Turla

Turla is a cyber espionage threat group that has been attributed to Russia's Federal Security Service (FSB). They have compromised victims in over 50 countries since at least 2004, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies. Turla is known for conducting watering hole and spearphishing campaigns, and leveraging in-house tools and malware, such as Uroburos.[1][2][3][4][5]

ID: G0010

ⓘ Associated Groups: IRON HUNTER, Group 88, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear, Secret Blizzard, BELUGASTURGEON

Contributors: Matthieu Faou, ESET; Edward Millington

Version: 5.1

Created: 31 May 2017

Last Modified: 26 June 2024

Version Permalink

Associated Group Descriptions

Name	Description
IRON HUNTER	[6]
Group 88	[7]
Waterbug	Based similarity in TTPs and malware used, Turla and Waterbug appear to be the same group.[8]
WhiteBear	WhiteBear is a designation used by Securelist to describe a cluster of activity that has overlaps with activity described by others as Turla, but appears to have a separate focus.[9][10]
Snake	[3][11][10]
Krypton	[3]
Venomous Bear	[3][10]
Secret Blizzard	[12]
BELUGASTURGEON	[13]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1134	.002	Access Token Manipulation: Create Process with Token	Turla RPC backdoors can impersonate or steal process tokens before executing commands.[11]