RST THREAT FEED

GCC THREAT LANDSCAPE

Know Before They Strike

- **Targeted threats and APT groups**
  - AvosLocker
  - Nanocore
  - *Kitten APTs
  - TigerRAT
  - APT37
  - NjRAT
- **Compliance**
  - Cybercrime and Data protection laws
  - Contries cybersecurity strategy
  - Central Bank
  - ISO and other standarts

With the rapid adoption of digital technologies, the Gulf Cooperation Council countries have become very attractive targets for cyber criminals.

All GCC countries face "traditional" cyberthreats, including ransomware, cybercriminal fraud, and hacktivism. On the other hand, the GCC has been the target of many advanced persistent threats (APTs) or state-sponsored campaigns.

These threats have targeted individual businesses, commercial organizations, and state entities. According to IBM's latest Cost of a Data Breach Report, the global cost of a data breach averaged AED27.4m for the GCC region. The most targeted industries for the GCC are financial, followed by healthcare, and then energy.

KNOWN APT AND MALWARE CAMPAIGNS AT GCC REGION:

- Conti ransomware attack through targeted region phishing
- Avos Locker campaign
- Nanocore used by APT groups to target energy, aviation, and petrochemical production
- Spread of TigerRAT
- DarkSide ransomware (RaaS) campaign
- NjRAT (also known as Bladabindi)
- MuddyWater APT group targeting victims in Middle East

Future of Cyber Threats: What to Expect

- Wide ransomware attacks
- Usage of public online resources in cyberattacks (clouds, mobile apps, web)
- The rise of destructive high-profile cyberattacks
- The rise of APT groups and hack-and-leak attacks

Website: https://rstcloud.com

Contacts: Anna Mikhaylova anna.mikhaylova@rstcloud.net

General Inquires: info@rstcloud.net

Samples: https://github.com/rstcloud/rstthreats/tree/master/feeds/full

RST THREAT FEED

AGGREGATION. FILTERING. ENRICHMENT. SCORING

Consolidate knowledge from diverse threat intelligence sources in one convenient service

- **More than 260 TI sources**
  - Twitter
  - Pastebin
  - Github
  - Sandboxes
  - RST Cloud honeypot etc
- **More than 90 sources of TI reports**
- **Social media analysis**
- **Integration with all popular SIEM, SOAR, NGFW, TIP solutions**

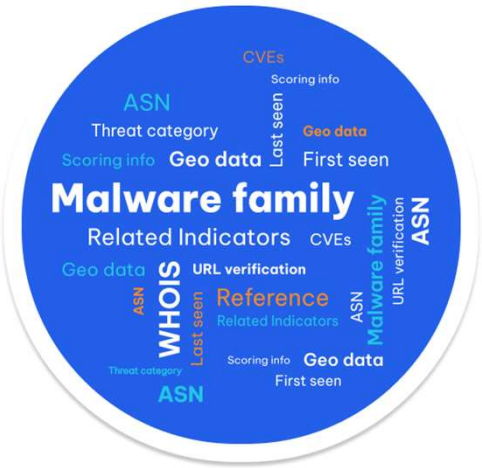
Numerous publicly available TI sources form a massive knowledgebase of up-to-date threats that is independently updated and maintained by professionals worldwide as a part of the global cybercommunity. Dozens of TI reports, tweets and posts from researchers and enthusiasts around the world provide actual, accurate, and valuable information about cyber threats and adversaries. The issue is that all of this information is unstructured, unverified, and unrelated.

RST Threat Feed consolidates all that data, verifies it piece by piece, and enriches it with context and relationships. For the following indicator types: **IP, Domain, URL, and Hash (MD5, SHA1, SHA256)**, the feed provides collected, normalized, filtered, enriched and scored IoCs from the most valuable TI sources.

