

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:47:31 UTC

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


Tool: NewPass

Names	NewPass
Category	Malware
Type	Dropper , Loader , Backdoor , Info stealer , Exfiltration
Description	<p>(Telsy) NewPass is quite a complex malware composed by different components that rely on an encoded file to pass information and configuration between each other. There are at least three components of the malware: a dropper, that deploys the binary file; a loader library, that is able to decode the binary file extracting the last component, responsible for performing specific operations, such as communicate with the attackers' command and control server (the "agent")</p> <p>The loader and the agent share a JSON configuration resident in memory that demonstrate the potential of the malware and the ease with which the attackers can customize the implant by simply changing the configuration entries' values.</p>
Information	< https://www.telsy.com/turla-venomous-bear-updates-its-arsenal-newpass-appears-on-the-apt-threat-scene/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.newpass >

Last change to this tool card: 24 April 2021

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

All groups using tool NewPass

Changed	Name	Country	Observed
APT groups			
	Turla , Waterbug , Venomous Bear		1996-2024

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=d41d2836-84ec-437b-8be4-f112271f88e9>