

LevelBlue - Open Threat Exchange

By TheNewRaikage

Archived: 2026-04-05 21:43:54 UTC

We've found 3

results for "tag:Ratsnif"

Pulses (3

)

Users (0

)

Groups (0

)

Indicators (0

)

Malware Families (0

)

Industries (0

)

Adversaries (0

)

Show:

All

Sort:

Recently Modified



[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

 Author Url

[Ratsnif - New Network Vermin from OceanLotus](#)

FileHash-MD5: 49 | **FileHash-SHA256:** 4 | **URL:** 1 | **Domain:** 6 | **Hostname:** 42

Blackberry Cylance threat researchers have analyzed the Ratsnif trojans, which offer a veritable swiss-army knife of network attack techniques. The trojans, under active development since 2016, combine capabilities like packet sniffing, gateway/device ARP poisoning, DNS poisoning, HTTP injection, and MAC spoofing.

- 374,016 Subscribers

 Author Url

- 1,344 Subscribers

Sort:

Most Pulses

Sort:

Most Members

Indicators Search

Filter by:

Reset Filters

All Time

Show expired indicators

Indicator Type

All (0)

CIDR (0)

CVE (0)

Domain (0)

Email (0)

FileHash-IMPHASH (0)

FileHash-MD5 (0)

FileHash-PEHASH (0)

FileHash-SHA1 (0)

FileHash-SHA256 (0)

FilePath (0)

Hostname (0)

IPv4 (0)

IPv6 (0)

Mutex (0)

NIDS (0)

URI (0)

URL (0)

YARA (0)

Role

Adware

Backdoor

Bruteforce

Command & Control

Delivery Email

Document Exploit

Domain Owner

Exploit Kit

Exploit Source

File Scanning

Hacking Tools

Hunting

Macro Malware

Malvertising

Malware Hosting

Memory Scanning

PCAP Scanning

Phishing

RAT

Ransomware

Scanning Host

Trojan

Unknown

Web Attack

Worm

Sort:

Recently Modified

Sort:

Name Ascending

Sort:

Ascending

Sort:

Ascending

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