SoreFang, Software S0516 | MITRE ATT&CK®

Archived: 2026-04-02 10:52:03 UTC

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	SoreFang can collect usernames from the local system via `net.exe user`.[2]
		.002	Account Discovery: Domain Account	SoreFang can enumerate domain accounts via `net.exe user /domain`.[2]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	SoreFang can use HTTP in C2 communications.[2][1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	SoreFang can decode and decrypt exfiltrated data sent to C2.[2]
Enterprise	T1190		Exploit Public-Facing Application	SoreFang can gain access by exploiting a Sangfor SSL VPN vulnerability that allows for the placement and delivery of malicious update binaries.[2]
Enterprise	T1083		File and Directory Discovery	SoreFang has the ability to list directories.[2]
Enterprise	T1105		Ingress Tool Transfer	SoreFang can download additional payloads from C2.[2][1]
Enterprise	T1680		Local Storage Discovery	SoreFang can collect disk space information on victim machines by executing Systeminfo.[2]

Domain	ID		Name	Use
Enterprise	T1027		Obfuscated Files or Information	SoreFang has the ability to encode and RC6 encrypt data sent to C2.[2]
Enterprise	T1069	.002	Permission Groups Discovery: Domain Groups	SoreFang can enumerate domain groups by executing `net.exe group /domain`.[2]
Enterprise	T1057		Process Discovery	SoreFang can enumerate processes on a victim machine through use of Tasklist.[2]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	SoreFang can gain persistence through use of scheduled tasks.[2]
Enterprise	T1082		System Information Discovery	SoreFang can collect the hostname, operating system configuration, and product ID on victim machines by executing Systeminfo.[2]
Enterprise	T1016		System Network Configuration Discovery	SoreFang can collect the TCP/IP, DNS, DHCP, and network adapter configuration on a compromised host via `ipconfig.exe /all`.[2]
