

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:12:02 UTC

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

## Tool: ISMInjector

Names	ISMInjector Agent Injector
Category	<a href="#">Malware</a>
Type	<a href="#">Loader</a>
Description	<a href="#">(Palo Alto)</a> In August 2017, we found this threat group has developed yet another Trojan that they call 'Agent Injector' with the specific purpose of installing the <a href="#">ISMAgent</a> backdoor. We are tracking this tool as ISMInjector. It has a sophisticated architecture and contains anti-analysis techniques that we have not seen in previous tools developed by this threat group. The complex structure and inclusion of new anti-analysis techniques may suggest that this group is increasing their development efforts in order to evade detection and gain higher efficacy in their attacks.
Information	< <a href="https://unit42.paloaltonetworks.com/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/">https://unit42.paloaltonetworks.com/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/</a> >
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S0189/">https://attack.mitre.org/software/S0189/</a> >
AlienVault OTX	< <a href="https://otx.alienvault.com/browse/pulses?q=tag:ISMInjector">https://otx.alienvault.com/browse/pulses?q=tag:ISMInjector</a> >

Last change to this tool card: 22 April 2020

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

### All groups using tool ISMInjector

Changed	Name	Country	Observed	
<b>APT groups</b>				
	<a href="#">OilRig</a> , <a href="#">APT 34</a> , <a href="#">Helix Kitten</a> , <a href="#">Chrysene</a>		2014-Sep 2024	

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

Source: <https://apt.eta-da.or.th/cgi-bin/listgroups.cgi?u=323162c2-b731-4641-8797-5870730ddb32>