Threat Category: APT / Backdoor Implant

Threat Description: The YARA rule rule14_h detects Grizzly Steppe-related backdoor implants, used by APT28/APT29 (Fancy Bear and Cozy Bear). The malware is associated with Russian state-sponsored cyber-espionage campaigns.

Indicators of Compromise (IoCs)

Obfuscated loader signature:

{6A ?? E8 ?? ?? FF FF 59 85 C0 74 0B 8B C8 E8 ?? ?? FF FF 8B F0 EB 02 33 F6 8B CE E8 ?? ?? FF FF 85 F6 74 0E 8B CE E8 ?? ?? FF FF 56 E8 ?? ?? FF FF 59}

Detection Mechanism:

Must be a Windows PE file with MZ (0x5A4D) header

Must match obfuscated implant loader signature

Possible Attribution & Use Cases:

Used in cyber-espionage campaigns against US and European entities

Linked to Russian intelligence-backed threat actors

Recommended Actions:

Investigate: Identify suspicious backdoor activity and C2 communications

Contain & Mitigate: Remove backdoor implants and block associated domains

Author & Attribution:

Rule Author: US CERT

Rule Version: 1

Reference ID: eb3fc39b-08ca-51df-a9b4-7b28b107b700