KEY BENEFITS:

- Great coverage (**numerous TI sources** and extensive **honeypot** network)
- Outstanding **True Positive/False Positive rate**
- **Filtered-out noise data** (MS Updates, CDPs, Well-known IPs, etc.)
- **Indicator ranking** to focus on the most actual and dangerous threats
- **Rich contextual information** for every IoC

RST Cloud Threat Intelligence engine



- **Cross-verified and filtered indicators**

  More than 250k unique indicators per day
- **Full Context**

  Threat category, malware names, WHOIS, ASN, Hosting provider and many more fields
- **Scoring**

  Sets the understanding of how actual and impactful is an indicator

Website: https://rstcloud.com

Contacts: Anna Mikhaylova anna.mikhaylova@rstcloud.net

General Inquires: info@rstcloud.net

Samples: https://github.com/rstcloud/rstthreats/tree/master/feeds/full

RST THREAT FEED

IP. DOMAIN. URL. HASH

RST Threat Feed covers multiple IoCs types to detect and prevent all sorts of cyber attacks

- **More than 250 000 IoCs per day**
- **Threat attribution**
- **Context parcing and enrichment**
- **Comprehensive filtering methodology (reducing FP Rate)**
- **Industry tag**

Threat intelligence, distributed at the level of legislation, is a world practice, and it is applied all over the world. This is a trend in the GCC region too. Development of actionable intelligence from the threats analysis, incident and vulnerability data, approved and required by such regulators as TRA and Central Bank of Bahrain, CITRA in the National Cyber Security Strategy of the State of Kuwait, Qatar National Center for Information Security, UAE Telecommunications Regulatory Authority, and others.

RST Cloud use a combination of numerous external sources and own proprietary methods to consistently and reliably collect indicators of compromises (IoC) and their context. This helps cybersecurity professionals more effectively assess the threat level of indicators and decide on appropriate courses of action quicker.

To help reduce the occurrence of false positives and false negatives, our verification engine filters out noise data that is not relevant to threat analysis. This helps to shorten investigation time and increase the efficiency of threat analysis by focusing on the most reliable and actionable indicators. By verifying the validity of IoCs, our verification process helps cybersecurity professionals more accurately assess the threat level of indicators and make more informed decisions about how to respond to potential threats.

	Description	Benefits
IP Address Reputation	List of IP Addresses that are known to be used by cyber criminals (for example, C2 servers)	Gives undestanding if your networks are hacked already or not, detects participations of your assets in botnets, etc
Malicious Domains	A list of malicious Domains	Used to detect or prevent phishing, malware, data exfiltration, ransomware
Malicious URL	A list of malicious URLs	Detect or prevent actions to download malicious content or visit phishing resources
Malware File Hashes	List of malware files hashes (MD5, SHA1, SHA256)	Detect and prevent Ransomware, Trojans, Spyware, Keyloggers, RAT etc

Website: https://rstcloud.com

Contacts: Anna Mikhaylova anna.mikhaylova@rstcloud.net

General Inquires: info@rstcloud.net

Samples: https://github.com/rstcloud/rstthreats/tree/master/feeds/full

RST THREAT FEED

MALWARE. PHISHING. RANSOMWARE. ATTACKS

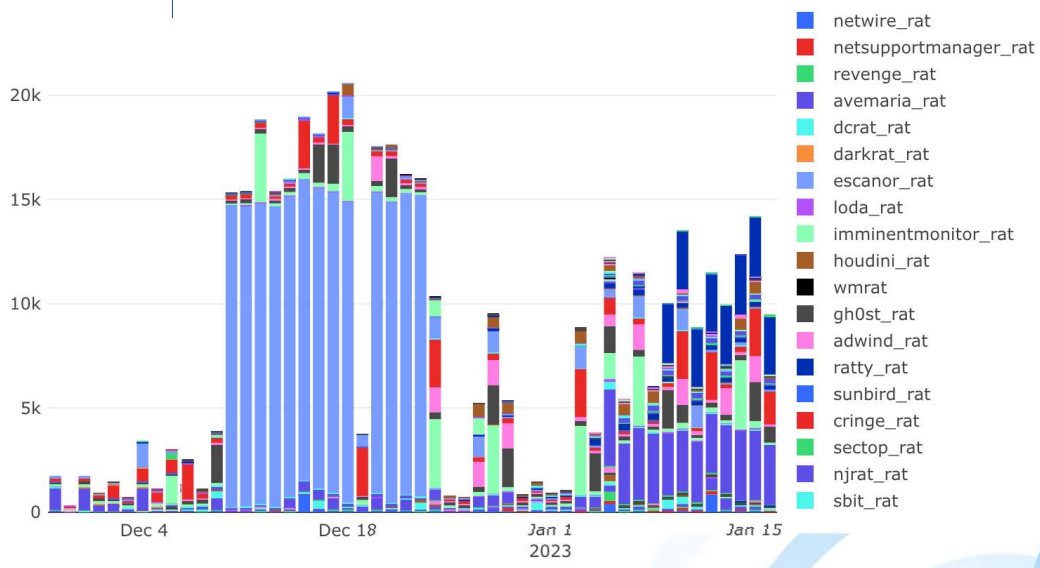
Get global threat intelligence context from RST Cloud

