Deloitte.

panda

Anti-Ransomware services

Collaboration between Deloitte and Panda Security

Content

What is Ransomware?

1,445,000

Ransomware is a type of malicious IT programme that restricts access to certain parts or files of the infected system, and requests a ransom in exchange for their release. Some types of ransomware encrypt files in the operating system, rendering the device unusable and coercing the user to pay the ransom.

Exponential growth

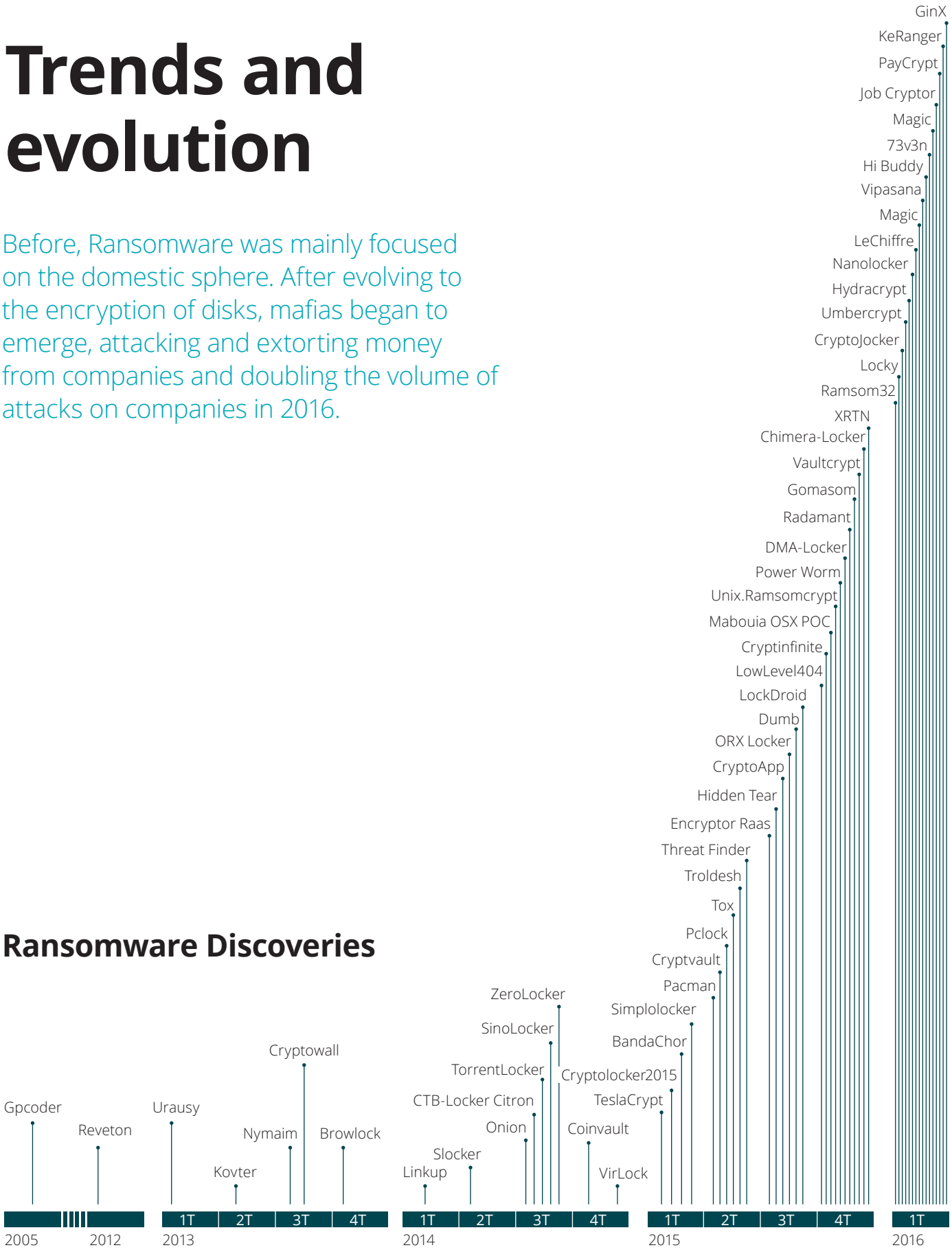
This became popular in Russia and its use has become more and more widespread internationally. In recent months we have experienced massive and worrying attacks such as Wannacry and Petya.

In 2016, more than 1,445,000 users (including companies) across the world became victims of this type of malware.

Trends and evolution

Before, Ransomware was mainly focused on the domestic sphere. After evolving to the encryption of disks, mafias began to emerge, attacking and extorting money from companies and doubling the volume of attacks on companies in 2016.

Ransomware Discoveries



Source: Backtrack Academy


Classification of the most representative current ransomware
Teslacrypt 48,81%
CTB-Locker 21,61%
Scatter 8,66%
Cryakl 7,13%
CryptoWall 5,21%
Shade 2,91%
Mor 1,56%
Aura 0,65%
Locky 0,65%
Lortok 0,42%
Others 2,41%

Our goal

Our objective is to cooperate, in structure and methodology between Panda Security and Deloitte EMEA.

