

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:41:07 UTC

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

## Tool: Alma Communicator

Names	Alma Communicator
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a> , <a href="#">Tunneling</a>
Description	<a href="#">(Palo Alto)</a> Recently, we observed a new version of the <a href="#">Clayslide</a> delivery document used to install a new custom Trojan whose developer calls it “ALMA Communicator”. The delivery document also saved the post-exploitation credential harvesting tool known as <a href="#">Mimikatz</a> , which we believe the threat actors will use to gather account credentials from the compromised system.
Information	< <a href="https://unit42.paloaltonetworks.com/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/">https://unit42.paloaltonetworks.com/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/</a> > < <a href="https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/">https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.alma_communicator">https://malpedia.caad.fkie.fraunhofer.de/details/win.alma_communicator</a> >

Last change to this tool card: 13 May 2020

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

### All groups using tool Alma Communicator

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.or.th/cgi-bin/listgroups.cgi?u=0b467acc-1e16-4e2d-9946-0e84e679c343>