Adaptive Defense 360

panda

Halloween

Las ciber pesadillas más peligrosas de los últimos años

Halloween es el momento para disfrazarse de personajes aterradores, ver películas de miedo y contar historias de sucesos espeluznantes. Sucesos como los que en los últimos años mantiene en alerta a numerosas empresas, que están viendo como cada día se incrementan los ciberataques perpetrados por grupos de hackers organizados.

En tan solo unos instantes, estas amenazas, son capaces desde desestabilizar grandes corporaciones robando grandes sumas de dinero en información sensible, como generar conflictos entre potencias mundiales. La peor pesadilla para tu organización puede ocurrir en cualquier momento.

Échale un vistazo a los cibertaques más terroríficos de los últimos años

2010

Operación Aurora

Serie de ataques cibernéticos a escala mundial, dirigidos a 34 empresas, entre ellas Google. El ataque fue perpetrado por un grupo de hackers chinos.

Gobierno Australiano

Ataques de denegación de servicio, llevados a cabo por la comunidad online anónima, contra el gobierno australiano.

Operation Payback

Conjunto de ataques coordinados a los oponentes de la piratería en Internet, por activistas.

2011

RSA SecurID

La empresa RSA sufrió una brecha de seguridad como consecuencia de un ciberataque que buscaba detalles sobre su sistema SecureID.

PlayStation Network

77 millones de cuentas se vieron comprometidas y evitó que los usuarios de PlayStation 3 y PlayStation Portable accedieran al servicio durante 23 días.

2012

Stratfor

Publicación y difusión de correos electrónicos de carácter interno, entre personal de la agencia privada de inteligencia de espionaje Stratfor, así como del personal de la empresa con sus clientes.

Linkedin

Las contraseñas de casi 6,5 millones de cuentas de usuario fueron robadas por ciberdelincuentes rusos.

2013

Ciberataque a Corea del Sur

Las redes cibernéticas de los principales bancos surcoreanos y de las cadenas de televisión se apagaron en un presunto acto de guerra cibernética.

Snapchat

4.6 millones de nombres de usuario y números de teléfono de Snapchat fueron filtrados en "SnapchatDB.info"

Yahoo!

Entre 2013 y 2014 se robó la información asociada a 1.000 millones de cuentas de correo

2014

Fotos de famosos

500 fotografías privadas de varias celebridades, en su mayoría mujeres, fueron colocadas en 4chan y posteriormente difundidas por otros usuarios en redes sociales.

Sony Pictures

Un grupo de hackers conocido como #GOP, filtró datos confidenciales del estudio de cine Sony Pictures en el mayor ataque conocido a la industria del cine. Este se cree que pudo estar relacionado con el lanzamiento de la película “The Interview”.

El robo de contraseñas de Hackers rusos

Este ataque resultó en el robo de más de 1.2 billones de nombres de usuario y contraseñas asociados a más de 500 millones de direcciones de correo electrónico. 420,000 sitios web se vieron afectados.

2015

Anthem medical

Esta aseguradora médica, la segunda más grande de EEUU, sufrió el robo de 80 millones de registros, con datos tan sensibles sobre los clientes como su número de la Seguridad Social.

Oficina de Administración de Personal de los Estados Unidos

La brecha de datos ascendió a 21,5 millones. Ha sido la mayor infracción de datos gubernamentales registrada en la historia de los EEUU.

Hacking Team

La filtración evidenció que esta compañía estaba vendiendo software de vigilancia a gobiernos de 35 países como Rusia, EEUU, Suiza, Arabia Saudí, Italia, Nigeria o Sudán, lo que desató una discusión global sobre el uso legal de estas herramientas.

Ashley Madison

Un grupo de hackers robó información personal sobre la base de usuarios del sitio y amenazó con divulgar los nombres de los usuarios y la información personal si Ashley Madison no se cerraba inmediatamente.

VTech

Fue víctima de una violación de datos que expuso datos personales de millones de personas, incluidos niños.

SWIFT

Serie de ciberataques perpetrados por “Lazarus” utilizando la red bancaria de SWIFT, lo que resultó en el exitoso robo de millones de dólares.

2016

Bangladesh Bank

Un grupo de atacantes consiguió infectar el sistema con malware e intentó realizar transferencias fraudulentas por un valor de 951 millones de dólares. Finalmente 'únicamente' se robaron 81 millones de dólares.

Hollywood Presbyterian Medical Center

El sistema informático del hospital fue secuestrado por un ransomware. Finalmente pagaron un rescate de 40 bitcoin a los hackers (US $ 17,000) para recuperar el acceso a su sistema.

Comité Nacional Demócrata

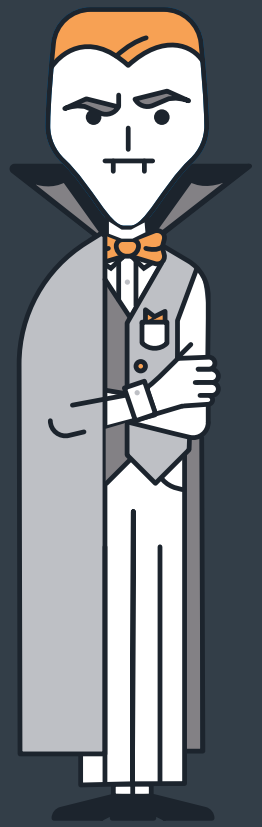
La organización mediática WikiLeaks, por medio de su sitio web, público 19.252 correos electrónicos y 8.034 archivos adjuntos cuyo propietario era el órgano de gobierno interno del Partido Demócrata de los EEUU.

