Las tres amenazas para la seguridad online 2018

Los hackers prefieren los métodos más fáciles para atacar. **Hay tres tendencias de seguridad online importantes este año**, según el volumen número 23 del Informe de Inteligencia de Seguridad de Microsoft (SIR), que incluyen botnets, ransomware y phishing.

Con este último ataque cibernético, los delincuentes evitan las largas rutas para hacerse cargo de los sistemas, **vulnerando a la cadena más débil: el usuario**. La ingeniería social trata de obtener datos confidenciales, dispositivos o redes a través del contacto personal con las víctimas.

Las botnets continúan afectando a millones de computadoras en todo el mundo, infectándolas con formas antiguas y nuevas de malware, según Microsoft.

Los ciberdelincuentes continúan atacando implacablemente las computadoras y participando en la actividad de botnets con la intención de construir una gran infraestructura que puedan extraer datos confidenciales y extorsionar a sus víctimas, como es el caso del ransomware.

Contraataque

El 29 de noviembre de 2017, la unidad de crímenes digitales de Microsoft (DCU) abordó una **botnet líder que infectó a 23 millones de direcciones IP: Gamarue**. La operación global coordinada resultó en la desconexión de los servidores que este código malicioso afectó, e interrumpió una de las operaciones de malware más grandes del mundo. La acción de Microsoft dio como resultado un descenso de 30% en dispositivos infectados en tan sólo un periodo de tres meses.

La interrupción del botnet Gamarue se logró a través de una **asociación público/privada con agencias policiales de todo el mundo**, incluyendo el Buró Federal de Investigaciones de los Estados Unidos (FBI), el Luneburg Central Criminal Investigation Inspection, el European Cybercrime Center de Europol, el socio privado de la industria, los investigadores de seguridad de Microsoft y la DCU.

Los piratas informáticos aún encuentran muchas víctimas fáciles, y están más centrados en métodos de “bajo riesgo” como la ingeniería social o phishing, en lugar de métodos más costosos (en términos de tiempo y esfuerzo) como tratar de eludir las medidas de seguridad.

El phishing fue el principal vector de amenazas para correos electrónicos basados en Office 365 en la segunda mitad de 2017. El phishing y el spear phishing de amplia base se basan en lo que con mayor frecuencia se cita como el eslabón más débil de la seguridad: las personas.

El ransomware seguirá siendo una fuerza a tener en cuenta este 2018, pues es un método popularmente utilizado por los ciberdelincuentes para solicitar dinero a las víctimas. Tres brotes globales, WannaCrypt, Petya/NotPetya y BadRabbit, ilustraron cómo este código malicioso está siendo un real impacto. Afectaron redes corporativas y redujeron los servicios críticos, como los hospitales, el transporte y los sistemas de tráfico.

El informe se basa en datos de redes corporativas y servicios en la nube recopilados entre febrero de 2017 y enero de 2018, incluidos Windows, Bing, Office 365 y Azure.