A Segurança na Web 3.0

DISPOSITIVOS - INFORMAÇÃO

- Até ao 3.0

> Índice

- Alguns Dados Estatísticos
- A Informação
- Os Ataques
- A Segurança
- A Solução?
- Resumo/Conclusões

BACK FORWARD

-1.0

> Até ao 3.0

- Html estático
- Sites sem serviços

-2.0

- Sites com serviços associados
- Redes Sociais
- Partilha de informação cruzada (pc+iNet)
- Jogos

-3.0

- Web Semântica
- Perfil de gostos
- Interpretação das pesquisas
- Widgets -> Mashup
- App's
- Banca
- Etc…

- Os nomes:
  - Web services
  - Utility computing
  - Grid computing
  - Server Based Compunting

- São muitos nomes para uma só ideia:
  - Cloud Computing

- Ver o mundo digital como se de um nuvem se tratasse, onde "tudo é de todos" e aparece no ecrã de forma simplificada;
  - Processadores, Memória, etc.

- Traduz-se num baixo custo (relativo), pelo aproveitamento dos recursos/serviços existentes

- Na era do 3.0;
  - A informação é bidirecional
  - Dinâmica

- A Web chega a quase todas as casas…
  - Pelos dispositivos móveis
  - Pela televisão
  - Pelos eletrodomésticos

- … e a todos os lugares…
  - Em viagem
  - No escritório
  - No carro

  - … de forma massiva!

> Existirão duas variáveis incontornáveis e comuns a todas as infraestruturas:

1-A INFORMAÇÃO

2-OS DISPOSITIVOS

A realidade atual

>ALGUNS DADOS…

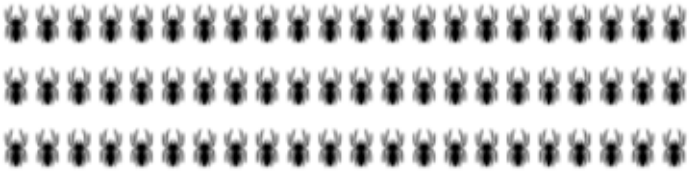
> Evolução das ameaças I

1994

One new virus every hour

2006

One new virus every minute



Evolution of malware waves we have to deal with

2011

One new virus every second

Or 70.000 samples/day

What about

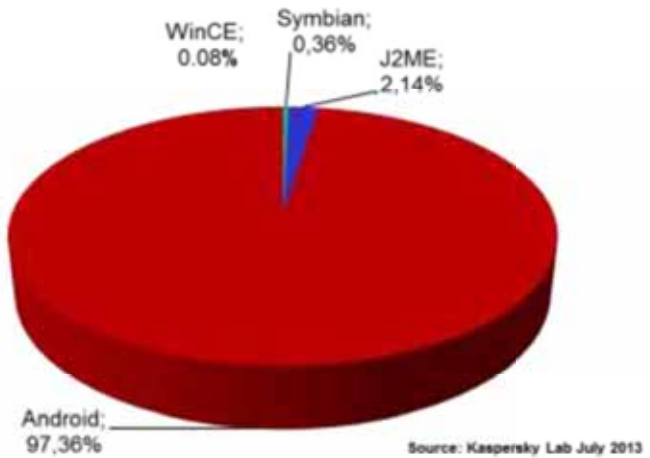
2013

?


Kaspersky Lab
is currently processing
200.000
unique malware samples
EVERY DAY

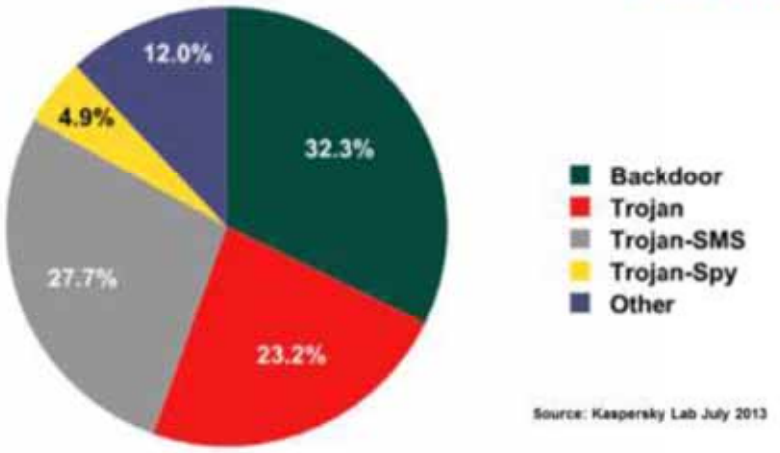
> Alguns dados
- Mobile Malware

Mobile malware written for specific platforms:



