RST CLOUD
THREAT INTELLIGENCE

RST CTI ASSISTANT

INSTANT AND INTELLIGENT CTI ADVISOR THAT NEVER SLEEPS

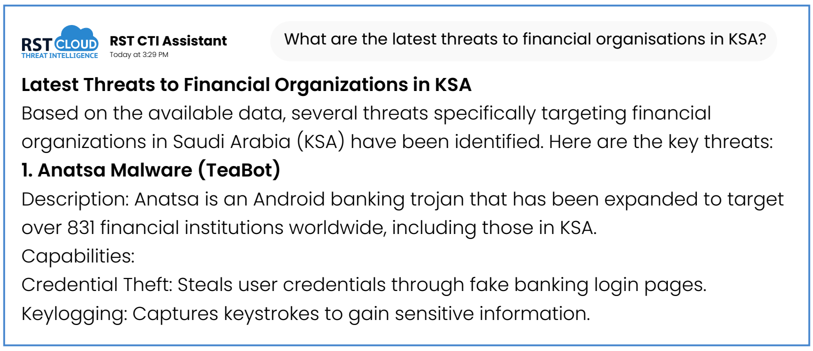
Ask any CTI question whenever needed, across any topic: the evolving threat landscape, threat actors and malware profiles, detailed TTPs, and relevant indicators.

Powered by RST Cloud's extensive threat intelligence knowledge base, this AI-driven retrieval augmented generation (RAG) assistant serves as your on-demand CTI advisor. This OpenAI-compatible LLM API delivers clear, accurate, and actionable responses to support fast and confident threat intelligence decision-making.

What threats target in finance in KSA?
Give me TTPs for DragonForce
What do you know about this IP?
Which files are created by this malware?

The Assistant examines relevant tactics, techniques, procedures (TTPs), indicators of compromise (IOCs), threat actor groups, malware, and various threats that impact your organisation and gives you comprehensive answer.

Our API works seamlessly with existing OpenAI clients or libraries, enabling easy integration



RST CTI Assistant Today at 3:29 PM

What are the latest threats to financial organisations in KSA?

Latest Threats to Financial Organizations in KSA

Based on the available data, several threats specifically targeting financial organizations in Saudi Arabia (KSA) have been identified. Here are the key threats:

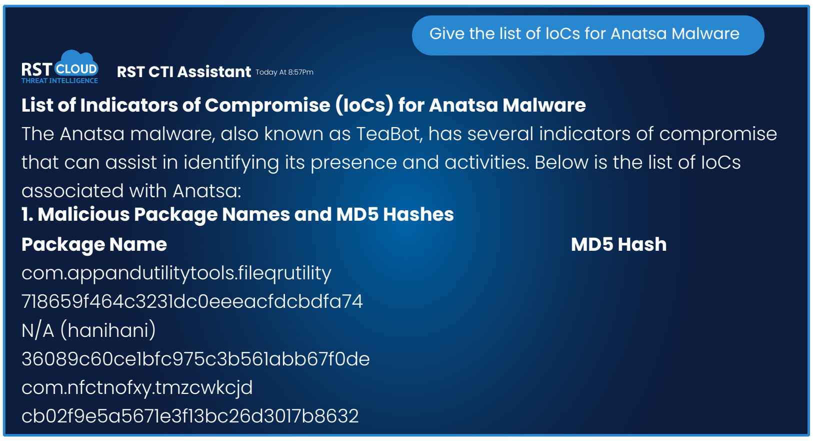
1. Anatsa Malware (TeaBot)

Description: Anatsa is an Android banking trojan that has been expanded to target over 831 financial institutions worldwide, including those in KSA.

Capabilities:

Credential Theft: Steals user credentials through fake banking login pages.

Keylogging: Captures keystrokes to gain sensitive information.



Give the list of IoCs for Anatsa Malware

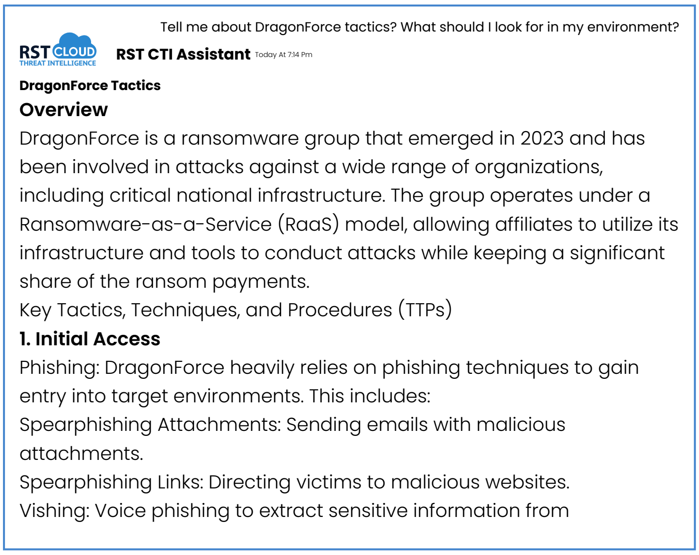
RST CTI Assistant Today At 8:57Pm

List of Indicators of Compromise (IoCs) for Anatsa Malware

The Anatsa malware, also known as TeaBot, has several indicators of compromise that can assist in identifying its presence and activities. Below is the list of IoCs associated with Anatsa:

1. Malicious Package Names and MD5 Hashes

Package Name **MD5 Hash**
com.appandutilitytools.fileqrutility
718659f464c3231dc0eeeacfdcbdfa74
N/A (hanihani)
36089c60ce1bfc975c3b561abb67f0de
com.nfctnofxy.tmzcwkcjd
cb02f9e5a5671e3f13bc26d3017b8632



Tell me about DragonForce tactics? What should I look for in my environment?

RST CTI Assistant Today At 7:14 Pm

DragonForce Tactics

Overview

DragonForce is a ransomware group that emerged in 2023 and has been involved in attacks against a wide range of organizations, including critical national infrastructure. The group operates under a Ransomware-as-a-Service (RaaS) model, allowing affiliates to utilize its infrastructure and tools to conduct attacks while keeping a significant share of the ransom payments.

Key Tactics, Techniques, and Procedures (TTPs)

1. Initial Access

Phishing: DragonForce heavily relies on phishing techniques to gain entry into target environments. This includes:

Spearphishing Attachments: Sending emails with malicious attachments.

Spearphishing Links: Directing victims to malicious websites.

Vishing: Voice phishing to extract sensitive information from

KEY BENEFITS:

Speed and Flexibility:
Provides rapid, accurate threat intelligence, adaptable to evolving threats, with no manual search or analysis required

Comprehensive Knowledge Base and Global Coverage:
Leverages a vast RST Cloud repository of global threat reports,IoCs, and intelligence, offering up-to-date insights across industries and regions

Cost-Effective:
Reduces the need for large, specialised teams and costly development by out-of-the-box automationof time-consuming threat analysis tasks, significantly lowering security costs

info@rstcloud.net
https://rstcloud.com
trial@rstcloud.net