Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:57:51 UTC

Tool: DeputyDog

Names	DeputyDog Fexel
Category	Malware
Type	Backdoor
Description	(FireEye) FireEye detected the payload used in these attacks on August 23, 2013 in Japan. The payload was hosted on a server in Hong Kong (210.176.3.130) and was named “img20130823.jpg”. Although it had a .jpg file extension, it was not an image file. The file, when XORed with 0x95, was an executable (MD5: 8aba4b5184072f2a50cbc5ecfe326701). Upon execution, 8aba4b5184072f2a50cbc5ecfe326701 writes “28542CC0.dll” (MD5: 46fd936bada07819f61ec3790cb08e19) to this location: C:\Documents and Settings\All Users\Application Data\28542CC0.dll In order to maintain persistence, the original malware adds this registry key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\28542CC0 The registry key has this value: rundll32.exe “C:\Documents and Settings\All Users\Application Data\28542CC0.dll”,Launch The malware (8aba4b5184072f2a50cbc5ecfe326701) then connects to a host in South Korea (180.150.228.102). This callback traffic is HTTP over port 443 (which is typically used for HTTPS encrypted traffic; however, the traffic is not HTTPS nor SSL encrypted).
Information	<https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.deputydog>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:deputydog>

Last change to this tool card: 26 May 2020

Download this tool card in JSON format

All groups using tool DeputyDog

Changed	Name	Country	Observed	
APT groups				
	APT 17, Deputy Dog, Elderwood, Sneaky Panda		2009-Jun 2024	
	Axiom, Group 72		2008-2008/2014	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=af3da544-f3b5-4e82-805b-4cd731f625ca