Rio 2016 CSI RT

Creation, operations and lessons learned – Rômulo Rocha
Bio

• Rômulo Rocha
• From Rio de Janeiro, Brazil
• @romrocha
• Love topics related to hunting and incident response
• Security Consultant at Tempest Security Intelligence
Agenda

• Olympics briefing
• CSIRT (strategy, timeline, operations, channels, etc)
• Wargames
• Games Time! (*focus only on Olympic games)
• Lessons Learned
Olympics briefing
Two Events in the same city
TECH IN THE FIELD

- CIS
- INTERCOM
- OVR
- PA
- PA
- CELULAR
- VIDEObOARD
- SCOREBOARD
- WI-FI
- T&S
- BROADCAST
- SCOREBOARD
Hacktivists

A number of hacktivist campaigns may attach themselves to the upcoming Olympics simply to take advantage of the on-looking audience. For example, the hacktivist group, Anonymous Caucasus, has launched what appears to be a threat against any company that finances or supports the winter games. This group states the Sochi games infrastructure was built on the graves of 1 million innocent Caucasians who were murdered by the Russians in 1884. According to Trusted Third Party analysis, the group has been linked to distributed denial of service (DDoS) attacks on Russian banks in October 2013. Therefore, the group is likely capable of waging similar attacks on the websites of organizations they believe financed Olympic related activities; however, no specific threat or target has been identified at the time of this report.

Announced plans to attack 10 Russian banks in protest at the 2014 Winter Olympics

A Twitter account claiming to be part of the Anonymous hacktivist group has announced plans to attack 10 Russian banks in protest at the 2014 Winter Olympics, which will take place in Sochi, Russia.
CSIRT
Strategy

• Necessity of a CSIRT were clear for Rio 2016 employees and C level, some threat actors were active by end of World Cup 2014 and politic clashes were erupting all around

• Defined a strategy at beginning and followed until the end, simple is better

• Well defined rules and responsibilities

• Training of employees and trust of CSIRT inside company.

• Communication is key, be announced globally and have clear/strong communication channels with local ISP, content providers, Cert.br, CDCiber (army), government agencies, sponsors and local security community.

• Trying not recreate the wheel, use what you have already.
Wargames
How it worked?

Objectives:
- Stimulates communication
- Team readiness and rehearsal
- Test effectiveness of incident response processes and procedures
- Evaluate alert triggering on tools (bonus)
- Assess exposure of the corporate network to attack vectors (bonus)
- Based on common practices (Mitre, Nato, Enisa, Poland Cyber, etc)
Our Wargames

• Three times, lasting around 1 week
• Full live (on production)
• To achieve the highest realism possible, blue and red teams had no contact and worked in different physical environments
• None of the teams were aware of their capabilities
• Scenarios based on threat intel and common knowledge collected previously
• Number of participants was increasing during time
• After each session, a lot of data were generated, helping us to improve our capabilities
**WG1 briefing**

- 28th Sep – 2nd Oct, 2015
- Scope: Corporate Network (some interfaces with Games Network as well)
- Over 20 people
- 16 Scenarios

<table>
<thead>
<tr>
<th>Red team briefing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intentions:</strong></td>
</tr>
<tr>
<td><strong>Capabilities:</strong></td>
</tr>
</tbody>
</table>
| **Goals:**         | • Compromise and alter Rio 2016 websites  
                      • Compromise Rio 2016 social media presence  
                      • Access and leak confidential documents  
                      • Access and leak volunteers information  
                      • Access and leak financial information |
# WG1 in a nutshell

<table>
<thead>
<tr>
<th>Red Team</th>
<th>Blue Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used a lot smoke screen attacks to distract Blue Team</td>
<td>Detected and blocked all smoke screen attacks</td>
</tr>
<tr>
<td>Send spear phishing attacks to important accounts based on social media gatherings</td>
<td>Detected and contained a spear phishing attack but did not investigated source of attack</td>
</tr>
<tr>
<td>Got administrative control over domain</td>
<td>Triage was not effective</td>
</tr>
<tr>
<td>Got administrative control over switches and Wifi</td>
<td>Tools getting alarms, but lacking correlation and automatization</td>
</tr>
<tr>
<td>Lateral movement and persistence on network</td>
<td>Lack of procedures</td>
</tr>
<tr>
<td>Completed all scenarios, including taking accounts of mascots in twitter</td>
<td>Preventive controls and fine adjustment on tools still needed</td>
</tr>
<tr>
<td>Unleashed #op_olympic_chaos in the last day</td>
<td></td>
</tr>
</tbody>
</table>
## WG2 briefing

- Feb 22 Nd – Feb 26th – 2016
- Repeated the first, to validate improvements
- CSIRT more structured and with processes
- Over 40 people
- 16 Scenarios

