

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:34:50 UTC

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

## Tool: ZeroT

Names	ZeroT
Category	<a href="#">Malware</a>
Type	<a href="#">Downloader</a>
Description	( <a href="#">Proofpoint</a> ) Since the summer of 2016, this group began using a new downloader known as ZeroT to install the <a href="#">PlugX</a> remote access Trojan (RAT) and added Microsoft Compiled HTML Help (.chm) as one of the initial droppers delivered in spear-phishing emails.
Information	< <a href="https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zero-t-plugx">https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zero-t-plugx</a> >
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S0230/">https://attack.mitre.org/software/S0230/</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.zerot">https://malpedia.caad.fkie.fraunhofer.de/details/win.zerot</a> >

Last change to this tool card: 23 April 2020

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

### All groups using tool ZeroT

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">TA459</a>		2017-Apr 2022

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