The Spamhaus Project (@spamhaus@infosec.exchange)

By The Spamhaus Project

Published: 2024-10-31 · Archived: 2026-04-02 10:38:37 UTC

❗Spamhaus Malware researchers have observed a malspam distributor previously associated with Darkgate / SSLoad targeting the Ukraine audience 🇺🇦

The malspam impersonates State Tax of Ukraine, informing potential victims of "Illegal Activities" on their properties.

➡️ The emails have a .zip attachment containing two .html forms / files, mimicking a CAPTCHA page, employing the "ClickFix" technique to prompt users to execute the malicious payload.

➡️ The infection chain’s final payload is a malicious Windows executable with info-stealing and external payload-downloading capabilities.

➡️ Encrypted command-and-control servers, including decoy ones, are embedded within the binary.

🤖 C2:
hxxp://178.215.224.252
hxxp://178.215.224.74
hxxp://178.215.224.161
hxxp://178.215.224.251
hxxp://178.215.224.65

🔥 IOC (ThreatFox): https://threatfox.abuse.ch/browse/tag/P442/

Are you seeing this too?

Source: https://infosec.exchange/@spamhaus/113402246487904714