>Number of mobile malware families to-date: 679
>Number of mobile malware modifications to-date: 107,068
>Mobile malware found in July 2013: 4,181 new modifications

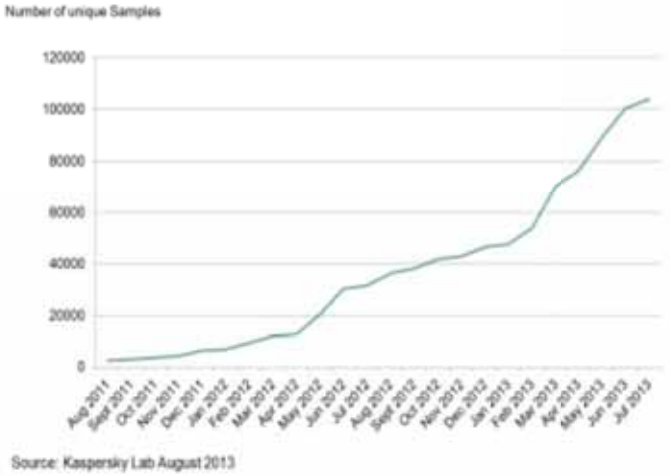
>Distribution of malware targeting Android OS detected on user devices by behavior, Q2 2013



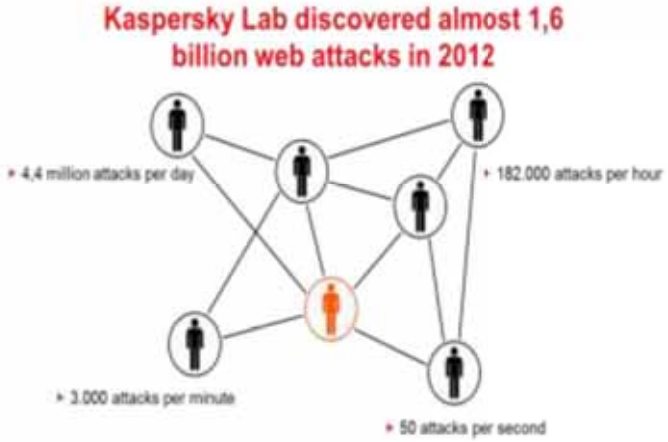
A Informação

>A DINÂMICA DO 3.0

> A dinâmica nos dias atuais



Source: Kaspersky Lab August 2013



Source: Kaspersky Lab 2012

BACK FORWARD

ATEC
Academia de Formação

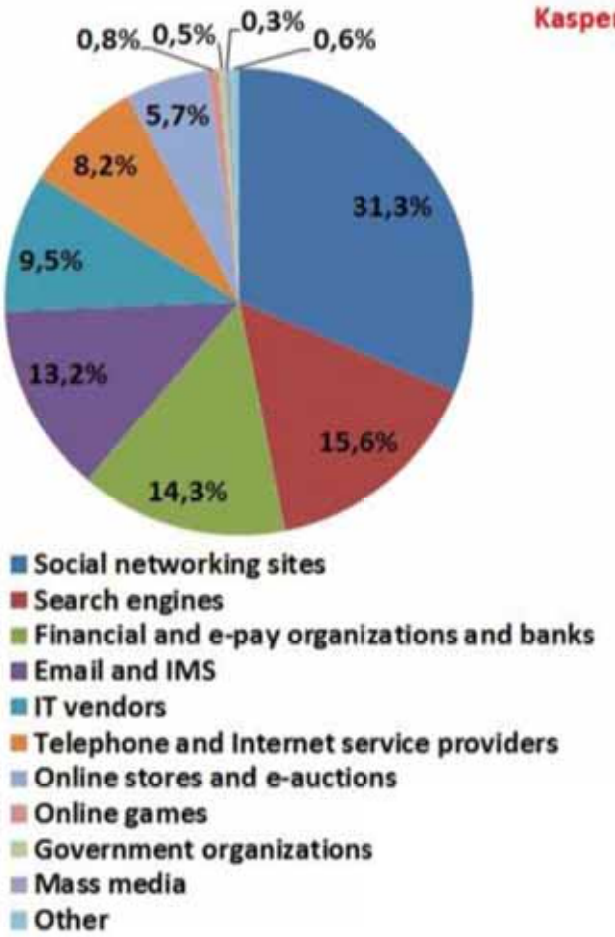
Os ataques

> PARA ALÉM DO QUE PODEMOS IMAGINAR

BACK FORWARD

> Phishing – JUNE13

