

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:50:53 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Elise

## Tool: Elise

Names	Elise BKDR_ESILE EVILNEST Page
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a> , <a href="#">Exfiltration</a>
Description	<a href="#">(Palo Alto)</a> We believe that the Lotus Blossom group developed the Elise malware specifically to meet the needs of the attack campaigns, and we've observed three variants across 50 samples during the three-year period of these attacks. Elise is a relatively sophisticated tool, including variants with the ability to evade detection in virtual environments, connect to command-and-control servers for additional instruction, and exfiltrate data.
Information	< <a href="https://unit42.paloaltonetworks.com/operation-lotus-blossom/">https://unit42.paloaltonetworks.com/operation-lotus-blossom/</a> > < <a href="https://www.accenture.com/t20180127T003755Z_w_/us-en/acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf">https://www.accenture.com/t20180127T003755Z_w_/us-en/acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf</a> > < <a href="https://researchcenter.paloaltonetworks.com/2016/02/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/">https://researchcenter.paloaltonetworks.com/2016/02/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/</a> > < <a href="https://www.joesecurity.org/blog/8409877569366580427">https://www.joesecurity.org/blog/8409877569366580427</a> >
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S0081/">https://attack.mitre.org/software/S0081/</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.elise">https://malpedia.caad.fkie.fraunhofer.de/details/win.elise</a> >


Last change to this tool card: 30 December 2022

Download this tool card in [JSON](#) format

## All groups using tool Elise

Changed	Name	Country	Observed
---------	------	---------	----------

## APT groups

	<a href="#">Lotus Blossom, Spring Dragon, Thrip</a>		2012-Aug 2024	
--	---	--	---------------	--

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f16f218c-6241-45d3-a9e3-9c4551aab26d>