



# How Major Sports Events Put Mobile Users at Risk

**Allot MobileTrends Report**  
**UEFA Euro 2016**

**Allot**  
communications

# Contents

<b>Executive Summary</b>	<b>1</b>
<b>Major Sports Events and Malware Risk</b>	<b>2</b>
<b>Research Methodology</b>	<b>3</b>
<b>Findings</b>	<b>5</b>
<b>Major Sports Events Increase Risky Online Behavior</b>	<b>5</b>
<b>Sports Betting and Sharing is a Risky Business</b>	<b>6</b>
<b>Who is at Risk?</b>	<b>8</b>
<b>Big Event, Big Opportunity</b>	<b>9</b>
<b>Euro 2016 Risk Assessment Chart</b>	<b>10</b>
<b>Protecting Sports Fans at Risk</b>	<b>11</b>
<b>Key Take Aways</b>	<b>12</b>
<b>Further Reading</b>	

## Executive Summary



Mobile broadband and smartphones are changing the way people experience sporting events like UEFA Euro 2016 as football fans shift to the digital arena to watch, record, and share their reactions to the games. This online activity also exposes them to malware risk as cyber criminals leverage their enthusiasm and involvement to trick sports fans into downloading infected apps or clicking malicious links.

Our previous Allot MobileTrends Report found that online behavior affects the risk for malware, and that some behavior patterns are potentially riskier than others.

This Allot MobileTrends Report goes a step further to determine whether major events cause a change in online behavior that increases the potential risk for online threats such as malware. To that end, we analyzed usage data from a random sample of one million European mobile subscribers before and during the UEFA Euro 2016 games.

Our findings reveal that:

- **17%** of mobile users who exhibited little or no use of sports apps or websites before the games, became active sports fans during the games. **Nearly 50%** of these event-driven fans transitioned into online behavior profiles that are at high potential risk for malware.
- The total number of mobile sports fans at risk for malware **more than doubled** during the games.
- Increases in online sports betting and social networking are major contributors to increased cyber risk.
- The percentage of mobile sports fans accessing betting sites **more than doubled** during the games. Before the games, 1 in 9 users visited sports betting sites. During the games, 1 in 4 visited sports betting sites. Gambling sites/apps are correlated with risk for malware.
- During the games, the percentage of sports fans using social media apps or sites **tripled** over their pre-event activity. Intense social media activity is correlated with risk for malware.

These changes in online behavior that result in increased exposure to risk are not limited to Euro 2016. They could be triggered by any major sports event because cyber criminals are always on the lookout for new victims to exploit. Service providers should view this as an opportunity to educate mobile customers regarding cyber threats and to engage and onboard them with network-based web security services as part of an overall campaign to assure their mobile experience during major sports events. The increase in the addressable market for security services coupled with timely event-driven offers may result in the only win-win outcome at the games!

## Major Sports Events and Malware Risk



The UEFA European championship games are as exciting today as they were when the first tournament took place in France in 1960. While the games are once again being played in France and there are still 22 players and one ball on the pitch, much of the action before and during Euro 2016 is happening online.

Mobile broadband and increasingly powerful smartphones are changing the way people experience sporting events. Apps and websites are used by millions to check the scores, watch the replays, read the commentary, book tickets, buy branded merchandise, bet on outcomes, watch live games, and share photos, videos and reactions with others in their social circles.

However, this online activity also exposes them to intensified cyber security threats as opportunistic cyber criminals leverage fan enthusiasm and involvement to gain quick

and lucrative rewards by means of fraud, phishing, ransomware and other methods. Before the UEFA Euro 2016 games began, researchers were already raising the red flag regarding attempts to trick unsuspecting users into downloading infected apps and clicking malicious links.

Our previous Allot MobileTrends Report found that online behavior affects the risk for malware, and that some behavior patterns are potentially riskier than others.

In this Allot MobileTrends Report, our research goes a step further to determine whether major events trigger a change in online behavior that increases the potential risk for malware. To that end, we analyzed usage data from a random sample of one million mobile subscribers before and during UEFA Euro 2016.







## Source Data

This MobileTrends research is based on data usage records from a random sample of one million mobile users in countries participating in UEFA Euro 2016. Allot professionals collected and sampled data at two different time-frames in order to analyze behavior patterns before and during the event.

