

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:50:53 UTC

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



## Tool: GRAYFISH

Names	GRAYFISH
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a>
Description	( <a href="#">Kaspersky</a> ) The most sophisticated attack platform from the EQUATION group. It resides completely in the registry, relying on a bootkit to gain execution at OS startup.
Information	< <a href="https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf">https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf</a> >
AlienVault OTX	< <a href="https://otx.alienvault.com/browse/pulses?q=tag:grayfish">https://otx.alienvault.com/browse/pulses?q=tag:grayfish</a> >

Last change to this tool card: 20 April 2020

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

### All groups using tool GRAYFISH

Changed	Name	Country	Observed	
<b>APT groups</b>				
	<a href="#">Equation Group</a>		2001-Aug 2016	

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a0e07804-b87f4150-abe9-cc9fb0fd147f>