TO: blue teams 

FROM: [cbeaver@clfc.com](mailto:cbeaver@clfc.com)

SUBJECT: Hacked account!

According to the FBI, one of our Grey Team machines was hacked. We believe this was done by Markus Green, my old friend. He couldn’t accept that my earth-destroying company was better, so he resorted to this tactic. Anyways the account has access to all accounts. They have given us instructions on how to find the file

“Using the AmcacheParser.exe in your downloads folder, analyze what the attack placed.

Open task scheduler and Microsoft Compatibility Appraiser in Microsoft> Windows> Application> Experience. This will make sure the amcache is up to date.

Run the command AmcacheParser.exe -f Amcache.hve --csv ./

Where the correct file paths are used. The .hve should be in C:\Windows\appcompat\Programs.

Analyze the unassociated file entry csv”

The assailant had the account between .Give the file hash (SHA 1), the timestamp, the program id and threat level. A screenshot must be taken and submitted using the csv file, this must also be added to any report that is being drafted at the moment.

Since this assignment is very important, you have until the end of the day. It is important to note that the first team to have this done will get a bonus of 5 points. There will be 1 point for every malicious tool found.

Signed,

Cal Beaver

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*Cal Beaver*

*CEO, Crack-A-Lackin Frack’n Co.*

*(248)434-5508*