Carson Hedrich
CS 3235
December 5, 2024

Forensics Project Report

Verdict

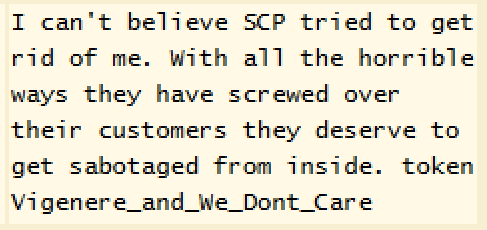
Based on the evidence collected, George is guilty of several crimes, including violating the Computer Fraud and Abuse Act, membership in a criminal enterprise, intent to commit cyberterrorism.

Prior to being fired by SCP, George joined a hacker group called SabotageWorks, dedicated to "taking down" organizations/companies they have grievances with, as evidenced by a conversation found on George's hard drive in a password-protected zip folder. Additionally, a different conversation was found where George contacted an individual in the hacker group expressing a desire to join, as well as a list of vulnerable hosts (implied to be within SCP). The individual, "Shepard" then gave a link to weratewasps.buzz/info.pdf.

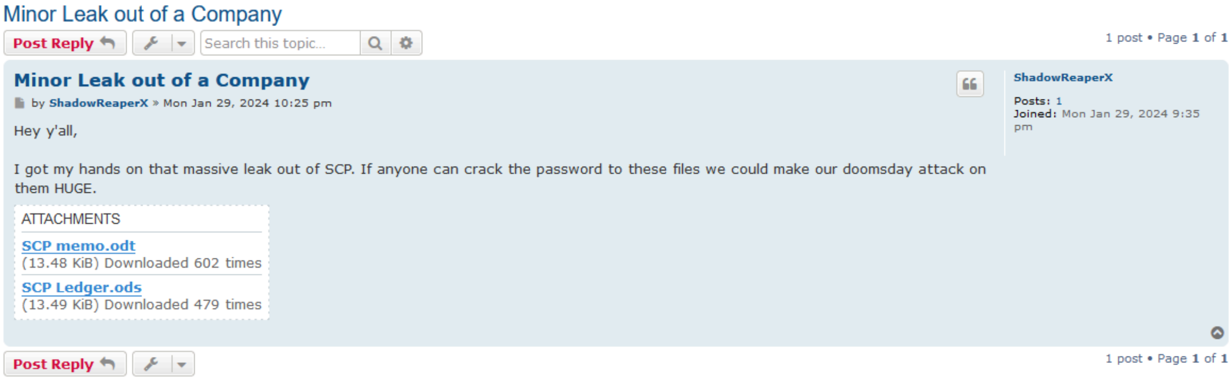
This same pdf was found on George's hard drive, and once cracking the password to it, it was revealed that weratewasps.buzz was actually a secret hub for the hacker group's communications. Once we used George's sslkey.log to find the specific user-agent to reveal this secret hub, we discovered the same conversation that was stored in the previously mentioned zip folder.

After George was fired from SCP, he became very angry, as detailed by his message to this secret hub: "POIJWEF:OJISF:OIJSDF*@#$* I GOT FIRED. THAT UNGRATEFUL COMPANY FIRED ME. AFTER ALL THE WORK I'VE DONE FOR THEM AND THEY LET ME GO. GAH." Then he later said: "wish me luck. todays the day. going to get back at them." With "them" suggested to be SCP.

Once authenticating our identity as George using a private key stored on his hard drive, we were provided a link to their new hub, accessible only using Tor. On this site, leaks from SCP were found, as well as a rant encoded with a Vignere cipher. Once decoded, it was revealed to be a rant, heavily implied to be written by George.



```
I can't believe SCP tried to get
rid of me. With all the horrible
ways they have screwed over
their customers they deserve to
get sabotaged from inside. token
Vigenere_and_We_Dont_Care
```



Minor Leak out of a Company

1 post • Page **1** of **1**

Minor Leak out of a Company

by **ShadowReaperX** » Mon Jan 29, 2024 10:25 pm

Hey y'all,

I got my hands on that massive leak out of SCP. If anyone can crack the password to these files we could make our doomsday attack on them HUGE.

ATTACHMENTS

SCP memo.odt
(13.48 KiB) Downloaded 602 times

SCP Ledger.ods
(13.49 KiB) Downloaded 479 times

ShadowReaperX

Posts: 1
Joined: Mon Jan 29, 2024 9:35 pm

1 post • Page **1** of **1**

Exploring different parts of George's hard drive revealed other evidence. In one file titled imsorry.mp4, an apology to his father was found, explaining that George had chosen a life of crime, he had to flee, and "Sketchy Computer People deserved it. I hope that they perish." In George's web searches, several searches like "passport for leaving us", "how can i flee to north korea", and a site called "Seek Asylum in North Korea" (dprk.asylum.com) were found. Upon attempting a SQL injection to access the site, access was rejected, and nothing further was found here.

In George's .bash_history, he was found to have cloned a git repository for a zip bomb, and he was found to have accessed a honeypot at choam.space. After brute-forcing George's login, we were able to access the files contained within, with one being an incident report from a prior breach from Breadit. This report detailed choam.space's new domains after the attack they suffered.

George was revealed to have used steganography to try and hide some of his messages. We found an image in a password-protected zip folder titled submit_to_boss titled election.jpg. Steg analysis revealed a message between two agents, both within SCP, with one highly likely being George.

George listed his hacker tools in a plaintext file named "hacker_tool_list", with the tools including hydra, steghide, and metasploit framework. Without this obvious name, these tools could have easily just been used for pen testing. However, the name suggests they were used for malicious hacking, also lending themselves to George's guilt in his cybercrimes.