CRYPTOGEDDON

The threat level is severe.
Cyber War has begun.

Mission Name:
The Rogue CSEC Agent

Created by Todd Dow

CRYPTOGEDDON
Online Cyber Security War Game

Sector 2013 Edition: The Rogue CSEC Agent

By Todd Dow

Cryptogeddon Sector 2013 Edition: The Rogue CSEC Agent

Copyright © 2013, Todd Dow

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means - electronic, mechanical, photocopy, recording or any other - except for brief quotations embedded in critical articles and reviews, without the prior written permission of the author.

All of the characters, companies and incidents mentioned in this book are fictitious. Any resemblance to actual persons living or dead is purely coincidental.

HACK RESPONSIBLY

Cryptogeddon is a game. It is a simulation that is for education and entertainment purposes only. Under no circumstances do we encourage or condone using information security tools or techniques for malicious or illegal activities.

For more information and to find additional missions, visit:
cryptogeddon.com, @cryptogeddon
or
toddhdow.com

1/ Synopsis

A Communications Security Establishment Canada (CSEC) cybersecurity 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.

Earlier today, the CSEC cybersecurity analyst narrowly avoided capture at a local cyber cafe, but during his escape, he left behind a USB drive, which contained our only clues thus far:

- files.zip

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

Your assignment is to 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.

2/ Objectives

Your objectives are as follows:

1. Make sense of the files included on the USB drive;
2. Identify the location of the data cache;
3. Extract the data from the cache;
4. Decrypt the data and obtain the identities of the agent(s);

3/ Asset List

To begin this exercise, you will need to download the initial files found on the USB drive. These files can be retrieved here:
URL: http://download.cryptogeddon.com/Sector2013.enc
md5 hash: 3b9a70b0e2659b044f7d7e7144b2887d
Use TrueCrypt to open the file using the password CSEC2013.

Ensure that your uncompressed initial download includes the following files:

- files.zip

Additional assets will be discovered as you work through this scenario. Sufficient details will be provided within the context of the scenario to identify the location of and obtain these additional assets. If you find yourself stuck and unable to obtain a particular asset, please review the solution section of this document. If you are still unable to obtain any additional assets, please post your question as a comment on the "Cryptogeddon - FAQ" page on cryptogeddon.com. Support will be provided on a regular basis.

4/ Support Services

Questions pertaining to installation of any of the above tools can be found at the various vendor websites or through numerous other helpful resources (When in doubt, trust Google). Product links are included in the solution (where pertinent), along with specific instructions where it makes sense. There will be a certain level of assumed knowledge and/or a basic expectation of research on the reader's part, but I will do my best to provide the exact steps required to complete each step of the mission.

Questions pertaining to the quality and accuracy of this document, obtaining or interacting with the assets used in this scenario and any other issues pertaining to this specific scenario can be directed to the "Cryptogeddon - FAQ" page on cryptogeddon.com. Support will be provided on a regular basis.

STOP READING - SPOILER ALERT!

The following pages contain an inventory of tools and the complete solution to this mission.

Feel free to continue reading, but keep in mind that if you want to solve this mission without assistance, then you should turn back until you've completed all of the objectives.

Don't say I didn't warn you!

TO BE CONTINUED

This Mission Pack is being released as part of Sector 2013. The tool list and solution will be revealed during my SecTor talk entitled, “CRYPTOGEDDON Sector 2013 Edition: Online Cyber Security War Game” on Wednesday October 9, 2013.

If you can’t make it to that session, don’t worry. I will be updating this document after the conference to include the tool list and the solution. You will receive an email when this document is updated.

Good luck and f you do solve this puzzle in advance of my session talk, please tweet @cryptogeddon to let me know.

7/ Keeping in Touch and Feedback

Thank you for participating in this Cryptogeddon Mission Pack. Your ongoing interest in and feedback for Cryptogeddon is valuable to help improve the quality of future missions. There are two ways for you to keep in touch and offer feedback:

First, you can sign up for our Cryptogeddon mailing list. Subscribing to the mailing list ensures that you receive the latest news and updates pertaining to Cryptogeddon, including new mission pack releases and special announcements. To sign up for the mailing list, go to http://cryptogeddon.com and enter your email address in the “Newsletter” box at the bottom right hand corner of any page on the website.

Second, you can offer feedback. Your feedback can help shape future missions, the format of the mission packs and it can increase the overall quality of the Cryptogeddon experience. I encourage you to provide your feedback, no matter how big or small, to help improve this product. You can provide your feedback at any time by using one of these three methods:

1. Submit your feedback on the FAQ page: http://cryptogeddon.com/blogs/news/9120555-faq
2. Complete a feedback survey: http://www.surveymonkey.com/s/V8NHVYX
1. Email me directly at toddhdow [at] gmail [dot] com;

Thanks again for participating in this mission pack and I look forward to hearing from you in the near future to either offer feedback and/or to sign up for the mailing list.

Talk soon!

Todd