Tracking the Field

Eight cybersecurity considerations around Rio 2016

digital shadows_

Introduction

On August 5, 2016, the world's biggest sporting event will arrive in Rio de Janeiro. Although, for many, primarily a sporting spectacle, an event of this magnitude also represents an exhibition of cyber activity, and one that tourists, event organizers and sponsors need to be prepared for. The global coverage and the influx of millions of tourists produce a highly potent cocktail of risks and threats when paired with Brazil's current economic and political challenges and its longstanding reputation for cybercriminal activity. So what type of activity can we expect ahead of the big event?

Cybercrime

Brazil has a strong and unenviable reputation for cybercriminal activity, and the 2014 World Cup saw an increase in banking fraud and widespread scam campaigns. But what specifically makes an event like Rio 2016 such an attractive target for cybercriminals?

One way of illustrating this would be to take an "attacker's eye view" of Brazil and assess it as a target in the same way a potential threat actor might do.

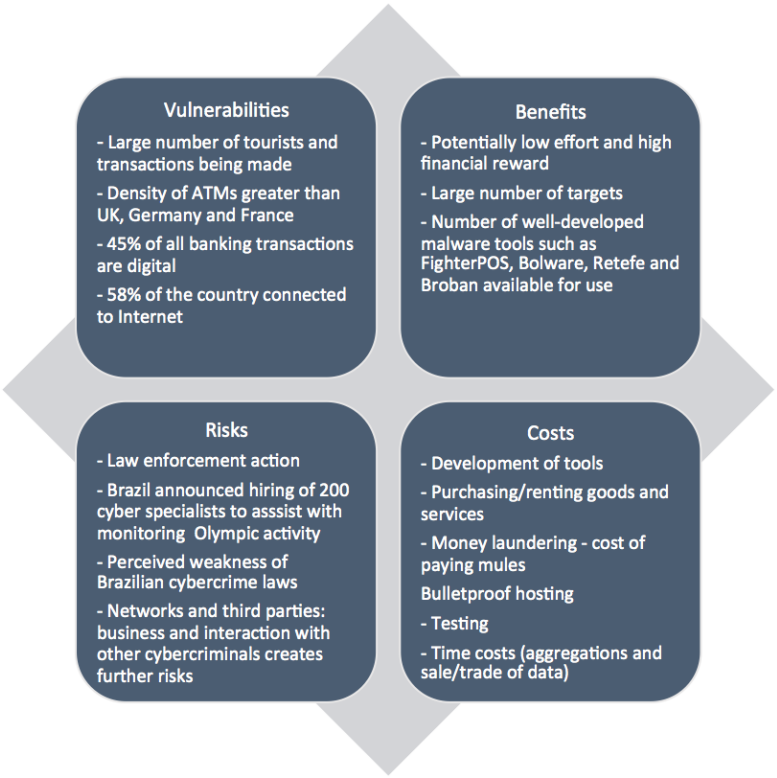

Figure 1: Threat target assessment of Rio 2016

Taking into account Brazil's well-established cyber threat environment, the prospect of an estimated half a million tourists to the country, and the associated banking transactions, consumer activity, and use of unprotected local WiFi networks, the possibilities for cybercriminals are endless.

With this in mind, here are the top 4 things we can expect:

1. **POS malware.** Cybercriminals are likely to exploit the large number of economic transactions conducted on an event of this scale, particularly in areas of high tourist density such as city centres, hotels and shopping malls. Last year, it was reported that the credential harvesting malware known as FighterPOS had affected over 100 organizations throughout Brazil.

2. **ATM skimming.** Known locally as the "Chupra-cabra", ATM skimming is a threat across Brazil – the World Bank estimates that the Brazil has the largest number of ATM machines worldwide – and users withdrawing cash at public machines should remain vigilant. In 2014, 14 ATM machines at Rio de Janeiro's Tom Jobim airport were reportedly fitted with skimming equipment, exploiting the high number of tourists and travellers making cash withdrawals.

3. **Scam.** Brazilian cybercriminals are likely to use fraudulent websites and fake promotional offers as a means of luring victims in search of event tickets and travel deals. During the 2014 World Cup, cybercriminals sent phishing messages advertising fraudulent giveaways such as free hotel accommodation to unsuspecting victims that required the user to input personal information and credit card data.

4. **Banking fraud.** A major issue in Brazil regardless of the upcoming event, Brazil has been ranked second in the world in online banking criminal activity. Cybercriminals looking to target victims in Brazil have a whole host of banking Trojans and malware available to them on the clear and dark web. In Brazil specifically, cybercriminals increasingly promote their malware online on social media – such as an individual who recently advertised the rent of a "fully functional" banking Trojan for approximately $600 USD via YouTube (see Figure 2). Moreover, Brazilian cybercriminals are adept at creating customized malware targeting popular payment systems such as the Brazilian Boleto. Boleto malware such as Broban is commonly spread through spam and phishing emails containing the malware that can modify the account details of a Boleto voucher.

