Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:05:50 UTC

Tool: FinFisher

Names	FinFisher FinFisher RAT FinSpy
Category	Malware
Type	Backdoor, Info stealer
Description	FinFisher is a government-grade commercial surveillance spyware reportedly sold exclusively to government agencies for use in targeted and lawful criminal investigations. It is heavily obfuscated and uses multiple anti-analysis techniques. It has other variants including Wingbird.
Information	<https://www.microsoft.com/security/blog/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/> <https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/> <https://artemonsecurity.blogspot.de/2017/01/finfisher-rootkit-analysis.html> <https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html> <https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/> <https://www.welivesecurity.com/wp-content/uploads/2018/01/WP-FinFisher.pdf> <http://www.msreverseengineering.com/blog/2018/1/23/a-walk-through-tutorial-with-code-on-statically-unpacking-the-finspy-vm-part-one-x86-deobfuscation> <https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/> <https://en.wikipedia.org/wiki/FinFisher> <https://securelist.com/finspy-unseen-findings/104322/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0182/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.finfisher> <https://malpedia.caad.fkie.fraunhofer.de/details/win.finfisher>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:finfisher>

Last change to this tool card: 02 November 2021

Download this tool card in JSON format

All groups using tool FinFisher

Changed	Name	Country	Observed	
APT groups				
	BlackOasis	[Middle East]	2015-Oct 2017	
	Dark Caracal		2007-Jun 2024	
	SandCat		2018	

3 groups listed (3 APT, 0 other, 0 unknown)

↑

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0475a304-5916-40c5-9b5b-8fce9f52e783