# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:06:13 UTC



## Tool: DNSpionage

| | |
|---|---|
| Names | DNSpionage<br>Agent Drable<br>AgentDrable |
| Category | Malware |
| Type | Backdoor |
| Description | (Talos) Based on this actor's infrastructure and TTPs, we haven't been able to connect them with any other campaign or actor that's been observed recently. This particular campaign utilizes two fake, malicious websites containing job postings that are used to compromise targets via malicious Microsoft Office documents with embedded macros. The malware utilized by this actor, which we are calling 'DNSpionage,' supports HTTP and DNS communication with the attackers.<br><br>In a separate campaign, the attackers used the same IP to redirect the DNS of legitimate .gov and private company domains. During each DNS compromise, the actor carefully generated Let's Encrypt certificates for the redirected domains. These certificates provide X.509 certificates for TLS free of charge to the user. We don't know at this time if the DNS redirections were successful. |
| Information | <https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html><br><https://www.us-cert.gov/ncas/alerts/AA19-024A><br><https://blog-cert.opmd.fr/dnspionage-focus-on-internal-actions/><br><https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/><br><https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html><br><https://www.lastline.com/labsblog/threat-actor-cold-river-network-traffic-analysis-and-a-deep-dive-on-agent-drable/><br><https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.dnspionage> |

| | |
|---|---|
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:DNSpionage> |

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

### All groups using tool DNSpionage

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Cold River | | 2019-Jan 2025 | |
| | DNSpionage | | 2019-Apr 2019 | |
| | OilRig, APT 34, Helix Kitten, Chrysene | | 2014-Sep 2024 | |

*3 groups listed (3 APT, 0 other, 0 unknown)*

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3b9f0a41-e890-4c2e-aacb-fab6def66f87