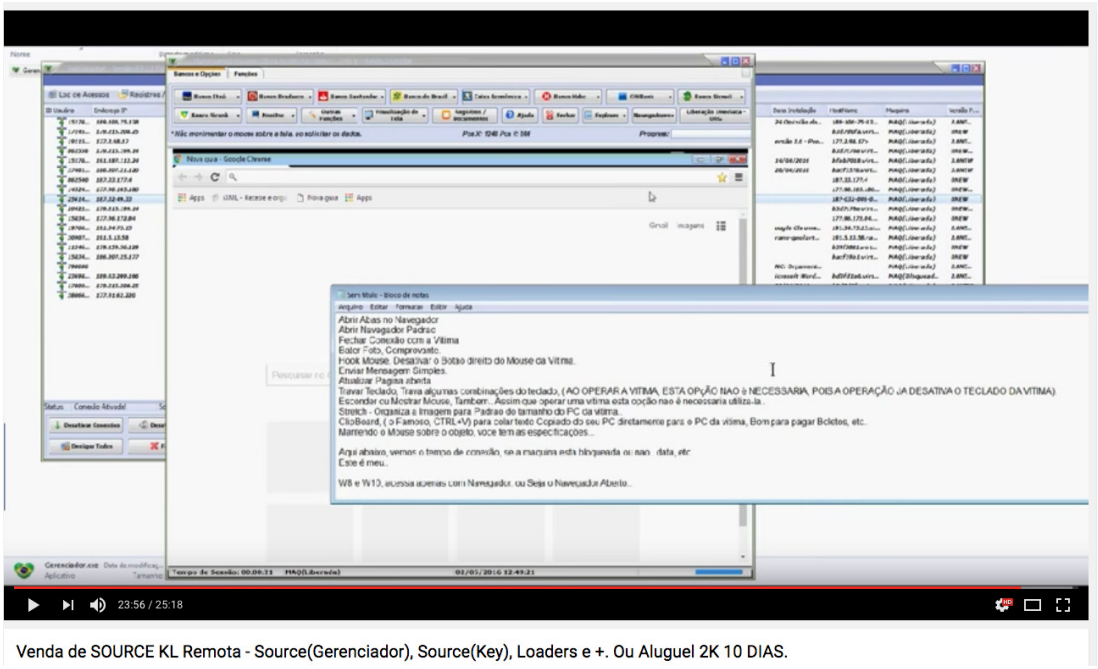

Figure 2: YouTube video promoting "fully functional" Brazilian banking Trojan for rent.

Hacktivism

Worldwide events attract considerable media attention, but the reverse of this is that they also motivate hacktivist actors driven by public attention, either for themselves or the issues they claim to represent. In February 2016, we reported on the announcement of the hacktivist operation OpOlympicHacking by members of Anonymous Brasil and an affiliate group known as ASOR Hack Team.[1] The operation was announced as a reaction against the Brazilian government's over-expenditure in comparison to the current economic difficulties faced by many Brazilians. To compound matters, Brazil is in the midst of a number of political and health challenges - namely the ongoing impeachment of President Dilma Rousseff and worldwide health concerns over the Zika virus – that provide fertile fodder for a variety of hacktivist actors.

Despite the activity observed so far, Rio-related cyber activity has not been of the same high frequency observed during the World Cup in 2014. The reasons for this are unclear at the time of writing, but lessons learned from the campaign in 2014 and increased mitigation strategies from target organizations may have played a role. Moreover, the protracted political upheaval and fears over health issues such as the Zika virus may have also dominated the attention of threat actors and media alike away from the upcoming event itself. With the opening ceremony fast approaching, however, there is still a realistic possibility that hacktivist activity will increase, and new campaigns may be announced, particularly after the event begins.