**T1: Before the event** - aggregated data collected in May

**T2: During the event** - aggregated data collected June 10-17, first week of the tournament

## Analysis

Allot data science experts identified 500 apps and 500 URLs that were most popular with our user sample before the event (T1). The experts at Kaspersky Lab assisted us in grouping the URLs into relevant content categories. Similar categories were used for grouping apps.

Potential risk scores were assigned to each content category based on off-line research of known criteria that contribute to malware risk such as file-sharing, downloads, storage, encryption, and commercial transactions.

First, our analysis derived online behavior profiles according to mobile use of apps and URLs. Next, each profile was correlated with the potential malware risk of their online behavior based on two major dimensions of risk: sports betting activity and time spent on social media that exceeded the average. Finally, we compared the overall online behavior as well as each profile separately before the event (at T1) and during the event (at T2) to determine and quantify changes triggered by the event.

## Profiling Sports Fans

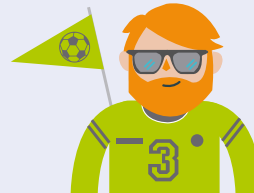
Our analysis identified six distinct “sports fan” profiles based on the volume, diversity, and intensity of online activity with sports and social media sites and apps.



**Light Sports Fan** has very little activity on sports apps and websites.



**Sports Info Seeker** uses multiple apps and websites to consume information about sports, but does not share info via social media.



**Sports Info Guzzler** uses multiple apps and websites frequently and consumes very large volumes of data during intense online sessions.



**Sports Social Monitor** watches what friends and others are doing on social networks and occasionally uses sports-related apps and websites.



**Sports Social Mingler** is very active with friends and others on social media, but is less engaged with sports-related apps and URLs.



**Sports Mover & Shaker** combines the intense social activity of a “Mingler” with the intense sports engagement of a “Guzzler.”







## Usage Volume, Diversity, Intensity

The different sports fan profiles were derived by analyzing the volume, diversity and intensity of their social media and sports content consumption. Volume represents their sports or social media usage as a percent of overall consumption. Diversity represents the unique sports or social apps/websites they access daily. Intensity represents their average number of transactions per app or website.

For example, the Sports Info Guzzler consumes the highest volume of sports content (34%) with great intensity (65.9 transactions per site/app) in relation to other profiles. The Sports Guzzler also uses social media, but less intensely than other profiles like the Sports Social Mingler or the Sports Mover & Shaker. Table 1 summarizes the usage patterns of each profile per our data.

Table1

### Sports and social activities by sports fan profile during Euro 2016

												
	Light Sports User		Sports Info Seeker		Sports Info Guzzler		Sports Social Monitor		Sports Social Mingler		Sports Mover & Shaker	
	Sport	Social	Sport	Social	Sport	Social	Sport	Social	Sport	Social	Sport	Social
Volume	6%	14%	26%	15%	34%	27%	1%	1%	13%	25%	21%	20%
Diversity	1.2	2.3	1	2.2	2.5	2.5	1.1	0.9	1.1	3	2.8	3.1
Intensity	1.1	2.5	28.3	2.7	65.9	3.3	17.4	12.0	15.4	16.7	74.8	17.4

