Threat Category: Malware / HackTool, EQGRP Toolset

Threat Description: The YARA rule is designed to detect files from the EQGRP toolset, specifically targeting the file "noclient-3.0.5.3". This rule identifies specific string patterns and file characteristics associated with this tool.

The detection mechanism focuses on identifying files that either:

Begin with the magic bytes 0x7F45 and are smaller than 700KB, and contain at least one of the specified string patterns.

Contain all of the following string patterns:

"-C %s 127.0.0.1" scripme -F -t JACKPOPIN4 '&"

"Command too long!\nWhat the HELL are you trying to do to me?!?\nTry one smaller than %d bozo."

"sh -c "ping -c 2 %s; grep %s /proc/net/arp >/tmp/gx ""

"Error from ourtn, did not find keys=target in tn.spayed"

"ourtn -d -D %s -W 127.0.0.1:%d -i %s -p %d %s %s"

Indicators of Compromise (IoCs):

Specific string patterns within the file (see Threat Description)

File size less than 700KB

Magic bytes 0x7F45

Possible Attribution & Use Cases:

The rule is designed to detect tools from the EQGRP toolset, indicating potential use by this threat actor.

EQGRP tools have been associated with sophisticated cyber operations, including espionage and exploitation of vulnerabilities.

Detection of this tool can indicate potential intrusion or use of leaked exploit frameworks.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, conduct a thorough investigation to determine the presence of other EQGRP tools and potential impact on the system.

Containment and Remediation: Isolate affected systems and remove any identified EQGRP tools. Apply appropriate patches and security measures to prevent further compromise.

Threat Hunting: Use this rule and other EQGRP indicators to proactively search for related activity within the network.

Intelligence Sharing: Share information about detected EQGRP activity with relevant security communities and organizations.

Author & Attribution:

Rule Author: Florian Roth (Nextron Systems)

Rule Version: Not specified

Reference: Research

Rule Identifier: af7472ce-0605-5f50-8180-23438d2196b8