LaZagne, Software S0349 | MITRE ATT&CK®

Archived: 2026-04-05 17:28:46 UTC

Domain	ID		Name	Use
Enterprise	T1555		Credentials from Password Stores	LaZagne can obtain credentials from databases, mail, and WiFi across multiple platforms.[1]
		.001	Keychain	LaZagne can obtain credentials from macOS Keychains.[1]
		.003	Credentials from Web Browsers	LaZagne can obtain credentials from web browsers such as Google Chrome, Internet Explorer, and Firefox.[1]
		.004	Windows Credential Manager	LaZagne can obtain credentials from Vault files.[1]
Enterprise	T1003	.001	OS Credential Dumping: LSASS Memory	LaZagne can perform credential dumping from memory to obtain account and password information.[1]
		.004	OS Credential Dumping: LSA Secrets	LaZagne can perform credential dumping from LSA secrets to obtain account and password information.[1]
		.005	OS Credential Dumping: Cached Domain Credentials	LaZagne can perform credential dumping from MSCache to obtain account and password information.[1]

Domain	ID		Name	Use
		.007	OS Credential Dumping: Proc Filesystem	LaZagne can use the `<PID>/maps` and `<PID>/mem` files to identify regex patterns to dump cleartext passwords from the browser's process memory.[1][2]
		.008	OS Credential Dumping: /etc/passwd and /etc/shadow	LaZagne can obtain credential information from /etc/shadow using the shadow.py module.[1]
Enterprise	T1552	.001	Unsecured Credentials: Credentials In Files	LaZagne can obtain credentials from chats, databases, mail, and WiFi.[1]

Source: https://attack.mitre.org/software/S0349/