Adaptive Defense 360

panda

Halloween

Os pesadelos cibernéticos mais perigosos dos últimos anos

Chegou o Halloween, a altura do ano em que nos mascaramos, vemos filmes de terror e contamos histórias de arrepiar.

Nos últimos anos, temos assistido a diversos acontecimentos que mantêm as empresas em alerta máximo, com o aumento diário do número de ciberataques realizados por grupos organizados de hackers.

Estas ameaças são capazes de desestabilizar grandes empresas, roubando informação sensível, e até mesmo originar conflitos entre potências mundiais.

Conheça os piores ataques dos últimos anos.

2010

Operação Aurora

Série de ataques à escala mundial, direccionados a 34 empresas, incluindo a Google. Os ataques foram realizados por um grupo de hackers chineses.

Governo Australiano

Ataques DDoS contra o governo australiano, executados pela comunidade online Anonymous.

Operação Payback

Conjunto de ataques coordenados, executados por activistas e direccionados aos opositores da pirataria informática.

2011

RSA SecurID

A empresa RSA sofreu uma falha de segurança resultado de um ciberataque cujo objectivo era obter pormenores sobre o sistema SecureID.

PlayStation Network

Foram comprometidas 77 milhões de contas e os utilizadores da PS3 e PSP ficaram impedidos de aceder ao serviço durante 23 dias.

2012

Stratfor

Publicação e difusão de emails internos trocados entre os funcionários da agência de espionagem Stratfor, bem como de emails trocados com os clientes da empresa.

Linkedin

As passwords das contas de quase 6.5 milhões utilizadores foram roubadas por ciberatacantes russos.

2013

Ciberataque na Coreia do Sul

As redes cibernéticas dos principais bancos sul coreanos e estações televisivas foram desligadas num presumível acto de guerra cibernética.

Snapchat

4.6 milhões de nomes e números de telefone foram divulgados em SnapchatDB.info.

Yahoo

Entre 2013 e 2014 foram roubados dados pessoais associados a 1 bilião de contas.

2014

Fotos de Celebridades

500 fotografias privadas de celebridades, maioritariamente mulheres, foram colocadas no site 4chan e consequentemente divulgados nas redes sociais por outros utilizadores.

Sony Pictures

Um grupo de hackers conhecido como #GOP divulgou dados confidenciais da Sony Pictures, naquele é o maior ataque conhecido à indústria do cinema. Pensa-se que este está relacionado com o lançamento do filme “The Interview”.

Roubo de Passwords por Hackers Russos

O ataque resultou no roubo de mais de 1.2 triliões de nomes de utilizadores e passwords associados a mais de 500 milhões de endereços de email. Foram afectados 420 000 websites.

panda

Adaptive Defense 360

2015

Anthem medical

Foram roubados 80 milhões de registos dados desta seguradora médica, a segunda maior nos Estados Unidos, contendo informação de clientes sensível, incluindo o número de segurança social.

US Office of Personnel Management

A fuga de informação ascendeu aos 21.5 milhões. Foi a maior fuga de dados governamentais na história dos EUA.

Hacking Team

A fuga forneceu provas de que a empresa vendia software de vigilância para os governos de 35 países, incluindo Rússia, Estados Unidos, Suíça, Arábia Saudita, Itália, Nigéria e Sudão, iniciando uma discussão global sobre o uso legal dessas ferramentas.

Ashley Madison

Um grupo de hackers roubou informção da base de dados do site e ameaçou divulgar os nomes dos utilizadores e informação pessoal caso o site Ashley Madison não encerrasse de imediato.

VTech

Foi vítima de uma fuga de informação que expôs dados pessoais de milhões de pessoas, incluindo crianças.

SWIFT

Série de ciberataques, realizados pelo grupo “Lazarus”, que utilizaram a rede SWIFT e que resultaram no roubo de milhões de dólares.

2016

Banco do Bangladesh

Um grupo de atacantes conseguiu infectar o sistema com malware e tentou efectuar diversas transferências no valor de 951 milhões de dólares. No final “só” conseguiram roubar 81 milhões de dólares.

Hollywood Presbyterian Medical Center

O sistema informático do hospital foi sequestrado por um ransomware. O hospital pagou 40 bitcoins (cerca de 17 000 dólares) para conseguir aceder ao sistema.

