

## Amadey, Software S1025 | MITRE ATT&CK®

Archived: 2026-04-05 18:31:44 UTC

Enterprise [T1071 .001 Application Layer Protocol: Web Protocols](#)

[Amadey](#) has used HTTP for C2 communications.<sup>[2]</sup>

Enterprise [T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder](#)

[Amadey](#) has changed the Startup folder to the one containing its executable by overwriting the registry keys.<sup>[1][2]</sup>

Enterprise [T1005 Data from Local System](#)

[Amadey](#) can collect information from a compromised host.<sup>[2]</sup>

Enterprise [T1140 Deobfuscate/Decode Files or Information](#)

[Amadey](#) has decoded antivirus name strings.<sup>[1]</sup>

Enterprise [T1568 .001 Dynamic Resolution: Fast Flux DNS](#)

[Amadey](#) has used fast flux DNS for its C2.<sup>[1]</sup>

Enterprise [T1041 Exfiltration Over C2 Channel](#)

[Amadey](#) has sent victim data to its C2 servers.<sup>[2]</sup>

Enterprise [T1083 File and Directory Discovery](#)

[Amadey](#) has searched for folders associated with antivirus software.<sup>[1]</sup>

Enterprise [T1105 Ingress Tool Transfer](#)

[Amadey](#) can download and execute files to further infect a host machine with additional malware.<sup>[2]</sup>

Enterprise [T1112 Modify Registry](#)

[Amadey](#) has overwritten registry keys for persistence.<sup>[2]</sup>

Enterprise [T1106 Native API](#)

[Amadey](#) has used a variety of Windows API calls, including `GetComputerNameA` , `GetUserNameA` , and `CreateProcessA` .<sup>[2]</sup>

Enterprise [T1027 Obfuscated Files or Information](#)

[Amadey](#) has obfuscated strings such as antivirus vendor names, domains, files, and others.<sup>[2]</sup>

Enterprise [T1518 .001 Software Discovery: Security Software Discovery](#)

[Amadey](#) has checked for a variety of antivirus products.<sup>[1][2]</sup>

Enterprise [T1553 .005 Subvert Trust Controls: Mark-of-the-Web Bypass](#)

[Amadey](#) has modified the `:Zone.Identifier` in the ADS area to zero.<sup>[1]</sup>

Enterprise [T1082 System Information Discovery](#)

[Amadey](#) has collected the computer name and OS version from a compromised machine.<sup>[1][2]</sup>

Enterprise [T1614 System Location Discovery](#)

[Amadey](#) does not run any tasks or install additional malware if the victim machine is based in Russia.<sup>[2]</sup>

Enterprise [T1016 System Network Configuration Discovery](#)

[Amadey](#) can identify the IP address of a victim machine.<sup>[2]</sup>

Enterprise [T1033 System Owner/User Discovery](#)

[Amadey](#) has collected the user name from a compromised host using `GetUserNameA`.<sup>[2]</sup>

---

Source: <https://attack.mitre.org/software/S1025/>