Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:56:32 UTC

Tool: POWBAT

Names	POWBAT
Category	Malware
Type	Info stealer, Exfiltration, Tunneling
Description	(FireEye) After the macro successfully creates the scheduled task, the dropped VBScript, update.vbs (Figure 5), will be launched every three minutes. This VBScript performs the following operations: 1. Leverages PowerShell to download content from the URI hxxp://go0gIe[.]com/sysupdate.aspx?req=xxx\dwn&m=d and saves it in the directory %PUBLIC%\Libraries\dn. 2. Uses PowerShell to download a BAT file from the URI hxxp://go0gIe[.]com/sysupdate.aspx?req=xxx\bat&m=d and saves it in the directory %PUBLIC%\Libraries\dn. 3. Executes the BAT file and stores the results in a file in the path %PUBLIC%\Libraries\up. 4. Uploads this file to the server by sending an HTTP POST request to the URI hxxp://go0gIe[.]com/sysupdate.aspx?req=xxx\upl&m=u. 5. Finally, it executes the PowerShell script dns.ps1, which is used for the purpose of data exfiltration using DNS.
Information	<https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html> <https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool POWBAT

Changed	Name	Country	Observed

APT groups

	Chafer, APT 39		2014-Sep 2020	
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e87032a7-d42b-4d9b-a20e-9380e1c51cd7