Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:19:07 UTC

Tool: PyFlash

Names	PyFlash
Category	Malware
Type	Backdoor
Description	(ESET) This second stage backdoor is a py2exe executable. py2exe is a Python extension to convert a Python script into a standalone Windows executable. To our knowledge, this is the first time the Turla developers have used the Python language in a backdoor. The backdoor communicates with its hardcoded C&C server via HTTP. The C&C URL and other parameters such as the AES key and IV used to encrypt all network communications are specified at the beginning of the script. The C&C server can also send backdoor commands in JSON format. The commands implemented in this version of PyFlash are: • Download additional files from a given HTTP(S) link. • Execute a Windows command using the Python function subprocess32.Popen. • Change the execution delay: modifies the Windows task that regularly (every X minutes; 5 by default) launches the malware. • Kill (uninstall) the malware.
Information	<https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PyFlash>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool PyFlash

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=c48d96e8-d9ad-4bfa-beb4-ba44b70c77cd