Tiger RAT (Malware Family)

By Fraunhofer FKIE

This is third stage backdoor mentioned in the Kaspersky blog, "Andariel evolves to target South Korea with ransomware". The third stage payload was created via the second stage payload, is interactively executed in the operation and exists in both x64 and x86 versions. Most of them use Internet Explorer or Google Chrome icons and corresponding file names to disguise themselves as legitimate internet browsers. The malware decrypts the embedded payload at runtime. It uses an embedded 16-byte XOR key to decrypt the base64 encoded payload. The decrypted payload is another portable executable file that runs in memory. Before getting decrypted with a hardcoded XOR key, the backdoor also checks for sandbox environment.
The backdoor has some code overlap with a know malware family PEBBLEDASH, attributed to Lazarus/LABYRINTH CHOLLIMA.

▶ [TLP:WHITE] win_tiger_rat_auto (20251219 | Detects win.tiger_rat.)
