PROYECTO: Sistema de detección de malware basado en patrones de llamadas al sistema en GNU/Linux.

Resumen Técnico

Existen diferentes taxonomías para clasificar a los malwares, cada una de ellas sirve para determinados propósitos y normalmente dependerá del contexto y del analista. Se puede clasificar malwares según su comportamiento, en la cual se distingue a gusanos, troyanos, ransomwares, keyloggers, entre otros. Cabe aclarar que un malware puede no pertenecer a una sola categoría. Cada uno de estos malwares intentan generar algún daño y para lograrlo es normal que utilicen al núcleo del sistema operativo para acceder a los recursos que necesitan. Entonces, de acuerdo a la categoría del malware, se puede inferir que existirán patrones de llamadas al sistema que permitirían descubrir qué tipo de malware se está ejecutando y de esa manera reaccionar ante un ataque de estas características.
El resultado del proyecto es el desarrollo de un sistema de monitoreo y detección de malware para sistemas GNU/Linux, compuesto de dos herramientas. La primera será una herramienta de monitoreo sobre las llamadas al sistema que cada proceso ejecuta y la cual generará diferentes vistas para que la información pueda ser comprensible. La segunda se integrará con la primera y permitirá detectar patrones posiblemente maliciosos en los procesos para informar al usuario de esta situación, pudiendo tomar una decisión.

Autores:

Gibellini, Fabian Alejandro Director
Quinteros Sergio Ramon CoDirector
CICERI, Leonardo Ramón; PARISI, Germán Nicolás; ZEA CARDENAS, Milagros; BERTOLA, Federico Javier; BARRIONUEVO, Ileana Maricel; Zallocco Facundo; Ballester Diego; NOTRENI, Juliana María

Duración: Inicio: 01/01/2020 - Fin: 31/12/2022