Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:53:07 UTC

Tool: BadHatch

Names	BadHatch
Category	Malware
Type	POS malware, Backdoor, Info stealer
Description	(Trend Micro) Security researchers found threat group FIN8 reappearing after two years with a new point-of-sale (PoS) malware named Badhatch, which is designed to steal credit card information. Researchers from Gigamon analyzed the sample and found similarities with PunchBuggy, but Badhatch features new capabilities that allow it to scan for victim networks, provide attackers with remote access, install a backdoor, and deliver other modified malware payloads such as PoSlurp and PunchBuggy, among other features. Badhatch begins infection much like its predecessor PowerSniff, by sending a customized phishing email via a weaponized Word document. Once the victim enables the macros, it executes PowerShells and shellcode scripts for PowerSniff, installing a backdoor in the process. Its network scan capability makes it different from PowerSniff; it is unable to check if the systems infected is in the education or healthcare sector. The researchers also noted that it lacks the sandbox detection and anti-virus analysis evasion features, as well as the long-term persistence tools that its predecessor had. However, they note that this also serves as an advantage as the attackers can execute the routine after infection and have greater control on how the malware can be used, thereby avoiding automated sandboxing features.
Information	<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fin8-reemerges-with-new-pos-malware-badhatch> <https://www.bitdefender.com/files/News/CaseStudies/study/394/Bitdefender-PR-Whitepaper-BADHATCH-creat5237-en-EN.pdf> <https://team-cymru.com/blog/2021/03/15/fin8-badhatch-threat-indicator-enrichment/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1081>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.badhatch>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BADHATCH>

Last change to this tool card: 30 June 2025

Download this tool card in JSON format

All groups using tool BadHatch

Changed	Name	Country	Observed	
APT groups				
	FIN8	[Unknown]	2016-Dec 2022	

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