APT-C-36, Blind Eagle, Group G0099

attack.mitre.org/groups/G0099/

APT-C-36

APT-C-36 is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.[1]

Associated Group Descriptions

Name	Description
Blind Eagle	[1]

Techniques Used

Domain	ID	Name	Use	
Enterprise	T1059	.005	Command and Scripting Interpreter: Visual Basic	APT-C-36 has embedded a VBScript within a malicious Word document which is executed upon the document opening.[1]
Enterprise	T1105	Ingress Tool Transfer	APT-C-36 has downloaded binary data from a specified domain after the malicious document is opened.[1]	

Domain	ID	Name	Use	
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	APT-C-36 has disguised its scheduled tasks as those used by Google.[1]
Enterprise	T1571	Non-Standard Port	APT-C-36 has used port 4050 for C2 communications.[1]	
Enterprise	T1027	Obfuscated Files or Information	APT-C-36 has used ConfuserEx to obfuscate its variant of Imminent Monitor, compressed payload and RAT packages, and password protected encrypted email attachments to avoid detection.[1]	
Enterprise	T1588	.002	Obtain Capabilities: Tool	APT-C-36 obtained and used a modified variant of Imminent Monitor.[1]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	APT-C-36 has used spearphishing emails with password protected RAR attachment to avoid being detected by the email gateway.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	APT-C-36 has used a macro function to set scheduled tasks, disguised as those used by Google.[1]
Enterprise	T1204	.002	User Execution: Malicious File	APT-C-36 has prompted victims to accept macros in order to execute the subsequent payload.[1]

Software

ID	Name	References	Techniques
S0434	Imminent Monitor	[1]	Audio Capture, Command and Scripting Interpreter, Credentials from Password Stores: Credentials from Web Browsers, Deobfuscate/Decode Files or Information, Exfiltration Over C2 Channel, File and Directory Discovery, Hide Artifacts: Hidden Files and Directories, Impair Defenses: Disable or Modify Tools, Indicator Removal: File Deletion, Input Capture: Keylogging, Native API, Obfuscated Files or Information, Process Discovery, Remote Services: Remote Desktop Protocol, Resource Hijacking, Video Capture

References

1. QiAnXin Threat Intelligence Center. (2019, February 18). APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations. Retrieved May 5, 2020.