- **More than 4000 threat actors and malware types in the database**
- **More than 26 threat categories, incl malware types**
  - spyware
  - keylogger
  - backdoor
  - trojan
  - dropper
  - rat
  - rootkit
  - ransomware
  - stealer etc

Many indicators come with little or no context, which can make it challenging for cybersecurity professionals to determine the appropriate course of action. This can lead to extra work as they try to assess the threat level of indicators and decide whether to action them or further investigate potential threats.

OUR ENRICHMENT PROCESS ADDS THREAT CONTEXT TO INDICATORS:

- Threat category (e.g. phishing, malware, ransomware)
- Malware family (e.g. Emotet, Trickbot, Ryuk)
- Common Vulnerabilities and Exposures (CVE)
- Threat actors (e.g. APT groups, cybercrime organizations)
- Toolkits and malicious frameworks (e.g. alfashell, aspshell, Metasploit, Mimikatz)



Website: https://rstcloud.com

Contacts: Anna Mikhaylova anna.mikhaylova@rstcloud.net

General Inquires: info@rstcloud.net

Samples: https://github.com/rstcloud/rstthreats/tree/master/feeds/full

RST THREAT FEED

AGGREGATION. FILTERING. ENRICHMENT. SCORING

Consolidate knowledge from diverse threat intelligence sources in one convenient service

- **Ready-to-use integration with**
  - Splunk
  - Palo Alto XSOAR
  - IBM Qradar
  - FortiNet
  - Cisco
  - Elastic
  - ArcSight
  - LogPoint
  - MISP
  - OpenCTI
- **IoC Lookup API**
- **Whois API**
- **TI Report Hub API**

RST Threat Feed is a subscription-based service that delivers indicators of compromise collected, aggregated, filtered, and scored from hundreds of threat intelligence sources.

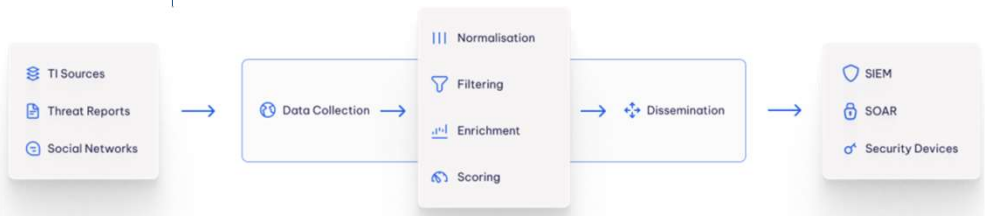
Our mission is to provide cybersecurity professionals with a single, convenient service for consolidating, normalizing, enriching, filtering, and ranking all publicly available cyber threat intelligence from around the world

RST Threat Feed is available with out-of-the-box integration with the most popular SIEM, SOAR, NGFW, and TIP solutions.

RST THREAT FEED CAN BE USED THROUGH:

- API requests for full feed download
- RST Download agent for specific integrations
- API requests for specific feed (specific tags, specific score, etc)
- IoC Lookup API
- Whois API
- TI Report Hub API

RST Cloud Engine



Partners and integrations

Website: https://rstcloud.com

Contacts: Anna Mikhaylova anna.mikhaylova@rstcloud.net

General Inquires: info@rstcloud.net

Samples: https://github.com/rstcloud/rstthreats/tree/master/feeds/full