OutSteel, Software S1017 | MITRE ATT&CK®

Archived: 2026-04-05 15:51:05 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	OutSteel has used HTTP for C2 communications.[1]
Enterprise	T1119		Automated Collection	OutSteel can automatically scan for and collect files with specific extensions.[1]
Enterprise	T1020		Automated Exfiltration	OutSteel can automatically upload collected files to its C2 server.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	OutSteel has used `cmd.exe` to scan a compromised host for specific file extensions.[1]
		.010	Command and Scripting Interpreter: AutoHotKey & AutoIT	OutSteel was developed using the AutoIT scripting language.[1]
Enterprise	T1005		Data from Local System	OutSteel can collect information from a compromised host.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	OutSteel can upload files from a compromised host over its C2 channel.[1]
Enterprise	T1083		File and Directory Discovery	OutSteel can search for specific file extensions, including zipped files.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	OutSteel can delete itself following the successful execution of a follow-on payload.[1]

Domain	ID		Name	Use
Enterprise	T1105		Ingress Tool Transfer	OutSteel can download files from its C2 server. [1]
Enterprise	T1570		Lateral Tool Transfer	OutSteel can download the Saint Bot malware for follow-on execution.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	OutSteel attempts to download and execute Saint Bot to a statically-defined location attempting to mimic svchost: `%TEMP%\svjhost.exe` .[1]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	OutSteel has been distributed as a malicious attachment within a spearphishing email.[1]
		.002	Phishing: Spearphishing Link	OutSteel has been distributed through malicious links contained within spearphishing emails.[1]
Enterprise	T1057		Process Discovery	OutSteel can identify running processes on a compromised host.[1]
Enterprise	T1204	.001	User Execution: Malicious Link	OutSteel has relied on a user to click a malicious link within a spearphishing email.[1]
		.002	User Execution: Malicious File	OutSteel has relied on a user to execute a malicious attachment delivered via spearphishing.[1]

Source: https://attack.mitre.org/software/S1017