Malware Analysis Project 3
CSCI 4976 - Fall 2015
Malware Analysis

FROM: unknown
TO: malwarefall2015@gmail.com

This requires some explaining. Let me begin at the beginning.
The year was 2004. I was a little punk in South Dakota. After we finished math class, Jenny invited me to a party she was throwing down. I wasn't really sure if I wanted to go, after all I would rather spend my Saturday on playing world of warcraft... but nonetheless, I really liked her, so I said sure.
I wish I never agreed to this.
Saturday night, Jenny and some friends and I were having some youthful fun. Froman got some cupcakes out he made for all of us, and before we definitely enjoyed that. I looked into Jenny's eyes, she looked at mine, or something... but then I noticed a gleaming ray of light coming out the window. I'm paranoid as a coyote, thinking like -- oh no, it's the police, we're so screwed. I look out the window, and the ray of light dissappears, Froman and Jenny start laughing at me. I'm like, whatever. Suddenly we all heard some rumbling, I look out the window again, and suddenly my body is smashing through the frame like a ragdoll upwards towards the sky. I couldn’t comprehend how high up I was.
This is what I can remember so far...
I woke up naked on this cold metal table, just what feels like a few hours ago. And these... green people... are staring at me.
They walk me over to a room with an old CRT screen. They tell me that I have three conditions.
ONE, I can only send one message per 10 years, and receive one message per 10 years, with and from any email address I want from any time period. So, they have like a time travelling email system, or something about the speed of light. And I can't download anything particularly large.
TWO, I am to live in this room for the rest of my life, with this one computer... running windows XP.
THREE... the only application I can run on this computer is some game they gave me. They want to test their hypothesis that people can survive by purely on video games. AND NO DONT ASK ME IF I KNOW PYTHON I CANT PROGRAM. THATS PROBABLY WHY THEY CHOSE ME.
Well, it's been days, and I finally succumbed to opening the game... but... it says I need a CD!
Please help. There's no hope for me, the only entertainment I have is this message box telling me I need the original CD. The aliens tell me I can try to brute force it… PLEASE I'M LIKE 14 MILLION LIGHT YEARS AWAY I NEED SOME HACKER TO CRACK IT FOR ME.

- Resident 7326

----------Courtesy of xerphn----------

You feel a burning desire to help this kid out, plus, you **have** to see what crazy game the aliens gave him. Since he can only receive one message every 10 years, it has to count. You decide to include as much information as possible, in case something doesn't work quite right he'll have a chance to figure it out on his own.
You must include the following in your message…

1. A detailed write-up containing your process, troubles you encountered, and how you got around them. If your code doesn't work this'll be the kids only hope.
2. One or more scripts for automating the unpacking process, plus any new tools you used. He should be able to execute a program or two when the aliens aren't looking.
3. The final, unpacked, working, game executable, with the CD check patched out.
4. A creative message embedded and visible in the game so he knows who to set up deposit accounts for, he can time travel, right?

Rubric

Below is the point breakdown for what is expected of you in this assignment.

Pts	Title	Description
5	**README**	Make sure I know what your scripts/tools are for, how to use them, and in what order.This can be plain text file.
10	**Unpacked and patched**	Each stage of the unpacking process, patching the CD check, and adding credz/greetz are each worth several points.
20	**Automation**	You have one or more scripts that are able to automate the unpacking and patching process. You will be graded on their completeness and ease of use. You may use whatever language/tools you like (Ollyscript, python, etc).
20	**Report**	This should be similar to your previous writeups, as well as the example given for project 1. Detail your unpacking process, what worked, what didn't. What problems you encountered, and how you solved them. Screenshots are a must.
5	**Anti-Analysis**	You will receive 1 point (up to 5) for each anti-analysis technique you locate, identify and describe in your report. Checking every box in phant0m won't get you credit here.
60	**Total**	