Sykipot, Software S0018 | MITRE ATT&CK®

Archived: 2026-04-05 13:56:58 UTC

Domain	ID		Name	Use
Enterprise	T1087	.002	Account Discovery: Domain Account	Sykipot may use `net group "domain admins" /domain` to display accounts in the "domain admins" permissions group and `net localgroup "administrators"` to list local system administrator group membership.[3]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Sykipot has been known to establish persistence by adding programs to the Run Registry key.[2]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	Sykipot uses SSL for encrypting C2 communications.[2]
Enterprise	T1056	.001	Input Capture: Keylogging	Sykipot contains keylogging functionality to steal passwords.[1]
Enterprise	T1111		Multi-Factor Authentication Interception	Sykipot is known to contain functionality that enables targeting of smart card technologies to proxy authentication for connections to restricted network resources using detected hardware tokens.[1]
Enterprise	T1057		Process Discovery	Sykipot may gather a list of running processes by running `tasklist /v`.[3]
Enterprise	T1055	.001	Process Injection: Dynamic-link Library Injection	Sykipot injects itself into running instances of outlook.exe, iexplore.exe, or firefox.exe.[3]

Domain	ID	Name	Use
Enterprise	T1018	Remote System Discovery	Sykipot may use `net view /domain` to display hostnames of available systems on a network.[3]
Enterprise	T1016	System Network Configuration Discovery	Sykipot may use `ipconfig /all` to gather system network configuration details.[3]
Enterprise	T1049	System Network Connections Discovery	Sykipot may use `netstat -ano` to display active network connections.[3]
Enterprise	T1007	System Service Discovery	Sykipot may use `net start` to display running services.[3]