- In March, Social networking sites continued to be the most attractive target for phishing attacks though their share fell 3.15 percentage points and averaged 31.3%.
- The Top 3 also included Search engines (15.6%) and Financial and e-pay organizations (14.3%) which came 2nd and 3rd respectively.
- 4th place was taken by Email and IMSIT (13.2%), followed by IT vendors (9.5%) and Telephone and Internet service providers (8.2%).

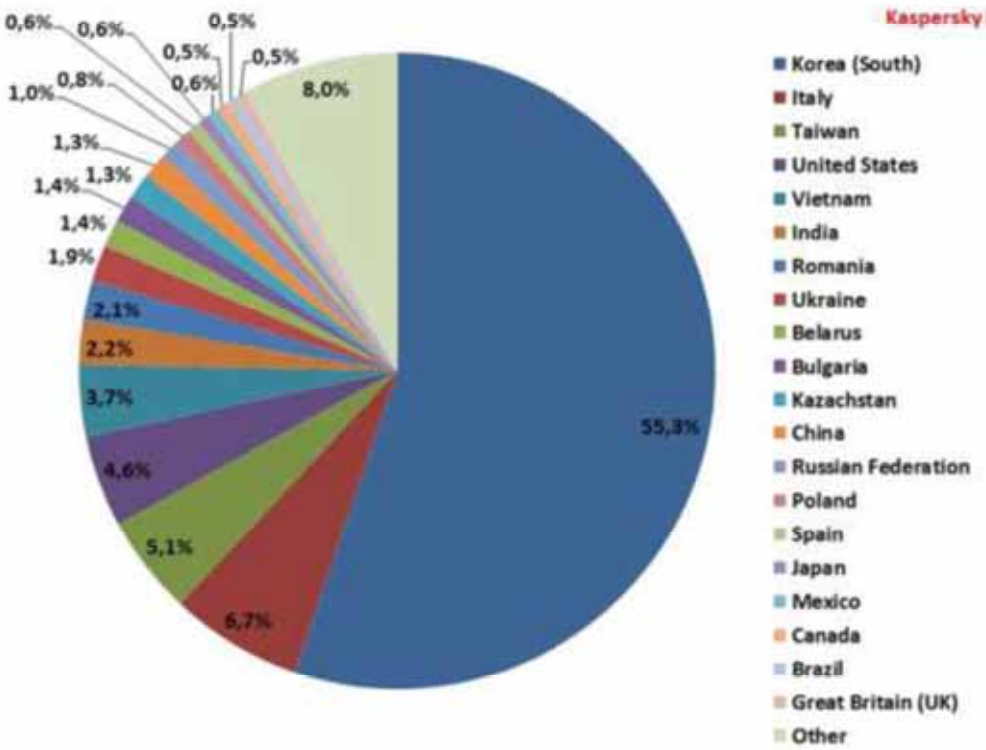


BACK FORWARD

>Source: Kaspersky Lab June 2013

> Spam – JUNE13

Sources of Spam by Country



BACK FORWARD

>Source: Kaspersky Lab June 2013

ATEC
Academia de Formação

>Uma nova ameaça: STUXNET

Ciber-terrorismo ou Ciber-guerra?

