RDAT, Software S0495 | MITRE ATT&CK®

Archived: 2026-04-05 13:47:18 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

RDAT can use HTTP communications for C2, as well as using the WinHTTP library to make requests to the Exchange Web Services API.[1]

.003 Application Layer Protocol: Mail Protocols

RDAT can use email attachments for C2 communications.[1]

.004 Application Layer Protocol: DNS

RDAT has used DNS to communicate with the C2.[1]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

RDAT has executed commands using `cmd.exe /c` .[1]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

RDAT has created a service when it is installed on the victim machine.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

RDAT can communicate with the C2 via base32-encoded subdomains.[1]

.002 Data Encoding: Non-Standard Encoding

RDAT can communicate with the C2 via subdomains that utilize base64 with character substitutions.[1]

Enterprise T1001 Data Obfuscation

RDAT has used encoded data within subdomains as AES ciphertext to communicate from the host to the C2.[1]

.002 Steganography

RDAT can process steganographic images attached to email messages to send and receive C2 commands. RDAT can also embed additional messages within BMP images to communicate with the RDAT operator.[1]

Enterprise T1030 Data Transfer Size Limits

RDAT can upload a file via HTTP POST response to the C2 split into 102,400-byte portions. RDAT can also download data from the C2 which is split into 81,920-byte portions.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

RDAT can deobfuscate the base64-encoded and AES-encrypted files downloaded from the C2 server.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

RDAT has used AES ciphertext to encode C2 communications.[1]

Enterprise T1041 Exfiltration Over C2 Channel

RDAT can exfiltrate data gathered from the infected system via the established Exchange Web Services API C2 channel.[1]

Enterprise T1008 Fallback Channels

RDAT has used HTTP if DNS C2 communications were not functioning.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

RDAT can issue SOAP requests to delete already processed C2 emails. RDAT can also delete itself from the infected system.[1]

Enterprise T1105 Ingress Tool Transfer

RDAT can download files via DNS.[1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

RDAT has used Windows Video Service as a name for malicious services.[1]

.005 Masquerading: Match Legitimate Resource Name or Location

RDAT has masqueraded as VMware.exe.[1]

Enterprise T1027 .003 Obfuscated Files or Information: Steganography

RDAT can also embed data within a BMP image prior to exfiltration.[1]

Enterprise T1113 Screen Capture

RDAT can take a screenshot on the infected system.[1]