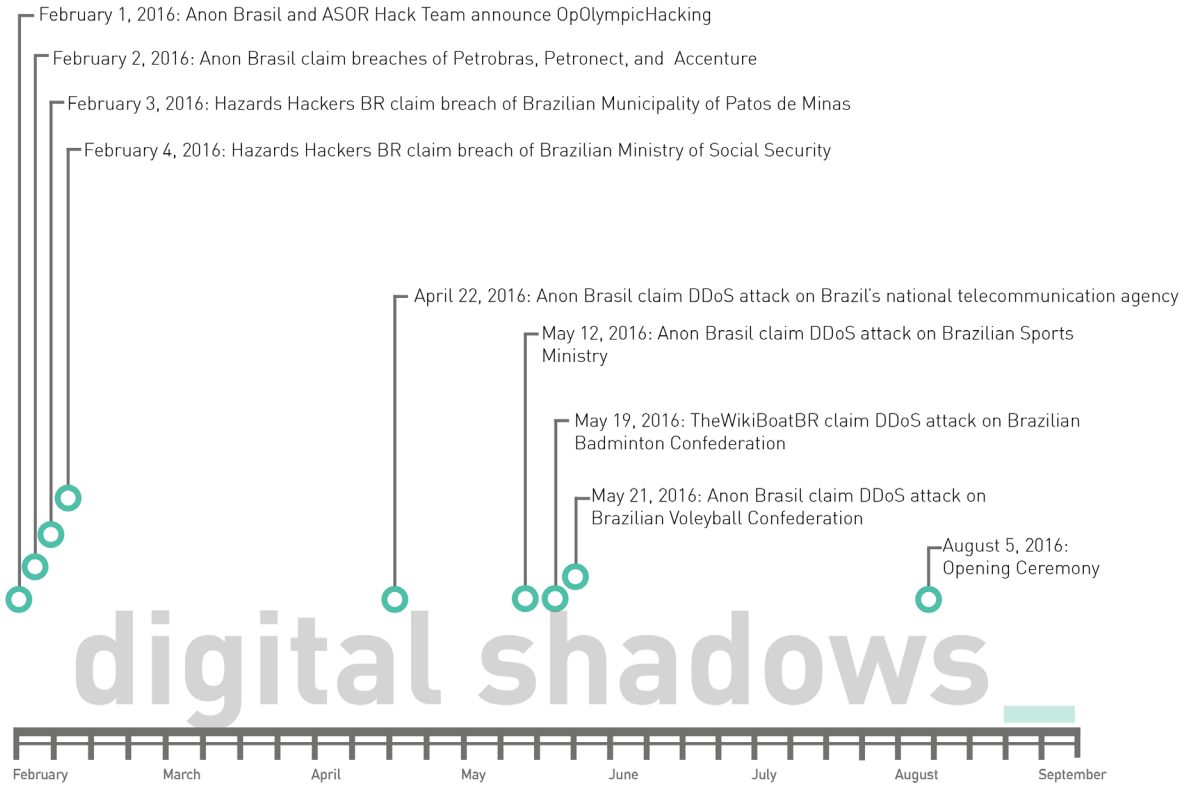

Figure 3: detected hacktivist activity targeting Rio

So from a hacktivist perspective, what can we expect?

1. **DDoS attacks.** Perhaps the most likely tactic employed by hacktivist actors. As with previous large sporting events such as the 2014 World Cup in Brazil, hacktivist actors are expected to target event organisers and its main sponsors.

2. **Website defacement.** Like DDoS attacks, threat actors may use website defacements as a means of disrupting the operations of their victims, or as a means of establishing kudos. Given the scale of the event, actors with even tenuous grievances with the games may choose to use the event as a way to promote their cause or demonstrate their capability – the campaign OpNimr that aims to highlight the execution of Shia cleric Nimr Baqir al-Nimr by Saudi Arabian authorities, for example, has been used concurrently with the OpOlympicHacking hashtag in protest against Saudi Arabia's expected involvement in the 2016 games.

Figure 4: Anonymous image promoting OpNimr and OpOlympicHacking campaigns

3. **Data leaks**. Hacktivist groups, such as Anonymous Brasil and Hazards Hackers BR, have claimed to have conducted successful data breaches of large Brazilian companies, including Petrobras and government departments.

4. **Physical protest.** Throughout 2015 and 2016 a series of protests were held against government corruption. With Brazil's economic and political troubles showing no immediate signs of cessation, further physical protest activity could transpire. Likewise, some protesters around the time of the World Cup in 2014 blamed unnecessary government spending on the event as a prime reason for public ire, and it is a realistic possibility that similar protests may occur in the lead up to this year's event.

So as we approach the opening ceremony, what's the state of play? Given the very high number of potential victims and the variety of threat actors associated with an international sporting event of this scale, the threat is assessed as high. Previous events of a similar magnitude (London 2012) and in the same location (World Cup 2014), have demonstrated the intent and success of threat actors targeting individuals for financial theft and fraud, which is likely to be similar in the case of Rio. As for the threat from hacktivist activity, the tactics used would most likely be of low capability, but it remains to be seen whether there is an increase in activity once the event commences.

Author

Digital Shadows Analyst Team

End Notes

1. OpOlympics, A Hurdle for Rio's Sponsors to Vault https://www.digitalshadows.com/blog-and-research/opolympichacking-a-hurdle-for-rios-sponsors-to-vault/

About Digital Shadows

Digital Shadows provides cyber situational awareness that helps organizations protect against cyber attacks, loss of ntellectual property, and loss of brand and reputational integrity.

Its flagship solution, Digital Shadows SearchLight™, is a scalable and easy-to-use data analysis platform that provides a view of an organization's digital footprint and the profile of its attackers. It is complemented with intelligence operations analyst expertise to ensure extensive coverage, tailored intelligence and frictionless deployment. It continually monitors more than 100 million data sources in 27 languages across the visible, deep and dark web and other online sources to create an up-to-the minute view of an organization and the risks requiring mitigation.
The company is jointly headquartered in London and San Francisco.

digitalshadows.com

London

Level 39, One Canada Square, London, E14 5AB

+44 (0) 203 393 7001 info@digitalshadows.com

San Francisco

332 Pine Street, Suite 600 San Francisco, CA 94104

+1 (888) 889 4143

digital shadows_