Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:06:52 UTC

Tool: Multigrain

Names	Multigrain Multigrain POS
Category	Malware
Type	POS malware, Credential stealer
Description	(FireEye) FireEye recently discovered a new variant of a point of sale (POS) malware family known as NewPosThings. This variant, which we call “MULTIGRAIN”, consists largely of a subset of slightly modified code from NewPosThings. The variant is highly targeted, digitally signed, and exfiltrates stolen payment card data over DNS. The addition of DNS-based exfiltration is new for this malware family; however, other POS malware families such as BernhardPOS and BlackPOS have used this technique in the past.
Information	<https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html> <https://www.pandasecurity.com/mediacenter/malware/multigrain-malware-pos/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.multigrain_pos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:multigrain>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool Multigrain

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=4af3fb73-4104-49ad-b124-59d1ae82939f