# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:12:49 UTC



## Tool: DRIFTPIN

| | |
|---|---|
| Names | DRIFTPIN<br>Toshliph<br>Spy.Agent.ORM |
| Category | Malware |
| Type | Reconnaissance, Backdoor, Info stealer |
| Description | Driftpin is a small and simple backdoor that enables the attackers to assess the victim. When executed the trojan connects to a C&C server and receives commands to grab screenshots, enumerate running processes and get information about the system and campaign ID. |
| Information | <https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html><br><https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf><br><https://www.welivesecurity.com/2015/09/08/carbanak-gang-is-back-and-packing-new-guns/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.driftpin> |

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

### All groups using tool DRIFTPIN

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Carbanak, Anunak | | 2013-Apr 2023 | |

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

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5237bab9-26a6-4f50-9d15-ecd3d9bdb811