PoetRAT, Software S0428 | MITRE ATT&CK®

Archived: 2026-04-05 13:16:53 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

PoetRAT has used HTTP and HTTPs for C2 communications.[2]

.002 Application Layer Protocol: File Transfer Protocols

PoetRAT has used FTP for C2 communications.[2]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

PoetRAT has the ability to compress files with zip.[1]

Enterprise T1119 Automated Collection

PoetRAT used file system monitoring to track modification and enable automatic exfiltration.[1]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

PoetRAT has added a registry key in the hive for persistence.[1]

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

PoetRAT has called cmd through a Word document macro.[2]

.005 Command and Scripting Interpreter: Visual Basic

PoetRAT has used Word documents with VBScripts to execute malicious activities.[1][2]

.006 Command and Scripting Interpreter: Python

PoetRAT was executed with a Python script and worked in conjunction with additional Python-based post-exploitation tools.[1]

.011 Command and Scripting Interpreter: Lua

PoetRAT has executed a Lua script through a Lua interpreter for Windows.[2]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

PoetRAT has used a Python tool named Browdec.exe to steal browser credentials.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

PoetRAT has used LZMA and base64 libraries to decode obfuscated scripts.[2]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

PoetRAT used TLS to encrypt command and control (C2) communications.[1]

Enterprise T1048 Exfiltration Over Alternative Protocol

PoetRAT has used a .NET tool named dog.exe to exiltrate information over an e-mail account.[1]

.003 Exfiltration Over Unencrypted Non-C2 Protocol

PoetRAT has used ftp for exfiltration.[1]

Enterprise T1041 Exfiltration Over C2 Channel

PoetRAT has exfiltrated data over the C2 channel.[2]

Enterprise T1083 File and Directory Discovery

PoetRAT has the ability to list files upon receiving the `ls` command from C2.[1]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

PoetRAT has the ability to hide and unhide files.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

PoetRAT has the ability to overwrite scripts and delete itself if a sandbox environment is detected.[1]

Enterprise T1105 Ingress Tool Transfer

PoetRAT has the ability to copy files and download/upload files into C2 channels using FTP and HTTPS.[1][2]

Enterprise T1056 .001 Input Capture: Keylogging

PoetRAT has used a Python tool named klog.exe for keylogging.[1]

Enterprise T1559 .002 Inter-Process Communication: Dynamic Data Exchange

PoetRAT was delivered with documents using DDE to execute malicious code.[1]

Enterprise T1112 Modify Registry

PoetRAT has made registry modifications to alter its behavior upon execution.[1]

Enterprise T1571 Non-Standard Port

PoetRAT used TLS to encrypt communications over port 143[1]

Enterprise T1027 Obfuscated Files or Information

PoetRAT has used a custom encryption scheme for communication between scripts.[1]

.010 Command Obfuscation

PoetRAT has `pyminifier` to obfuscate scripts.[2]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

PoetRAT used voStro.exe, a compiled pypykatz (Python version of Mimikatz), to steal credentials.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

PoetRAT was distributed via malicious Word documents.[1]

Enterprise T1057 Process Discovery

PoetRAT has the ability to list all running processes.[1]

Enterprise T1018 Remote System Discovery

PoetRAT used Nmap for remote system discovery.[1]

Enterprise T1113 Screen Capture

PoetRAT has the ability to take screen captures.[1][3]

Enterprise T1082 System Information Discovery

PoetRAT has the ability to gather information about the compromised host.[1]

Enterprise T1033 System Owner/User Discovery

PoetRAT sent username, computer name, and the previously generated UUID in reply to a "who" command from C2.[1]

Enterprise T1204 .002 User Execution: Malicious File

PoetRAT has used spearphishing attachments to infect victims.[1]

Enterprise T1125 Video Capture

PoetRAT has used a Python tool named Bewmac to record the webcam on compromised hosts.[1]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

PoetRAT checked the size of the hard drive to determine if it was being run in a sandbox environment. In the event of sandbox detection, it would delete itself by overwriting the malware scripts with the contents of

"License.txt" and exiting.[1]
