



# Halloween

The most dangerous cyber nightmares in recent years

---



Halloween is the time of year for dressing up, watching scary movies, and telling hair-raising tales. Events in recent years have kept companies on high alert. Every day we are seeing an increase in cyberattacks carried out by organized hacker organizations.

In a matter of seconds, these threats can destabilize large corporations, stealing large quantities of money and personal data, as well shake the very foundations of entire world powers.

Have a look at some of the most terrifying attacks of recent years.



2010



### Operation Aurora

A series of cyberattacks carried out worldwide, targeting 34 companies, including Google. The attack was perpetrated by a group of Chinese hackers.

### Australian Government

DDoS attacks, carried out by the online community Anonymous, against the Australian Government.

### Operation Payback

An attack coordinated jointly against opponents of Internet piracy.

2011



### RSA SecurID

RSA suffered a security breach as a result of a cyberattack that sought details about its SecureID system.

### PlayStation Network

77 million accounts were compromised and blocked PS3 and PlayStation Portable users from accessing the service for 23 hours.

2012



### Stratfor

Publication and dissemination of internal emails exchanged between personnel of the private intelligence espionage agency Stratfor, as well as emails exchanged with clients of the firm.

### Linkedin

The passwords of nearly 6.5 million user accounts were stolen by Russian cybercriminals.

2013



### Cyberattack in South Korea

Cyber networks of major South Korean banks and television networks were shut down in an alleged act of cyber warfare.

### Snapchat

4.6 million usernames and phone numbers were leaked in "SnapchatDB.info".

### Yahoo!

Between 2013-2014, personal data associated with 1 billion accounts was stolen.

2014



### Celebrity photos

500 private photographs of several celebrities, mostly women, were placed on 4chan and subsequently spread by other users on social networks.

### Sony Pictures

A group of hackers known as #GOP leaked confidential data from the film studio Sony Pictures in the biggest attack the film industry has ever witnessed. The attack is believed to have been linked to the release of the movie "The Interview."

### Russian hacker password theft

This attack resulted in the theft of more than 1.2 trillion usernames and passwords associated with more than 500 million e-mail addresses. 420,000 websites were affected.



2015



### Anthem medical

This medical insurer, the second largest in the United States, was robbed of 80 million records containing sensitive client data, including Social Security numbers.

### US Office of Personnel Management

The largest breach in government data ever recorded in the history of the US. Affected 21.5 million.

### Hacking Team

The leak provided evidence that the company was selling surveillance software to governments in 35 countries, including Russia, the United States, Switzerland, Saudi Arabia, Italy, Nigeria, and Sudan, sparking a global discussion on the legal use of these tools.

### Ashley Madison

A group of hackers stole data on the site's user base and threatened to disclose user names and personal information if Ashley Madison did not close immediately.

### VTech

Fell victim to a data breach that exposed the personal information of millions, including children.

### SWIFT

Series of cyberattacks perpetrated by "Lazarus" using the SWIFT banking network, resulting in the successful theft of millions of dollars

2016



### Bangladesh Bank

A group of attackers managed to infect the system with malware and attempted to make fraudulent transfers amounting to \$951 million. In the end, “only” \$81 million was stolen.

### Hollywood Presbyterian Medical Center

The hospital's computer system was hijacked by ransomware. They ended up paying a 40 bitcoin ransom to the hackers (US \$17,000) to regain access to their system.

### Democratic National Committee

WikiLeaks published 19,252 emails and 8,034 attachments belonging to the internal governing body of the US Democratic Party.

### Dyn

Multiple DDoS attacks on systems operated by Dyn Domain Name Service (DNS) left large platforms and Internet services inaccessible to users in Europe and North America.

### Russian interference in U.S. election

The US Intelligence Community reported that there was Russian interference in the US presidential elections of 2016.



2017



### WannaCry

Attack targeting the Microsoft Windows operating system. WannaCry has been described as an attack unprecedented in size. It infected 230,000 computers in more than 150 countries.

### Westminster

Cyberattack which aimed to gain access to the e-mail accounts of a large number of politicians in the UK parliament.

