Threat Category: APT / Exploit Tool

Threat Description: The YARA rule detects the "installdate.pl" script, a tool from the Equation Group (EQGRP) toolset. This script is likely used for extracting system installation dates from registry entries, aiding in reconnaissance and persistence assessment during targeted operations. The Equation Group, an elite cyber espionage team linked to the NSA, has had many of its hacking tools leaked by The Shadow Brokers.

Indicators of Compromise (IoCs)

Code execution artifacts:

```
#Provide hex or EP log as command-line argument or as input
print \"Gimme hex: \";
"if ($line =~ /Reg_Dword:  (\\d\\d:\\d\\d:\\d\\d.\\d+ \\d+ - )?(\\S*)/) {" fullword ascii
```

Detection Mechanism:

File size must be < 2KB (suggesting lightweight Perl scripting)

Must contain script-based registry enumeration functions

Possible Attribution & Use Cases:

Linked to Equation Group?s leaked NSA hacking tools

Used for reconnaissance in cyber-espionage operations

Can be leveraged by threat actors who repurpose leaked NSA tools

Recommended Actions:

Investigate: Review affected systems for unauthorized script execution

Contain & Mitigate: Remove scripts and monitor system registry modification attempts

Threat Intelligence Sharing: Share detection findings with trusted cybersecurity partners

Author & Attribution:

Rule Author: Florian Roth (Nextron Systems)

Rule Version: 1

Reference ID: 029b1213-1206-5b7c-bd72-93239a23fe8a