Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:42:33 UTC

Tool: Backoff

Names	Backoff Backoff POS
Category	Malware
Type	POS malware, Reconnaissance, Backdoor, Keylogger, Credential stealer, Botnet
Description	(Trend Micro) Backoff – a successor of Alina POS (aka Track) whose variants are known for scanning all running processes to retrieve card track data and gather affected system information, Backoff, uses the same installation technique used in the Alina family of PoS RAM-scraping malware. Based on our research, Backoff implements an updated data search function and drops a watchdog process to ensure that it continuously runs in the system. Discovered by the US Computer Emergency Readiness Team (US CERT), this PoS malware targeted the US. Interestingly, we saw a clear decrease of hits during “dead hours” specifically at 2:00 AM, and an apparent recurring rise of hits at 10:00 AM. This trend follows regular business operation hours wherein PoS devices are more likely to be active and in use. Generally, the hits increase during business hours and decline during off-hours.
Information	<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-evolution-of-point-of-sale-pos-malware> <https://www.us-cert.gov/ncas/alerts/TA14-212A> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.backoff>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Backoff

Changed	Name	Country	Observed

Unknown groups

	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6dc5bc96-090e-4f1d-904a-bf9d92766450