Sowbug, Group G0054 | MITRE ATT&CK®

Archived: 2026-04-05 16:46:21 UTC

Domain	ID		Name	Use
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	Sowbug extracted documents and bundled them into a RAR archive.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Sowbug has used command line during its intrusions. [1]
Enterprise	T1039		Data from Network Shared Drive	Sowbug extracted Word documents from a file server on a victim network.[1]
Enterprise	T1083		File and Directory Discovery	Sowbug identified and extracted all Word documents on a server by using a command containing * .doc and *.docx. The actors also searched for documents based on a specific date range and attempted to identify all installed software on a victim.[1]
Enterprise	T1056	.001	Input Capture: Keylogging	Sowbug has used keylogging tools.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	Sowbug named its tools to masquerade as Windows or Adobe Reader software, such as by using the file name adobecms.exe and the directory `CSIDL_APPDATA\microsoft\security`.[1]
Enterprise	T1135		Network Share Discovery	Sowbug listed remote shared drives that were accessible from a victim.[1]

Domain	ID	Name	Use
Enterprise	T1003	OS Credential Dumping	Sowbug has used credential dumping tools.[1]
Enterprise	T1082	System Information Discovery	Sowbug obtained OS version and hardware configuration from a victim.[1]

Source: https://attack.mitre.org/groups/G0054/