Comité Democrático Nacional

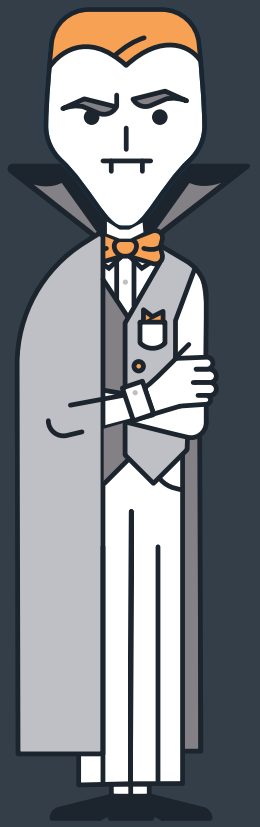
O site Wikileaks publicou 19 252 emails e 8034 anexos pertencentes ao governo interno do Partido Democrata dos EUA.

Dyn

Vários ataques DDoS em sistemas operados pelo Dyn Domain Name Service (DNS) deixaram as grandes plataformas e serviços de Internet inacessíveis aos utilizadores na Europa e na América do Norte.

Interferência Russa nas Eleições Americanas

A Comunidade de Inteligência dos EUA informou que houve interferência russa nas eleições presidenciais dos EUA de 2016.



2017

WannaCry

Ataque direccionado ao sistema operativo Microsoft Windows. Descrito com um ataque sem precedentes ao nível da sua dimensão, o WannaCry infectou 230 000 computadores em mais de 150 países.

Westminster

Ciberataque cujo objectivo era obter acesso às contas de email de um grande número de políticos do parlamento do Reino Unido.

Petya

A 27 de Junho de 2017 foi lançado um novo ataque mundial de ransomware. Conhecido como Petya, NotPetya e GoldenEye foi instalado com sucesso, pelos seus criadores, em algumas das mais importantes instituições ucranianas, como o Banco Nacional e o sistema do metropolitano de Kiev.

Equifax

Ciberataque que permitiu o acesso a informação sensível de pelo menos 143 milhões de Americanos. Foi o maior roubo de informação pessoal da história.

Hackers e 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

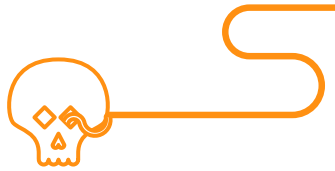
George Hotz
Guccifer
Hector Monsegur
Jeremy Hammond
Junaid Hussain
Kristoffer von Hassel
Mustafa Al-Bassam
MLT
Ryan Ackroyd
Topiary
The Jesterweev

Vulnerabilidades mais assustadoras

- 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



panda

Adaptive Defense 360

A solução: Adaptive Defense 360

Proteja a sua empresa o ano todo e tenha um Halloween arrepiante

Uma solução contra ameaças avançadas e ataques direccionados e que é capaz de detectar comportamentos suspeitos. Um sistema que pode assegurar a confidencialidade de dados, a privacidade de informação, os recursos e a reputação de uma empresa.

Uma plataforma inteligente que ajuda os responsáveis pela segurança das redes críticas a reagir mais rapidamente às ameaças e que garante que estes dispõem de toda a informação necessária para responder de forma adequada.

Assim é o Adaptive Defense, o único sistema de cibersegurança avançada que combina protecção de última geração e a mais recente tecnologia de detecção e remediação com a capacidade de classificar 100% dos processos em execução.

O Adaptive Defense 360 classifica todos os processos activos em todos os endpoints, garantindo protecção contra malware conhecido, ataques de dia-zero e ameaças persistentes avançadas.

A plataforma utiliza lógica contextual para revelar padrões de comportamento malicioso e gerar acções de ciberdefesa avançada contra ameaças conhecidas e desconhecidas.

Analisa, categoriza e correlaciona todos os dados obtidos sobre as ciberameaças para realizar tarefas de Prevenção, Detecção, Resposta e Remediação.

Determina como e quem acede à informação e controla a fuga de informação, seja por via de malware ou realizada pelos funcionários da empresa.

Descobre e resolve vulnerabilidades do sistema e dos programas instalados e previne a utilização de aplicações indesejáveis.

panda

Para mais informações:

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

Contacte-nos:

+351 21 041 44 00