Threat Category: APT / Exploit Tool

Threat Description: The YARA rule detects the "dn.1.0.2.1.linux" tool, part of the Equation Group (EQGRP) toolset. This tool appears to be a network reconnaissance or traffic manipulation utility, leveraging commands related to MAC addresses and packet interception.

Indicators of Compromise (IoCs)

Network-based IoCs:

"Valid commands are: SMAC, DMAC, INT, PACK, DONE, GO"

"invalid format suggest DMAC=00:00:00:00:00:00"

"SMAC=%02x:%02x:%02x:%02x:%02x:%02x"

"Not everything is set yet"

Detection Mechanism:

Must be a Linux ELF executable (identified by 0x457f header)

File size must be < 30KB

Must contain at least two network-related command strings

Possible Attribution & Use Cases:

Linked to Equation Group?s cyber espionage toolkit

Used for network traffic manipulation, MAC spoofing, or reconnaissance

May be repurposed by threat actors leveraging leaked NSA tools

Recommended Actions:

Investigate: Analyze network logs for unauthorized MAC or packet manipulation activity

Contain & Mitigate: Block execution of the tool and monitor for network anomalies

Threat Intelligence Sharing: Report detections to national and enterprise security teams

Author & Attribution:

Rule Author: Florian Roth (Nextron Systems)

Rule Version: 1

Reference ID: 24b5fb51-2463-56ef-818a-949b4b3bbf5b