WellMail, Software S0515 | MITRE ATT&CK®

Archived: 2026-04-05 17:32:56 UTC

Domain	ID		Name	Use
Enterprise	T1560		Archive Collected Data	WellMail can archive files on the compromised host.[1]
Enterprise	T1005		Data from Local System	WellMail can exfiltrate files from the victim machine.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	WellMail can decompress scripts received from C2.[1]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	WellMail can use hard coded client and certificate authority certificates to communicate with C2 over mutual TLS.[1][2]
Enterprise	T1105		Ingress Tool Transfer	WellMail can receive data and executable scripts from C2.[1]
Enterprise	T1095		Non-Application Layer Protocol	WellMail can use TCP for C2 communications.[1]
Enterprise	T1571		Non-Standard Port	WellMail has been observed using TCP port 25, without using SMTP, to leverage an open port for secure command and control communications.[1][2]
Enterprise	T1016		System Network Configuration Discovery	WellMail can identify the IP address of the victim system.[1]

Domain	ID	Name	Use
Enterprise	T1033	System Owner/User Discovery	WellMail can identify the current username on the victim system.[1]

Source: https://attack.mitre.org/software/S0515