Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:23:09 UTC

Tool: DMSniff

Names	DMSniff
Category	Malware
Type	POS malware, Backdoor, Credential stealer, Botnet
Description	(Flashpoint) Point-of-sale malware previously only privately sold has been used in breaches of small- and medium-sized businesses in the restaurant and entertainment industries. The malware, known as DMSniff, also uses a domain generation algorithm (DGA) to create lists of command-and-control domains on the fly. This technique is valuable to an attacker because if domains are taken down by law enforcement, technology companies, or hosting providers, the malware can still communicate and receive commands or share stolen data.
Information	<https://www.flashpoint-intel.com/blog/dmsniff-pos-malware-actively-leveraged-target-medium-sized-businesses/> <https://cis.verint.com/2019/05/07/the-awakening-of-pos-malware-or-has-it-really-been-dormant/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dmsniff>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DMSniff>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool DMSniff

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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