Threat Group Cards: A Threat Actor Encyclopedia

Tool: Pylot

Names	Pylot Travle
Category	Malware
Type	Backdoor, Info stealer
Description	(Carbon Black) The Pylot (or Travle) malware family appears to be an evolution of the NetTraveler malware family (which has been linked to attackers out of China by numerous sources). Over the last year a variant has been observed as a secondary payload often used in conjunction with malicious carrier files (typically MS Office or Rich Text Format (RTF) documents). The Pylot malware has been observed being installed via shellcode from known CVEs in Office products as well as by malware loaders (or first stage malware variants, specifically the CMStar malware family). In late 2017 samples of the Pylot family were submitted, by customers, to the Carbon Black Threat Analysis Unit (TAU) as part of ongoing investigation.
Information	<https://www.carbonblack.com/2018/01/26/threat-analysis-pylot-travle-malware-family/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PYLOT>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Pylot

Changed	Name	Country	Observed	
APT groups				
	Vicious Panda		2015-Mar 2020	

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