Operation Windigo - Threat Group Cards: A Threat Actor Encyclopedia

Other threat group: Operation Windigo

Names	Operation Windigo *(ESET)* G0124 *(MITRE)*
Country	Russia
Motivation	Financial gain
First seen	2011
Description	(ESET) This document details a large and sophisticated operation, code named “Windigo”, in which a malicious group has compromised thousands of Linux and Unix servers. The compromised servers are used to steal SSH credentials, redirect web visitors to malicious content and send spam. This operation has been ongoing since at least 2011 and has affected high profile servers and companies, including cPanel – the company behind the famous web hosting control panel – and Linux Foundation’s kernel.org – the main repository of source code for the Linux kernel. However this operation is not about stealing company resources or altering Linux’s source code as we will unveil throughout the report. The complexity of the backdoors deployed by the malicious actors shows out of the ordinary knowledge of operating systems and programming. Additionally, extra care was given to ensure portability, meaning the various pieces of malware will run on a wide range of server operating systems and to do so in an extremely stealthy fashion. The Windigo operation does not leverage any new vulnerability against Linux or Unix systems. Known systemic weaknesses were exploited by the malicious actors in order to build and maintain their botnet.
Observed	Countries: Worlwide.
Tools used	Calfbot, CDorked, Ebury.

Counter operations	Mar 2017	Russian Citizen Pleads Guilty for Involvement in Global Botnet Conspiracy <https://www.justice.gov/opa/pr/russian-citizen-pleads-guilty-involvement-global-botnet-conspiracy>
Information	<https://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0124/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
