WellMess, Software S0514 | MITRE ATT&CK®

Archived: 2026-04-05 16:45:25 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	WellMess can use HTTP and HTTPS in C2 communications.[2][4][1][3]
		.004	Application Layer Protocol: DNS	WellMess has the ability to use DNS tunneling for C2 communications.[2][3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	WellMess can execute PowerShell scripts received from C2.[2][1]
		.003	Command and Scripting Interpreter: Windows Command Shell	WellMess can execute command line scripts received from C2.[2]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	WellMess has used Base64 encoding to uniquely identify communication to and from the C2.[1]
Enterprise	T1005		Data from Local System	WellMess can send files from the victim machine to C2.[2][1]
Enterprise	T1001	.001	Data Obfuscation: Junk Data	WellMess can use junk data in the Base64 string for additional obfuscation.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	WellMess can decode and decrypt data received from C2.[2][4][1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	WellMess can encrypt HTTP POST data using RC6 and a dynamically generated

Domain	ID		Name	Use
				AES key encrypted with a hard coded RSA public key.[2][4][1]
		.002	Encrypted Channel: Asymmetric Cryptography	WellMess can communicate to C2 with mutual TLS where client and server mutually check certificates.[2][4][1][3]
Enterprise	T1105		Ingress Tool Transfer	WellMess can write files to a compromised host.[2][1]
Enterprise	T1069	.002	Permission Groups Discovery: Domain Groups	WellMess can identify domain group membership for the current user.[1]
Enterprise	T1082		System Information Discovery	WellMess can identify the computer name of a compromised host.[2][1]
Enterprise	T1016		System Network Configuration Discovery	WellMess can identify the IP address and user domain on the target machine.[2][1]
Enterprise	T1033		System Owner/User Discovery	WellMess can collect the username on the victim machine to send to C2.[1]

Source: https://attack.mitre.org/software/S0514/