## Findings

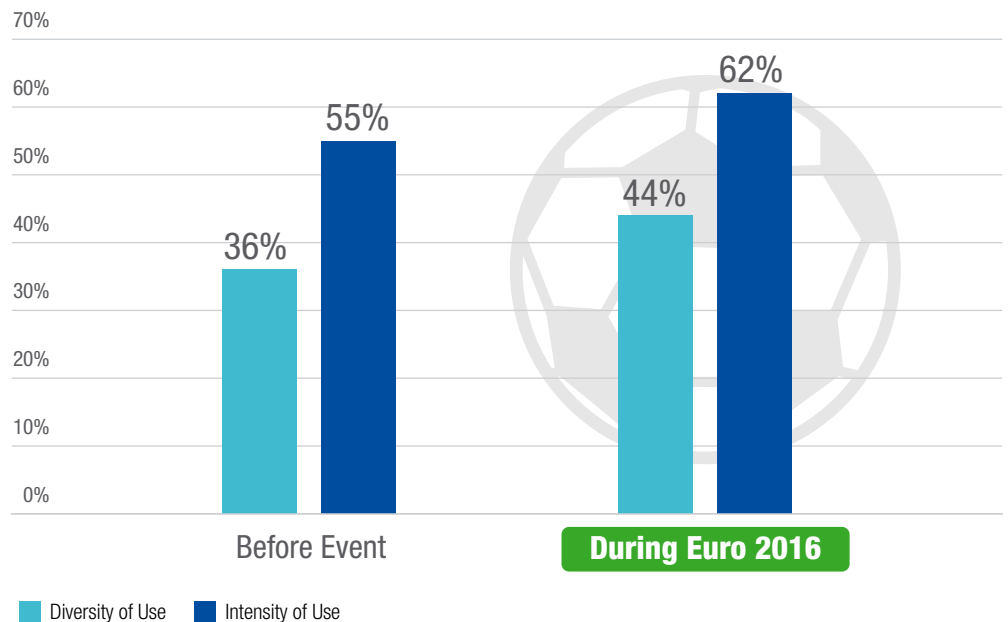


### Major Sports Events Increase Risky Online Behavior

Our previous Allot MobileTrends report showed that the intensity and diversity of online behavior increases the potential risk for malware. Our current findings show that Euro 2016 triggered an increase in the baseline intensity and diversity of online sports engagement, which contributes directly to an increase in overall risk for malware, especially when mobile fans use potentially risky apps and sites. As shown in Graph 1, fans accessing at least two sports-related apps/websites per day increased 22% (from 36% to 44%). More intense fans who access at least 6 sports-related apps/websites per day increased 13% (from 55% to 62%).

Graph 1

#### Percentage of sports fans with diverse and intense activity before and during Euro 2016



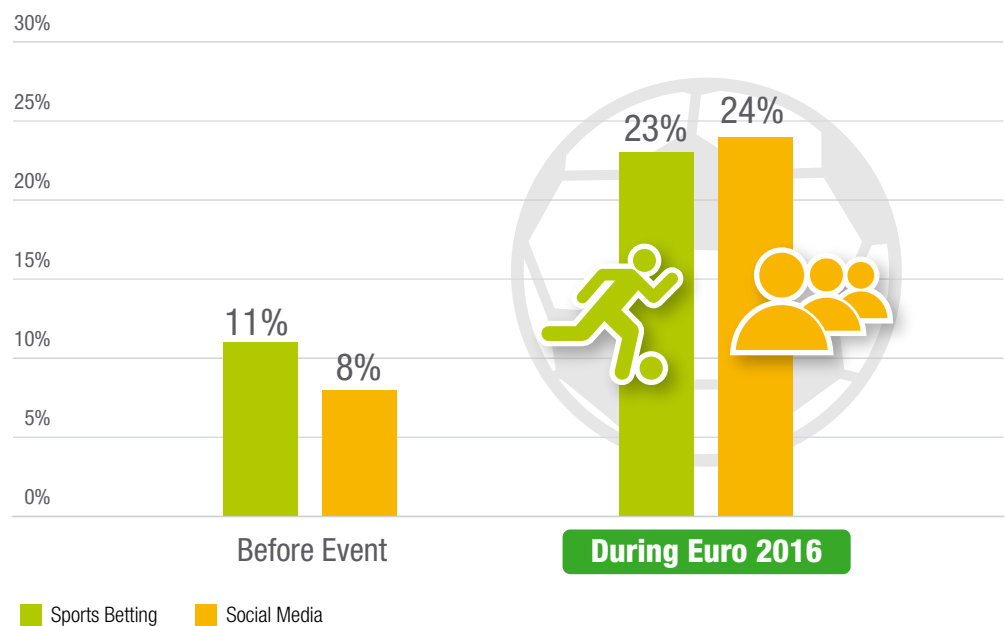


## Sports Betting and Sharing is a Risky Business

Our analysis of online behavior identified two major risk categories - sports betting and social media. This risk assessment is based on data from the previous Allot MobileTrends Report, *Mobile Users at Risk*. Our findings in Graph 2 show that during Euro 2016, the percent of sports fans accessing betting sites more than doubled while spending time on social media tripled from baseline measures taken before the event.

