APT-C-36, Blind Eagle, Group G0099

Archived: 2026-04-02 11:20:35 UTC

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]
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.

Domain	ID		Name	Use
				[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]

Source: https://attack.mitre.org/groups/G0099/