Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:30:54 UTC

Tool: PinchDuke

Names	PinchDuke
Category	Malware
Type	Loader, Info stealer, Credential stealer, Exfiltration
Description	(F-Secure) The PinchDuke toolset consists of multiple loaders and a core information stealer trojan. The loaders associated with the PinchDuke toolset have also been observed being used with CosmicDuke. The PinchDuke information stealer gathers system configuration information, steals user credentials, and collects user files from the compromised host transferring these via HTTP(S) to a C&C server. We believe PinchDuke's credential stealing functionality is based on the source code of the Pinch credential stealing malware (also known as LdPinch) that was developed in the early 2000s and has later been openly distributed on underground forums. Credentials targeted by PinchDuke include ones associated with the following software or services: • The Bat! • Yahoo! • Mail.ru • Passport.Net • Google Talk • Netscape Navigator • Mozilla Firefox • Mozilla Thunderbird • Internet Explorer • Microsoft Outlook • WinInet Credential Cache • Lightweight Directory Access Protocol (LDAP) PinchDuke will also search for files that have been created within a predefined timeframe and whose file extension is present in a predefined list.

Information	<https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0048/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.pinchduke>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PinchDuke>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool PinchDuke

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ab078dbf-23c7-41b1-9be0-667ec1ca050c