Graph 2

### Percentage of sports fans engaging in social media and sports betting activity before and during Euro 2016



**“ Cybercriminals are actively exploiting the growing interest in major sports events, targeting sports fans with malicious links on social media, fake ticket scams, malware-ridden emails and phishing attacks. ”**

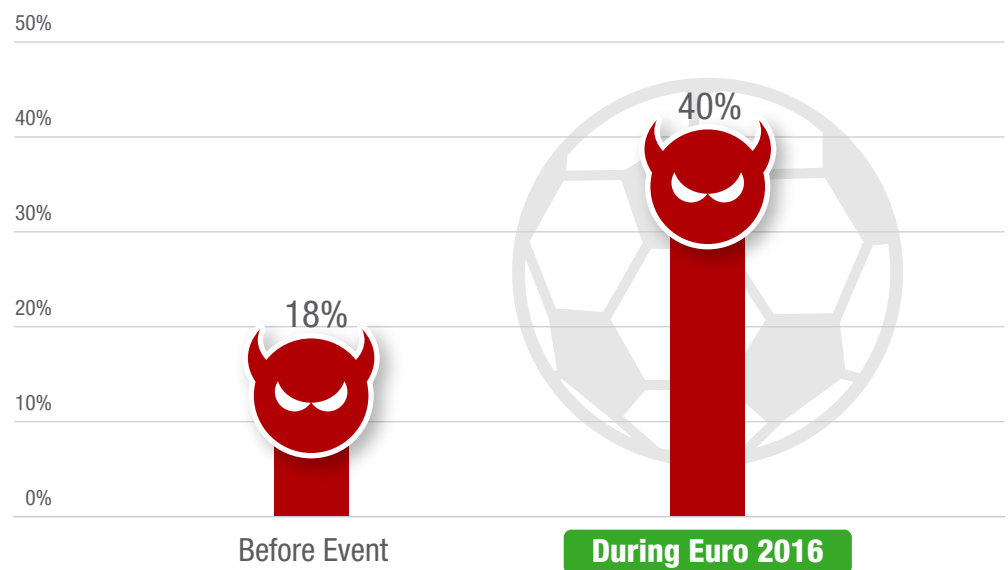
**Andrey Kostin, Senior Web Content Analyst, Kaspersky Lab**



The aggregated impact of our two major risk categories shows a dramatic increase the potential for malware risk as shown in Graph 3. Prior to the Euro 2016 games, 18% of mobile users were at risk. During the games, 40% were at risk. Bear in mind that our second sample was taken during the initial group stage. We anticipate that a third sample taken during the semi-finals or finals would show an even greater increase in these risky behaviors.

Graph 3

### Percentage of sports fans at risk before and during Euro 2016


















## Who is at Risk?

When comparing the online behavior of each profile before and during the games, our findings show the percentage of fans in each profile group who are at risk for malware increased across the board. These findings are summarized in Table 2. The most significant increases in potential malware risk were exhibited by Sports Social Mingler and Sports Social Monitor due to the increased time they spend on social media apps and websites.

Table 2














### Percentage of fans at risk before and during Euro 2016

	 Light Sports User	 Sports Info Seeker	 Sports Info Guzzler	 Sports Social Monitor	 Sports Social Mingler	 Sports Mover & Shaker
Before Event	18%	7%	27%	10%	17%	30%
During Euro 2016	32% 	15% 	50% 	34% 	51% 	69% 

Our findings also indicate that changes in online behavior caused many sports fans to shift out of one profile group and into another. For the most part, fans shifted into profiles with riskier behaviors as shown in Table 3 where we see a significant increase in the size of the Sports Info Guzzler group and the Sports Mover & Shaker group, while other groups shrunk. In addition, we saw an overall increase in the number of people engaging in sports which represents a big opportunity for service providers.

Table 3

### Percentage of fans in each profile before and during Euro 2016

	 Light Sports User	 Sports Info Seeker	 Sports Info Guzzler	 Sports Social Monitor	 Sports Social Mingler	 Sports Mover & Shaker
Before Event	26%	23.1%	21.4%	1.9%	17.5%	10%
During Euro 2016	21% 	22.9% 	28.8% 	1.8% 	14.2% 	11.3% 



## Big Event, Big Opportunity

A major sports event like Euro 2016 generates a lot of interest from regular sports fans and often entices new fans to get into the game. Our findings bear this out. We've already shown how Euro 2016 triggered changes in the online behavior of sports fans - exposing them to greater risk for malware. In addition, our findings in Graph 4 show that this popular event triggered a 17% increase in sport interest among mobile users in general. In our sample, tens of thousands who had no sports-related activity before the event, suddenly became users of sports-related apps and websites during the games. About half of these event-driven fans adopted high-risk behaviors as shown in Table 4. This increase was observed during the first week of the tournament and we estimate that online activity and exposure to cyber threats increased even more during final stages of the tournament.

