Ciberseguridad 2015: desafíos ante la resistencia de los ataques Colaboración del sector

Los atacantes están tomando control de infraestructura legítima y están sacando millones en ganancias.

A los defensores les está costando trabajo detectar y combatir amenazas y están perdiendo la confianza en ellos mismos.

Los atacantes se escapan y se reorganizan

Los atacantes están reforzando sus operaciones. Si son detectados, se reorganizan rápidamente y pueden adoptar nuevos sistemas con nuevas IP en minutos.

Angler

Este ataque a menudo no se detecta y toma control de recursos de alta reputación

Sitios web de referencia

15 000 sitios únicos que redirigen el tráfico por malvertising

Servidores proxy

Varios servidores sin malware, pero con recursos mezclados en proveedores de alojamiento legítimos dirigieron a usuarios hacia servidores con vulnerabilidades de seguridad

Los servidores con vulnerabilidades de seguridad

60% con datos de pagos son ransomware.

El resultado es global y a través de varios proveedores

Servidores de estado

si el estado del funcionamiento está en riesgo o se detecta una alteración, los atacantes reciben avisos

Infraestructura de IP pequeña

Los atacantes pueden rotar las IP en 8-12 sistemas activos por día

$60 millones

al año es la ganancia que se calcula de solamente dos de las campañas identificadas

SSHPsycho

La iniciativa colaboración global, ataques de fuerza bruta

DDoS

10,000 X máquinas utilizadas

Configuración de Botnet

1. Ataques de fuerza bruta a las contraseñas desde China para crear Botnet
2. 24 Horas después, con inicio de sesión desde Estados Unidos con contraseñas recogidas para descargar el kit de raíz DDoS en dispositivos en riesgo

SSHPsycho

35% tuvo un efecto masivo al poner en riesgo todo el tráfico SSH a través de Internet

Mezclados y en riesgo

221% de aumento en sitios WordPress en riesgo

Confianza en descenso

La confianza generada por la posesión de la tecnología de vanguardia disminuyó un 59%

NO poseer la última tecnología aumentó un 37%

Defensores Falta de colaboración

La confianza de los defensores en su capacidad para detectar, proteger y recuperarse de ataques cibernéticos está disminuyendo, mientras que los reguladores e inversionistas están tratando de tener más visibilidad a la estrategia contra los ataques cibernéticos de las empresas.

Antes

54% de confianza en la capacidad para verificar que ocurrió un ataque

Durante

54% de confianza en la capacidad para defenderse de los ataques

Después

45% de confianza en la capacidad de analizar y detener un ataque

Riesgo y segmentación

92% de los dispositivos de Cisco examinados a través de Internet ejecutaban vulnerabilidades conocidas, con un promedio de 26 cada uno

31% de los dispositivos Cisco examinados estaban en estado EOS

5% de los dispositivos de Cisco estaban en estado EOL

56% tienen políticas de seguridad regularmente

Restricciones

Las organizaciones no colaboran mucho: durante los incidentes de seguridad solamente

- 21% notifican a sus partners de negocios
- 18% notifican a las autoridades externas
- 15% a las compañías de seguros

Barreras para adoptar tecnología de seguridad avanzada

- 39% Presupuesto
- 32% Problemas de compatibilidad
- 25% Requisitos de certificaciones

cisco

Descargue el Informe anual de seguridad de Cisco 2016
www.cisco.com/go/asr2016