Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:42:51 UTC

Tool: DealersChoice

Names	DealersChoice
Category	Malware
Type	Loader
Description	(Palo Alto) Weaponizing documents to exploit known Microsoft Word vulnerabilities is a common tactic deployed by many adversary groups, but in this example, we discovered RTF documents containing embedded OLE Word documents further containing embedded Adobe Flash (.SWF) files, designed to exploit Flash vulnerabilities rather than Microsoft Word. We have named this tool that generates these documents DealersChoice. In addition to the discovery of this new tactic, we were able to identify two different variants of the embedded SWF files: the first being a standalone version containing a compressed payload which we have dubbed DealersChoice.A and a second variant being a much more modular version deploying additional anti-analysis techniques which we have dubbed DealersChoice.B. The unearthing of DealersChoice.B suggests a possible code evolution of the initial DealersChoice.A variant. Also, artifacts within DealersChoice suggests that Sofacy created it with the intentions to target both Windows and OSX operating systems, as DealersChoice could potentially be cross-platform due to its use of Adobe Flash files.
Information	<https://unit42.paloaltonetworks.com/unit42-dealerschoice-sofacys-flash-player-exploit-platform/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0243/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DealersChoice>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool DealersChoice

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8c0669d9-d7f3-401a-acfa-58e3a502e38e