Graph 4

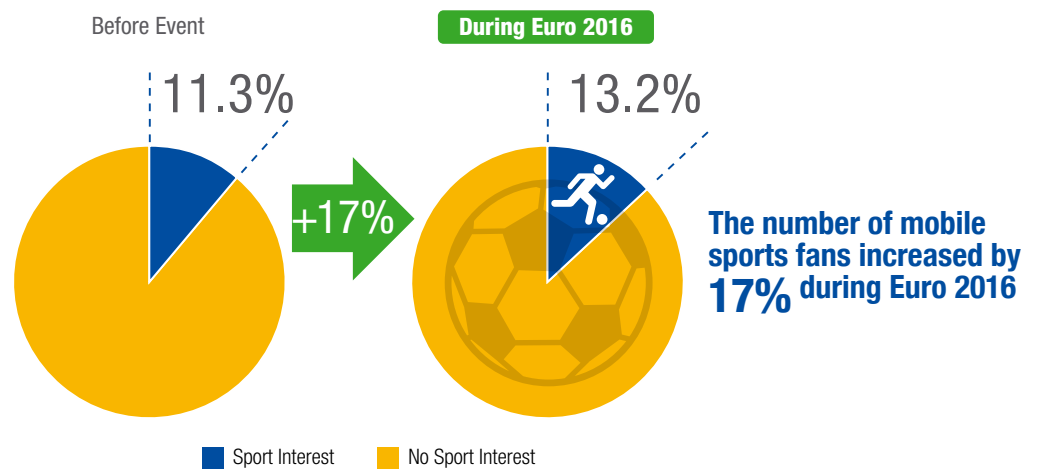
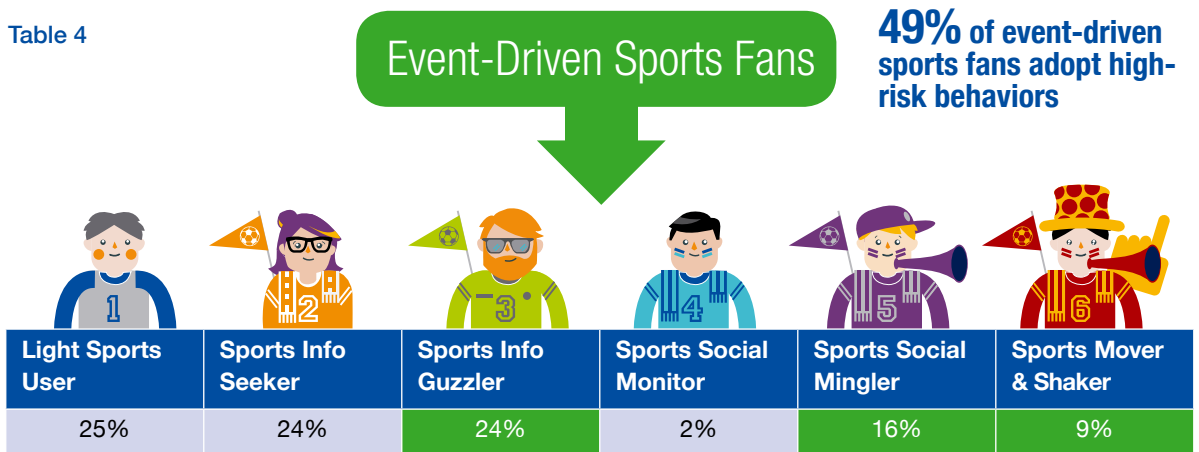