Panda Security and Deloitte EMEA have reached a collaborative agreement to deploy a managed security service using Adaptive Defense technology.

An example of this is Deloitte's own use of Panda Security's Anti-Ransomware Endpoint (Adaptive Defense) for all employees in the Spanish Firm.

The services built around this technology are the following:

Software deployment

Adaptive Defense software's centralised and automatic deployment.

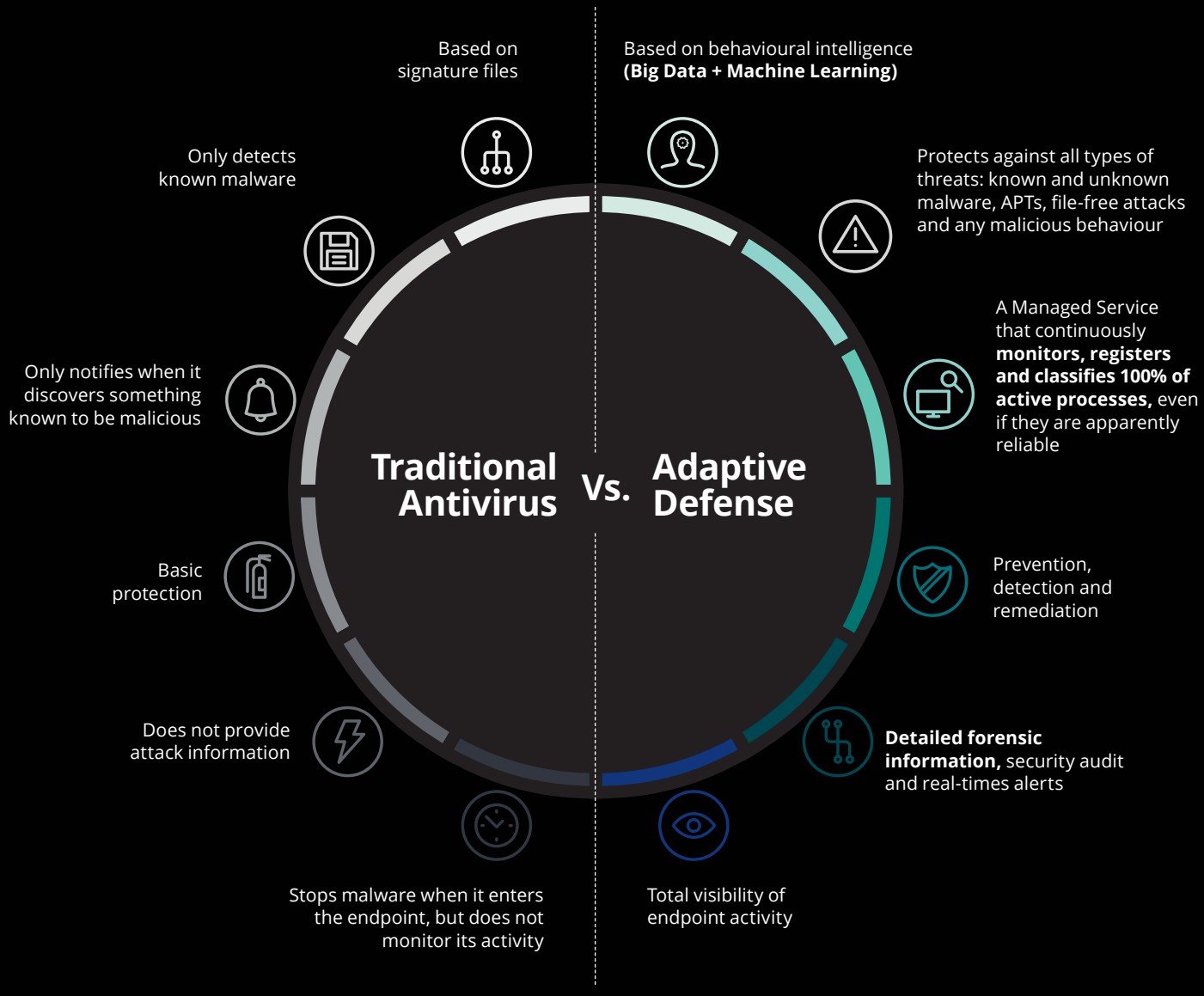
Adaptive Defense Management

- Keeping the product up-to-date is vital, not only from a version point of view, but also taking the continuous evolution of the other software of the protected endpoint into consideration.
- Reduction of the total amount of incidents through learning about the nature of each one, guaranteeing optimal device functioning.
- Control of results and certainty that everything is working correctly.

Cyber Incident Response (CIR)

C.I.R aims to manage the situation to limit damage and allow business operations to return to normal as quickly as possible.

Adaptive Defense Technology



100%

Panda Adaptive Defense is an advanced managed cyber security service based on three principles: continuous monitoring of the endpoint, classification of 100% of the active processes thanks to Big Data and Machine Learning technologies, and behaviour analysis carried out by expert technicians.

