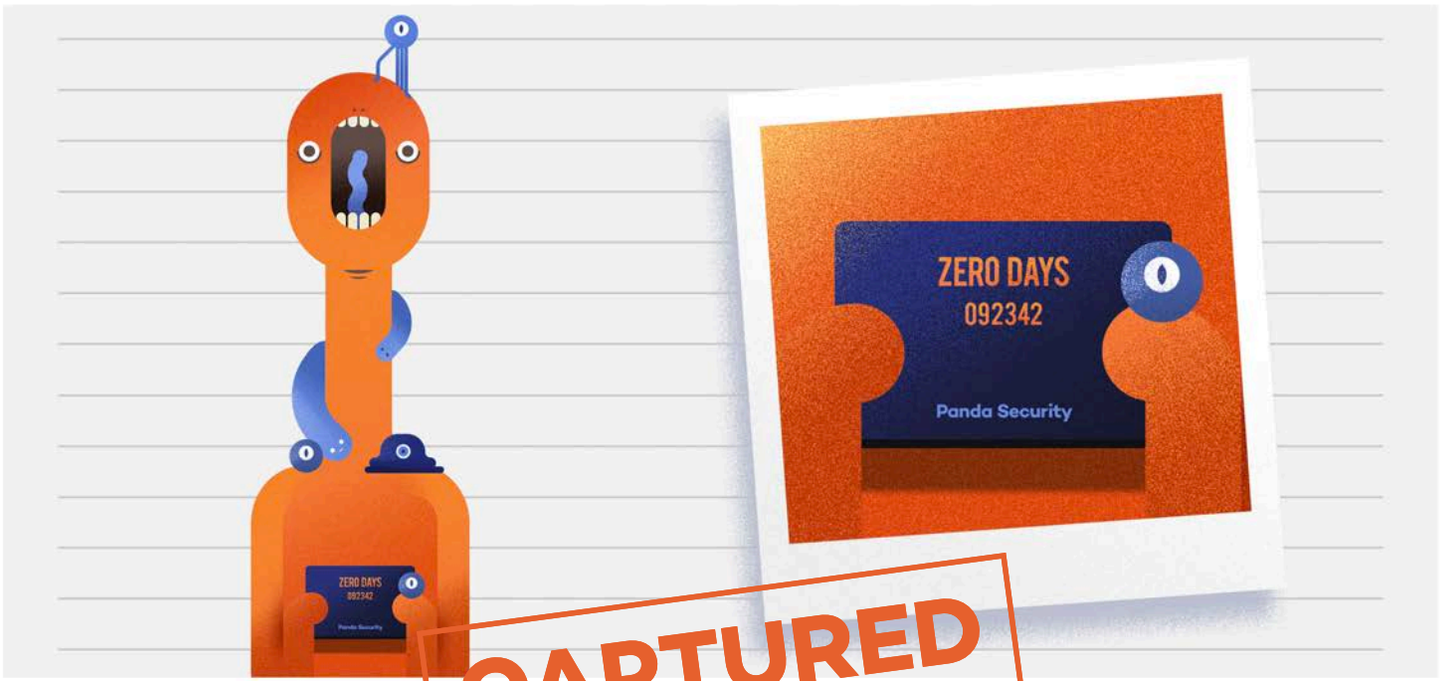

Name

Zero days

Date of Birth

2010

Origin

Unknown

Modus Operandi

'Zero Day' is the name given to any attack that is launched using the window of opportunity provided by recently discovered vulnerabilities. In other words, a rapid attack, deployed by cybercriminals before security providers are able to repair the vulnerability or even before they've heard of it.

They are one of the most commonly used resources for certain governments when it comes to undermining other countries' critical systems or the companies that developed these systems

Arrest

This threat has already been arrested and neutralized by Panda Security.

But if you are not a Panda Security client and you catch sight of it on the company network, contact us immediately to facilitate its capture.

900 90 70 80

info@pandasecurity.com

Criminal Record

Stuxnet

Computer worm that affected computers running Windows, discovered in June 2010. It was the first worm known to spy on and reprogram industrial systems.

The target of this worm was Iran's nuclear infrastructures that used Siemens control systems. Some media outlets attributed it to the US and Israeli secret services

Sony Pictures attack

In 2014, Sony Pictures suffered one of the worst attacks in its history. The hacking group known as 'Guardians of Peace" used a zero day attack to bring Sony's corporate network to a standstill and, over several weeks, steal sensitive information from the company.

The data included personal information about employees and their families, confidential emails, information about company executives' salaries, and copies of unreleased films. A large part of this information was published online.

Democratic National Committee

Thanks to six vulnerabilities in Microsoft Windows 10, Adobe Flash and Java, in 2016, Russian hackers backed by intelligence agencies managed to infiltrate the system of the Democratic National Committee (the US Democratic Party's formal governing body).

In order to exploit these vulnerabilities, phishing emails were sent to different members of the DNC and other political targets, aiming to steal their passwords.

The data obtained was mainly leaked by WikiLeaks.