Grateful POS - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:01:46 UTC

Tool: Grateful POS

Names	Grateful POS TRINITY
Category	Malware
Type	POS malware, Info stealer
Description	POS malware targets systems that run physical point-of-sale device and operates by inspecting the process memory for data that matches the structure of credit card data (Track1 and Track2 data), such as the account number, expiration date, and other information stored on a card's magnetic stripe. After the cards are first scanned, the personal account number (PAN) and accompanying data sit in the point-of-sale system's memory unencrypted while the system determines where to send it for authorization. Masked as the LogMein software, the GratefulPOS malware appears to have emerged during the fall 2017 shopping season with low detection ratio according to some of the earliest detections displayed on VirusTotal. The first sample was upload in November 2017. Additionally, this malware appears to be related to the BlackPOS malware, which was linked to some of the high-profile merchant breaches in the past.
Information	<https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf> <https://www.vkremez.com/2017/12/lets-learn-reversing-grateful-point-of.html> <https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.grateful_pos>

Last change to this tool card: 22 May 2020

Download this tool card in JSON format

All groups using tool Grateful POS

Changed	Name	Country	Observed

APT groups

	FIN6, Skeleton Spider	[Unknown]	2015-Oct 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5fd2dd27-ea9b-4c29-b6fd-b64ee1a5c0bb