# Las empresas valencianas sufrirán más hackeos este 2020 por el virus Ransomware, según Acción Informática

**Durante el 2019 la industria de la ciberseguridad ha comenzado a explorar soluciones basadas en inteligencia artificial para combatir los ataques que se han estado originando en la red. En los próximos meses se prevé que los ciberdelincuentes comiencen a hacer lo mismo, integrando la inteligencia artificial y el aprendizaje automático en sus programas de malware**

La empresa valenciana Acción Informática, especializada en soluciones informáticas y protección, alerta a las empresas que durante el próximo 2020 los hackers aumentarán el uso de la inteligencia artificial para analizar los mecanismos de defensa y simular patrones de comportamiento, evitando así los controles de seguridad y aprovechando los análisis y el aprendizaje automático para "piratear" los documentos de las organizaciones.

Ransomware, el virus más utilizado

Este año, muchas compañías a lo largo del mundo han empezado a sufrir ciberataques basados en inteligencia artificial. El mes pasado varias empresas españolas, entre las que se encontraba la Cadena Ser , se vieron afectadas por el ciberataque de un virus *de tipo ransomware*.

Se trata de un *malware* que permite la extorsión cibernética para obtener ganancias financieras. Los ciberdelincuentes insertan enlaces nocivos en correos electrónicos o páginas web aparentemente normales, pero que en realidad lo que hacen es poner en marcha el código del malware. Una vez activado el virus, este impide a los usuarios acceder a sus propios archivos, aplicaciones o sistemas. ¿Cómo? Encriptando los archivos y bases de datos, de forma que la información contenida en los mismos queda ilegible e inaccesible hasta que se pague un rescate.

La empresa informática valenciana alerta de que esta amenaza supone un grave peligro para las empresas, ya que les causa pérdidas de información, pérdidas económicas, interrumpen su actividad normal y, además, repercute en su reputación.

Los ataques de ransomware web, tienden a utilizar programas automáticos (exploits), que atacan vulnerabilidades del navegador, la plataforma y el sistema o se basan en publicidad maliciosa que pueden redirigir a los usuarios a sitios que alojan kits de exploits. Una vez que el ransomware se apodera de un sistema, se puede propagar a otros sistemas o servidores conectados en la red.

El ransomware del correo electrónico generalmente se usa en ataques dirigidos y se basa en una variedad de métodos, que incluyen phishing, spear phishing, archivos adjuntos maliciosos y enlaces a URL's nocivas.

Medidas contra el ramsomware
Los servicios informáticos que se ofrecen en la rama de la protección cibernética están basados en la detección y en la respuesta ante el problema. Pero a medida que los atacantes comiencen a aprovechar la inteligencia artificial para evitar las soluciones actuales, las empresas quedarán en una desventaja significativa contra este tipo de campañas aparentemente indetectables.

La empresa Acción Informática, partner de Microsoft Valencia recomienda a las

Empresas educar a sus empleados frente a este tipo de amenazas y, además, realizar

siempre copias de seguridad de todos sus archivos, actualizar regularmente los sistemas

de antivirus y no proporcionar información personal al responder un correo electrónico.

A la hora de defenderse adecuadamente contra el *ransomware*, la empresa valenciana recomienda varias acciones principales:

- Mantener actualizados los equipos con los últimos parches de seguridad, tanto del sistema operativo como de las aplicaciones instaladas.

- Mantener los sistemas de Antispam, Antivirus, Antimalware, etc., Debidamente configurados y actualizados

- Tener siempre actualizado un sistema adecuado de Backup, para minimizar la pérdida de los datos y para que el tiempo de recuperación sea el mínimo posible

- Informar y concienciar a los usuarios de la amenaza real que sufren las empresas con este tipo de ataques, y hacerlos participes de la lucha contra el ransomware. Un usuario formado y concienciado puede ser vital a la hora de evitar un ataque.

- En el caso de sufrir un ataque, tener las herramientas adecuadas para poder analizar a fondo el origen del ataque y detectar las vulnerabilidades del sistema.

- El código malicioso debe estudiarse para determinar su propósito y signos de actividad.

- Se debe bloquear el acceso de las máquinas infectadas a los servidores de comando y control.

Estas nuevas técnicas de defensa serán cruciales durante el 2020 , ya que los ataques serán cada vez más sofisticados y, por tanto, más difíciles de detectar.

---