El Machete - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:05:57 UTC

APT group: El Machete

Names	El Machete *(Kaspersky)* TEMP.Andromeda *(FireEye)* APT-C-43 *(Qihooo 360)* ATK 97 *(Thales)* TAG-NS1 *(Recorded Future)* G0095 *(MITRE)*	
Country	[Unknown]	
Motivation	Information theft and espionage	
First seen	2010	
Description	(Kaspersky) “Machete” is a targeted attack campaign with Spanish speaking roots. We believe this campaign started in 2010 and was renewed with an improved infrastructure in 2012. The operation may be still “active”. The malware is distributed via social engineering techniques, which includes spear-phishing emails and infections via Web by a fake Blog website. We have found no evidence of exploits targeting zero-day vulnerabilities. Both the attackers and the victims appear to be Spanish-speaking. In some cases, such as Russia, the target appears to be an embassy from one of the countries of this list.	
Observed	Sectors: Defense, Education, Embassies, Energy, Government, Telecommunications. Countries: Argentina, Belgium, Bolivia, Brazil, Canada, China, Colombia, Cuba, Dominican Republic, Ecuador, France, Germany, Guatemala, Malaysia, Mexico, Nicaragua, Peru, Russia, South Korea, Spain, Sweden, UK, Ukraine, USA, Venezuela and others.	
Tools used	LokiBot, Machete, Pyark, Living off the Land.	
Operations performed	Mar 2017	We’ve found that this group has continued to operate successfully, predominantly in Latin America, since 2014. All attackers simply moved to new C2 infrastructure, based largely around dynamic DNS domains, in addition to making minimal changes to the malware in

		order to evade signature-based detection. <https://threatvector.cylance.com/en_us/home/el-machete-malware-attacks-cut-through-latam.html>
	Mar 2019	From the end of March up until the end of May 2019, ESET researchers observed that there were more than 50 victimized computers actively communicating with the C&C server. This amounts to gigabytes of data being uploaded every week. <https://www.welivesecurity.com/2019/08/05/sharpening-machete-cyberespionage/>
	Jun 2020	Operation “HpReact” In June 2020, 360 Security Center discovered a new backdoor Pyark written in Python by the fileless attack protection function. <https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/>
	Mar 2022	In mid-March, El Machete was spotted sending spear-phishing emails to financial organizations in Nicaragua, with an attached Word document titled “Dark plans of the neo-Nazi regime in Ukraine.” <https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/>
Information	<https://securelist.com/el-machete/66108/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0095/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
