Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:38:58 UTC

Tool: Z*Stealer

Names	Z*Stealer ZStealer
Category	Malware
Type	Backdoor, Credential stealer
Description	(Forecepoint) ZS.DLL.C is another Delphi based library, this time for stealing both OS and application login credentials. As with the cryptocurrency stealer, once the password scan is completed the extracted information is transferred to the C2 by HTTP POST request to a PHP page on the server side. Based on data retrieved from the C2 servers, the credential stealing capability seems to be comparatively successful at retrieving data. A range of commonly used applications are supported.
Information	<https://www.forcepoint.com/blog/x-labs/quantize-or-capitalize>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.zstealer>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool Z*Stealer

Changed	Name	Country	Observed	
Other groups				
	Guru Spider		2014-Mar 2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=728e24c5-46cb-438a-b2c4-b4f8fd637829