

# Lotus Blossom, DRAGONFISH, Spring Dragon, RADIUM, Raspberry Typhoon, Bilbug, Thrip, Group G0030

Archived: 2026-04-05 14:16:35 UTC

Enterprise [T1134 Access Token Manipulation](#)

[Lotus Blossom](#) has retrieved process tokens for processes to adjust the privileges of the launch process or other items.<sup>[3]</sup>

Enterprise [T1087 .001 Account Discovery: Local Account](#)

[Lotus Blossom](#) has used commands such as `net` to profile local system users.<sup>[3]</sup>

[.002 Account Discovery: Domain Account](#)

[Lotus Blossom](#) has used `net` commands and tools such as [AdFind](#) to profile domain accounts associated with victim machines and make Active Directory queries.<sup>[3][2]</sup>

Enterprise [T1560 .001 Archive Collected Data: Archive via Utility](#)

[Lotus Blossom](#) has used WinRAR for compressing data in RAR format.<sup>[3][2]</sup>

[.003 Archive Collected Data: Archive via Custom Method](#)

[Lotus Blossom](#) has used custom tools to compress and archive data on victim systems.<sup>[3]</sup>

Enterprise [T1543 .003 Create or Modify System Process: Windows Service](#)

[Lotus Blossom](#) has configured tools such as [Sagerunex](#) to run as Windows services.<sup>[3]</sup>

Enterprise [T1074 .001 Data Staged: Local Data Staging](#)

[Lotus Blossom](#) has locally staged compressed and archived data for follow-on exfiltration.<sup>[3]</sup>

Enterprise [T1482 Domain Trust Discovery](#)

[Lotus Blossom](#) has used tools such as [AdFind](#) to make Active Directory queries.<sup>[2]</sup>

Enterprise [T1083 File and Directory Discovery](#)

[Lotus Blossom](#) has used commands such as `dir` to examine the local filesystem of victim machines.<sup>[3]</sup>

Enterprise [T1112 Modify Registry](#)

[Lotus Blossom](#) has installed tools such as [Sagerunex](#) by writing them to the Windows registry.<sup>[3]</sup>

Enterprise [T1046 Network Service Discovery](#)

[Lotus Blossom](#) has used port scanners to enumerate services on remote hosts.<sup>[2]</sup>

Enterprise [T1588 .002 Obtain Capabilities: Tool](#)

[Lotus Blossom](#) has used publicly-available tools such as a Python-based cookie stealer for Chrome browsers, [Impacket](#), and the Venom proxy tool.<sup>[3]</sup>

Enterprise [T1090 .001 Proxy: Internal Proxy](#)

[Lotus Blossom](#) has used publicly available tools such as the Venom proxy tool to proxy traffic out of victim environments.<sup>[3]</sup>

[.003 Proxy: Multi-hop Proxy](#)

[Lotus Blossom](#) has used tools such as the publicly available HTran tool for proxying traffic in victim environments.<sup>[3]</sup>

Enterprise [T1012 Query Registry](#)

[Lotus Blossom](#) has run commands such as `reg query HKLM\SYSTEM\CurrentControlSet\Services\[service name]\Parameters` to verify if installed implants are running as a service.<sup>[3]</sup>

Enterprise [T1018 Remote System Discovery](#)

[Lotus Blossom](#) has used [Ping](#) to identify remote systems.<sup>[2]</sup>

Enterprise [T1539 Steal Web Session Cookie](#)

[Lotus Blossom](#) has used publicly-available tools to steal cookies from browsers such as Chrome.<sup>[3]</sup>

Enterprise [T1016 System Network Configuration Discovery](#)

[Lotus Blossom](#) has used commands such as `ipconfig` and `netstat` to gather network information on compromised hosts.<sup>[3]</sup>

[.001 Internet Connection Discovery](#)

[Lotus Blossom](#) has performed checks to determine if a victim machine is able to access the Internet.<sup>[3]</sup>

Enterprise [T1049 System Network Connections Discovery](#)

[Lotus Blossom](#) has used commands such as `netstat` to identify system network connections.<sup>[3]</sup>

Enterprise [T1047 Windows Management Instrumentation](#)

[Lotus Blossom](#) has used WMI to enable lateral movement.<sup>[3]</sup>

Source: <https://attack.mitre.org/groups/G0030>