Adam Finkelstein - July 2015

Giving Cyber-Crime the Boot

Cyber Security at Major Sporting Event

Since the inception of the internet, every major sporting event has become a target of cybercrime. With hundreds of thousands of fans, sponsors and governmental agencies invested in global sporting events, it is clear to see why they present the perfect opportunity for criminals to take advantage of all the frenzied activity, excitement and perhaps most importantly, the increasing reliance on technology.

Learning from previous sporting events?

To give an idea of the possible threats and their scale, we can analyse the data from previous global sporting events. During the 2008 Beijing Olympics games, it was reported that over 12 million cyber-attacks per day were directed towards event organisers. This resulted in the loss of millions of pounds as a result of online ticket scamming and the rise of fake ticket websites.

By 2010, cyber-attacks were a common occurrence at all major sporting events. Spam text messages and emails were a growing trend, affecting both the FIFA World Cup in South Africa and the Delhi Commonwealth Games. London 2012 was described as the first truly connected summer Games. During the Games, teams of Cyber Security professionals were assembled. They defended against at least one hacktivist campaign every day, handled 11,000 malicious requests per second and blocked 212 million malicious connection attempts. This represents a significant increase from previous sporting events.

Fast-forward again to 2014, and the intensity and variety of cybercrime has further grown. In the run up to the 2014 FIFA World Cup, both the Brazilian government and the organising committee were targeted by hacktivists who were successful at leaking data from the Ministry of Foreign Affairs computing network and causing a plethora of DDoS attacks which shut down internal systems for considerable periods of time.

It is clear to see that in only a relatively short time span how the ferocity and frequency of cyber threats targeting sporting events have increased in their sophistication, power and impact.

The Threat Landscape

Imagine for an instant the consequences of denial-of-service attacks against official event websites or the spreading of a malware within the internal network of the organisation. These threats are particularly offensive and could cause significant problems for event organisers. The threat landscape includes not only reputational aspects but also direct financial, regulatory and operational dimensions.

Distributed-denial-of-service (DDoS) - this is one of the most common mechanism used by attackers to damage not only the reputation of sporting event organisers by denying sport fans access to event websites, but also presents a direct financial impact if the target is ticketing or Point Of Sale systems. DDoS attacks have dramatically evolved in both volume and complexity with sophisticated botnets now capable of executing complicated multitier attacks against their targets.

Malware attacks - these are used to trick both sport fans and employees which form part of the event organiser's workforce. Unsuspecting users are tempted into downloading malware from bogus replica sites, spam emails or via direct access to the event organiser's network. As an example, during the Pan American Games held in the Dominican Republic, malware was used to compromise internal networks resulting in the latest scores and results from competitions not being available to the media and sport fans from around the world.

Credit card skimming - with the abundance of retail opportunities at key sporting venues, credit card cloning and point of sale attacks are used to pilfer card data and steal funds. This can be performed via skimmer devices attached to PoS devices and ATMs. Hackers have also found ways to get malware on to PIN pads, where the information is gleaned and sent to the criminals' computers.

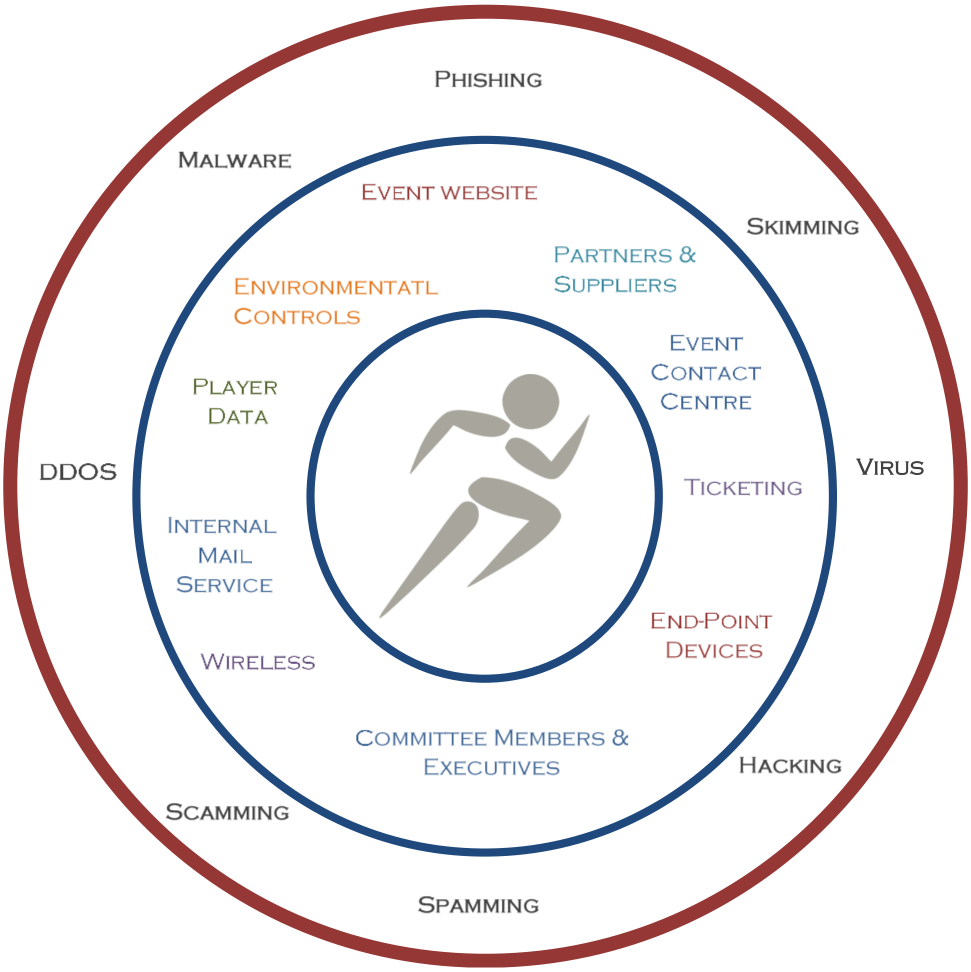
Ticket fraud - prior to the ticket launch for this year's Rugby World Cup organised criminals with links to the arms and drugs trade were plotting to hijack the Rugby World Cup ticket launch and hold countless ordinary fans to ransom on the secondary market. Tournament organisers and senior police officers admitted the second biggest sporting event ever held in the UK would definitely be targeted by gangs of cyber criminals using state-of-the-art software allowing them to harvest huge numbers and then offer then for or resale at extortionate prices.