### Red team briefing

<table>
<thead>
<tr>
<th>Intentions:</th>
<th>Abuse the brand and public image of games to spread politically motivated message.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capabilities:</td>
<td>Not cutting-edge attacks, 0days, attacks like SQLi, XSS, Spear Phishing, Password attacks, Wifi, Common-grade malwares, Windows Attacks (passhash, lateral movement, AD compromise, etc)</td>
</tr>
<tr>
<td>Goals:</td>
<td>• Compromise and alter Rio 2016 websites • Compromise Rio 2016 social media presence • Access and leak confidential documents • Access and leak volunteers information • Access and leak financial information</td>
</tr>
</tbody>
</table>
## WG2 in a nutshell

<table>
<thead>
<tr>
<th>Red Team</th>
<th>Blue Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used a lot smoke screen attacks to distract Blue Team in critical moments</td>
<td>Majority of smoke screen attacks didn't take time to contain, but drained team resources</td>
</tr>
<tr>
<td>Send spear phishing attacks to important accounts</td>
<td>Successfully detected and contained the majority of the high-impact attacks performed by the red team</td>
</tr>
<tr>
<td>Got credentials to CSIRT back office system using spear phishing against one team member</td>
<td>Communication was way better but still lacking procedures and investigations in depth, should take more intel from attacks</td>
</tr>
<tr>
<td>Got credentials mining emails</td>
<td>Tools getting alarms and some automatization</td>
</tr>
<tr>
<td>Got Rio 2016 Facebook credentials</td>
<td>Triage was better</td>
</tr>
<tr>
<td>Created a spear phishing hosted in one of our websites</td>
<td>More preventive tools in place (endpoint hardening, network monitoring, etc)</td>
</tr>
<tr>
<td>In the end, received gold ticket to create a hard scenario for blue team</td>
<td>Better SIEM adjustments and triggering, correlation stills weak</td>
</tr>
</tbody>
</table>
WG3 briefing

Jun 20th – 24th – 2016

Scope: Corporate Network (some interfaces with Games Network as well)

Over 70 people

3 Shifts working like GT

Same team structure as GT, including Security Manager.

34 Scenarios

Red team briefing

Intentions: Use same techniques as attackers, which are: hacktivists, fraudsters and bankers.

Capabilities: Rogue APs, BruteForce, Evil Twind, Spoofing, DDoS, Spear Phishing, Social Eng, Network Attacks, Windows Exploitation, Information Leakage, etc

Goals: Test blue team response to some specific scenarios. (table below)
# WG3 in a nutshell

<table>
<thead>
<tr>
<th>Red Team</th>
<th>Blue Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used a lot smoke screen attacks to distract Blue Team</td>
<td>Still needs automatization for some types of attacks</td>
</tr>
<tr>
<td>Still getting network credentials in ticket systems</td>
<td>Ticket system was too slow for incident response</td>
</tr>
<tr>
<td>Spear phishing specially crafted to administrators in third party companies</td>
<td>Contained majority of attacks</td>
</tr>
<tr>
<td>Disruption of SIEM tool</td>
<td>Triage working better</td>
</tr>
<tr>
<td>Bypassed 802.1x auth and implanted Rogue AP in new networks</td>
<td>Still lacking some procedures for incident response</td>
</tr>
</tbody>
</table>
### Marks between Wargames

<table>
<thead>
<tr>
<th>CWG1</th>
<th>CWG2</th>
<th>CWG3</th>
</tr>
</thead>
<tbody>
<tr>
<td>+20 people</td>
<td>+40 people</td>
<td>+70 people</td>
</tr>
</tbody>
</table>

#### CWG1
- Rules and responsibilities diffused, team without instructions
- Lot of failures in tools configurations and infrastructure not mature.
- Privileged local accounts on border
- Domain admins without necessity
- Critical accounts without proper security (2fa)
- Lateral movement easily
- Network segmentation immature
- Triage inefficient, low severity incidents consuming analysts time
- Lack of integration with important areas like communication and social media

#### CWG2
- Better infrastructure and monitoring
- Critical accounts monitored
- Triage and incident classification
- Cyber Kill Chain and TTP idea adopted by the team
- Improvement on documentation and processes
- Better network segmentation
- Endpoint hardening improvements
- Better CSIRT notifications (templates and automatization)
- Post-Mortem still bad
- IOCs monitoring and sharing being used, but in not all cases
- Better integration with service desk and field services

#### CWG3
- Rules and responsibilities well defined and understood by team
- Incident response process documented
- 802.1x auth in the network
- Better network segmentation (avoiding network lateral movement)
- Endpoint hardened
- Better intel extraction after incidents
- Utilization of IOCs
- Windows accounts sanitization and control in place
Lessons learned from Wargames

• Training your team under high pressure is essential, you will be surprised
• Rules and responsibilities must be aligned and understood by everyone
• Communication between teams and shifts are key, incident analysis should flow no matter who is in the charge
• Yes, still have to tune that tool =D
• Briefing before critical moments is valuable
• Your backoffice tool, should be more secure than anything. (and have backup)

• Use a back office tools, that gives speed, security and an excellent flow for incident and investigation procedures
• The importance to understand TTPs of adversaries is key for training and proper incident response methods, intel have to been extracted from attacks
• People still sharing passwords through email, 2fa is a must
• When triage does not work well, nothing works well
• Review every admin account that used in our domain, specially if they are running as a service, avoid that with your heart (MS LAPS can help too)
• User education is a relief during a scenario of attacks, they helped a lot in spear phishing attacks detection
Photos
Games time!

