Machete

attack.mitre.org/groups/G0095/

Machete is a suspected Spanish-speaking cyber espionage group that has been active since at least 2010. It has primarily focused its operations within Latin America, with a particular emphasis on Venezuela, but also in the US, Europe, Russia, and parts of Asia. Machete generally targets high-profile organizations such as government institutions, intelligence services, and military units, as well as telecommunications and power companies.[1][2][3][4]

ID: G0095

ⓘ

Associated Groups: APT-C-43, El Machete

Contributors: Matias Nicolas Porolli, ESET

Version: 2.0

Created: 13 September 2019

Last Modified: 06 October 2021

Version Permalink
Live Version

Associated Group Descriptions

Name	Description
APT-C-43	[4]
El Machete	[1]

Techniques Used

Domain	ID	Name	Use	
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Machete has used batch files to initiate additional downloads of malicious files.[4]
		.005	Command and Scripting Interpreter: Visual Basic	Machete has embedded malicious macros within spearphishing attachments to download additional files.[4]
		.006	Command and Scripting Interpreter: Python	Machete used multiple compiled Python scripts on the victim's system. Machete's main backdoor Machete is also written in Python.[1][3][4]
Enterprise	T1189	Drive-by Compromise	Machete has distributed Machete through a fake blog website.[2]	
Enterprise	T1036	.005	Masquerading: Match Legitimate Name or Location	Machete's Machete MSI installer has masqueraded as a legitimate Adobe Acrobat Reader installer.[4]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Machete has delivered spearphishing emails that contain a zipped file with malicious contents.[2][3][4]
		.002	Phishing: Spearphishing Link	Machete has sent phishing emails that contain a link to an external server with ZIP and RAR archives.[1][3]

Domain	ID	Name	Use	
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Machete has created scheduled tasks to maintain Machete's persistence.[4]
Enterprise	T1218	.007	System Binary Proxy Execution: Msiexec	Machete has used msiexec to install the Machete malware.[4]
Enterprise	T1204	.001	User Execution: Malicious Link	Machete has has relied on users opening malicious links delivered through spearphishing to execute malware.[1][2][3]
		.002	User Execution: Malicious File	Machete has relied on users opening malicious attachments delivered through spearphishing to execute malware.[1][2][3][4]

Software

ID	Name	References	Techniques

ID	Name	References	Techniques
S0409	Machete	[2][3]	Application Layer Protocol: Web Protocols, Application Layer Protocol: File Transfer Protocols, Application Window Discovery, Archive Collected Data: Archive via Custom Method, Archive Collected Data, Audio Capture, Automated Exfiltration, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Browser Bookmark Discovery, Clipboard Data, Command and Scripting Interpreter: Python, Credentials from Password Stores: Credentials from Web Browsers, Data Encoding: Standard Encoding, Data from Local System, Data from Removable Media, Data Staged: Local Data Staging, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, Encrypted Channel: Asymmetric Cryptography, Exfiltration Over C2 Channel, Exfiltration Over Physical Medium: Exfiltration over USB, Fallback Channels, File and Directory Discovery, Hide Artifacts: Hidden Files and Directories, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Input Capture: Keylogging, Masquerading: Masquerade Task or Service, Masquerading: Match Legitimate Name or Location, Obfuscated Files or Information: Software Packing, Obfuscated Files or Information, Peripheral Device Discovery, Process Discovery, Scheduled Task/Job: Scheduled Task, Scheduled Transfer, Screen Capture, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, Unsecured Credentials: Private Keys, Video Capture

References

The Cylance Threat Research Team. (2017, March 22). El Machete's Malware Attacks Cut Through LATAM. Retrieved September 13, 2019. Kaspersky Global Research and Analysis Team. (2014, August 20). El Machete. Retrieved September 13, 2019. ESET. (2019, July). MACHETE JUST GOT SHARPER Venezuelan government institutions under attack. Retrieved September 13, 2019. kate. (2020, September 25). APT-C-43 steals Venezuelan military secrets to provide intelligence support for the reactionaries — HpReact campaign. Retrieved November 20, 2020.