PinchDuke, Software S0048 | MITRE ATT&CK®

Archived: 2026-04-05 17:03:16 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	PinchDuke transfers files from the compromised host via HTTP or HTTPS to a C2 server.[1]
Enterprise	T1555		Credentials from Password Stores	PinchDuke steals credentials from compromised hosts. PinchDuke's credential stealing functionality is believed to be based on the source code of the Pinch credential stealing malware (also known as LdPinch). Credentials targeted by PinchDuke include ones associated with many sources such as The Bat!, Yahoo!, Mail.ru, Passport.Net, Google Talk, and Microsoft Outlook.[1]
		.003	Credentials from Web Browsers	PinchDuke steals credentials from compromised hosts. PinchDuke's credential stealing functionality is believed to be based on the source code of the Pinch credential stealing malware (also known as LdPinch). Credentials targeted by PinchDuke include ones associated with many sources such as Netscape Navigator, Mozilla Firefox, Mozilla Thunderbird, and Internet Explorer. [1]
Enterprise	T1005		Data from Local System	PinchDuke collects user files from the compromised host based on predefined file extensions.[1]
Enterprise	T1083		File and Directory Discovery	PinchDuke searches for files created within a certain timeframe and whose file extension matches a predefined list.[1]
Enterprise	T1003		OS Credential Dumping	PinchDuke steals credentials from compromised hosts. PinchDuke's credential stealing functionality is believed to be based on the source code of the Pinch credential stealing malware (also known as LdPinch). Credentials

Domain	ID	Name	Use
			targeted by PinchDuke include ones associated many sources such as WinInet Credential Cache, and Lightweight Directory Access Protocol (LDAP).[1]
Enterprise	T1082	System Information Discovery	PinchDuke gathers system configuration information.[1]

Source: https://attack.mitre.org/software/S0048/