Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:30:11 UTC

Tool: EtherealGh0st

Names	EtherealGh0st
Category	Malware
Type	Backdoor
Description	(Bitdefender) A variant of Gh0st RAT, evolved from TranslucentGh0st. The execution of the EthrealGh0st agent starts with the decryption of c2 addresses and ports, which are base64 encoded strings. After decoding, a SUB 6 operation is performed on the resulting buffer, and the c2 and port are passed down to establish the connection. Although the port is also encoded, it always has the same value, “Ojo5,” which corresponds to 443 after decryption.
Information	<https://blogapp.bitdefender.com/labs/content/files/2024/05/Bitdefender-Report-DeepDive-creat7721-en_EN.pdf>

Last change to this tool card: 18 June 2024

Download this tool card in JSON format

All groups using tool EtherealGh0st

Changed	Name	Country	Observed	
APT groups				
	Unfading Sea Haze		2018	

1 group listed (1 APT, 0 other, 0 unknown)