Dyn

El ciberataque se basó en múltiples ataques de denegación de servicio (DoS) a sistemas operados por el proveedor de nombres de dominio (DNS) Dyn, que dejó inaccesibles grandes plataformas y servicios de Internet a usuarios de Europa y Norteamérica.

Russian interference in U.S. election

La Comunidad de Inteligencia estadounidense comunicó que hubo interferencia rusa en las elecciones presidenciales de EEUU de 2016.



2017

WannaCry

Ataque dirigido al sistema operativo Windows de Microsoft. Wannacry ha sido descrito como el ataque sin precedentes en tamaño. Infectó 230.000 ordenadores en más de 150 países.

Westminster

Ciberataque cuyo objetivo fue tener acceso a las cuentas del correo electrónico de un gran número de políticos del parlamento de Reino Unido.

Petya

El 27 de junio de 2017, comenzó un nuevo ciberataque mundial de “ransomware” que paralizó empresas de todo el mundo. Conocido como Petya, NotPetya y GoldenEye, sus creadores consiguieron situarlo en algunas de las instituciones más importantes de Ucrania, como el Banco Nacional y el sistema de metro de Kiev.

Equifax

Ciberatque que permitió el acceso a información sensible de al menos 143 millones de estadounidenses.

El mayor robo de datos personales de la historia.

Hackers y grupos organizados

Grupos organizados

Anonymous
Bureau 121
Cozy Bear
CyberBerkut
Derp
Equation Group
Fancy Bear
GNAA
Goatse Security
Guccifer 2.0
Hacking Team
Iranian Cyber Army
Lizard Squad
LulzRaft
LulzSec
New World Hackers
NullCrew
NSO Group
PayPal 14
PLA Unit 61398
PLATINUM
Pranknet
RedHack
Rocket Kitten
The Shadow Brokers
Syrian Electronic Army
TeaMp0isoN
Tailored Access Operations
UGNazi
Yemen Cyber Army

Hackers

George Hotz
Guccifer
Hector Monsegur
Jeremy Hammond
Junaid Hussain
Kristoffer von Hassel
Mustafa Al-Bassam
MLT
Ryan Ackroyd
Topiary
The Jesterweev

Vulnerabilidades más tenebrosas

- 2010: Evercookie
- 2013: iSeeYou
- 2014: Heartbleed, Shellshock, POODLE, Rootpipe, Row hammer
- 2015: JASBUG, Stagefright
- 2016: DROWN, Badlock, Dirty COW
- 2017: Cloudbleed, Broadcom Wi-Fi, EternalBlue, DoublePulsar, Silent Bob is Silent

Malware diabólico

- The Mask
- CryptoLocker
- Dexter
- Duqu
- Duqu 2.0
- FinFisher
- Flame
- Gameover ZeuS
- Mahdi
- Metulji botnet
- Mirai
- NSA ANT
- Pegasus
- R2D2
- Shamoon
- Stars virus
- Stuxnet
- Vault 7
- WannaCry
- X-Agent

La solución: Adaptive Defense 360 :

Protege tu empresa durante todo el año y disfruta de un Halloween escalofriante

Una protección contra amenazas avanzadas y ataques dirigidos, e incluso, que sea capaz de detectar comportamientos extraños.

Un sistema que pueda asegurar la confidencialidad de los datos, la privacidad de la información, el patrimonio y reputación empresarial. Una plataforma inteligente que ayude al personal de seguridad de las redes críticas a reaccionar de forma más rápida ante las amenazas y garantizar que puedan disponer de la información correcta necesaria para responder de forma adecuada.

Esto es Adaptive Defense 360, el único sistema de ciberseguridad avanzado que combina protección de última generación y la última tecnología de detección y remediación con la capacidad de clasificar el 100% de los procesos en ejecución.

Adaptive Defense 360 clasifica absolutamente todos los procesos activos en todos los endpoint, garantizando la protección contra el malware conocido y contra amenazas avanzadas del tipo Zero-Day, Advanced Persistent Threats y Ataques Dirigidos.

La plataforma utiliza la lógica contextual para revelar patrones de comportamiento malicioso y generar acciones de ciberdefensa avanzada contra amenazas conocidas y desconocidas.

Analiza, categoriza y correlaciona todos los datos que obtiene sobre las ciberamenazas, para llevar a cabo tareas de Prevención, Detección, Respuesta y Remediación.
Averigua quién y cómo accede a tus datos y controla la fuga de información, la que intente realizar un malware o la que realicen tus empleados.

Descubre y soluciona las vulnerabilidades de los sistemas y de los programas instalados y previene la utilización de los no deseables (barras de navegación, adwares, add-ons,...).

Visibilidad sin límites, control absoluto

panda

Más información:

pandasecurity.com/enterprise/solutions/adaptive-defense-360

Contacta:

900 90 70 80