Retefe (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 02:05:49 UTC

Retefe is a Windows Banking Trojan that can also download and install additional malware onto the system using Windows PowerShell. It's primary functionality is to assist the attacker with stealing credentials for online banking websites. It is typically targeted against Swiss banks. The malware binary itself is primarily a dropper component for a Javascript file which builds a VBA file which in turn loads multiple tools onto the host including: 7zip and TOR. The VBA installs a new root certificate and then forwards all traffic via TOR to the attacker controlled host in order to effectively MITM TLS traffic.

▶ [TLP:WHITE] win_retefe_auto (20251219 | Detects win.retefe.)
