Threat Category: APT / Command and Control (C2) Infrastructure

Threat Description: The YARA rule detects Cozy Bear and Fancy Bear (APT28/APT29) C2 (Command and Control) server IP addresses used in cyber-espionage campaigns. These Russian state-sponsored APT groups have been linked to intrusions against governments, political entities, and critical infrastructure.

Indicators of Compromise (IoCs)

Known C2 IPs associated with APT28/APT29 operations:

185.100.84.134

58.49.58.58

218.1.98.203

187.33.33.8

185.86.148.227

45.32.129.185

23.227.196.217

Detection Mechanism:

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

File must contain one or more Cozy/Fancy Bear C2 IP addresses

Possible Attribution & Use Cases:

Linked to Russian state-sponsored cyber-espionage

Used to track compromised machines communicating with APT28/APT29 C2 servers

Recommended Actions:

Investigate: Check if flagged endpoints are actively communicating with these IPs

Contain & Mitigate: Block associated IPs and domains at the firewall level

Threat Intelligence Sharing: Report findings to relevant cybersecurity organizations

Author & Attribution:

Rule Author: Florian Roth (Nextron Systems)

Rule Version: 1

Reference ID: e81b4368-7383-5a48-a89a-f91b9306326e