Fingerprinting

file sketchy.jse (tab finish)

file cs-http.exe

Get Hashes

sha256sum sketchy.jse

md5sum sketchy.jse

VirusTotal:

https://www.virustotal.com/gui/file/ffcd2ce8658392c30c9936d9262b5f758238c7d772923360fab7dc4647d4fb38

Do research

whois 185.180.199.102

grep -F "185.180.199.102" firewall.log

dig differentia.ru

whois 35.231.151.7

nmap -Pn 35.231.151.7

curl 35.231.151.7

(Spreadsheet Demo)

Download threat feed

wget https://rules.emergingthreats.net/blockrules/compromised-ips.txt

Build a script to do API lookups of some IPs

head iplist.txt

nano lookup-geo.sh

./lookup-geo.sh

tail ipresult.csv

Use grep to filter it

grep -v "India" ipresult\_final.csv > ipresult-OutsideIndia.csv