Reconnaissance

meta:

author = "Flores"

date = "03/03/2022"

type = "APT14"

description = "Simple Mail Transfer Protocol"

ref= https://img.deusm.com/darkreading/Whitepaper_SecurityConcernstotheAviationIndustry.pdf

strings:

$a = "APT14 phishing message "

$b = "GetClipboardData"

$magic = {47 6C 6F 62 61 6C 5C [5-9] 20 25 64

condition:

$text_a or $text_

Weaponization

rule Gh0st : RAT

meta:

author = "Flores"

date = "03/03/2022"

type = "APT14"

description = "Poison Ivy: Assessing Damage and Extracting Intelligence"

ref= https://www.mandiant.com/sites/default/files/2021-09/rpt-poison-ivy.pdf

strings:

$b = "KeyLogging"

$c = “ScreenCapturing”

$d = “VideoCapturing”

$e = “FileTransfer”

$magic = {47 6C 6F 62 61 6C 5C [5-9] 20 25 64

condition:

$text_a or $text_b

Delivery

meta:

author = "Flores"

date = "03/03/2022"

type = "APT14"

description = "Spear Phishing"

ref= https://www.secureblink.com/cyber-security-news/biopass-a-recently-discovered-malware-exploits-obs-studio-to-spy-on-its-users

$SHA = ba413753ea3b2376110c33784620e78e6d6ddf2b97cfb99d528dc357337d7925

strings:

$a = "Loader"

$b = "Install Scheduler"

$c = "CDaemon module"

$d = "BIOPASS RAT"

$e = "Communication"

condition:

$text_a or $text_b

Exploitation

meta:

author = "Flores"

date = "03/03/2022"

type = "APT"

description = "Remote Access Software "

ref= **https://attack.mitre.org/techniques/T1219/**

strings:

$a = "startlog "

$b = "Screenshots"

$c = "RATACCESS.EXE"

$d= “%s%s%s=%d,%s=%d”

$e = "stoplog"

$f = "CommandAndControl"

condition:

$text_a or $text_b

Installation

meta:

author = "Flores"

date = "03/03/2022"

type = "APT"

description = "Backdoor RAT"

ref= hhttps://www.2-spyware.com/remove-gh0st-rat.html

strings:

$a = ".\\\\start.dll "

$b = "Windows DLL WARNING”

$c = “intaller_ransomware”

$d=”OPEN|Wrong.info.sc”

$e= “OPEN|RIGHT.info.sc”

$f=www.anchorpanda.com

$g=”/javascript/view.php”

$h=”gh0st_bat”

condition:

$text_a or $text_b

Command and Control

meta:

author = "Flores"

date = "03/03/2022"

type = "APT14"

hash = “654280d4f7d46e82af51f5a8cf40fecddd7d10d1d73b331925085d02c3c202ce”

description = "Command and Scripting Interpreter"

ref= https://attack.mitre.org/techniques/T1059/

strings:

$a = "Command "

$b = "RAT_CN.dll"

$c = “setup.cn”

$a = "connection\\.dll"

$e = "255.255.223"

$f = “Established_SSH”

condition:

$text_a or $text_b

Actions on Objectives

meta:

author = "Flores"

date = "03/03/2022"

type = "APT"

description = "Trafficking Data "

ref= https://attack.mitre.org/techniques/T1205/

hash=”6as6a676e7777s7e7&e7e7a7sd77s78ssee8e8s8s8”

strings:

$a = "collect1.tff "

$b = " collect2.tff "

$c = “collect3.tff”

$a = " collect4.tff "

$e = " collect1.tff

$f = “collect1.tff”

condition:

$text_a or $text_