BELLHOP (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:39:48 UTC

BELLHOP

Actor(s): Anunak

• BELLHOP is a JavaScript backdoor interpreted using the native Windows Scripting Host(WSH).
After performing some basic host information gathering, the BELLHOP dropper downloads a base64-encoded blob of JavaScript to disk and sets up persistence in three ways:
• Creating a Run key in the Registry
• Creating a RunOnce key in the Registry
• Creating a persistent named scheduled task
• BELLHOP communicates using HTTP and HTTPS with primarily benign sites such as Google Docs and PasteBin.

References

There is no Yara-Signature yet.
