# LevelBlue - Open Threat Exchange

By TheNewRaikage

Archived: 2026-04-06 00:16:17 UTC

## Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

## MoonWind

MoonWind is a remote access trojan (RAT) that was used with the Trochilus RAT from September 2016 through late November 2016 by the same threat actor. It was compiled using the same compiler as BlackMoon banking trojan.

- 8 Subscribers

## Trochilus and New MoonWind RATs Used In Attack Against Thai Organizations

**FileHash-SHA256:** 6 | **IPv4:** 1 | **Hostname:** 1

From September 2016 through late November 2016, a threat actor group used both the Trochilus RAT and a newly idenfied RAT we've named MoonWind to target organizations in Thailand, including a utility organization. We chose the name 'MoonWind' based on debugging strings we saw within the samples, as well as the compiler used to generate the samples. The attackers compromised two legitimate Thai websites to host the malware, which is a tactic this group has used in the past. Both the Trochilus and MoonWind RATs were hosted on the same compromised sites and used to target the same organization at the same time. The attackers used different command and control servers (C2s) for each malware family, a tactic we believe was meant to thwart attempts to tie the attacks together using infrastructure alone. The compromised websites are the site for a group of information technology companies in Thailand, and all the tools were stored in the same directory.

- 374,032 Subscribers

---

Source: https://otx.alienvault.com/browse/pulses?q=tag:moonwind