EnvyScout, Software S0634 | MITRE ATT&CK®

Archived: 2026-04-05 13:44:54 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	EnvyScout can use cmd.exe to execute malicious files on compromised hosts.[1]
		.007	Command and Scripting Interpreter: JavaScript	EnvyScout can write files to disk with JavaScript using a modified version of the open-source tool FileSaver.[1]
Enterprise	T1005		Data from Local System	EnvyScout can collect sensitive NTLM material from a compromised host.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	EnvyScout can deobfuscate and write malicious ISO files to disk.[1]
Enterprise	T1480		Execution Guardrails	EnvyScout can call `window.location.pathname` to ensure that embedded files are being executed from the C: drive, and will terminate if they are not.[1]
Enterprise	T1187		Forced Authentication	EnvyScout can use protocol handlers to coax the operating system to send NTLMv2 authentication responses to attacker-controlled infrastructure.[1]
Enterprise	T1564	.001	Hide Artifacts: Hidden Files and Directories	EnvyScout can use hidden directories and files to hide malicious executables.[1]

Domain	ID		Name	Use
Enterprise	T1036		Masquerading	EnvyScout has used folder icons for malicious files to lure victims into opening them.[1]
Enterprise	T1027	.006	Obfuscated Files or Information: HTML Smuggling	EnvyScout contains JavaScript code that can extract an encoded blob from its HTML body and write it to disk.[1]
		.013	Obfuscated Files or Information: Encrypted/Encoded File	EnvyScout can Base64 encode payloads.[1]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	EnvyScout has been distributed via spearphishing as an email attachment.[1]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	EnvyScout has the ability to proxy execution of malicious files with Rundll32.[1]
Enterprise	T1082		System Information Discovery	EnvyScout can determine whether the ISO payload was received by a Windows or iOS device.[1]
Enterprise	T1204	.002	User Execution: Malicious File	EnvyScout has been executed through malicious files attached to e-mails.[1]