Endpoint Detection and Response

monitoring, analysis and categorisation 100% of active processes in all endpoints in the corporate network. Certifying all applications in execution.

Dynamic Exploit Detection

its anti-exploit technology neutralises the attack as soon as an exploitation attempt is detected in a trusted application, identifying known and unknown exploits.

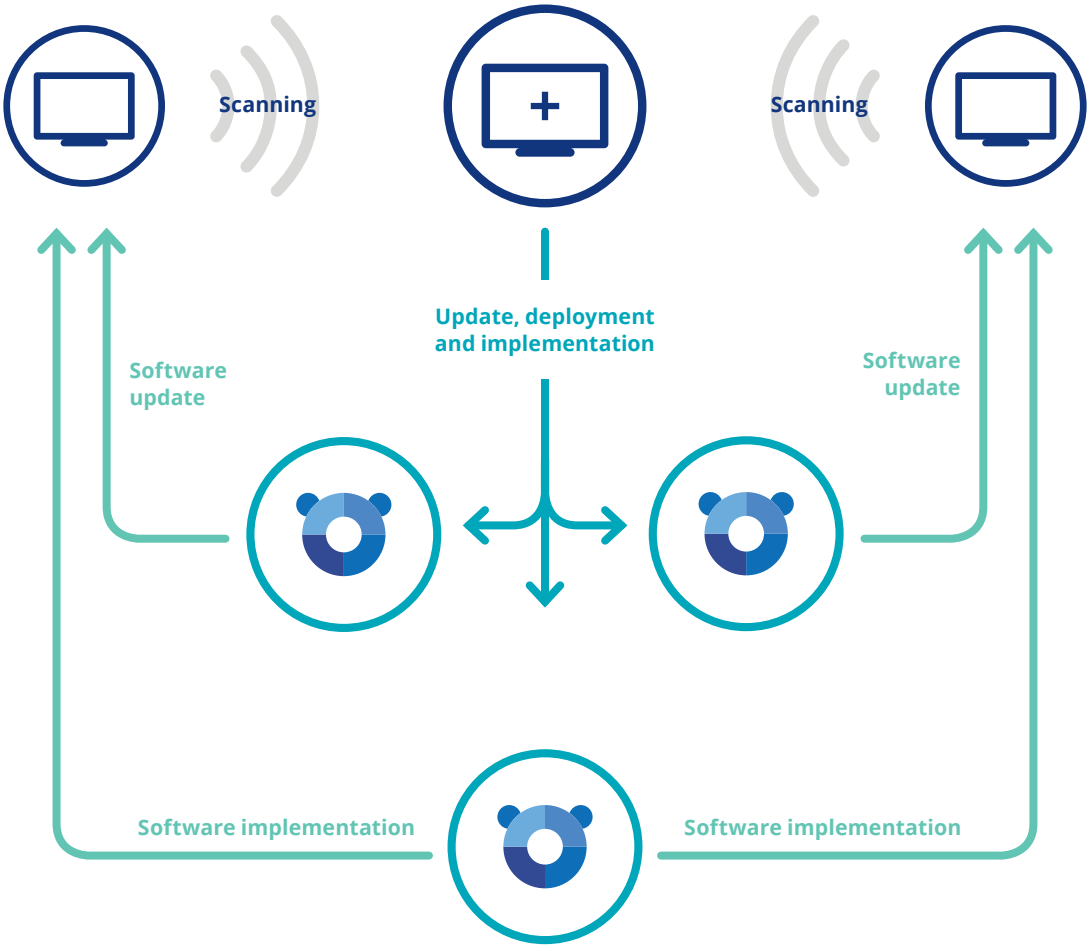
Malware Intelligence Platform

the correlation of data configures a security intelligence system capable of revealing patterns of malicious behaviour to get ahead of the threats.

ASSOCIATED SERVICES

Endpoint Adaptive Defense deployment

As a first point at the beginning of the Anti-Ransomware service provision, Deloitte will offer the deployment of the Panda Adaptive Defense solution in company devices (in close coordination with their own team).



ASSOCIATED SERVICES

Immediate response: Cyber Incident Response

The aim of C.I.R is to manage the situation, limit the damage and allow business operations to return to normal as quickly as possible.

Our service provides capabilities to identify, contain and minimise the risk when faced with this type of incident, as well as measures to prevent this from happening again.

The casuistry of this type of incidents could be, for example

- Security incident management
- Forensic analysis
- Malware analysis
- Shell scripting, perl, Python or other programming.
- Revision of systems
- Revision of logs

Cyber Incident Response

24/7/365		Immediate phone call
154		In 154 countries

Our team will offer immediate answers and will help you to face the crisis. Our specialists provide the necessary knowledge and tools to determine what has happened and how to resolve it.

CIR is an advanced service, prepared to respond to security incidents, regardless of the cause. This represents an organised way to manage security breaches, attacks or incidents.

Deloitte.

For further information, please visit www.deloitte.es

Designed and produced by the Communications, Brand and Business Development department, Madrid.