# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:04:59 UTC



## Tool: LockPOS

| | |
|---|---|
| Names | LockPOS |
| Category | Malware |
| Type | POS malware, Credential stealer |
| Description | (Cylance) LockPOS is a point-of-sale malware discovered in 2017 that is used to exfiltrate payment card data from targeted point-of-sale systems' memory. The most recent version of LockPOS examined here changed its injection technique to drop the malware directly to the kernel to evade detection and bypass traditional antivirus (AV) hooks. |
| Information | <https://threatvector.cylance.com/en_us/home/threat-spotlight-lockpos-point-of-sale-malware.html> <https://www.arbornetworks.com/blog/asert/lockpos-joins-flock/> <https://www.cyberbit.com/new-lockpos-malware-injection-technique/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.lock_pos> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:LockPoS> |

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

### All groups using tool LockPOS

| 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=d309aab8-3ff4-4f80-8d7f-a1834714fac9