

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:33:37 UTC

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

## Tool: StarsyPound

Names	StarsyPound
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a>
Description	( <a href="#">Trend Micro</a> ) When the malware is run, it drops a backdoor such as STARSYPOUND or <a href="#">Bouncer</a> . These first stage tools push a backdoor to the attacker for later access. (These could be considered first stage tools). It allows the attacker to maintain persistence and get access to the system at a later time.
Information	< <a href="https://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/">https://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/</a> > < <a href="http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.starsypound">https://malpedia.caad.fkie.fraunhofer.de/details/win.starsypound</a> >

Last change to this tool card: 23 April 2020

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

### All groups using tool StarsyPound

Changed	Name	Country	Observed	
<b>APT groups</b>				
	<a href="#">Comment Crew, APT 1</a>		2006-May 2018	

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2975e579-d0cc-40fb-b1c8-b085a79c83d6>