Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:31:31 UTC

Other threat group: Avalanche

Names	Avalanche *(?)*	
Country	Russia	
Motivation	Financial gain	
First seen	2006	
Description	(US-CERT) Cyber criminals utilized Avalanche botnet infrastructure to host and distribute a variety of malware variants to victims, including the targeting of over 40 major financial institutions. Victims may have had their sensitive personal information stolen (e.g., user account credentials). Victims' compromised systems may also have been used to conduct other malicious activity, such as launching denial-of-service (DoS) attacks or distributing malware variants to other victims' computers. In addition, Avalanche infrastructure was used to run money mule schemes where criminals recruited people to commit fraud involving transporting and laundering stolen money or merchandise. Avalanche used fast-flux DNS, a technique to hide the criminal servers, behind a constantly changing network of compromised systems acting as proxies. Avalanche has been observed to distribute GozNym (operated by Bamboo Spider, TA544|used-by}} and much of the malware from TA505, Graceful Spider, Gold Evergreen.	
Observed	Countries: Worldwide.	
Tools used	Avalanche.	
Operations performed	May 2010	Worst Phishing Pest May be Revving Up <https://www.pcworld.com/article/196304/worst_phishing_pest_may_be_revving_up.html
Counter operations	Dec 2016	'Avalanche' network dismantled in international cyber operation <https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation>
Information	<https://en.wikipedia.org/wiki/Avalanche_(phishing_group)> <https://www.us-cert.gov/ncas/alerts/TA16-336A>	

Last change to this card: 15 May 2020

Download this actor card in PDF or JSON format
