4th Annual e-Crime Securing Online Gaming

October 2nd, 2018, London, UK

SECURING
ONLINE GAMING

eGaming, eGambling and eSports in the crosshairs

Online gaming firms are testbeds for adversaries. How can they stay ahead?

www.akjassociates.com/event/gaming

AKJ Associates

Securing Online Gaming 2018: it just gets harder

"We wanted to make sure we could focus on improving product delivery [but] we needed controls to reduce the risk around access management for the developers," Vasile Dorca, Head of Security Compliance and Assurance at Paddy Power Betfair

"[Cyberattacks are] constant, which means we're using a lot of technology to stop those patterns of behaviour. How do you spot a pattern that's different from the normal? [One way is] by deploying machine learning algorithms," Finbarr Joy, chief technology officer at William Hill

In January 2018, researchers at Google Project Zero revealed an exploit affecting every currently supported release from Blizzard, the publisher of a series of popular online games with a monthly active user count of some 40 million.

The vulnerability was contained in an update agent that applied upgrades and patches to games with millions of worldwide users. It permitted commands to install, uninstall and change settings on the devices used for playing these games. Blizzard's initial fix itself was problematic as was its communication with the researcher who discovered the DNS-binding exploit.

It's not just software. The graphics cards in gamers' high-end PCs are ready-made for the cryptomining malware that is now being delivered via gaming and sports apps and sites such as the Google Play Store.

And because of its financial and security profile, the online gambling industry is still a go-to test bed for hackers looking to develop new exploits.

This incident is just the latest evidence that the huge numbers of connected devices, the vast sums of money now involved in eSports and online gaming and gambling and the complexity of the sector's use of mobile, tablet and desktop hardware are increasingly attracting the attentions of the most sophisticated and organised cyber-criminals and not just the traditional lone-wolves looking to demonstrate coding skills to their fellow gamers and hackers.

So how can eGaming, eGambling and eSports companies keep up with the evolving threats to their business models? What new technologies and techniques are being developed to ensure that they stay one-step ahead? And what do gaming/gambling CISOs need to focus on?

e-Crime Securing Online Gaming will cover these and other key subjects for its audience of professionals tasked with safeguarding digital assets and sensitive data. There will be real-life case studies, strategic talks and technical break-out sessions to help end-users understand how new technologies can be cost-effectively deployed in real-life business situations.

e-Crime Securing Online Gaming 2018: key themes

Key Themes

Securing digital identity
- Identity analytics and 'Smart IdAM' for mobile and IoT devices
- Geolocation, biometrics, multi-factor authentication, mobile push authentication, adaptive access control – help!!

SOC as a service
- All the benefits, none of the costs?
- Functionality versus budget: what's out there?
- Securing multi-tenanted SaaS

Identity as a service
- Better security and cost savings too – what's the catch?
- Adaptive multi-factor authentication, single sign-on, universal directories – what is the best way to use IdaaS?
- Choosing an IdaaS provider

Improving web security
- How many websites do you have? Auditing web presence and applications
- Advanced web attacks and exploitation
- Stopping SQL injection and XSS attacks once and for all

AI in alert prioritization and data analysis
- Separate the signal from the noise
- Automating incident response
- Is AI plus human analysts the optimum combination?

Core security: DNS security, DDoS etc.
- Defeating DNS rebinding, spoofing and hijacking
- Beating the DDoS'ers
- Buying mitigation services

Demonstrate your solutions

End-users and security professionals need your help …

1 To improve detection and deterrence

Data is not enough. Often it's too much. Intelligence should be just that: intelligent, otherwise it simply creates more problems. But how can security professionals choose from so many solutions? **This is your opportunity to showcase yours.**

2 To counter common cyber frauds

Some of the best cyber-security solutions train employees so well that they become part of an organisation's cyber defences. These providers work with IT and HR to make this a reality. **Show how your products can do this.**

3 To comply with new regulations

Cyber-security is going mandatory. Voluntary commercial codes are not enough. Regulators want companies to demonstrate true cyber-security as well as basic compliance. **How can you help CISOs with this?**

4 To build more secure applications

Gaming/gambling companies need constant product iteration and innovation to stay competitive. But rapid application development can compromise security and damage the business> **Can your products help?**

5 To secure payments and personal data

Financial services companies struggle with new and legacy systems, retailers struggle with PCI DSS, and everyone is worried about new payment methods such as contactless and phone. **Which solutions are available, scaleable and easy to implement?**

6 To outsource what they cannot do in-house

Many organisations cannot afford in-house SOCs or security teams big enough to counter cyber threats effectively. So what can they outsource and does outsourcing really solve the underlying risk problem? **What can you offer?**

Demonstrate your expertise

They are looking for solutions in …

DNS-based hacks

Oldies but goldies

DNS and Border Gateway Protocol (BGP)-based attacks strike at the heart of the way the internet works. Hacking these protocols is an old trick but one that continues to work. Last December, a BGP hijack saw traffic to major websites, including those of Apple, Facebook, Google and Microsoft, redirected to Russia. In January, $400,000 in the Stellar Lumen cryptocurrency (XLM) was stolen and the MyEtherWallet hack is more recent still. What solutions fix the problem?

Leveraging identity analytics

Smarter ways to guard the network

The adoption of identity analytics for identity governance and administration as well as authentication can reduce organizational risk and administrative efforts, while improving user experience. Products without analytics capabilities will over time increase administrative overhead and risk undiscovered security problems. What should CISOs look out for?

SOC-as-a-service

All the functionality you need, none of the hassle. Too good to be true?

Organisations considering procuring a Security Operations Centre (SOC) from a third party need to look first as the pros and cons versus establishing their own in-house SOC. They then need to look at which of the many possible functions of a SOC that they need and to evaluate the different deployment options available, the SOC lifecycle, and other considerations. What are the issues and what does a good SOC plan look like?

