Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:59:05 UTC

Home > List all groups > List all tools > List all groups using tool NetFlash

Tool: NetFlash

Names	NetFlash
Category	Malware
Type	Dropper
Description	(ESET) a .NET application that dropped an installer for Adobe Flash v32 in %TEMP%\adobe.exe, and NetFlash (a .NET downloader) in %TEMP%\winhost.exe. According to their compilation timestamps, the malware samples were compiled at the end of August 2019 and at the beginning on September 2019, right before being uploaded to the watering hole's C&C server. NetFlash downloads its second stage malware from a hardcoded URL and establishes persistence for this new backdoor using a Windows scheduled task. Figure 5 shows the NetFlash function that downloads the second stage malware, named PyFlash.
Information	<https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.netflash>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:NetFlash>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool NetFlash

Changed	Name	Country	Observed	
APT groups				
	Turla, Waterbug, Venomous Bear		1996-2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8f1534db-c4ab-4e5d-927f-36b3cd4c632d