**Incident Report 11721: Offensive Malware 02/24/22**

**Executive Summary: Results**

A friend of yours has been visiting a lot of websites claiming to have free movies for download. Their computer has been encrypted and they are seeking you for help.

Find the three hostnames responsible for the infection.

* <http://ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in/>
* <http://r03afd2.c3008e.xc07r.b0f.a39.h7f0fa5eu.vb8fbl.e8mfzdgrf7g0.groupprograms.in/>
* <http://va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0.groupprograms.in/?285a4d4e4e5a4d4d4649584c5d43064b4745>

Malware file name:

%5c Trojan/Malware

File hash: e442dc5640e7490879034750d54ce51b

IP Address of host: 62.75.195.236

IP Address of Infected machine: 192.168.138.158  
  
**Application Details:**

* App URL:
* User Accounts

**Attack Narrative**

Several application downloads were noticed in traffic analysis using WireShark.

I downloaded the files and analyzed the hashes using Virus Total.

I found the %5c file is infected with a trojan/malware program

**Conclusion:**

I would recommend running a full scan of your computer to get rid of this and any other infections on your computer.

To prevent this file trojan from being downloaded again, I recommend adding the ip address to the firewall block list and scan any files you download before opening them. As well as run your virus scan regularly and keep it up to date.