

## EXTENSIVE REGIONAL THREAT INTELLIGENCE

### Leveraging RST Threat Feed in Trend Vision One™

#### Multiple CTI sources:

X/Twitter  
Telegram  
WeChat  
Github  
Sandboxes

RST Honeypot  
threat reports  
and more

#### Outstanding True Positive/ False Positive rate

#### Filtered-out noise data:

MS Updates  
CDPs  
Well-known IPs  
etc

#### Designed for:











Alert triage  
Threat Detection  
Threat Prevention  
Threat Hunting

RST Threat Feed for Trend Vision One™ delivers a daily feed of high-fidelity indicators (IP, Domain, URL, Hash) that are aggregated, filtered, enriched, cross-correlated, and ranked from hundreds of threat intelligence sources. By leveraging global threat intelligence and collecting data from diverse sources worldwide, including RST Honeypot Network, online sandboxes, numerous TI reports, social networks, and community sources, we provide a detailed view of threats specific to countries across APAC, EMEA, LATAM, NA, and other regions.

### Key benefits:

#### Regional Threat Perspective

Users gain indicators relevant to their regional threat landscape. By leveraging the internal mapping of threats to certain locations, this integration allows for automatic monitoring of threats related to a specific country or region.

Object	Risk level	Action ①	Expiration	Source	Source details	Description
 servuicpmmmander-pmmanmanderlmander...	Medium	Log	2024-09-29	User defined	API	IOC with tags: phishing
 servuicpmmmander-pmmanmanderlmander...	Medium	Log	2024-09-29	User defined	API	IOC with tags: phishing
 https://hergunavantaj.com.tr/6iocpu8t4c/ac...	High	Block / Quarantine	2024-10-06	User defined	API	IOC with tags: phishing
 bioc4remi2be.com	High	Block / Quarantine	2024-10-06	User defined	API	IOC with tags: malware. Related threats: ta569_...
 luciocastanolora09.duckdns.org	High	Block / Quarantine	2024-10-06	User defined	API	IOC with tags: malware. Related threats: remco...
 lime.pulsebiocconnect.com.tr	High	Block / Quarantine	2024-10-06	User defined	API	IOC with tags: malware
 1.r14n788iocyo5epmpy6klmejchjtzddoekjn...	Medium	Log	2024-10-05	User defined	API	IOC with tags: malware. Related threats: asynchr...
 wons36ahnufsoprdmiocc.cfd	High	Block / Quarantine	2024-10-04	User defined	API	IOC with tags: malware. Related threats: kimsuk...
 http://mortgageboss.ca/link.aspx?cl=960&l...	High	Block / Quarantine	2024-10-07	User defined	API	IOC with tags: malware
 https://delivery.attempt.failure.ebbs.co.za/p...	High	Block / Quarantine	2024-10-07	User defined	API	IOC with tags: phishing

#### Context-Enriched Indicators of Compromise (IoCs)

Indicators are enriched with contextual information, including attribution to threats, APT groups, threat types, and more.

#### Detailed Risk Scoring

Each IoC is assigned a current risk score, considering factors such as threat type, current state, source trustworthiness, frequency of occurrence, and other metrics. This detailed information assists in incident triage and incident prioritization.

Suspicious Object Details

Object type:  
Domain

Object value:  
luciocastanolora09.duckdns.org

Risk level:  
High

Action:  
Block / Quarantine

Description:  
IOC with tags: malware. Related threats: remcos\_rat

Website: <https://rstcloud.com>

Contacts: [info@rstcloud.net](mailto:info@rstcloud.net)

Trial: [trial@rstcloud.net](mailto:trial@rstcloud.net)