ToddyCat, Group G1022 | MITRE ATT&CK®

Archived: 2026-04-05 17:24:28 UTC

Enterprise T1087 .002 Account Discovery: Domain Account

ToddyCat has run `net user %USER% /dom` for account discovery.[2]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

ToddyCat has leveraged xcopy, 7zip, and RAR to stage and compress collected documents prior to exfiltration.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

ToddyCat has used Powershell scripts to perform post exploit collection.[2]

.003 Command and Scripting Interpreter: Windows Command Shell

ToddyCat has used .bat scripts and `cmd` for execution on compromised hosts.[2]

Enterprise T1005 Data from Local System

ToddyCat has run scripts to collect documents from targeted hosts.[2]

Enterprise T1074 .002 Data Staged: Remote Data Staging

ToddyCat manually transferred collected files to an exfiltration host using xcopy.[2]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

ToddyCat has used a DropBox uploader to exfiltrate stolen files.[2]

Enterprise T1190 Exploit Public-Facing Application

ToddyCat has exploited the ProxyLogon vulnerability (CVE-2021-26855) to compromise Exchange Servers at multiple organizations.[1]

Enterprise T1083 File and Directory Discovery

ToddyCat has run scripts to enumerate recently modified documents having either a .pdf, .doc, .docx, .xls or .xlsx extension.[2]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

ToddyCat has hidden malicious scripts using `powershell.exe -windowstyle hidden` .[2]

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

Prior to executing a backdoor ToddyCat has run `cmd /c start /b netsh advfirewall firewall add rule name="SGAccessInboundRule" dir=in protocol=udp action=allow localport=49683` to allow the targeted system to receive UDP packets on port 49683.[2]

Enterprise T1680 Local Storage Discovery

ToddyCat has collected information on bootable drives including model, vendor, and serial numbers.[2]

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

ToddyCat has used the name `debug.exe` for malware components.[1]

Enterprise T1106 Native API

ToddyCat has used `WinExec` to execute commands received from C2 on compromised hosts.[2]

Enterprise T1095 Non-Application Layer Protocol

ToddyCat has used a passive backdoor that receives commands with UDP packets.[2]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

ToddyCat has executed `net group "domain admins" /dom` for discovery on compromised machines.[2]

Enterprise T1566 .003 Phishing: Spearphishing via Service

ToddyCat has sent loaders configured to run Ninja as zip archives via Telegram.[1]

Enterprise T1057 Process Discovery

ToddyCat has run `cmd /c start /b tasklist` to enumerate processes.[2]

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

ToddyCat has used locally mounted network shares for lateral movement through targated environments.[2]

Enterprise T1018 Remote System Discovery

ToddyCat has used `ping %REMOTE_HOST%` for post exploit discovery.[2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

ToddyCat has used scheduled tasks to execute discovery commands and scripts for collection.[2]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

ToddyCat can determine is Kaspersky software is running on an endpoint by running `cmd /c wmic process where name="avp.exe"` .[2]

Enterprise T1049 System Network Connections Discovery

ToddyCat has used `netstat -anop tcp` to discover TCP connections to compromised hosts.[2]

Enterprise T1078 .002 Valid Accounts: Domain Accounts

ToddyCat has used compromised domain admin credentials to mount local network shares.[2]

Enterprise T1047 Windows Management Instrumentation

ToddyCat has used WMI to execute scripts for post exploit document collection.[2]