- **O primeiro worm que espia e reprograma sistemas industriais;**
  - O cenário mais sofisticado detectado até hoje
- **Ataca Sistemas SCADA (Siemens Simatic WinCC)**
  - Controlo e monitorização industrial, de infra-estrutura e acesso a instalações
  - Usados em oleodutos, centrais eléctricas, grandes sistemas de comunicações, aeroportos, portos e instalações militares a nível global
- **Usa a tecnologia "rootkit" para se esconder**
  - Classic Windows rootkit
  - Execução silenciosa em PLC (Programmable Logic Controllers) em que o código alterado está igualmente escondido
- **Propaga-se via discos externos, rede e partilhas de rede**
  - As máquinas infectadas torna-me parte da "botnet" Stuxnet
  - Recolhe informação sobre os servidores e configurações de rede
  - Conecta-se às bases de dados associadas a sistemas SCADA
- **Usa 5 vulnerabilidades do Windows incluindo 4 defeitos "zero-day" em SO Windows novos e antigos**
- **Serve-se de 2 certificados roubados da Realtek e JMicron para assinar "drivers" malware e rootkits**

BACK FORWARD

> Mac OS X botnet Flashfake

First major outbreak of malware targeting Macs

We saw a peak of more than 700,000 infected machines

It is being distributed via infected websites as a Java applet that pretends to be an update for Adobe Flash Player

The Java applet then downloads and installs the main component

Main infection vector: hacked Wordpress sites

Geographical distribution of Flashback bots

BACK FORWARD

>Source: Kaspersky Lab June 2013

>NetTraveler

- Cyber-espionage campaign
  - 350 victims in 40 countries
  - Most victims found in 2010-13, but the code may date back to 2004-05
  - Targets include Tibetan and Uyghur activists, oil companies, scientific research facilities, universities, private companies, government and diplomatic bodies and military contractors
- Attacks are launch via spear-phishing e-mails with malicious Office documents
- Data stolen from target organizations includes DOC, XLS, PPT, PDF and other files
  - In total, 22GB of data was found on C2 servers controlling the attacks

> Red October

BACK FORWARD

Advanced Persistent Threats

> CYBER WEAPONS


Number of victims
300K
100K
10K
1K
50
20
over 300K
over 100K
10K
2500
5-6K
700
50-60
20
50-60
10-20
Stuxnet
Gauss
Flame
DUQU
Duqu
miniFlame
Number of incidents (Kaspersky Lab statistics)
Approximate number of incidents


Cyber weapons
6 cyber weapons are known – 5 were active in 2012.
DUQU
DUQU
CLASSIFICATION
Espionage Program
DETECTION TIME
September 2011
ACTIVE SINCE
August 2007
FACTS OF DUQU:
• built on same platform as Stuxnet (Tilded)
• destroys all traces of activity
• core module never detected
• no further modifications discovered since Feb. 2012

