LevelBlue - Open Threat Exchange

By bd.taylor

Archived: 2026-04-06 15:17:29 UTC

Show:

All

Sort:

Recently Modified

ACTIVIDAD MALICIOSA | Relacionada con Amadey 05-05-2025

FileHash-MD5: 60 | **FileHash-SHA1:** 61 | **FileHash-SHA256:** 60 | **URL:** 5 | **YARA:** 1

If you want to create an interactive image, try Genially, a free online design and design app that lets you design, create and create interactive images for your friends, family and friends..

- 26 Subscribers

- 841 Subscribers

- 480 Subscribers

- 480 Subscribers

- 65 Subscribers

- 480 Subscribers

- 560 Subscribers

ta413

CVE: 5 | **FileHash-MD5:** 2 | **FileHash-SHA1:** 2 | **FileHash-SHA256:** 4 | **URL:** 2 | **Domain:** 10

Recorded Future’s new report on Chinese state-sponsored cyber espionage and intelligence-gathering highlights the group's persistent targeting of ethnic and religious minority communities, as well as those targeted by the Tibetan community.

- 128 Subscribers

- 841 Subscribers

- 164 Subscribers

- 258 Subscribers

- 181 Subscribers

- 354 Subscribers

Threat Profile: RedLine Infostealer

FileHash-MD5: 308 | **FileHash-SHA1:** 308 | **FileHash-SHA256:** 307 | **URL:** 54 | **Domain:** 7 | **Email:** 1 | **Hostname:** 10

information stealer, named RedLine Stealer by the author, was identified being delivered through spam email campaigns, the malware is offered for sale on Russian dark web forums and as a tiered subscription allowing threat actors to use the information stealer, subscribe at different costs and purchase different access levels. In addition to being a password stealer, RedLine has the capabilities to steal login information, autocomplete data, passwords, and credit cards information from browsers.

- 240 Subscribers

Threat Profile: RedLine Infostealer

FileHash-MD5: 308 | **FileHash-SHA1:** 308 | **FileHash-SHA256:** 307 | **URL:** 54 | **Domain:** 7 | **Email:** 1 | **Hostname:** 10

information stealer, named RedLine Stealer by the author, was identified being delivered through spam email campaigns, the malware is offered for sale on Russian dark web forums and as a tiered subscription allowing threat actors to use the information stealer, subscribe at different costs and purchase different access levels. In addition to being a password stealer, RedLine has the capabilities to steal login information, autocomplete data, passwords, and credit cards information from browsers.

- 240 Subscribers

- 354 Subscribers

- 354 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

WastedLocker (Malware Family)

A new strain of ransomware known as WastedLocker has been detected by researchers at the University of California, San Francisco and the US National Security Agency (NSSA) in the United States.

- 36 Subscribers

- 354 Subscribers

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