HAWKBALL, Software S0391 | MITRE ATT&CK®

Archived: 2026-04-05 15:03:59 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	HAWKBALL has used HTTP to communicate with a single hard-coded C2 server.[1]
Enterprise	T1560	.003	Archive Collected Data: Archive via Custom Method	HAWKBALL has encrypted data with XOR before sending it over the C2 channel. [1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	HAWKBALL has created a cmd.exe reverse shell, executed commands, and uploaded output via the command line.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	HAWKBALL has sent system information and files over the C2 channel.[1]
Enterprise	T1203		Exploitation for Client Execution	HAWKBALL has exploited Microsoft Office vulnerabilities CVE-2017-11882 and CVE-2018-0802 to deliver the payload.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	HAWKBALL has the ability to delete files. [1]
Enterprise	T1559	.002	Inter-Process Communication: Dynamic Data Exchange	HAWKBALL has used an OLE object that uses Equation Editor to drop the embedded shellcode.[1]
Enterprise	T1106		Native API	HAWKBALL has leveraged several Windows API calls to create processes,

Domain	ID		Name	Use
				gather disk information, and detect debugger activity.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	HAWKBALL has encrypted the payload with an XOR-based algorithm.[1]
Enterprise	T1082		System Information Discovery	HAWKBALL can collect the OS version, architecture information, and computer name.[1]
Enterprise	T1033		System Owner/User Discovery	HAWKBALL can collect the user name of the system.[1]

Source: https://attack.mitre.org/software/S0391