(*focus only on Olympic games)
OLIMPIC GAMES

11,303 athletes

207 delegations

205 Countries
+ Team of Refugees
+ Independent athletes

974 Medals
+6.1 millions tickets
(London 2012: 8.8 millions)

701 sport sessions
GAMES

VISIBILITY

+4.5 BI SPECTATORS

+350,000
HOURS OF TRANSMISSIONS
(London 2012: 200,000)

+500 CHANNELS

+250 DIGITAL PLATFORMS
7,262
IT & TELECOM professionals

5,509
Partners and contractors

1,341
Volunteers
Wrap up for CSIRT

• Operations initiated 24x7 in 4th July 2016
• Clients: Press, Olympic family, Sponsors and Partners.
• Escope: Rio 2016 infrastructure (on premise and cloud)
• Around 80 people in CSIRT team
• 15 companies
• Red team inside CSIRT team
• Threat intelligence covering more than 9 languages (with help of Japan)
• Cooperation with government agencies
• Remote and on-site IR.
Other Hacktivism activities

Target list updated to include CBF, construction contractors and companies.
Anon BR released texts and videos calling for engagement on #OpOlympicHacking.
Released tool to perform DDoS attacks against targets.
#OpOlympicHacking gained visibility on international media.

Leaks of personal data of:
- Mayor and Governor of RJ;
- Sports Minister;
- Presidents of COB and CBF;
- Managers of construction companies that were on the target list.

New targets added:
- Sponsors
- IOC
- COB (Brazilian OC)

1st video released
Brazilian hacktivist made contact with Cyberguerrilha
IRC channel created
1st target list released
1st leak of a sports confederation's DB

Ghost Squad attacks government websites

Main activities
- Sponsors removed from target list
- Anon BR starts to spread #OpOlympicHacking on social media
- Pastebin post describing operation in 3 languages: Portuguese, English and Spanish.

#OpOlympicHacking restarted
DB leaks of several sports confederations
- DDoS attacks against website "www.rj.gov.br"
- Leaked personal data of heads of RJ Gov. offices

AnonOpsBR hacked OBS (Olympic Broadcasting Services) main website and leaked an associated DB

WADA announced it received phishing attacks on early Aug and confirmed Yuliya Stepanova’s (Russian whistleblower) account was compromised.
Russian group “Fancy Bears” hacked WADA and leaked sensitive information of Olympic Athletes from several countries:
- Doping tests;
- Certificates for therapeutic usage of prohibited drugs.

WADA confirmed the hack

Asor Hack Team defaced the website of Cyrela and leaked personal data stored in it

Russian group "Fancy Bears" hacked WADA and leaked sensitive information of Olympic Athletes from several countries:
- Doping tests;
- Certificates for therapeutic usage of prohibited drugs.

WADA confirmed the hack

AnonOpsBR hacked OBS (Olympic Broadcasting Services) main website and leaked an associated DB

Anon BR releases "summary" of #OpOlympicHacking

Anon Poland criticizes Olympic Games and promises new attacks against WADA
- Anon Poland says the group attacked “teamusa.org” and “paralympic.org”
- Our assessment classified that as false claims
Security Numbers

- +20m of alerts
- 181 incidents
- 50,000 authentications using 2FA (around 5800 users)
- Around +800 malware blocked on AntiSpam.
- +50 takedowns during the games time period
- +30m WAF blocks (website e mobile app)
- +100k connected equipments
- Major incidents: Anon ransomware, Wada attacks detected on our network
Lessons learned from whole experience

• Understand you public, scope and start small
• Know your communication channels, exercise them regularly
• Brief and contact external partners before critical periods
• Fine tuning forever
• Triage is key, cannot be underlooked as someone without experience
• Centralize your documentation, make it easy for newcomers
• Attention to shift hand-off, contextual information can be lost. (overlaying is a good option)
• Avoid at all cost, the “ticket closing” behavior, incidents should be investigated until the end. TTPs and IOCs must be determined and returned to monitoring
• Situational awareness meetings/reports is nice to have, set team in the mood and prepare for difficult situations
• Automatize everything as possible
Thank you