

## Pupy, Software S0192 | MITRE ATT&CK®

Archived: 2026-04-05 15:04:33 UTC

Enterprise [T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control](#)

[Pupy](#) can bypass Windows UAC through either DLL hijacking, eventvwr, or appPaths.<sup>[1]</sup>

Enterprise [T1134 .001 Access Token Manipulation: Token Impersonation/Theft](#)

[Pupy](#) can obtain a list of SIDs and provide the option for selecting process tokens to impersonate.<sup>[1]</sup>

Enterprise [T1087 .001 Account Discovery: Local Account](#)

[Pupy](#) uses PowerView and Pywerview to perform discovery commands such as net user, net group, net local group, etc.<sup>[1]</sup>

Enterprise [T1557 .001 Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay](#)

[Pupy](#) can sniff plaintext network credentials and use NBNS Spoofing to poison name services.<sup>[1]</sup>

Enterprise [T1071 .001 Application Layer Protocol: Web Protocols](#)

[Pupy](#) can communicate over HTTP for C2.<sup>[1]</sup>

Enterprise [T1560 .001 Archive Collected Data: Archive via Utility](#)

[Pupy](#) can compress data with Zip before sending it over C2.<sup>[1]</sup>

Enterprise [T1123 Audio Capture](#)

[Pupy](#) can record sound with the microphone.<sup>[1]</sup>

Enterprise [T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder](#)

[Pupy](#) adds itself to the startup folder or adds itself to the Registry key

```
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

 for persistence.<sup>[1]</sup>

[.013 Boot or Logon Autostart Execution: XDG Autostart Entries](#)

[Pupy](#) can use an XDG Autostart to establish persistence.<sup>[2]</sup>

Enterprise [T1059 .001 Command and Scripting Interpreter: PowerShell](#)

[Pupy](#) has a module for loading and executing PowerShell scripts.<sup>[1]</sup>

[.006 Command and Scripting Interpreter: Python](#)

[Pupy](#) can use an add on feature when creating payloads that allows you to create custom Python scripts ("scriptlets") to perform tasks offline (without requiring a session) such as sandbox detection, adding persistence, etc.<sup>[1]</sup>

Enterprise [T1136 .001 Create Account: Local Account](#)

[Pupy](#) can use PowerView to execute "net user" commands and create local system accounts.<sup>[1]</sup>

[.002 Create Account: Domain Account](#)

[Pupy](#) can use PowerView to execute "net user" commands and create domain accounts.<sup>[1]</sup>

Enterprise [T1543 .002 Create or Modify System Process: Systemd Service](#)

[Pupy](#) can be used to establish persistence using a systemd service.<sup>[1]</sup>

Enterprise [T1555 Credentials from Password Stores](#)

[Pupy](#) can use Lazagne for harvesting credentials.<sup>[1]</sup>

[.003 Credentials from Web Browsers](#)

[Pupy](#) can use Lazagne for harvesting credentials.<sup>[1]</sup>

Enterprise [T1114 .001 Email Collection: Local Email Collection](#)

[Pupy](#) can interact with a victim's Outlook session and look through folders and emails.<sup>[1]</sup>

Enterprise [T1573 .002 Encrypted Channel: Asymmetric Cryptography](#)

[Pupy](#)'s default encryption for its C2 communication channel is SSL, but it also has transport options for RSA and AES.<sup>[1]</sup>

Enterprise [T1041 Exfiltration Over C2 Channel](#)

[Pupy](#) can send screenshots files, keylogger data, files, and recorded audio back to the C2 server.<sup>[1]</sup>

Enterprise [T1083 File and Directory Discovery](#)

[Pupy](#) can walk through directories and recursively search for strings in files.<sup>[1]</sup>

Enterprise [T1070 .001 Indicator Removal: Clear Windows Event Logs](#)

[Pupy](#) has a module to clear event logs with PowerShell.<sup>[1]</sup>

Enterprise [T1105 Ingress Tool Transfer](#)

[Pupy](#) can upload and download to/from a victim machine.<sup>[1]</sup>

Enterprise [T1056 .001 Input Capture: Keylogging](#)

[Pupy](#) uses a keylogger to capture keystrokes it then sends back to the server after it is stopped. <sup>[1]</sup>

Enterprise [T1046 Network Service Discovery](#)

[Pupy](#) has a built-in module for port scanning. <sup>[1]</sup>

Enterprise [T1135 Network Share Discovery](#)

[Pupy](#) can list local and remote shared drives and folders over SMB. <sup>[1]</sup>

Enterprise [T1003 .001 OS Credential Dumping: LSASS Memory](#)

[Pupy](#) can execute Lazagne as well as [Mimikatz](#) using PowerShell. <sup>[1]</sup>

[.004 OS Credential Dumping: LSA Secrets](#)

[Pupy](#) can use Lazagne for harvesting credentials. <sup>[1]</sup>

[.005 OS Credential Dumping: Cached Domain Credentials](#)

[Pupy](#) can use Lazagne for harvesting credentials. <sup>[1]</sup>

Enterprise [T1057 Process Discovery](#)

[Pupy](#) can list the running processes and get the process ID and parent process's ID. <sup>[1]</sup>

Enterprise [T1055 .001 Process Injection: Dynamic-link Library Injection](#)

[Pupy](#) can migrate into another process using reflective DLL injection. <sup>[1]</sup>

Enterprise [T1021 .001 Remote Services: Remote Desktop Protocol](#)

[Pupy](#) can enable/disable RDP connection and can start a remote desktop session using a browser web socket client. <sup>[1]</sup>

Enterprise [T1113 Screen Capture](#)

[Pupy](#) can drop a mouse-logger that will take small screenshots around at each click and then send back to the server. <sup>[1]</sup>

Enterprise [T1082 System Information Discovery](#)

[Pupy](#) can grab a system's information including the OS version, architecture, etc. <sup>[1]</sup>

Enterprise [T1016 System Network Configuration Discovery](#)

[Pupy](#) has built in commands to identify a host's IP address and find out other network configuration settings by viewing connected sessions.<sup>[1]</sup>

Enterprise [T1049 System Network Connections Discovery](#)

[Pupy](#) has a built-in utility command for `netstat`, can do net session through PowerView, and has an interactive shell which can be used to discover additional information.<sup>[1]</sup>

Enterprise [T1033 System Owner/User Discovery](#)

[Pupy](#) can enumerate local information for Linux hosts and find currently logged on users for Windows hosts.<sup>[1]</sup>

Enterprise [T1569 .002 System Services: Service Execution](#)

[Pupy](#) uses [PsExec](#) to execute a payload or commands on a remote host.<sup>[1]</sup>

Enterprise [T1552 .001 Unsecured Credentials: Credentials In Files](#)

[Pupy](#) can use [Lazagne](#) for harvesting credentials.<sup>[1]</sup>

Enterprise [T1550 .003 Use Alternate Authentication Material: Pass the Ticket](#)

[Pupy](#) can also perform pass-the-ticket.<sup>[1]</sup>

Enterprise [T1125 Video Capture](#)

[Pupy](#) can access a connected webcam and capture pictures.<sup>[1]</sup>

Enterprise [T1497 .001 Virtualization/Sandbox Evasion: System Checks](#)

[Pupy](#) has a module that checks a number of indicators on the system to determine if its running on a virtual machine.<sup>[1]</sup>

---

Source: <https://attack.mitre.org/software/S0192/>