# LevelBlue - Open Threat Exchange

By CyberHunter_NL

Archived: 2026-04-05 19:54:37 UTC

- 841 Subscribers

- 122 Subscribers

## Query Registry, Technique T1012 - Enterprise | MITRE ATT&CK®

**CVE:** 1 | **URL:** 6 | **Domain:** 2 | **Hostname:** 2

Adversaries can access the Windows Registry to gather information about the operating system, configuration, and installed software, as well as to make modifications to the system's registry, according to a report published in the Security Research Institute (CTI).

- 122 Subscribers

## namer

**FileHash-MD5:** 6 | **FileHash-SHA1:** 94 | **FileHash-SHA256:** 6 | **Domain:** 6 | **Hostname:** 8

- 25 Subscribers

**tange**

**FileHash-MD5:** 6 | **FileHash-SHA1:** 94 | **FileHash-SHA256:** 6 | **Domain:** 6 | **Hostname:** 8

The full text of the report on InvisiMole, which was published by WeLive security, has been published on the BBC's News Channel and is available to view on iPlayer.

- 25 Subscribers

## invismole

**YARA:** 5 | **Domain:** 7 | **Hostname:** 5

InvisiMole has been trojanized by security researchers, who have now identified the source of the malware and used the code to access the data for the first time in its history.

- 25 Subscribers

## Winar

**FileHash-MD5:** 6 | **FileHash-SHA1:** 94 | **FileHash-SHA256:** 6 | **YARA:** 5 | **Domain:** 7 | **Hostname:** 8

The InvisiMole software is based on the two-clause BSD 2-Clause (YARA) license, provided by ESET Research, and is available to the public.

- 25 Subscribers

- 146 Subscribers

- 15 Subscribers

- 35 Subscribers

- 35 Subscribers

- 35 Subscribers

- 35 Subscribers

- 35 Subscribers

- 35 Subscribers

- 35 Subscribers

- 35 Subscribers

- 35 Subscribers

- 35 Subscribers

- 35 Subscribers

---

Source: https://otx.alienvault.com/browse/pulses?q=tag:invisimole