MALWARES ACTUALES

Espinosa Sativa Gerxon Mauricio
gmes2237@gmail.com
Universidad Piloto de Colombia

Resumen— El presente documento muestra los diferentes Malwares que están siendo utilizados en la actualidad y la forma de cómo están avanzando, se muestra además en el contexto histórico las modalidades de ataque, los intereses por los cuales se realizan, el medio donde actúan los cybercriminales, el proceso de ataque e infección de los Malwares, la manera de contrarrestarlos y finalmente la relevancia que tienen en la actualidad.

Índice de Términos— Malwares, atacante, ataques, ciberdelicuentes, intrusión, exploits, colucion.

Abstract— This document shows the different Malwares that are being used today and how are advancing further shown in the historical context modes of attack, the interest with which made, the environment in which they act cybercriminals, the process of attack and infection of the malwares , how to counter them and ultimately the relevance today

Keywords— Malwares, attacker, attacks, cybercriminals, intrusion, exploits, colucion.

I. INTRODUCCIÓN

En la actualidad existen personas que de manera malintencionada son creadoras de Malwares y permanentemente buscan mejorar o crear nuevas técnicas y de esa manera lograr el fin, con diversos propósitos económicos, políticos, competitivos, etc. Lo anterior hace que la Seguridad de la Información haya tenido un gran avance en los últimos tiempos, en defensa de uno de los activos más importantes de las organizaciones

Teniendo en cuenta lo dicho anteriormente desde hace unos años atrás en el ámbito de la Seguridad de la Información ha aparecido un riesgo de Ciberdelicuente de suma importancia y con efectos muy perjudiciales y al que se le debe dar importancia y tomar las medidas adecuadas para no ser víctimas. Se trata de los Malwares (Malicious software) en español Software Malicioso. Malware es un tipo de software que tiene como objetivo colarse en cualquier tipo de dispositivos sin el permiso del propietario. El malware suele ser representado con símbolos de peligro, es muy utilizado por los profesionales de la informática para referirse a una variedad de software que molesta o afecta la información.

Además se aprovecha del desconocimiento básico de las personas, permitiendo que pase desapercibido, teniendo como último componente el ir dirigidos a un objetivo específico no solamente personal si no empresarial con el fin de afectar la información, para de esa manera obtener ventajas en cada escenario. No tendrán más remedio que pagar por la recuperación de la información o perderla de manera indefinida

A lo largo de este artículo se estará enfocado en describir más a fondo los Malware actuales.

II. CONTEXTO

Fue en 1949 [1] cuando Von Neumann estableció la idea de programa almacenado y expuso la teoría y organización de autómatas complejos, donde presentaba por primera vez la posibilidad de desarrollar pequeños programas replicantes y capaces de tomar el control de otros programas de similar estructura. Si bien el concepto tiene miles de aplicaciones en la ciencia, es fácil apreciar una aplicación negativa de la teoría expuesta por Von Neumann: los virus informáticos, programas que se reproducen a sí mismos el mayor número de veces posible y aumentan su población de forma exponencial.

En 1959, en los laboratorios de Bell Computer, tres jóvenes programadores: Robert Thomas Morris, Douglas McIlroy y Victor Vysottsky crean un juego denominado Core War basado en la teoría de Von Neumann y en el que el objetivo es que programas

compiten entre sí tratando de ocupar toda la memoria de la máquina eliminando así a los oponentes. Este juego es considerado el precursor de los virus informáticos. Fue en 1972 cuando Robert Thomas Morris creó el que es considerado como el primer virus propiamente dicho: el Creeper era capaz de infectar máquinas IBM 360 de la red ARPANET (la precedente de Internet) y emitía un mensaje en pantalla que decía ³ 6 R Una enredadera (creeper), atrápame si S X H G Para eliminarlo, se creó otro virus llamado Reaper (segadora) que estaba programado para buscarlo y eliminarlo. Este es el origen de los actuales antivirus.

En la década de los 80 los PC ganaban popularidad y cada vez más gente entendía la informática y experimentaba con sus propios programas. Esto dio lugar a los primeros desarrolladores de programas dañinos y en 1981, Richard Skrenta escribe el primer virus de amplia reproducción: Elk Cloner, que contaba el número de veces que arrancaba el equipo y al llegar a 50 mostraba un poema.

En 1984, Frederick B. Cohen acuña por primera vez el término virus informático en uno de sus estudios definiéndolo como ³ 3 U R J U que Pu de infectar a otros programas incluyendo una copia posiblemente evolucionada de sí P L V P R ´

En 1987 hace su aparición el virus Jerusalem o Viernes 13, que era capaz de infectar archivos .EXE y .COM. Su primera aparición fue reportada desde la Universidad Hebrea de Jerusalem y ha llegado a ser uno de los virus más famosos de la historia.

En 1999 surge el gusano Happy desarrollado por el francés Spanska que crea una nueva corriente en cuanto al desarrollo de malware que persiste hasta el día de hoy: el envío de gusanos por correo electrónico. Este gusano estaba encaminado y programado para propagarse a través del correo electrónico.

En el año 2000 hubo una infección que tuvo muchísima repercusión mediática debido a los daños ocasionados por la infección tan masiva que produjo. Fue el gusano I Love You o Love Letter, que, basándose en técnicas de ingeniería social infectaba a los usuarios a través del correo electrónico. Comenzaba aquí la época de grandes epidemias masivas que tuvieron su punto álgido en el año 2004.

Fue en ese año cuando aparecieron gusanos como el Mydoom, el Netsky, el Sasser, o el Bagle, que alarmaron a toda la sociedad y lo que buscaban era tener la mayor repercusión y reconocimiento posible. Ese fue el año más duro de este tipo epidemias y curiosamente el último. Los creadores de malware se dieron cuenta de que sus conocimientos servirían para algo más que para tener repercusión mediática para ganar dinero.

III. MALWARES ACTUALES

A. Ransomware

El ransomware aumentó un 24% [2] el segundo trimestre del año actual, en la línea de su rápido incremento, debido a que no se requiere muchos conocimientos para utilizar los kits de exploits para desplegar el malware. Es un software malicioso que al infectar el equipo le da al ciberdelincuente la capacidad de bloquear el PC desde una ubicación remota y encripta los archivos quitando el control de toda la información y datos almacenados.

La primera epidemia ransomware reales comenzó en año 2010 con miles de usuarios domésticos en Rusia y algunos países vecinos al encontrarse con ventanas que cubrían todos los demás ventanas en el escritorio. Estas ventanas por lo general contenían un mensaje a los delincuentes pidiendo a la víctima enviar dinero a un número dado, con el fin de desbloquear la pantalla o navegador del PC infectado

El aumento de los llamados bloqueadores fue impulsado principalmente por el hecho de que la creación de malware capaz de bloquear un navegador de escritorio del sistema operativo o no, requerían conocimientos de programación significativo lo que generaba un ingreso relativamente fiable para el criminal.

Ransomware regresa con encriptación la mayor diferencia entre los dos tipos de ransomware: bloqueador y cifrado. Incluso en el peor de los casos, el dueño de una PC infectada podría simplemente volver a instalar el sistema operativo para obtener

todossusarchivosde nuevo.En adición,la formaen que los bloqueadores trabajan permitió a los desarrolladoresdesarrollar software automatizado que ayude a desbloquear, incluso despuésde la infección.

Sin embargo,cuandose trata de cosasde cifrado los ransomwareson muchomáscomplicadosdebido a que los archivos cifrados son imposibles