# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:54:28 UTC



## Tool: FudModule

| | |
|---|---|
| Names | FudModule |
| Category | Malware |
| Type | Rootkit |
| Description | (Avast) The entire goal of the admin-to-kernel exploit was to corrupt the current thread's PreviousMode. This allows for a powerful kernel read/write primitive, where the affected user-mode thread can read and write arbitrary kernel memory using the Nt(Read\|Write)VirtualMemory syscalls. Armed with this primitive, the FudModule rootkit employs direct kernel object manipulation (DKOM) techniques to disrupt various kernel security mechanisms. It's worth reiterating that FudModule is a data-only rootkit, meaning it executes entirely from user space and all the kernel tampering is performed through the read/write primitive. |
| Information | <https://decoded.avast.io/janvojtesek/lazarus-and-the-fudmodule-rootkit-beyond-byovd-with-an-admin-to-kernel-zero-day/> <https://download.ahnlab.com/global/brochure/Analysis-Report-on-Lazarus-Groups-Rootkit-Attack-Using-BYOVD.pdf> <https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Lazarus-and-BYOVD-evil-to-the-Windows-core.pdf> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.fudmodule> |

Last change to this tool card: 07 March 2024

Download this tool card in JSON format

### All groups using tool FudModule

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

| | | | | |
|---|---|---|---|---|
| | Lazarus Group, Hidden Cobra, Labyrinth Chollima |  | 2007-May 2025 |  |

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

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=743359c4-0623-4c9a-b969-f318cb3aaa66