Threat Group Cards: A Threat Actor Encyclopedia

Other threat group: Andromeda Spider

Names	Andromeda Spider *(CrowdStrike)*	
Country	Belarus	
Motivation	Financial gain	
First seen	2011	
Description	(Virus Bulletin) Andromeda, also known as Gamaru and Wauchos, is a modular and HTTP-based botnet that was discovered in late 2011. From that point on, it managed to survive and continue hardening by evolving in different ways. In particular, the complexity of its loader and AV evasion methods increased repeatedly, and C&C communication changed between the different versions as well. We deal with versions of this threat on a daily basis and we have collected a number of different variants. The botnet first came onto our tracking radar at version 2.06, and we have tracked the versions since then. In this paper we will describe the evolution of Andromeda from version 2.06 to 2.10 and demonstrate both how it has improved its loader to evade automatic analysis/detection and how the payload varies among the different versions. This article could also be seen as a way to say 'goodbye' to the botnet: a takedown effort, followed by the arrest of the suspected botnet owner in December 2017, may mean we have seen the last of the botnet that has plagued Internet users for more than half a decade. The Andromeda botnet has been observed to be used by Transparent Tribe, APT 36.	
Observed	Countries: Worldwide.	
Tools used	Andromeda.	
Counter operations	Nov 2017	Andromeda botnet dismantled in international cyber operation <https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation>

Information	<https://blog.avast.com/andromeda-under-the-microscope> <https://www.virusbulletin.com/virusbulletin/2018/02/review-evolution-andromeda-over-years-we-say-goodbye/>

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format
