# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:03:37 UTC



## Tool: Gelup

| | |
|---|---|
| Names | Gelup |
| Category | Malware |
| Type | Downloader |
| Description | (Trend Micro) In the same June 20 campaign, we also found another apparently new, undisclosed malware, which we named “Gelup”. A custom packer was also used to pack some variants of this malware. Again, it uses the same packer that TA505 has been using.<br><br>The unpacked payload is written in C++ and basically works as a downloader for another malware. What makes Gelup different, however, is its obfuscation technique and UAC-bypassing function bymocking trusted directories (spoofing the file’s execution path in a trusted directory), abusing auto-elevated executables, and using the dynamic-link library (DLL) side-loading technique.<br><br>First, Gelup resolves most Windows application programming interfaces (APIs) by using the hash just before calling it —a common technique used by a lot of malware families. Second, the strings in Gelup’s code are decrypted at runtime. |
| Information | <https://documents.trendmicro.com/assets/Tech-Brief-Latest-Spam-Campaigns-from-TA505-Now-Using-New-Malware-Tools-Gelup-and-FlowerPippi.pdf> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:Gelup> |

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

### All groups using tool Gelup

| Changed | Name | Country | Observed |
|---|---|---|---|
| **APT groups** | | | |

| | | | | |
|---|---|---|---|---|
| | TA505, Graceful Spider, Gold Evergreen |  | 2006-Nov 2022 |  |

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

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fabed506-43cc-4663-8ad1-586396c8b76a