CRYPTOGEDDON

The threat level is severe.
Cyber war has begun.

SECTOR 2013

Mission Name: The Rogue CSEC Agent
Created by Todd Dow
@toddhdow, @cryptogeddon
WHAT IS CRYPTOGEDDON?

• Capture The Flag game
• An online scavenger hunt using hacker tools
• Collection of discrete, individual missions
• Use infosec tools to solve technology puzzles
CRYPTOGEDDON ORIGINS

After last year’s SecTor event, I told a friend that I wanted to see a session that fulfilled the following:

• A session that covers an entire infosec scenario
• Story-based
• Uses current tools & techniques
• Available on demand
• Cross-platform
• Repeatable & useable for education
Who is Todd Dow?

• Senior Digital Specialist at Postmedia
  – Major projects and operational optimizations

• Specialist in:
  – Information security
  – Risk management
  – IT operations

• CISA & PMP certified

@toddhdow, @cryptogeddon
TODAY’S DEMO

Mission Name:
The Rogue CSEC Agent

The Scenario:
A Communications Security Establishment Canada (CSEC) cyber security analyst has gone rogue. He has taken a large cache of top secret files that include the names and identities of several secret agents working in foreign countries. This rogue analyst has stowed these files on the internet in an encrypted format and he is now threatening to share the location of the files and the decryption keys with the public.
The Scenario - con’t:
Earlier today, the CSEC cyber security analyst narrowly avoided capture at a local cyber cafe, but during his escape, he left behind a USB drive, which contained our only clue thus far.

We suspect that he was using the files on the USB drive to access his online data store.
TODAY’S DEMO

Your Assignment:
Use the contents of the USB drive to recover the data cache and provide us with an inventory of the agent identities so that we can extract those agents before they are harmed.
TOOLS FOR TODAY’S DEMO

- md5
- TrueCrypt
- Kali Linux
- fcrackzip
- Text editor
- Amazon ec2
- Ssh
- Wordpress
- Nmap
- WebSlayer
- Nessus
- Binary to Text converter
- Openssl

@toddhdow, @cryptogeddon

Cryptogeddon missions utilize diverse information technology tools to accomplish the tasks included in each mission.
STEP 1 (OF 10)

Download the first piece:


- This will get you a download that appears to be an encoded file (the .enc extension suggests this as well).
STEP 2 (OF 10)

Verify md5 hash:
Command:
> md5 Sector2013.enc

Result = 3b9a70b0e2659b044f7d7e7144b2887d
STEP 3 (of 10)

Use TrueCrypt to open the file using this password:
• CSEC2013.

You should now have 1 unencrypted file entitled:
• Files.zip
Unzip an encrypted zip file:

- Install Kali Linux
- Use fcrackzip:
  
    → fcrackzip -buv -c a -l 5 files.zip
    
    → PASSWORD FOUND!!!!: pw == seven

- Two files are in the unzipped folder:
  
    → oasis.jpg
    
    → trees.jpg
STEP 5 (of 10)

Analyze the files:
oxas.jpg:
• doesn’t appear to be an image file
• Add .txt to the end;
• “BEGIN RSA PRIVATE KEY”
grapes.jpg:
• Try the same .txt extension;
• “Use Amazon ami-9d3667f4”
STEP 6 (of 10)

Open ami-9d3667f4 on Amazon Web Services:
1. Understand Amazon’s Free Tier
2. Sign up, then go to:

https://console.aws.amazon.com/ec2/
STEP 6 (of 10) – con’t

Open ami-9d3667f4 on Amazon Web Services:

3. Click the “Launch Instance” button.

4. Select the “Quick Launch Wizard”, select “More Amazon Machine Images” and click “Continue”.

@toddhdow, @cryptogeddon

Cryptogeddon Sector 2013 Edition

15
Open ami-9d3667f4 on Amazon Web Services:

5. Put “ami-9d3667f4” in the search box.

6. Click on the Cryptogeddon Mission and click “Continue”.

7. On the resulting screen, click the “Launch” button to continue.
STEP 7 (of 10)

Get address of the server and analyze it:

1 EC2 Instance selected.

**EC2 Instance:** i-9dab97f9

e2-54-227-106-89.compute-1.amazonaws.com

<table>
<thead>
<tr>
<th>Description</th>
<th>Status</th>
<th>Checks</th>
<th>Monitoring</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduled Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPC ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source/Dest. Check</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Placement Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAM Disk ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Pair Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Alarm Status:** none

**Security Groups:** cg-sector-2013, view rules

**State:** running

**Owner:** 345389117297

**Subnet ID:** -

**Virtualization:** paravirtual

**Reservation:** r-0b76926e

**Platform:** -

**Kernel ID:** aki-88aa75e1

**AMI Launch Index:** 0

@toddhdow, @cryptogeddon
Get address of the server and analyze it:

> nmap 54.227.106.89

Results = multiple ports, including:

• 22 / ssh
• 80 / http
• 3306 / mysql

What might this be? A Web Server?
Get address of the server and analyze it:
• Use WebSlayer to identify any subdirectories.
• Use dictionary list from /usr/share/wordlists/webslayer/general/common.txt.
• This will provide the following directories:
  – http://ec2-54-227-106-89.compute-1.amazonaws.com/
  – http://ec2-54-227-106-89.compute-1.amazonaws.com/blog/
STEP 8 (of 10)

Analyze the /blog/ URL:

• Poorly themed blog, performs slow. What’s wrong with it?

• You need to change the site URL:
  
  http://codex.wordpress.org/Changing_The_Site_URL

• Add these lines to the wp-config.php file:
  
  – define('WP_HOME','http://example.com');
  – define('WP_SITEURL','http://example.com');
Analyze the blog:
• The main blog post looks interesting.
• Might there be more content within the blog admin panel?
• How would we log in?
• Binary to text converter
• Login with those credentials at:
STEP 9 (of 10)

Analyze the blog:

• See “All Posts” – draft post entitled “If you can read this…”

• The draft post references a file called agentlist.enc

• Use openssl to decrypt agentlist.enc with the same password used earlier.

> openssl des3 -d -salt -in agentlist.enc -out agentlist.txt
STEP 10 (of 10)

Unencrypt the file `agentlist.enc`:

```shell
$ openssl des3 -d -salt -in agentlist.enc -out agentlist.txt
```

Read the resulting `agentlist.txt` file.
RECAP OF THE STEPS

1. Download the first piece
2. Verify the md5 hash
3. Open the file using TrueCrypt
4. Unzip encrypted zip file using fcrackzip
5. Analyze the files
6. Open Amazon ec2 instance
7. Get address of ec2 instance and analyze it
8. Analyze the /blog/ URL
9. Analyze the blog
10. Unencrypt agentlist.enc using openssl
RECAP OF THE TOOLS

- md5
- TrueCrypt
- Kali Linux
- fcrackzip
- Text editor
- Amazon ec2
- Ssh
- Wordpress
- Nmap
- WebSlayer
- Nessus
- Binary to Text converter
- Openssl

Cryptogeddon missions utilize diverse information technology tools to accomplish the tasks included in each mission.
CRYPTOGEDDON

The threat level is severe.
Cyber war has begun.

SECTOR 2013

Mission Name: The Rogue CSEC Agent
Created by Todd Dow
@toddhdow, @cryptogeddon