


# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:24:05 UTC

[Home](#) > [List all groups](#) > Operation SLOW#TEMPEST

## APT group: Operation SLOW#TEMPEST

Names	Operation SLOW#TEMPEST (?)
Country	 <a href="#">China</a>
Motivation	<a href="#">Information theft and espionage</a>
First seen	2024
Description	<a href="#">(Securonix)</a> The Securonix Threat Research team has uncovered a covert campaign targeting Chinese-speaking users with Cobalt Strike payloads likely delivered through phishing emails. The attackers managed to move laterally, establish persistence and remain undetected within the systems for more than two weeks.
Observed	Countries: <a href="#">China</a> .
Tools used	<a href="#">Cobalt Strike</a> , <a href="#">Mimikatz</a> .
Information	< <a href="https://www.securonix.com/blog/from-cobalt-strike-to-mimikatz-slowtempest/">https://www.securonix.com/blog/from-cobalt-strike-to-mimikatz-slowtempest/</a> > < <a href="https://unit42.paloaltonetworks.com/slow-tempest-malware-obfuscation/">https://unit42.paloaltonetworks.com/slow-tempest-malware-obfuscation/</a> >

Last change to this card: 16 August 2025

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

---

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=74200598-520d-4bf8-af62-e1fc08587450>