


# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:18:36 UTC

## APT group: Earth Lamia

|             |   |
|-------------|---|
| Names       | Earth Lamia ( <i>Trend Micro</i> )  |
| Country     |  <a href="#">China</a>   |
| Motivation  | <a href="#">Information theft and espionage</a>   |
| First seen  | 2023  |
| Description | <p>(<a href="#">Trend Micro</a>) Trend Research has identified Earth Lamia as an APT threat actor that exploits vulnerabilities in web applications to gain access to organizations, using various techniques for data exfiltration.</p> <p>Earth Lamia develops and customizes hacking tools to evade detection, such as PULSEPACK and BypassBoss.</p> <p>Earth Lamia has primarily targeted organizations in Brazil, India, and Southeast Asia since 2023. Initially focused on financial services, the group shifted to logistics and online retail, most recently focusing on IT companies, universities, and government organizations.</p> |
| Observed    | Sectors: <a href="#">Education</a> , <a href="#">Financial</a> , <a href="#">Government</a> , <a href="#">IT</a> , <a href="#">Retail</a> , <a href="#">Shipping and Logistics</a> .<br>Countries: <a href="#">Brazil</a> , <a href="#">India</a> , <a href="#">Indonesia</a> , <a href="#">Malaysia</a> , <a href="#">Philippines</a> , <a href="#">Thailand</a> , <a href="#">Vietnam</a> .   |
| Tools used  | <a href="#">BypassBoss</a> , <a href="#">PULSEPACK</a> .  |
| Information | < <a href="https://www.trendmicro.com/en_us/research/25/e/earth-lamia.html">https://www.trendmicro.com/en_us/research/25/e/earth-lamia.html</a> >   |

Last change to this card: 27 June 2025

Download this actor card in [PDF](#) or [JSON](#) format

---

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=17ebc5f9-e718-4b31-b0ba-5abe21916af5>