Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:12:14 UTC

Tool: BrutPOS

Names	BrutPOS
Category	Malware
Type	POS malware, Backdoor, Credential stealer, Botnet
Description	(FireEye) There have been an increasing number of headlines about breaches at retailers in which attackers have made off with credit card data after compromising point-of-sale (POS) terminals. However, what is not commonly discussed is the fact that one third of these breaches are a result of weak default passwords in the remote administration software that is typically installed on these systems. While advanced exploits generate a lot of interest, sometimes it’s defending the simple attacks that can keep your company from the headlines. In this report, we document a botnet that we call BrutPOS which uses thousands of compromised computers to scan specified IP address ranges for RDP servers that have weak or default passwords in an effort to locate vulnerable POS systems.
Information	<https://www.fireeye.com/blog/threat-research/2014/07/brutpos-rdp-bruteforcing-botnet-targeting-pos-systems.html> <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.brutpos>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool BrutPOS

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=d064434d-c204-495f-843d-11df9afc9c6f