Cinnamon Tempest, DEV-0401, Emperor Dragonfly, BRONZE STARLIGHT, Group G1021

Archived: 2026-04-05 18:07:24 UTC

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Cinnamon Tempest has used PowerShell to communicate with C2, download files, and execute reconnaissance commands.[5]

.003 Command and Scripting Interpreter: Windows Command Shell

Cinnamon Tempest has executed ransomware using batch scripts deployed via GPO.[1]

.006 Command and Scripting Interpreter: Python

Cinnamon Tempest has used a customized version of the Impacket wmiexec.py module to create renamed output files.[1]

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

Cinnamon Tempest has created system services to establish persistence for deployed tooling.[5]

Enterprise T1140 Deobfuscate/Decode Files or Information

Cinnamon Tempest has used weaponized DLLs to load and decrypt payloads.[5]

Enterprise T1484 .001 Domain or Tenant Policy Modification: Group Policy Modification

Cinnamon Tempest has used Group Policy to deploy batch scripts for ransomware deployment.[1]

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

Cinnamon Tempest has uploaded captured keystroke logs to the Alibaba Cloud Object Storage Service, Aliyun OSS.[5]

Enterprise T1190 Exploit Public-Facing Application

Cinnamon Tempest has exploited multiple unpatched vulnerabilities for initial access including vulnerabilities in Microsoft Exchange, Manage Engine AdSelfService Plus, Confluence, and Log4j.[1][7][5][4]

Enterprise T1657 Financial Theft

Cinnamon Tempest has maintained leak sites for exfiltrated data in attempt to extort victims into paying a ransom.[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Cinnamon Tempest has used search order hijacking to launch Cobalt Strike Beacons.[1][4] Cinnamon Tempest has also abused legitimate executables to side-load weaponized DLLs.[5]

Enterprise T1105 Ingress Tool Transfer

Cinnamon Tempest has downloaded files, including Cobalt Strike, to compromised hosts.[5]

Enterprise T1588 .002 Obtain Capabilities: Tool

Cinnamon Tempest has used open-source tools including customized versions of the Iox proxy tool, NPS tunneling tool, Meterpreter, and a keylogger that uploads data to Alibaba cloud storage.[5][4]

Enterprise T1572 Protocol Tunneling

Cinnamon Tempest has used the Iox and NPS proxy and tunneling tools in combination create multiple connections through a single tunnel.[5]

Enterprise T1090 Proxy

Cinnamon Tempest has used a customized version of the Iox port-forwarding and proxy tool.[5]

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

Cinnamon Tempest has used SMBexec for lateral movement.[5]

Enterprise T1080 Taint Shared Content

Cinnamon Tempest has deployed ransomware from a batch file in a network share.[1]

Enterprise T1078 Valid Accounts

Cinnamon Tempest has used compromised user accounts to deploy payloads and create system services.[5]

.002 Domain Accounts

Cinnamon Tempest has obtained highly privileged credentials such as domain administrator in order to deploy malware.[1]

Enterprise T1047 Windows Management Instrumentation

Cinnamon Tempest has used Impacket for lateral movement via WMI.[1][5]
