# Operation Wocao, Campaign C0014 | MITRE ATT&CK®

Archived: 2026-04-05 15:26:16 UTC

Enterprise T1087 .002 Account Discovery: Domain Account

During Operation Wocao, threat actors used the `net` command to retrieve information about domain accounts.[1]

Enterprise T1583 .004 Acquire Infrastructure: Server

For Operation Wocao, the threat actors purchased servers with Bitcoin to use during the operation.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

During Operation Wocao, threat actors' XServer tool communicated using HTTP and HTTPS.[1]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

During Operation Wocao, threat actors archived collected files with WinRAR, prior to exfiltration.[1]

Enterprise T1119 Automated Collection

During Operation Wocao, threat actors used a script to collect information about the infected system.[1]

Enterprise T1115 Clipboard Data

During Operation Wocao, threat actors collected clipboard data in plaintext.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

During Operation Wocao, threat actors used PowerShell on compromised systems.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

During Operation Wocao, threat actors spawned a new `cmd.exe` process to execute commands.[1]

.005 Command and Scripting Interpreter: Visual Basic

During Operation Wocao, threat actors used VBScript to conduct reconnaissance on targeted systems.[1]

.006 Command and Scripting Interpreter: Python

During Operation Wocao, threat actors' backdoors were written in Python and compiled with py2exe.[1]

Enterprise T1555 .005 Credentials from Password Stores: Password Managers

During Operation Wocao, threat actors accessed and collected credentials from password managers.[1]

Enterprise T1005 Data from Local System

During Operation Wocao, threat actors exfiltrated files and directories of interest from the targeted system.[1]

Enterprise T1001 Data Obfuscation

During Operation Wocao, threat actors encrypted IP addresses used for "Agent" proxy hops with RC4.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

During Operation Wocao, threat actors staged archived files in a temporary directory prior to exfiltration.[1]

Enterprise T1587 .001 Develop Capabilities: Malware

During Operation Wocao, threat actors developed their own custom webshells to upload to compromised servers.[1]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

During Operation Wocao, threat actors' proxy implementation "Agent" upgraded the socket in use to a TLS socket.[1]

Enterprise T1585 .002 Establish Accounts: Email Accounts

For Operation Wocao, the threat actors registered email accounts to use during the campaign.[1]

Enterprise T1041 Exfiltration Over C2 Channel

During Operation Wocao, threat actors used the XServer backdoor to exfiltrate data.[1]

Enterprise T1190 Exploit Public-Facing Application

During Operation Wocao, threat actors gained initial access by exploiting vulnerabilities in JBoss webservers.[1]

Enterprise T1133 External Remote Services

During Operation Wocao, threat actors used stolen credentials to connect to the victim's network via VPN.[1]

Enterprise T1083 File and Directory Discovery

During Operation Wocao, threat actors gathered a recursive directory listing to find files and directories of interest.[1]

Enterprise T1589 Gather Victim Identity Information

During Operation Wocao, threat actors targeted people based on their organizational roles and privileges.[1]

Enterprise T1562 .004 Impair Defenses: Disable or Modify System Firewall

During Operation Wocao, threat actors used PowerShell to add and delete rules in the Windows firewall.[1]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

During Operation Wocao, the threat actors deleted all Windows system and security event logs using `/Q /c wevtutil cl system` and `/Q /c wevtutil cl security`.[1]

.004 Indicator Removal: File Deletion

During Operation Wocao, the threat actors consistently removed traces of their activity by first overwriting a file using `/c cd /d c:\windows\temp\ & copy \\<IP ADDRESS>\c$\windows\system32\devmgr.dll \\<IP ADDRESS>\c$\windows\temp\LMAKSW.ps1 /y` and then deleting the overwritten file using `/c cd /d c:\windows\temp\ & del \\<IP ADDRESS>\c$\windows\temp\LMAKSW.ps1`.[1]

Enterprise T1105 Ingress Tool Transfer

During Operation Wocao, threat actors downloaded additional files to the infected system.[1]

Enterprise T1056 .001 Input Capture: Keylogging

During Operation Wocao, threat actors obtained the password for the victim's password manager via a custom keylogger.[1]

Enterprise T1570 Lateral Tool Transfer

During Operation Wocao, threat actors used SMB to copy files to and from target systems.[1]

Enterprise T1680 Local Storage Discovery

During Operation Wocao, threat actors discovered the local disks attached to the system and their hardware information including manufacturer and model.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

During Operation Wocao, the threat actors renamed some tools and executables to appear as legitimate programs.[1]

Enterprise T1112 Modify Registry

During Operation Wocao, the threat actors enabled Wdigest by changing the `HKLM\SYSTEM\\ControlSet001\\Control\\SecurityProviders\\WDigest` registry value from 0 (disabled) to 1 (enabled).[1]

Enterprise T1111 Multi-Factor Authentication Interception

During Operation Wocao, threat actors used a custom collection method to intercept two-factor authentication soft tokens.[1]

Enterprise T1106 Native API

During Operation Wocao, threat actors used the `CreateProcessA` and `ShellExecute` API functions to launch commands after being injected into a selected process.[1]

Enterprise T1046 Network Service Discovery

During Operation Wocao, threat actors scanned for open ports and used nbtscan to find NETBIOS nameservers.[1]

Enterprise T1135 Network Share Discovery

During Operation Wocao, threat actors discovered network disks mounted to the system using netstat.[1]

