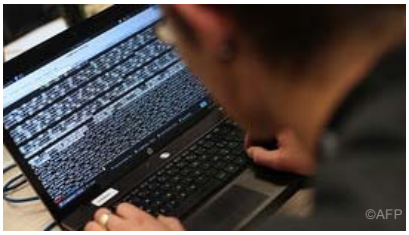
FINANCIAL TIMES

February 11, 2014 1:27 pm

Sochi Olympics is a cyber war zone, experts warn

By Hannah Kuchler in San Francisco



Foreign visitors to the Winter Olympics in Sochi are unknowingly wading into a cyber battlefield, the US government and security experts have warned.

Large international events – packed with diplomats, business leaders and celebrities – have become honeypots for computer hackers, while Russia is home to some of the most feared cyber criminals in the world.

The Sochi games have already been plagued by fears of a potential terrorist attack and US officials have warned American supporters and athletes about the dangers of attending the games, which began on Friday.

But in a sign of the mounting worries over the cyber threat, the US government issued guidance advising American visitors to Sochi to remove all important information from their computers and devices before they travel.

They were also told to assume their communications were being monitored and that they should have "no expectation of privacy" in Russia because of the twin threat from hackers and surveillance from the state.

Only last week the White House pointed the finger at Moscow after a potentially embarrassing recording of a conversation between two of its top-level diplomats about the stand-off in Ukraine was posted on the video sharing website YouTube.

Lookingglass Cyber Solutions, a US-based cyber threat intelligence company, said it saw evidence of hackers preparing the scene for crime around Sochi in the weeks before the games.

Chris Coleman, chief executive of Lookingglass, said botnets, which send spam to infect a computer and download its data, emerged in the area in recent weeks, targeting everything from the 4G networks for smartphones to popular hotel websites in Sochi.

"The Russian underground is very active, especially in financial exploitation of consumers. So they have had quite a robust, bulletproof infrastructure in place with a target rich environment next door," he said.

Mr Coleman said the company found one particularly prolific botnet called Cutwell, which is known for targeting online banking details on the computers it hacked.

The US government's Computer Emergency Readiness Team has warned the hacktivist group "Anonymous Caucasus" appears to be threatening any company that finances or supports the winter games.

The team said the group, which claims the Sochi games take place on the graves of a million Caucasians who were murdered in 1864, was linked to denial of service attacks on Russian banks last year.

"Sochi is the most interconnected Olympics ever so it can also be seen as the largest opportunity to monitor those participating in the Olympics," said Michael Coates, chairman of the Open Web Application Security Project, a non-profit organisation aiming to improve the security of software, and director of product security at Shape Security.

He said even though Russian cyber criminals operate around the world, they can do more when they are near the unencrypted traffic that crosses normal networks every day. Hackers will work "unbeknown to the user, quickly and quietly in the background", he warned.

One US-based cyber security company, Symantec, is offering its mobile security software Norton free for the duration of the games to keep data kept on smartphones safe.

Some snoopers may be spies. The Olympic Games is traditionally an arena for sports diplomacy but that does not mean suspicious countries leave their surveillance at the door.

Ken Geers, a senior global threat analyst with cyber security company FireEye and an ambassador for

FT Video

Russia optimistic about Sochi

February 7, 2014: On the day of the opening ceremony of the 2014 Winter Olympics, Moscow reporter Courtney Weaver says the mood in Russia is positive despite criticism in western media over the facilities in Sochi, security, and Russia's controversial anti-gay law.

In depth

Cyber warfare

As online threats race up national security agendas and governments look at ways of protecting their national infrastructures a cyber arms race is causing concern to the developed world

Nato's cyber defence centre, said diplomats and some business travellers were usually advised not to take any electronics to Russia.

"I think the Russians may assume this type of venue is a venue for Western spies to enter Russia as a class of potential aggressors," he said. "From a Russian perspective, they may treat everyone with some suspicion and compromise computers coming from outside Russia."

He said most normal citizens would not know or think that Sochi was a hub for malware, malicious software, used for espionage.

"An event like Sochi is a contest between intelligences services," he said. "Everyday folks get caught up to some degree."

RELATED TOPICS Olympic Games

Most Popular on Social Networks

Bank of England's Mark Carney drops jobs link with interest rates
Bitcoin plunges on Japan exchange halt
Hack attacks force wider Bitcoin halts
Without women, David Cameron is fighting a lost cause
Madrid proposes citizenship for Sephardic Jews
A dangerous mistake lies at Bitcoin's intellectual core
Chances are high of mass exodus from EM
Five apps for unfocused minds
Barclays raises bonuses and cuts jobs
We need a new Bismarck to tame the machines
Enslave the robots and free the poor
Courts, voters and the threat of another euro crisis
OECD admits to forecasting errors during eurozone crisis
The lowdown on the side-effects of stand-up desks
Beware the Faustian pact of the professions
Italy: Monti's secret summer
Investors warned over real estate risks
George Soros picks up $5.5bn as Quantum Endowment fund soars
China's 500-tonne gold gap fuels talk of stockpiling
Russia prepares crackdown on Bitcoin