Phishing attacks - historically these have skyrocketed around major sporting events; prior to the last FIFA World Cup, related spam increased by around 40% and over 4000 Phishing hosts were discovered every month during the tournament build up. Attackers use spam and phishing sites to try to steal recipients' personal information for purposes of identity theft and bank fraud.

Rogue wireless networks - here attackers may attempt to breach Wi-Fi configurations or launch attacks via public Wi-Fi points either controlled or monitored by attackers. When users get online via these Wi-Fi networks, their traffic can be intercepted enabling attackers to gain access to useful data, such as usernames and passwords.

Scamming - this usually involves email messages, purporting to originate from the event organiser. The messages are a variation of the recipient being declared as a winner of free event tickets provided by the organising committee.

Sporting Event: Assets and Attack Vectors



Addressing Cyber-Crime at Global Sporting Events?

In order to effectively prepare event hosts should invest in mapping their primary assets and understanding the potential attack surfaces. In the build up to the event, the following areas should be considered:

Websites and Portals - Starting several months before the event, efforts should be focused on monitoring the web, and especially social networks and forums, to identify potentially suspicious activities that could be related to the organisation of an attack. Through this analysis, it is possible to intercept attackers that are planning an action during the events. Particular attention is dedicated to the “Deep Web” the component of web that is largely used by cyber criminals for commerce activities and propaganda.

Internal Networks - This is the backbone of the IT architecture and appropriate planning must consider external attacks that could be launched by hackers but also internally either maliciously or accidently. Policies should address all aspects that could compromise the network infrastructure, such as the usage of personal mobile devices and storage devices (e.g. USB memory sticks). Possible attacks against the backbone could use for example targeted virus to infiltrate the network and compromise operations.

Financial Systems - Protecting financial systems and credit card data from fraud attacks, which are prevalent in the build up to sporting events, is crucial. This includes ensuring that PoS devices have not been tampered with via skimming devices or malware aiming to harvest user data.

The Human Factor - Employees and contractors should be trained to be aware of potential information security threats, with clear instruction on the actions they must take if encountering suspicious activity. Erroneous human behaviour can lead to unauthorised access to the information infrastructures or to the exposure of sensitive information used by the organising committee.

Sensitive Data - The location and classification of data should be reviewed to ensure appropriate access controls are in place to prevent data leakage. The data could be related to committee financial information, participant lists, medical data and HR records.

Telecommunications & Customer Contact Centers - With the majority of telephone systems being based on IP telephony, they are also vulnerable to DDoS or TDoS attacks aimed at taking communications off-line. Detecting and defending against these cyber threats is complex and it is essential to properly train contact centre staff to operate properly in every situation.

Third Parties - Event organisers are typically reliant on a number of third party providers who are often quasi-insiders, enjoying some degree of the trust and access to internal networks, data and users. Third-party deficiencies can result in unintended consequences for event organisers. For this reason, identification of key third party service providers, understanding their compliance level and evaluating key integration touch points, form an important part of the overall cyber readiness state of the sporting event.

Once the core assets and threat vectors have been defined, the IT environment must be tested for each of the probable attack scenarios, from both an external and internal attacks perspective. As an example, prior to the London Olympics, the entire IT infrastructure was heavily tested for a three month period in order to simulate different cyber-attack scenarios. The scenarios explored and the risks examined are a fundamental part of the risk identification process and should inform the implementation of a mitigation process both prior to and during the sporting event.

Once the sporting event is in progress, the availability and integrity of the complete IT environment must be retained seamlessly. All suspicious activity should be analysed in real time by experienced agents with the aid of advanced technologies that are able to detect any abnormality. The incident response teams must be prepared to respond to unpredictable events and meet any sudden need.

Author: Adam Finkelstein - Comsec Consluting April 2015

Comsec and Global Sporting Events

Comsec has experience working with large sporting organisations and those responsible for the organisation of major international events. We have helped to assess and counter the risks associated with attacks from cybercriminals. Drawing on a deep understanding of today's security threats and backed by almost 30 years of leadership in IT security, we are able to provide intelligence driven cyber security superiority to directly combat the tools, techniques, and procedures adopted by the most advanced attackers.

Comsec’s first-hand experience working closely with Government Ministries, Defence Agencies and providers of Critical National Infrastructure (Water, Electricity, Gas, Transportation networks) both in Israel and across the globe, has enabled Comsec to develop proven techniques to prevent and defend against Cyber-attacks. This unparalleled knowledge is derived from working closely with some of the most heavily targeted organisations across the Israeli Public and Private sectors.