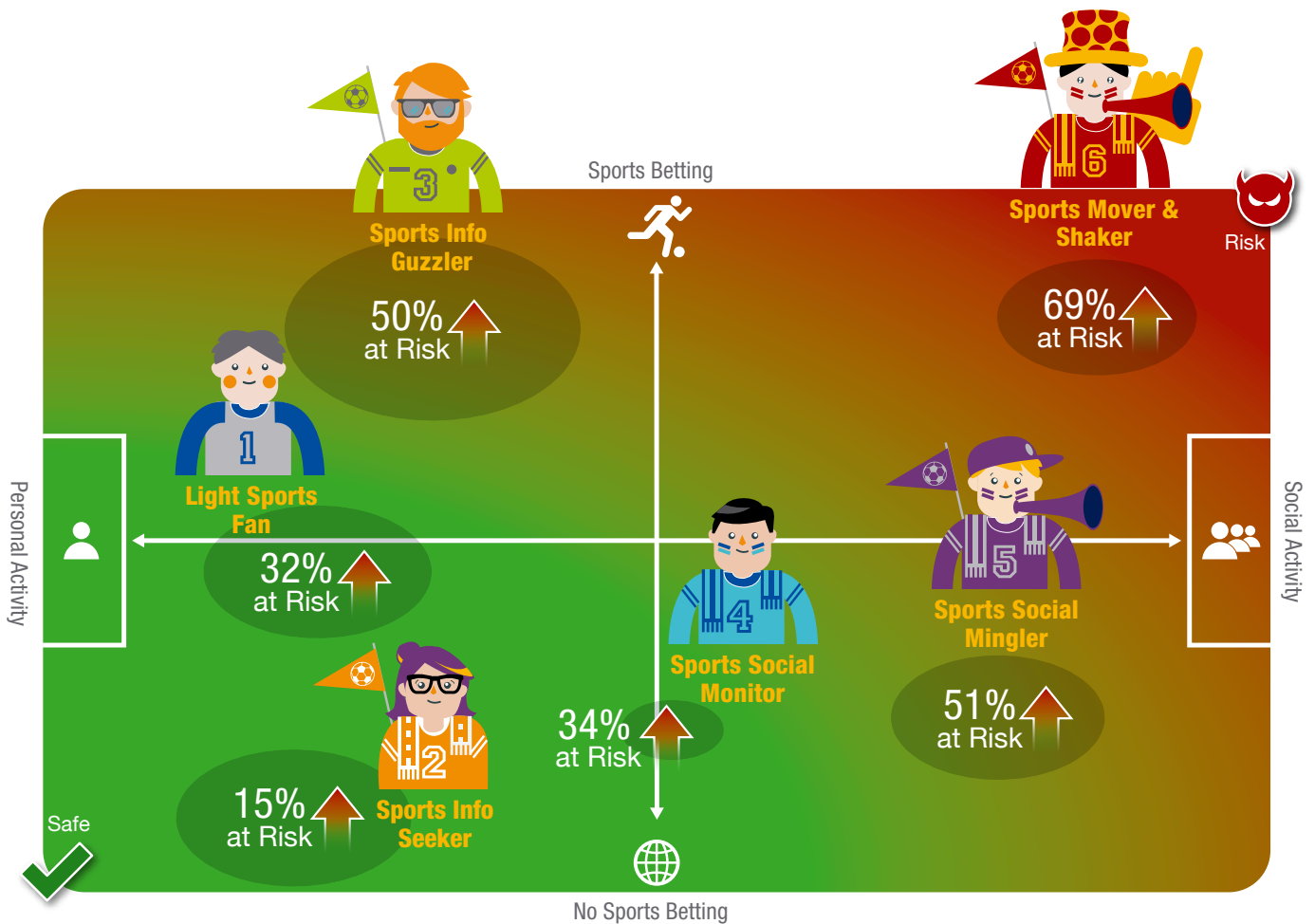
Table 4





## Euro 2016 Risk Assessment Chart

Euro 2016 Risk Assessment Chart is a mobile security heat map that summarizes our research findings. It maps the social media and sports betting activities that contribute to the potential cyber threat risk of each profile group. It also illustrates the size of each profile group to help mobile service providers estimate their addressable market for web security services during major sports events.



## Protecting Sports Fans at Risk



Perhaps the most startling discovery of this research was the large number of very occasional sports consumers who suddenly become intense users of diverse sports apps and websites almost overnight. From a service provider perspective, the addressable market segment of mobile sports fans grew significantly along with the microsegment of sports fans at risk. This shift in online behavior, triggered by a major event like Euro 2016, represents a clear opportunity for mobile service providers to target these customers with campaigns to educate them regarding cyber and malware risk, and to protect them with network-based security as a service for all their mobile devices.

Using timely network business intelligence like the behavior analytics delivered by Allot Data Science Services used in this report, service providers can leverage any major event to onboard customers to value-added security services and increase their loyalty. The table below suggests a number of onboarding opportunities for mobile service providers.

