Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:54:15 UTC

Tool: Ebury

Names	Ebury
Category	Malware
Type	Backdoor, Credential stealer, Botnet
Description	(ESET) An OpenSSH backdoor used to keep control of the servers and steal credentials.
Information	<https://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf> <https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/> <https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET-The_Dark_Side_of_the_ForSSHe.pdf> <https://www.welivesecurity.com/2017/10/30/windigo-ebury-update-2/> <https://web-assets.esetstatic.com/wls/en/papers/white-papers/ebury-is-alive-but-unseen.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0377/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.ebury>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Ebury>

Last change to this tool card: 18 June 2024

Download this tool card in JSON format

All groups using tool Ebury

Changed	Name	Country	Observed	
Other groups				
	Operation Windigo		2011-Mar 2017	

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

↑

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6e2c66f6-347d-427f-929e-425e298bb480