SimpleTea (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:37:04 UTC

SimpleTea

aka: PondRAT, SimplexTea

Actor(s): Lazarus Group

SimpleTea for Linux is an HTTP(S) RAT.

It was discovered in Q1 2023 as an instance of the Lazarus group's Operation DreamJob campaign for Linux. It was a payload downloaded in an execution chain which started with an HSBC-themed job offer lure. It shared the same C&C server as payloads from the 3CX incident around the same time.

It’s an object-oriented project, which does not run on Linux distributions without a graphical user interface, and decrypts its configuration from /home/%user%/.config/apdl.cf using 0x7E as the XOR key. It uses AES-GCM for encryption and decryption of its network traffic.

It supports basic commands that include operations on the victim’s filesystem, manipulation with its configuration, file exfiltration (via ZIP archives), and the download and execution of additional tools from the attacker’s arsenal. The commands are indexed by 16-bit integers, starting with the value 0x27C3.

SimpleTea for Linux seems like an updated version of BadCall for Linux, rewritten from C to C++, as there are similarities in class names and function names between the two.

References

There is no Yara-Signature yet.
