# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:58:14 UTC



## Tool: CredRaptor

| | |
|---|---|
| Names | CredRaptor |
| Category | Malware |
| Type | Credential stealer |
| Description | (ESET) After successful compromise of the network, attackers use various malicious tools in order to collect passwords, allowing them to subsequently perform a lateral movement within the compromised LAN.<br><br>A string, that contains a PDB-path to debug symbols, suggests one such tool was named CredRaptor by the attackers. This tool collects saved passwords from various browsers such as Google Chrome, Internet Explorer, Mozilla Firefox, and Opera. |
| Information | <https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.credraptor> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:CredRaptor> |

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

### All groups using tool CredRaptor

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | TeleBots | | 2015-Oct 2020 | |

*1 group listed (1 APT, 0 other, 0 unknown)*

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c076facc-c733-4ff3-8a62-450dd426fcea