Enterprise T1095 Non-Application Layer Protocol

During Operation Wocao, threat actors used a custom protocol for command and control.[1]

Enterprise T1571 Non-Standard Port

During Operation Wocao, the threat actors used uncommon high ports for its backdoor C2, including ports 25667 and 47000.[1]

Enterprise T1027 .005 Obfuscated Files or Information: Indicator Removal from Tools

During Operation Wocao, threat actors edited variable names within the Impacket suite to avoid automated detection.[1]

.010 Obfuscated Files or Information: Command Obfuscation

During Operation Wocao, threat actors executed PowerShell commands which were encoded or compressed using Base64, zlib, and XOR.[1]

Enterprise T1588 .002 Obtain Capabilities: Tool

For Operation Wocao, the threat actors obtained a variety of open source tools, including JexBoss, KeeThief, and BloodHound.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

During Operation Wocao, threat actors used ProcDump to dump credentials from memory.[1]

.006 OS Credential Dumping: DCSync

During Operation Wocao, threat actors used Mimikatz's DCSync to dump credentials from the memory of the targeted system.[1]

Enterprise T1120 Peripheral Device Discovery

During Operation Wocao, threat actors discovered removable disks attached to a system.[1]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

During Operation Wocao, threat actors used the command `net localgroup administrators` to list all administrators part of a local group.[1]

Enterprise T1057 Process Discovery

During Operation Wocao, the threat actors used `tasklist` to collect a list of running processes on an infected system.[1]

Enterprise T1055 Process Injection

During Operation Wocao, threat actors injected code into a selected process, which in turn launches a command as a child process of the original.[1]

Enterprise T1090 Proxy

During Operation Wocao, threat actors used a custom proxy tool called "Agent" which has support for multiple hops.[1]

.001 Internal Proxy

During Operation Wocao, threat actors proxied traffic through multiple infected systems.[1]

.003 Multi-hop Proxy

During Operation Wocao, threat actors executed commands through the installed web shell via Tor exit nodes.[1]

Enterprise T1012 Query Registry

During Operation Wocao, the threat actors executed `/c cd /d c:\windows\temp\ & reg query HKEY_CURRENT_USER\Software\<username>\PuTTY\Sessions\` to detect recent PuTTY sessions, likely to further lateral movement.[1]

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

During Operation Wocao, threat actors used Impacket's smbexec.py as well as accessing the C$ and IPC$ shares to move laterally.[1]

Enterprise T1018 Remote System Discovery

During Operation Wocao, threat actors used `nbtscan` and `ping` to discover remote systems, as well as `dsquery subnet` on a domain controller to retrieve all subnets in the Active Directory.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

During Operation Wocao, threat actors used scheduled tasks to execute malicious PowerShell code on remote systems.[1]

Enterprise T1505 .003 Server Software Component: Web Shell

During Operation Wocao, threat actors used their own web shells, as well as those previously placed on target systems by other threat actors, for reconnaissance and lateral movement.[1]

Enterprise T1518 Software Discovery

During Operation Wocao, threat actors collected a list of installed software on the infected system.[1]

.001 Security Software Discovery

During Operation Wocao, threat actors used scripts to detect security software.[1]

Enterprise T1558 .003 Steal or Forge Kerberos Tickets: Kerberoasting

During Operation Wocao, threat actors used PowerSploit's `Invoke-Kerberoast` module to request encrypted service tickets and bruteforce the passwords of Windows service accounts offline.[1]

Enterprise T1082 System Information Discovery

During Operation Wocao, threat actors discovered the OS versions of systems connected to a targeted network.[1]

Enterprise T1016 System Network Configuration Discovery

During Operation Wocao, threat actors discovered the local network configuration with `ipconfig`.[1]

.001 Internet Connection Discovery

During Operation Wocao, threat actors used a Visual Basic script that checked for internet connectivity.[1]

Enterprise T1049 System Network Connections Discovery

During Operation Wocao, threat actors collected a list of open connections on the infected system using `netstat` and checks whether it has an internet connection.[1]

Enterprise T1033 System Owner/User Discovery

During Operation Wocao, threat actors enumerated sessions and users on a remote host, and identified privileged users logged into a targeted system.[1]

Enterprise T1007 System Service Discovery

During Operation Wocao, threat actors used the `tasklist` command to search for one of its backdoors.[1]

Enterprise T1569 .002 System Services: Service Execution

During Operation Wocao, threat actors created services on remote systems for execution purposes.[1]

Enterprise T1124 System Time Discovery

During Operation Wocao, threat actors used the `time` command to retrieve the current time of a compromised system.[1]

Enterprise T1552 .004 Unsecured Credentials: Private Keys

During Operation Wocao, threat actors used Mimikatz to dump certificates and private keys from the Windows certificate store.[1]

Enterprise T1078 Valid Accounts

During Operation Wocao, threat actors used valid VPN credentials to gain initial access.[1]

.002 Domain Accounts

During Operation Wocao, threat actors used domain credentials, including domain admin, for lateral movement and privilege escalation.[1]

.003 Local Accounts

During Operation Wocao, threat actors used local account credentials found during the intrusion for lateral movement and privilege escalation.[1]

Enterprise T1047 Windows Management Instrumentation

During Operation Wocao, threat actors has used WMI to execute commands.[1]

---