

# LevelBlue - Open Threat Exchange

By Superpro

Archived: 2026-04-02 11:54:22 UTC



**[Golden Chickens Unveils TerraStealerV2 and TerraLogger: New Credential Theft Tools Identified by Insikt Group](#)**

**FileHash-MD5: 17 | FileHash-SHA1: 17 | FileHash-SHA256: 18 | URL: 2 | Domain: 3**

A recent campaign led by the financially motivated group Golden Chickens (aka Venom Spider) has introduced two new malware strains: TerraStealerV2 and TerraLogger. These tools are distributed under a Malware-as-a-Service (MaaS) model and aim to compromise systems through phishing lures, often disguised as job resumes or API documentation. Payloads are embedded in .LNK, .DLL, and .EXE formats and delivered via deceptive file-sharing platforms.

- 212 Subscribers



- 840 Subscribers



### [eSentire | Unmasking VENOM SPIDER](#)

**FileHash-MD5:** 2 | **FileHash-SHA1:** 2 | **FileHash-SHA256:** 4 | **Domain:** 11

Microsoft's eSentire offers a comprehensive range of security services, including multi-signal MDR services for small and medium businesses, and a dedicated Cyber Risk Advisor for executive meeting support for business leaders.

- 840 Subscribers



**[Threat Research | FireEye Inc](#)**

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers



- 1,344 Subscribers



- 373,203 Subscribers

---

Source: <https://otx.alienvault.com/browse/pulses?q=tag:TerraRecon>