# Zeus Panda, Software S0330 | MITRE ATT&CK®

Archived: 2026-04-05 16:12:47 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Zeus Panda uses HTTP for C2 communications.[1]

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

Zeus Panda adds persistence by creating Registry Run keys.[1][2]

Enterprise T1115 Clipboard Data

Zeus Panda can hook GetClipboardData function to watch for clipboard pastes to collect.[2]

Enterprise T1059 Command and Scripting Interpreter

Zeus Panda can launch remote scripts on the victim's machine.[2]

.001 PowerShell

Zeus Panda uses PowerShell to download and execute the payload.[1]

.003 Windows Command Shell

Zeus Panda can launch an interface where it can execute several commands on the victim's PC.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Zeus Panda decrypts strings in the code during the execution process.[1]

Enterprise T1083 File and Directory Discovery

Zeus Panda searches for specific directories on the victim's machine.[2]

Enterprise T1070 .004 Indicator Removal: File Deletion

Zeus Panda has a command to delete a file. It also can uninstall scripts and delete files to cover its track.[2]

Enterprise T1105 Ingress Tool Transfer

Zeus Panda can download additional malware plug-in modules and execute them on the victim's machine.[2]

Enterprise T1056 .001 Input Capture: Keylogging

Zeus Panda can perform keylogging on the victim's machine by hooking the functions TranslateMessage and WM_KEYDOWN.[2]

.004 Input Capture: Credential API Hooking

Zeus Panda hooks processes by leveraging its own IAT hooked functions.[2]

Enterprise T1112 Modify Registry

Zeus Panda modifies several Registry keys under `HKCU\Software\Microsoft\Internet Explorer\PhishingFilter\` to disable phishing filters.[2]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

Zeus Panda obfuscates the macro commands in its initial payload.[1]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Zeus Panda encrypts strings with XOR. Zeus Panda also encrypts all configuration and settings in AES and RC4.[1][2]

Enterprise T1057 Process Discovery

Zeus Panda checks for running processes on the victim's machine.[2]

Enterprise T1055 .002 Process Injection: Portable Executable Injection

Zeus Panda checks processes on the system and if they meet the necessary requirements, it injects into that process.[2]

Enterprise T1012 Query Registry

Zeus Panda checks for the existence of a Registry key and if it contains certain values.[2]

Enterprise T1113 Screen Capture

Zeus Panda can take screenshots of the victim's machine.[2]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Zeus Panda checks to see if anti-virus, anti-spyware, or firewall products are installed in the victim's environment.[1][2]

Enterprise T1082 System Information Discovery

Zeus Panda collects the OS version, system architecture, computer name, product ID, install date, and information on the keyboard mapping to determine the language used on the system.[1][2]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

Zeus Panda queries the system's keyboard mapping to determine the language used on the system. It will terminate execution if it detects LANG_RUSSIAN, LANG_BELARUSIAN, LANG_KAZAK, or LANG_UKRAINIAN.[1]

Enterprise T1124 System Time Discovery

Zeus Panda collects the current system time (UTC) and sends it back to the C2 server.[2]

---