Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:49:48 UTC

Tool: Cutwail

Names	Cutwail Pushdo
Category	Malware
Type	Botnet, Downloader
Description	Pushdo is usually classified as a 'downloader' trojan - meaning its true purpose is to download and install additional malicious software. There are dozens of downloader trojan families out there, but Pushdo is actually more sophisticated than most, but that sophistication lies in the Pushdo control server rather than the trojan.
Information	<https://www.blueliv.com/research/tracking-the-footproints-of-pushdo-trojan/> <https://www.trendmicro.de/cloud-content/us/pdfs/business/white-papers/wp_study-of-pushdo-cutwail-botnet.pdf> <https://www.secureworks.com/research/pushdo> <http://malware-traffic-analysis.net/2017/04/03/index2.html> <https://securityintelligence.com/posts/dridex-campaign-propelled-by-cutwail-botnet-and-powershell/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cutwail> <https://malpedia.caad.fkie.fraunhofer.de/details/win.pushdo>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:cutwail>

Last change to this tool card: 20 April 2021

Download this tool card in JSON format

All groups using tool Cutwail

Changed	Name	Country	Observed

Other groups

	Narwhal Spider	[Unknown]	2007-Oct 2018	

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