yty, Software S0248 | MITRE ATT&CK®

Archived: 2026-04-05 16:56:49 UTC

Enterprise T1005 Data from Local System

yty collects files with the following extensions: .ppt, .pptx, .pdf, .doc, .docx, .xls, .xlsx, .docm, .rtf, .inp, .xlsm, .csv, .odt, .pps, .vcf and sends them back to the C2 server.[1]

Enterprise T1083 File and Directory Discovery

yty gathers information on victim's drives and has a plugin for document listing.[1]

Enterprise T1056 .001 Input Capture: Keylogging

yty uses a keylogger plugin to gather keystrokes.[1]

Enterprise T1680 Local Storage Discovery

yty gathers the the serial number of the main disk volume.[1]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

yty packs a plugin with UPX.[1]

.016 Obfuscated Files or Information: Junk Code Insertion

yty contains junk code in its binary, likely to confuse malware analysts.[1]

Enterprise T1057 Process Discovery

yty gets an output of running processes using the `tasklist` command.[1]

Enterprise T1018 Remote System Discovery

yty uses the `net view` command for discovery.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

yty establishes persistence by creating a scheduled task with the command `SchTasks /Create /SC DAILY /TN BigData /TR " + path_file + "/ST 09:30"` .[1]

Enterprise T1113 Screen Capture

yty collects screenshots of the victim machine.[1]

Enterprise T1082 System Information Discovery

yty gathers the computer name, CPU information, Microsoft Windows version, and runs the command `systeminfo`.[1]

Enterprise T1016 System Network Configuration Discovery

yty runs `ipconfig /all` and collects the domain name.[1]

Enterprise T1033 System Owner/User Discovery

yty collects the victim's username.[1]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

yty has some basic anti-sandbox detection that tries to detect Virtual PC, Sandboxie, and VMware. [1]

Enterprise T1102 .002 Web Service: Bidirectional Communication

yty communicates to the C2 server by retrieving a Google Doc.[1]
