Rotexy, Software S0411 | MITRE ATT&CK®

Archived: 2026-04-05 14:39:48 UTC

Mobile T1437 .001 Application Layer Protocol: Web Protocols

Rotexy can communicate with the command and control server using JSON payloads sent in HTTP POST request bodies. It can also communicate by using JSON messages sent through Google Cloud Messaging.[1]

Mobile T1637 .001 Dynamic Resolution: Domain Generation Algorithms

Rotexy procedurally generates subdomains for command and control communication.[1]

Mobile T1521 .001 Encrypted Channel: Symmetric Cryptography

Rotexy encrypts JSON HTTP payloads with AES.[1]

Mobile T1628 .001 Hide Artifacts: Suppress Application Icon

Rotexy hides its icon after first launch.[1]

Mobile T1629 .002 Impair Defenses: Device Lockout

Rotexy can lock an HTML page in the foreground, requiring the user enter credit card information that matches information previously intercepted in SMS messages, such as the last 4 digits of a credit card number. If attempts to revoke administrator permissions are detected, Rotexy periodically switches off the phone screen to inhibit permission removal.[1]

Mobile T1417 .002 Input Capture: GUI Input Capture

Rotexy can use phishing overlays to capture users' credit card information.[1]

Mobile T1406 Obfuscated Files or Information

Starting in 2017, the Rotexy DEX file was packed with garbage strings and/or operations.[1]

Mobile T1644 Out of Band Data

Rotexy can be controlled through SMS messages.[1]

Mobile T1424 Process Discovery

Rotexy collects information about running processes.[1]

Mobile T1636 .003 Protected User Data: Contact List

Rotexy can access and upload the contacts list to the command and control server.[1]

.004 Protected User Data: SMS Messages

Rotexy processes incoming SMS messages by filtering based on phone numbers, keywords, and regular expressions, focusing primarily on banks, payment systems, and mobile network operators. Rotexy can also send a list of all SMS messages on the device to the command and control server.[1]

Mobile T1582 SMS Control

Rotexy can automatically reply to SMS messages, and optionally delete them.[1]

Mobile T1418 Software Discovery

Rotexy retrieves a list of installed applications and sends it to the command and control server.[1]

Mobile T1426 System Information Discovery

Rotexy collects information about the compromised device, including phone number, network operator, OS version, device model, and the device registration country.[1]

Mobile T1422 System Network Configuration Discovery

Rotexy collects the device's IMEI and sends it to the command and control server.[1]

Mobile T1633 .001 Virtualization/Sandbox Evasion: System Checks

Rotexy checks if it is running in an analysis environment.[1]
