OPSEC

Against APT’s reconnaissance phase

Antonio Villalón
Chief Security Officer
S2 Grupo CERT
APT stages

What is OPSEC?

Let’s start!

Sample scenario

Conclusions
APT stages
APT stages

Time

Real-Time/ Near-Real-Time

Postcompromise
(Days/Weeks)

Network

Network Traffic Analysis

Style 1

Payload Analysis

Style 3

Endpoint Behavior Analysis

Style 4

Payload

Payload Forensics

Style 2

Endpoint

Endpoint Forensics

Style 5

Where to Look

6
THE BOTTOM LINE ON OPSEC:
We all have information that the Bad Guys need to hurt us. We don't want them to get it. The OPSEC process helps us to look at our world through the eyes of an adversary and to develop measures in order to deny them. Get it?

The OPSEC Process:
1. Identify Critical Info
2. Analyze Threats
3. Analyze Vulnerabilities
4. Assess the Risks
5. Apply Countermeasures

THINK ABOUT IT... ALL THE TIME!

5 STEPS...
1 MINDSET

WHAT IS OPERATIONS SECURITY?
Operations Security, or OPSEC, is a risk management methodology used to deny an adversary information concerning our intentions and capabilities by identifying, controlling, and protecting critical information associated with the planning and execution of a mission.
Let’s start!
Our goal
Which info is valuable (org)?
Which info is valuable (ppl)?
Which info is NOT valuable?
Which are the threats?

INSERT YOUR FAVOURITE FLAG <HERE>
Information Sources: Any organization that desires to raise the flag of Islam high and proud, must gather as much information as possible about the enemy. Information has two sources:

1. Public Source: Using this public source openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy. The percentage

2. Secret Sources: It is possible, through these secret and dangerous methods, to obtain the 20% of information that is considered secret. The most important of these sources are:
   A. Individuals who are recruited as either volunteers or because of other motives
   B. Recording and monitoring
   C. Photography
   D. Interrogation
   E. Documents: By burglary or recruitment of personnel
   F. Drugging
   G. Surveillance, spying, and observation
Open sources
<table>
<thead>
<tr>
<th>Title</th>
<th>Author</th>
<th>Views</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is PyPy supported on Solaris?</td>
<td>De Alekz</td>
<td>19</td>
<td>11 de ene.</td>
</tr>
<tr>
<td>Getting stack size and pointer in a thread?</td>
<td>De <a href="mailto:hume.sp...@bofh.ca">hume.sp...@bofh.ca</a></td>
<td>20</td>
<td>5 de ene.</td>
</tr>
<tr>
<td>olwm won't load in X-Window on Linux. (arcane - really arcane)</td>
<td>De John Ferguson</td>
<td>19</td>
<td>21/12/16</td>
</tr>
<tr>
<td>Solaris 11, CUPS and RBAC</td>
<td>De YTC#1</td>
<td>19</td>
<td>16/12/16</td>
</tr>
<tr>
<td>no sol12?</td>
<td>De Joe Reid</td>
<td>117</td>
<td>15/12/16</td>
</tr>
<tr>
<td>coordinating users between systems</td>
<td>De Joe Reid</td>
<td>33</td>
<td>12/12/16</td>
</tr>
<tr>
<td>egrep for any number of space and/or tabs</td>
<td>De <a href="mailto:iandid...@googlemail.com">iandid...@googlemail.com</a></td>
<td>1209</td>
<td>8/12/16</td>
</tr>
</tbody>
</table>
Open sources

SOCIAL MEDIA

- microblogging
- weblogs
- network
- chats
- forums
- podcasts
- community
- bookmarking
- wikis
- video
- rating
- pictures
What are the bad guys doing?
What are the bad guys doing?
What are the bad guys doing?
Know your enemy and know yourself and you can fight a hundred battles without disaster

Sun Tzu, The art of war
What to do?
Sample scenario
We need to establish our own CERT

We need security procedures, policies...

ACME, our main competitor, has its own CERT up and running

Copying is easier than creating
What is ACME CERT? What is ACME?
Sample scenario

More about ACME CERT?
Sample scenario

Migrating user’s desktop to Ubuntu

Alice Cooper
ACME CERT Chief Technology Officer
alice.cooper@acmecert.com

November, 2015
Who works there?
Who is John Smith?
Who is John Smith?
Sample scenario

Let’s build the attack...
Let’s build the attack...

Sample scenario
...and deliver it!

Dear John,
I'm Foo Bar, colleague from the Canon Photo Club Springfield group at Facebook. I'm selling a CANON EF 70-300mm Lens, almost HALF OF ITS PRICE ($800), NOT USED. The reason: these Christmas I've received two of them as a present 😊.
I attach a PDF file with the description, technical details and price, and also some pics of the lens and its bundle. As you can see, it's in PERFECT state, ready to use.
Please drop me an e-mail if you are interested; we could arrange at some place at Springfield if you want to prove the lens by yourself.

Best regards,
Foo

CANON EF 70-300mm Lens
Conclusions
Main conclusions

The enemy is listening
He wants to know what you know
Keep it to yourself

Military Intelligence Division, War Department
Office of Naval Intelligence, Navy Department
Federal Bureau of Investigation, Department of Justice
THANK YOU!