### Petya

On June 27, 2017, yet another global ransomware attack began, paralyzing companies around the world. Known as Petya, NotPetya and GoldenEye, its creators succeeded in installing it in some of the most important Ukrainian institutions, such as the National Bank and the Kiev subway system.

### Equifax

Cyberattack that allowed access to the sensitive information of at least 143 million Americans. The biggest personal data theft in history.

# Hackers and Organized Groups

## Organized Groups

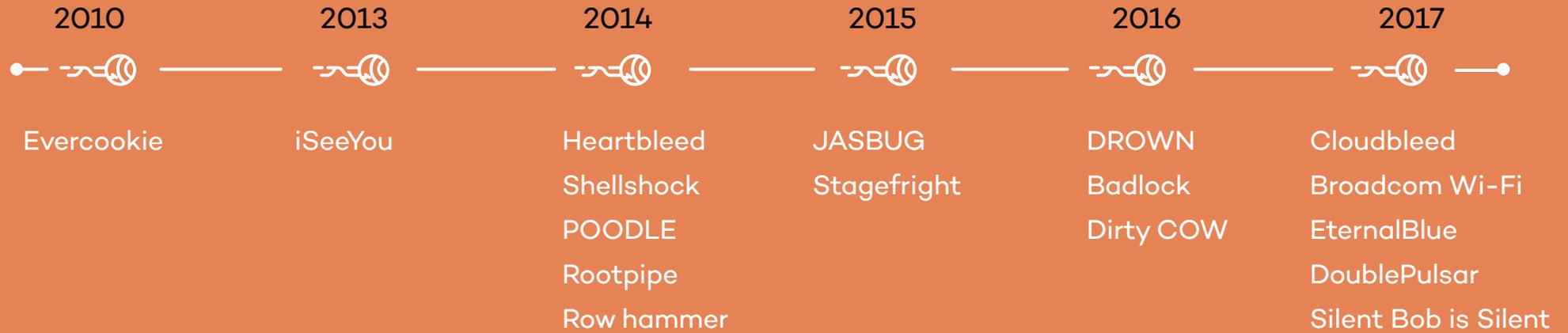
Anonymous	New World Hackers
Bureau 121	NullCrew
Cozy Bear	NSO Group
CyberBerkut	PayPal 14
Derp	PLA Unit 61398
Equation Group	PLATINUM
Fancy Bear	Pranknet
GNAA	RedHack
Goatse Security	Rocket Kitten
Guccifer 2.0	The Shadow Brokers
Hacking Team	Syrian Electronic Army
Iranian Cyber Army	TeaMp0isoN
Lizard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



# Spookiest Vulnerabilities



## Diabolic Malware

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

# The Solution: Adaptive Defense 360

Protect your business year-round and enjoy a bone-chilling Halloween

The solution consists of protection against advanced threats and targeted attacks, and that can even detect unusual or suspicious behavior. A system that can safeguard data confidentiality, information privacy, and the assets and reputation of a company.

An intelligent platform that can help security personnel on critical networks react rapidly to threats and guarantee that they have the information they need to formulate an adequate response.

This is **Adaptive Defense 360**, the only advanced cybersecurity system to combine latest generation protection and the latest detection and remediation technology with the ability to classify 100% of running processes.

Adaptive Defense 360 classifies absolutely all active processes on endpoints, guaranteeing protection against known malware as well as zero-day attacks, advanced persistent threats and targeted attacks.

The platform uses contextual logic to reveal malicious behavior patterns and generate advanced cyber-defense actions against known and unknown threats.

It analyzes, categorizes and correlates all the data gathered on cyber-threats, in order to carry out Prevention, Detection, Response and Remediation tasks.

It determines how data has been accessed and by whom and controls data leakage, whether due to malware or employees.

It discovers and resolves system vulnerabilities and those on installed programs and prevents the use of unwanted applications (toolbars, adware, add-ons, etc.).



More information:

[pandasecurity.com/enterprise/solutions/adaptive-defense-360](https://pandasecurity.com/enterprise/solutions/adaptive-defense-360)

 Adaptive Defense 360