UPPERCUT, Software S0275 | MITRE ATT&CK®

Archived: 2026-04-05 14:11:46 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	UPPERCUT has used HTTP for C2, including sending error codes in Cookie headers.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	UPPERCUT uses cmd.exe to execute commands on the victim’s machine.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Some versions of UPPERCUT have used the hard-coded string "this is the encrypt key" for Blowfish encryption when communicating with a C2. Later versions have hard-coded keys uniquely for each C2 address.[1]
Enterprise	T1083		File and Directory Discovery	UPPERCUT has the capability to gather the victim's current directory.[1]
Enterprise	T1105		Ingress Tool Transfer	UPPERCUT can download and upload files to and from the victim’s machine.[1]
Enterprise	T1113		Screen Capture	UPPERCUT can capture desktop screenshots in the PNG format and send them to the C2 server.[1]
Enterprise	T1082		System Information Discovery	UPPERCUT has the capability to gather the system’s hostname and OS version.[1]
Enterprise	T1016		System Network Configuration Discovery	UPPERCUT has the capability to gather the victim's proxy information.[1]

Domain	ID	Name	Use
Enterprise	T1033	System Owner/User Discovery	UPPERCUT has the capability to collect the current logged on user's username from a machine. [1]
Enterprise	T1124	System Time Discovery	UPPERCUT has the capability to obtain the time zone information and current timestamp of the victim's machine.[1]
