Threat Category: Advanced Persistent Threat (APT) ? Cyber Espionage Tools

Threat Name: Equation Group Hack Tool ? emptycriss

Threat Description:

The emptycriss tool, leaked by the ShadowBrokers group, facilitates unauthorized network access through telnet services. It uses command templates that attackers paste into telnet sessions to compromise target systems.

Indicators of Compromise (IoCs):

Three specific ASCII, fullword strings embedded in the file:

$s1 = "./emptycriss <target IP>"

$s2 = "Cut and paste the following to the telnet prompt:"

$s8 = "environ define TTYPROMPT abcdef"

Detection Mechanism:

The file must be smaller than 50KB.

Detection is triggered if at least one (1 of them) of the specified strings is found.

Strings are matched in ASCII encoding and fullword mode.

Rule name should be: EquationGroup_emptycriss.

Reference:

Public leak information: ShadowBrokers Article

Signature base project: Signature-Base GitHub

Author:

Florian Roth (Nextron Systems)

Rule Metadata:

description: "Equation Group hack tool leaked by ShadowBrokers - file emptycriss"

license: "Detection Rule License 1.1"

reference: "https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1"

date: "2017-04-08"

hash1: "a698d35a0c4d25fd960bd40c1de1022bb0763b77938bf279e91c9330060b0b91"

id: "658a0a2c-ea3a-5531-abea-54f0ed786e79"