Establishing a CSIRT for Rio 2016 Olympics

Creation, operations and lessons learned
$ whois

- Rômulo Rocha (call me Rom, is easier)
- From Rio de Janeiro, Brazil
- @romrocha / romrocha@gmail.com (pgpkey 0660024A)
- Former Rio 2016 Incident Response Leader
- Now Security Consultant at Tempest Security Intelligence
- Love topics related to hunting and incident response
What we have for today?

01. Olympics briefing (really fast)

02. CSIRT (know some timeline for us will help to understand whole picture and the strategy for our team)

03. Wargames and rehearsals (we did it, it was very interesting...)

04. Games Time! (I will focus only in Olympic Games, show some numbers, threat intel, cases timeline, incidents, etc)

05. Lessons Learned will be in the end of every topic and all around
Olympics briefing
Olympics
3 different networks. Games, Admin and Shared.
2014 scenario

- Regular security team, deploying preventive controls
- Around 10 people
- Hundred projects like crypto, endpoint protection, border control, ips, hardening, etc
- Minor incidents happening inside our network
- Moments of concern during World Cup and Sochi (also lot of activity at border)
- Lot of effort to maintain confidentiality of projects (Mascots, brand, medals, website)
- Incident response when possible, no process
- Running against time to deploy everything
- Threat intel monitoring and website takedown services were already running
Timeline, strategy and communications
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
• Protect Rio 2016 information assets, infrastructure and partners as well
• Defined a strategy at beginning and followed until the end, simple is better, no time to rethink
• Well defined rules and responsibilities inside the team
• Training of employees and trust of CSIRT inside and out of organization
• Be announced and have clear/strong communication channels with local ISP, content providers, Cert.br, CDCiber (army), CTIR.gov government agencies, sponsors and local security community.
What I’ve learned?

- Understand your audience, scope and start small
- Communication is very tricky and complex, understand every channel
- Centralization of documentation is a must, keep it clean and easy to newbies (try to remember those walkthrough from videogames, they are easy to follow)
- Make contact and open channels before crisis period, during crisis is the worst time to do it
- Announce your team to other CSIRTs, give everyone an identity as CSIRT members, it will help to start and make them more interested and motivated
- There is no “right” or “wrong” for your CSIRT team model, test and adapt.
Wargames

Really nice experience...
How it worked? Lot of teams...

Objectives:

• Stimulates communication
• Team readiness and rehearsal
• Test effectiveness of incident response processes and procedures for blueteam
• 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 team 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 were increasing during
• After each session, a lot of data were generated, helping us to improve our capabilities for incident response and preventive controls
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>Lateral movement and persistence on network</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>Got administrative control over domain and Golden Ticket</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
# 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

<table>
<thead>
<tr>
<th>Intentions:</th>
<th>Use same techniques as attackers, which are: hacktivists, fraudsters and bankers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capabilities:</td>
<td>Rogue Aps, BruteForce, Evil Twind, Spoofing, DDOS, Spear Phishing, Social Eng, Network Attacks, Windows Exploitation, Information Leakage, etc</td>
</tr>
<tr>
<td>Goals:</td>
<td>• Test blue team response to some specific scenarios. (table below)</td>
</tr>
</tbody>
</table>


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>
# Principal marks between WGs

## CWG1
- Sep 28th – Oct 2nd 2015
- +20 people
- Rules and responsibilities diffused, team without instructions
- Lot of failures in tools configurations and infrastructure not mature.
- High Privileged local spread around servers
- 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
- Feb 22nd – 26th 2016
- +40 people
- Better infrastructure and monitoring
- Critical accounts monitored
- Triage and incident classification
- Cyber Kill Chain and TTP idea adopted by the whole blue team
- Improvement on documentation and processes
- Better network segmentation
- Endpoint hardening improvements
- Better CSIRT notifications
- Post-Mortem still bad, “no time to it”
- IOCs monitoring and sharing being used, but in not all cases
- Better integration with service desk and field services

## CWG3
- Jun 20th – 24th 2016
- +70 people
- Rules and responsibilities well defined and understood by team
- Incident response process documented
- 802.1x auth in the network
- Endpoint better hardened
- Better intel extraction after incidents
- Utilization of IOCs
- Windows accounts sanitization and more controls in place
What we have learned...

• 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 back office 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
• People still sharing passwords through email, 2fa is a must
• **When triage of incidents does not work well, nothing works well**
• Review every privileged account that used in our domain, specially if they are running as a service, avoid that with your heart
• User awareness/education is a relief during a scenario of attacks, they helped a lot in spear phishing attacks detection
Games time!
(*focus only on Olympic games)
Olympic numbers

- 11,303 athletes
- 207 delegations from different countries
- 4,5 bi spectators
- 93k people working
- 57k press
- 18k athletes using wifi
- 1.2b pageviews
- 8m downloads of app
- 15k endpoints
- 850 servers
Wrap up for CSIRT

Operations initiated 24x7 in 4th July 2016
Clients: Press, Olympic family, Sponsors and Partners.
Scope: 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
Cooperation with government agencies
Remote and on-site IR.
Pretend, something is happening.
Threat intel Timeline

**July**
- Target list updated to include CBF, construction contractors and companies.
- 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.

**August**
- 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.

**September**
- Asor Hack Team defaced the website of Cyrela and leaked personal data stored in it.
- Anon BR releases “summary” of #OpOlympicHacking.
- Anon BR said he was being tracked.
- He deleted his Twitter profile.

Main activities:
- #OpOlympicHacking restarted
- 1st leak of a sports confederation’s DB
- Ghost Squad attacks government websites
- 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
- New targets added: Sponsors
- IOC
- COB (Brazilian OC)
- Brazilian hacktivist made contact with Cyberguerrilha.
- IRC channel created.
- 1st target list released.
- 1st video released.

Other Hacktivism activities:
- WADA announced it received phishing attacks on early Aug and confirmed Yuliya Stepanova’s (Russian whistleblower) account was compromised.
- WADA confirmed the hack.
- Anon Poland says the group attacked “teamusa.org” and “paralympic.org”.
- Our assessment classified that as false claims.
- Anon Poland criticizes Olympic Games and promises new attacks against WADA.
- Anon Poland disclosed DB of Court of Arbitration for Sport.
- 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.
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, database drop and Wada attacks detected on our network
**Lessons learned from games time**

<table>
<thead>
<tr>
<th>Know your communication channels, exercise them regularly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brief and contact external partners before critical periods (like sales period, games, announcements, ipo, etc)</td>
</tr>
<tr>
<td>Fine tuning forever</td>
</tr>
<tr>
<td>Proper triage of incidents is key for a good functioning of a CSIRT</td>
</tr>
<tr>
<td>Attention to shift hand-off, contextual information can be lost. (overlaying is a good option)</td>
</tr>
<tr>
<td>Situational awareness meetings/reports is nice to have, set team in the mood and prepare for difficult situations (in our case was a must to have!!!)</td>
</tr>
<tr>
<td>Automatize everything as possible</td>
</tr>
<tr>
<td>Avoid at all cost, the “ticket closing” behavior, incidents should be investigate until understanding of TTPs and IOCs for training, hunting and improvement of incident response methods</td>
</tr>
</tbody>
</table>
Thank you =D