Threat Group Cards: A Threat Actor Encyclopedia

Tool: TIDYELF

Names	TIDYELF
Category	Malware
Type	Dropper
Description	(FireEye) TIDYELF is a dropper for the WINTERLOVE backdoor. WINTERLOVE has been observed embedded within a resource within TIDYELF. TIDYELF will load the main WINTERLOVE component by injecting it into the iexplore.exe process. It will then create a registry key named HKLM\SOFTWARE\RAT to store configuration data for WINTERLOVE components to use.
Information	<https://paper.bobylive.com/Security/APT_Report/APT-41.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool TIDYELF

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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