Table 5

Security as a Service	Onboarding Opportunity	Engagement
<b>Try &amp; Buy Protection</b> 	Leading up to major sports events like Euro 2016, target fans at risk with limited-time offers to try network-based Anti-Malware protection. At the end of the period, users opt out or begin paying for the service.	Service includes daily notifications regarding apps and web pages scanned and malware events blocked so users see the value they are getting and will want to continue the service. 
<b>Bundled Protection</b> 	Bundle Anti-Malware services with HD streaming and bandwidth packages designed especially for the big event.	
<b>Premium Protection</b> 	Offer comprehensive Anti-Malware, Anti-Phishing, and Ad Blocker services to fans at high risk for malware. Entice customers with discount rates for the duration of the event and X months following.	

## Key Take Aways



- Major sports events like Euro 2016 trigger significant shifts in online behavior that increase the risk for malware infection and other cyber threats.
- The total number of mobile sports fans at risk for malware doubled during the Euro 2016 games, caused primarily by online sports betting and social activity.
- Major sport events create an ideal opportunity for mobile service providers to proactively educate customers regarding malware risk and to offer network-based security services that protect mobile users and their devices.
- Major sports events increase the addressable market for web security services as more mobile users engage in online sports activity and become targets for cyber criminals.



## Further Reading



1. **Sports as Bait: Cybercriminals Play to Win**  
<http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/99/sports-as-bait-cybercriminals-play-to-win>
2. **Cyber security at large sporting events**  
<http://securityaffairs.co/wordpress/7332/malware/cyber-security-at-large-sporting-events.html>
3. **Malware Growth a Threat to Mobile Users – Even Sports Fans**  
<http://www.mobilesportsreport.com/2013/04/malware-growth-a-threat-to-mobile-users-even-sports-fans/>
4. **Spammers all geared up for Euro 2016!**  
<https://securelist.com/blog/spam-test/74489/spammers-all-geared-up-for-euro-2016/>
5. **Fake FIFA Apps Highlight Malware Concerns Ahead Of Euro 2016**  
<http://www.itsecuritynews.info/2016/06/02/fake-fifa-apps-highlight-malware-concerns-ahead-of-euro-2016/>
6. **Social media highlights escalating security concerns ahead of Euro 2016**  
<http://www.itsecurityguru.org/2016/06/09/social-media-highlights-escalating-security-concerns-ahead-of-euro-2016/>
7. **Mobile Users at Risk (Allot Mobile Trends Report, H1 2016)**  
<http://www.allot.com/resource-library/mobiletrends-report-h12016/>
8. **Segmenting the Digital Lifestyle (Allot MobileTrends Report, H1 2013)**  
<http://www.allot.com/resource-library/mobiletrends-report-q1-2013/>



## Allot MobileTrends Report

UEFA Euro 2016

## About Allot Communications

Allot Communications (NASDAQ, TASE: ALLT) is a leading provider of security and monetization solutions that enable service providers to protect and personalize the digital experience. Allot's flexible and highly scalable service delivery framework leverages the intelligence in data networks, enabling service providers to get closer to their customers, safeguard network assets and users, and accelerate time-to-revenue for value-added services. We employ innovative technology, proven know-how and a collaborative approach to provide the right solution for every network environment. Allot solutions are currently deployed at 5 of the top 10 global mobile operators and in thousands of CSP and enterprise networks worldwide.

[www.allot.com](http://www.allot.com) [info@allot.com](mailto:info@allot.com)

- **Americas:** 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA · Tel: (781) 939-9300 · Toll free: 877-255-6826 · Fax: (781) 939-9393
- **Europe:** NCI – Les Centres d’Affaires Village d’Entreprises ‘Green Side’, 400 Avenue Roumanille, BP309, 06906 Sophia Antipolis Cedex, France · Tel: 33 (0) 4-93-001160 · Fax: 33 (0) 4-93-001165
- **Asia Pacific:** 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104 Tel: +65 67490213 Fax: +65 68481015
- **Japan:** 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 · Tel: 81 (3) 5297-7668 · Fax: 81(3) 5297-7669
- **Middle East and Africa:** 22 Hanagar Street, Industrial Zone B, Hod-Hasharon, 4501317, Israel · Tel: 972 (9) 761-9200 · Fax: 972 (9) 744-3626

