Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:38:34 UTC

Tool: DNSExfitrator

Names	DNSExfitrator
Category	Malware
Type	Exfiltration, Tunneling
Description	(Kasperksy) At the end of May, we observed that Oilrig had included the DNSExfitrator tool in its toolset. It allows the threat actor to use the DNS over HTTPS (DoH) protocol. Use of the DNS protocol for malware communications is a technique that Oilrig has been using for a long time. The difference between DNS- and DoH-based requests is that, instead of plain text requests to port 53, they would use port 443 in encrypted packets. Oilrig added the publicly available DNSExfiltrator tool to its arsenal, which allows DoH queries to Google and Cloudflare services. This time, the operators decided to use subdomains of a COVID-related domain which are hardcoded in the DNSExfitrator detected samples.
Information	<https://securelist.com/apt-trends-report-q2-2020/97937/>

Last change to this tool card: 30 July 2020

Download this tool card in JSON format

All groups using tool DNSExfitrator

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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