPS INSECURE LOW HANGING FRUIT?
June 22, 2017

MEDICAL CYBERATTACKS
December 18, 2017

LEAVE A COMMENT

- FINRA / Financia
- FISMA
- GDPR
  - Data Protectio
  - Privacy Shield
- HIPAA / Healthca
- HITECH
- HITRUST
- IRS E-file
- ISO 42001
- NERC CIP
- NIST 800-171 / D
  - NIST Special P 207 – Zero Trust
- NY DFS – 23 NYC
- PCI DSS
  - ASV Scanning
  - PCI 4.0
- PCI SSF
- PIPEDA
- SOC 2
- SOX 404
- Cyber Attacks
- eCommerce
- Cybersecurity Solut
- Architecture and
- Biz Alliances
- BYOD
- Cloud Security

Name*

Email*

Website

Save my name, email, and website in this browser for the next time I comment.

SUBMIT

- Cybersecurity Te
- Data Center Secu
- Email Security
- Encryption
- Firewall
- Identity and Acce
- Incident Manage
- Incident Respons
- Information / Ne
- IT Security & Cyb Training
- Managed Detecti
- Managed IT Servi
- Managed Security (MSSP)
- Mobile Device Ma
- Mobile Security
- Open Source Scan
- Outsourcing IT S
- Password Manage
- Patch Manageme
- Penetration Testi
- PII / PAN Scanne
- SaaS
- Security Maturity
- Security Program
- Telemedicine and
- Third Party Risk
- Threat & Vulnera
- Virtual CISO

- GRC Portal
- Infographics
- RSI Security News
  - Webinar

RSI Security is the nation's premier cybersecurity and compliance provider dedicated to helping organizations achieve risk-management success. We work with some of the world's leading companies, institutions, and governments to ensure the safety of their information and their compliance with applicable regulations.

AWARDS & RECOGNITION

IMPORTANT PAGES

Home
About RSI Security
Compliance Advisory Services
Cybersecurity Services
Checklist/Whitepapers
Past/Upcoming Events
Careers

Type and hit enter...

HEADQUART

10531 4s Comm
CA 92127
858-250-029
858-225-691
info@rsisecu

IRVINE, CA –

858-250-029
info@rsisecu

FACEBOOK TWITTER INSTAGRAM LINKEDIN YOUTUBE EM

BACK TO TOP