# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:29:09 UTC



## Tool: Baka

| | |
|---|---|
| Names | Baka |
| Category | Malware |
| Type | Banking trojan, Info stealer, Exfiltration |
| Description | (Visa) In February 2020, Visa Payment Fraud Disruption (PFD), using the eCommerce Threat Disruption (eTD) capability, identified a previously unknown ecommerce skimmer, and named the skimmer 'Baka'. PFD made the discovery while analyzing a command and control (C2) server that was previously observed hosting the ImageID skimmer variant. PFD's investigation revealed seven C2 servers hosting the Baka skimming kit. While the skimmer itself is basicand contains the expected features offered by many ecommerce skimming kits (e.g. data exfiltration using image requests and configurable target form fields), the Bakaskimming kit's advanced design indicates it was created by a skilled developer. |
| Information | <https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/visa-security-alert-baka-javascript-skimmer.pdf> |

Last change to this tool card: 17 September 2020

Download this tool card in JSON format

### All groups using tool Baka

| 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=ec9c9bc1-624c-407a-891f-cf4181410906