Securing mobile digital identity

Dealing with the business need for mobile

Mobility is the key to new services and enabling new revenue streams. But the mobile ecosystem introduces new risks and new challenges in identity verification both in terms of customers and employees. That said, many believe that it is mobile itself that will hep solve many of the key problems in identity. So what is the latest?

SECURING
ONLINE GAMING

Where market-leading solution providers know they will find buyers

We deliver a focused selling opportunity

Specific, actionable and relevant information for time-constrained industry professionals

Securing Online Gaming

The perfect platform for solution providers to deliver tailored advice to the right audience

Focus

Target growth

Each event represents a targeted opportunity to address the needs of a specific community whose need for your solutions and services is growing.

Leads

Boost sales

Sponsors can tailor messages to the needs of an audience that shares similar concerns and challenges, looking for solutions now.

Choice

Meet commercial aims

We work with sponsors to ensure they meet their commercial aims. We offer a number of sponsorship options, each providing specific benefits.

Value

Showcase solutions

Our events provide sponsors with a unique platform to showcase solutions, as well as provide advice on how best to solve delegates' key challenges.

SECURING
ONLINE GAMING

Where the real decision-makers allocate budgets

Why do so many blue-chip vendors work with us? Real buyers ...

100%

The most senior cyber-security solution buyers

You will be surrounded by the most senior and most sophisticated buying audience in the online gaming, gambling and eSports market.

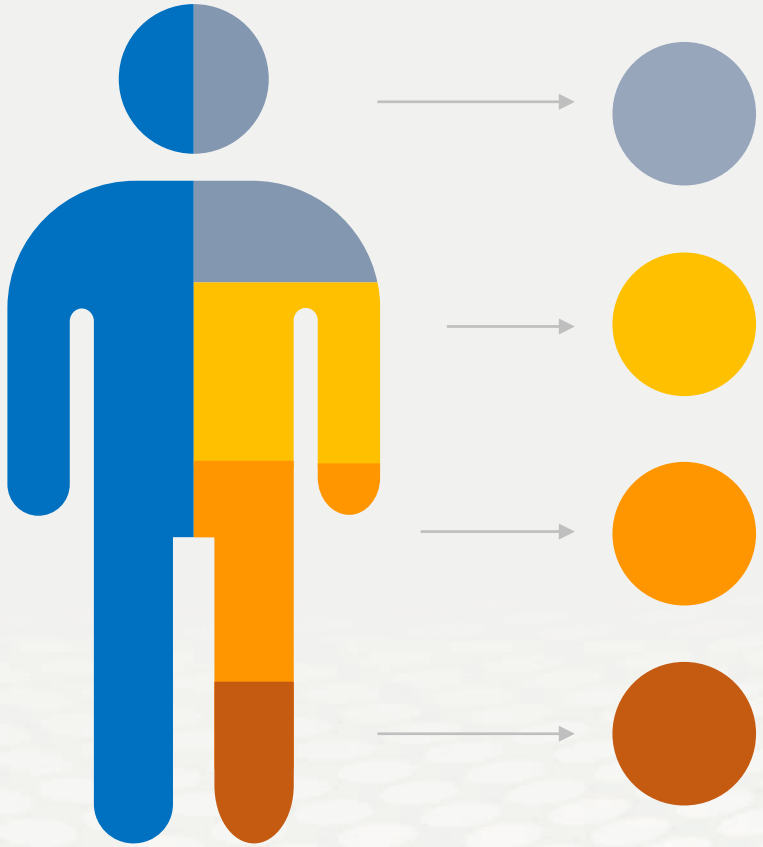
AKJ Associates has been building relationships with senior information risk and security professionals since 1999 and our cybersecurity community is the largest of its kind globally.

We know the senior executives who drive strategy from the top, we know the enterprise architects who often control the largest budgets and we know the IT Security Leads and Engineers who so often dictate the purchase process.

All of these job titles attend the Securing Online Gaming event.

We understand that every vendor needs to sell more. That is the bottom line.

Getting in front of the right people at the right time always increases the lead generation and always increases profitable sales activity



Cybersecurity

We have a 15-year track record of producing the events cybersecurity professionals take seriously

Risk Management

We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance

We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy

We are a key venue for decision-makers with budget and purchasing authority

SECURING
ONLINE GAMING

Where the top solution vendors get their message across

Why do so many blue-chip vendors work with us? Real benefits...

Talk to customers

Face-to-face interaction with the right buyers works! Our vendors tell us it does and they renew year after year

Build relationships

Relationships built from a personal meetings are stronger than those initiated by solely digital conversations

Save time

Meet dozens or hundreds of selected buyers in just one or two days – the value of a high quality event

Lead sourcing

We provide the best leads in the business. Each sponsor receives a delegate list.

Increase sales

All delegates are the right delegates. They have all been researched and confirmed as senior and with buying capacity

Get your message across

Delegates take all lunches and breaks are in the exhibition. So sponsors and exhibitors are always surrounded by qualified buyers

Our testimonials speak for themselves: we have many more

What our sponsors say about us

TESSIAN

An impeccably organised event with all the right people, genuinely interested in learning about new solutions. AKJ events definitely give you the opportunity to leave a mark on your attendees.

KASPERSKY lab

AKJ events have yet to disappoint – from the massive number of attendees to our packed speaking sessions, this is one event we always look forward to!

eset

We found the event very productive, it was good to meet potential customers and gives a chance for decision makers to meet us and understand what we do and how we can help them with their security.

Ninety five percent of our exhibitors and sponsors work with us on a number of occasions each year.

Our sponsor renewal rate is unrivalled in the marketplace.

This is because our sponsors generate real business at our events every year