ZxShell, Software S0412 | MITRE ATT&CK®

Archived: 2026-04-05 13:51:43 UTC

Enterprise T1134 .002 Access Token Manipulation: Create Process with Token

ZxShell has a command called RunAs, which creates a new process as another user or process context.[2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

ZxShell has used HTTP for C2 connections.[2]

.002 Application Layer Protocol: File Transfer Protocols

ZxShell has used FTP for C2 connections.[2]

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

ZxShell can launch a reverse command shell.[1][2][3]

Enterprise T1136 .001 Create Account: Local Account

ZxShell has a feature to create local user accounts.[2]

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

ZxShell can create a new service using the service parser function ProcessScCommand.[2]

Enterprise T1005 Data from Local System

ZxShell can transfer files from a compromised host.[2]

Enterprise T1499 Endpoint Denial of Service

ZxShell has a feature to perform SYN flood attack on a host.[1][2]

Enterprise T1190 Exploit Public-Facing Application

ZxShell has been dropped through exploitation of CVE-2011-2462, CVE-2013-3163, and CVE-2014-0322.[2]

Enterprise T1083 File and Directory Discovery

ZxShell has a command to open a file manager and explorer on the system.[2]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

ZxShell can kill AV products' processes.[2]

.004 Impair Defenses: Disable or Modify System Firewall

ZxShell can disable the firewall by modifying the registry key `HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile`.[2]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

ZxShell has a command to clear system event logs.[2]

.004 Indicator Removal: File Deletion

ZxShell can delete files from the system.[1][2]

Enterprise T1105 Ingress Tool Transfer

ZxShell has a command to transfer files from a remote host.[2]

Enterprise T1056 .001 Input Capture: Keylogging

ZxShell has a feature to capture a remote computer's keystrokes using a keylogger.[1][2]

.004 Input Capture: Credential API Hooking

ZxShell hooks several API functions to spawn system threads.[2]

Enterprise T1112 Modify Registry

ZxShell can create Registry entries to enable services to run.[2]

Enterprise T1106 Native API

ZxShell can leverage native API including `RegisterServiceCtrlHandler` to register a service.RegisterServiceCtrlHandler

Enterprise T1046 Network Service Discovery

ZxShell can launch port scans.[1][2]

Enterprise T1571 Non-Standard Port

ZxShell can use ports 1985 and 1986 in HTTP/S communication.[2]

Enterprise T1057 Process Discovery

ZxShell has a command, ps, to obtain a listing of processes on the system.[2]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

ZxShell is injected into a shared SVCHOST process.[2]

Enterprise T1090 Proxy

ZxShell can set up an HTTP or SOCKS proxy.[1][2]

Enterprise T1012 Query Registry

ZxShell can query the netsvc group value data located in the svchost group Registry key.[2]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

ZxShell has remote desktop functionality.[2]

.005 Remote Services: VNC

ZxShell supports functionality for VNC sessions.[2]

Enterprise T1113 Screen Capture

ZxShell can capture screenshots.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

ZxShell has used rundll32.exe to execute other DLLs and named pipes.[2]

Enterprise T1082 System Information Discovery

ZxShell can collect the local hostname, operating system details, CPU speed, and total physical memory.[2]

Enterprise T1033 System Owner/User Discovery

ZxShell can collect the owner and organization information from the target workstation.[2]

Enterprise T1007 System Service Discovery

ZxShell can check the services on the system.[2]

Enterprise T1569 .002 System Services: Service Execution

ZxShell can create a new service for execution.[2]

Enterprise T1125 Video Capture

ZxShell has a command to perform video device spying.[2]
