Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:30:03 UTC

Tool: Dexter

Names	Dexter LusyPOS StarDust
Category	Malware
Type	POS malware, Reconnaissance, Backdoor, Keylogger, Info stealer, Credential stealer, Botnet
Description	(Trend Micro) Based on our analysis of the malware, BKDR_DEXTR.A downloads files, sends information, and checks memory for i others. But the centerpiece of the malware is its ability to collect and send certain information to a remote server. Some of the possible stolen from POS systems include such as username, hostname, key to decrypt the sent information, OS information, and list of running data are then presumably duplicated by remote malicious users. The malware executable is found to be packed or encrypted and when loaded, it loads long garbage code to decrypt the actual code. H decryption routine involves only a combination of XOR and ADD instructions, with the use of a hardcoded key. The perpetrators behi probably done this to make analysis difficult.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/infostealer-dexter-targets-checkout-systems/> <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-dexter-malware-getting-your-hands-dirty/> <https://securitykitten.github.io/2014/12/01/lusypos-and-tor.html> <https://volatility-labs.blogspot.com/2012/12/unpacking-dexter-pos-memory-dump.html> <https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25658/en_US/McAfee_La LusyPOS.pdf> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf> <https://www.secureworks.com/research/point-of-sale-malware-threats> <https://www.us-cert.gov/ncas/alerts/TA14-002A>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dexter>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool Dexter

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

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