List the suspicious DNS (example: DNS1\_DNS2\_DNS3)

A screenshot of a computer

AI-generated content may be incorrect.

which DNS has the most http traffic with the victim

A screenshot of a computer

AI-generated content may be incorrect.

In what file format the data is being exfiltrated

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

what's the IP@ this data is being sent to



Now we need to follow http stream change show data as raw 🡪 then save as a bin file 🡪 then use binwalk -e

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

what's the malware family name

🡪LummaC2

what's the malware build date (dd-mm-yyyy)

🡪09-10-2023

what's the LID(Lumma ID)

🡪Zbbaau--Лакосте

what's the OS type and version of the infected system

🡪Windows 10 (10.0.19045)

what's the icon visible on the screenshot took from the system

A screenshot of a computer

AI-generated content may be incorrect.

what's the md5 hash value of the stealed cookies file

A screenshot of a computer

AI-generated content may be incorrect.

Save the http object exported from packet 1737 as a zip file 🡪 then extract it   
A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer code

AI-generated content may be incorrect.