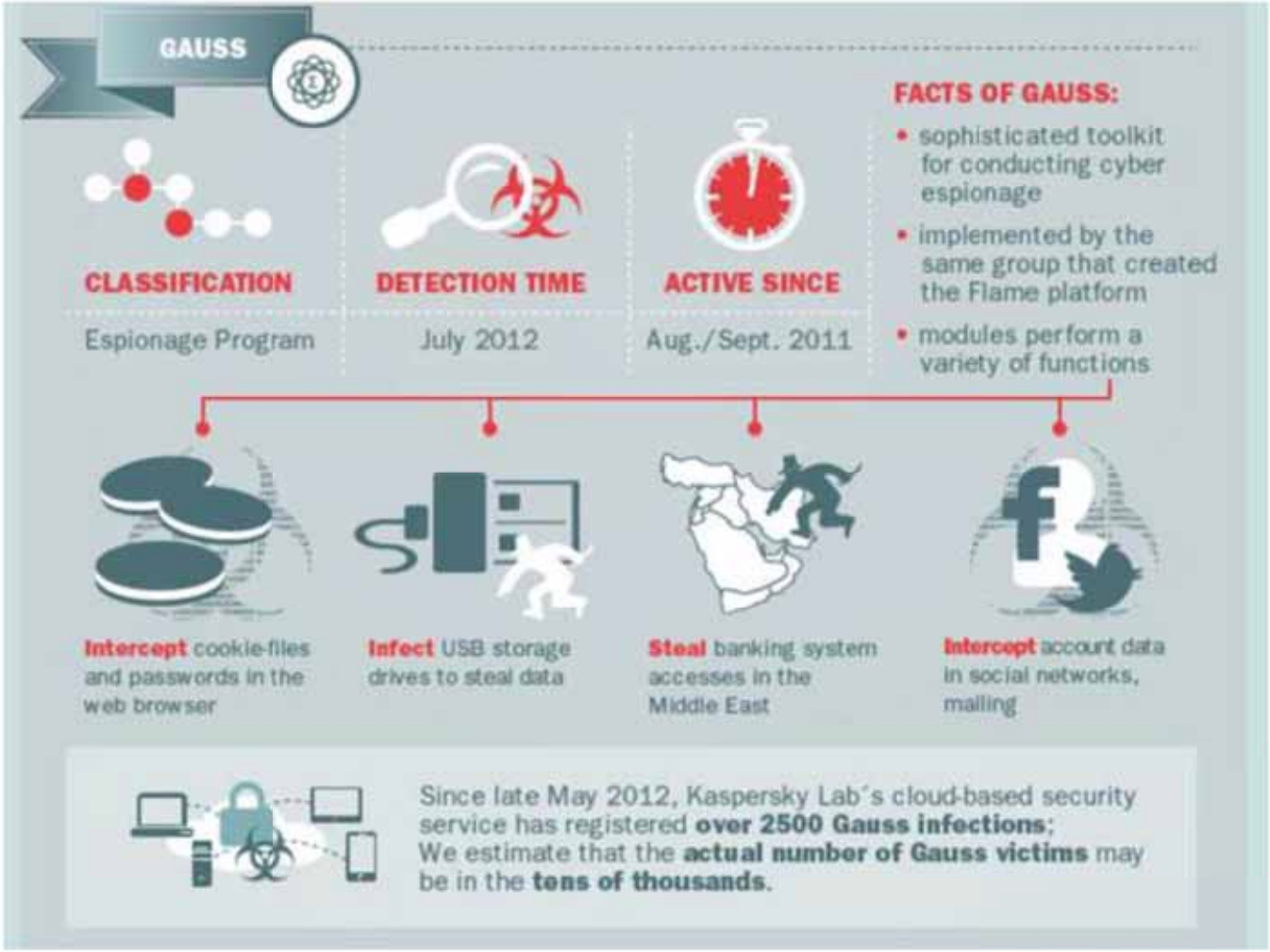
FLAME

CLASSIFICATION	DETECTION TIME	ACTIVE SINCE
Espionage Program	May 2012	2008

Flame incorporated **a unique funcionality** to propagate itself across the LAN; to that end, **it intercepted Windows update requests** and **substitued** them with its own module signed with a Microsoft certificate. Analysis of this certificate revealed **a unique cryptographic attack** which enabled cybercriminals to generate their **own bogus certificate** that was **indistinguishable** from a legal one.

FACTS OF FLAME:

- complex set of operations, including analyzing the network traffic, taking screenshots, recording voice communications, keystroke logging, etc.
- can download extra modules to victim computers
- 20 extension modules detected
- sophisticated toolkit, far more complex than Duqu
- module used in 2009 for the Stuxnet worm
- module in Flame used in Stuxnet 2009 version shows: developers of Flame and Stuxnet/Duqu collaborated at least once


GAUSS
CLASSIFICATION
Espionage Program
DETECTION TIME
July 2012
ACTIVE SINCE
Aug./Sept. 2011
FACTS OF GAUSS:
• sophisticated toolkit for conducting cyber espionage
• implemented by the same group that created the Flame platform
• modules perform a variety of functions
Intercept cookie-files and passwords in the web browser
Infect USB storage drives to steal data
Steal banking system accesses in the Middle East
Intercept account data in social networks, mailing
Since late May 2012, Kaspersky Lab's cloud-based security service has registered over 2500 Gauss infections;
We estimate that the actual number of Gauss victims may be in the tens of thousands.

MINIFLAME

CLASSIFICATION

Espionage Program

DETECTION TIME

October 2012

ACTIVE SINCE

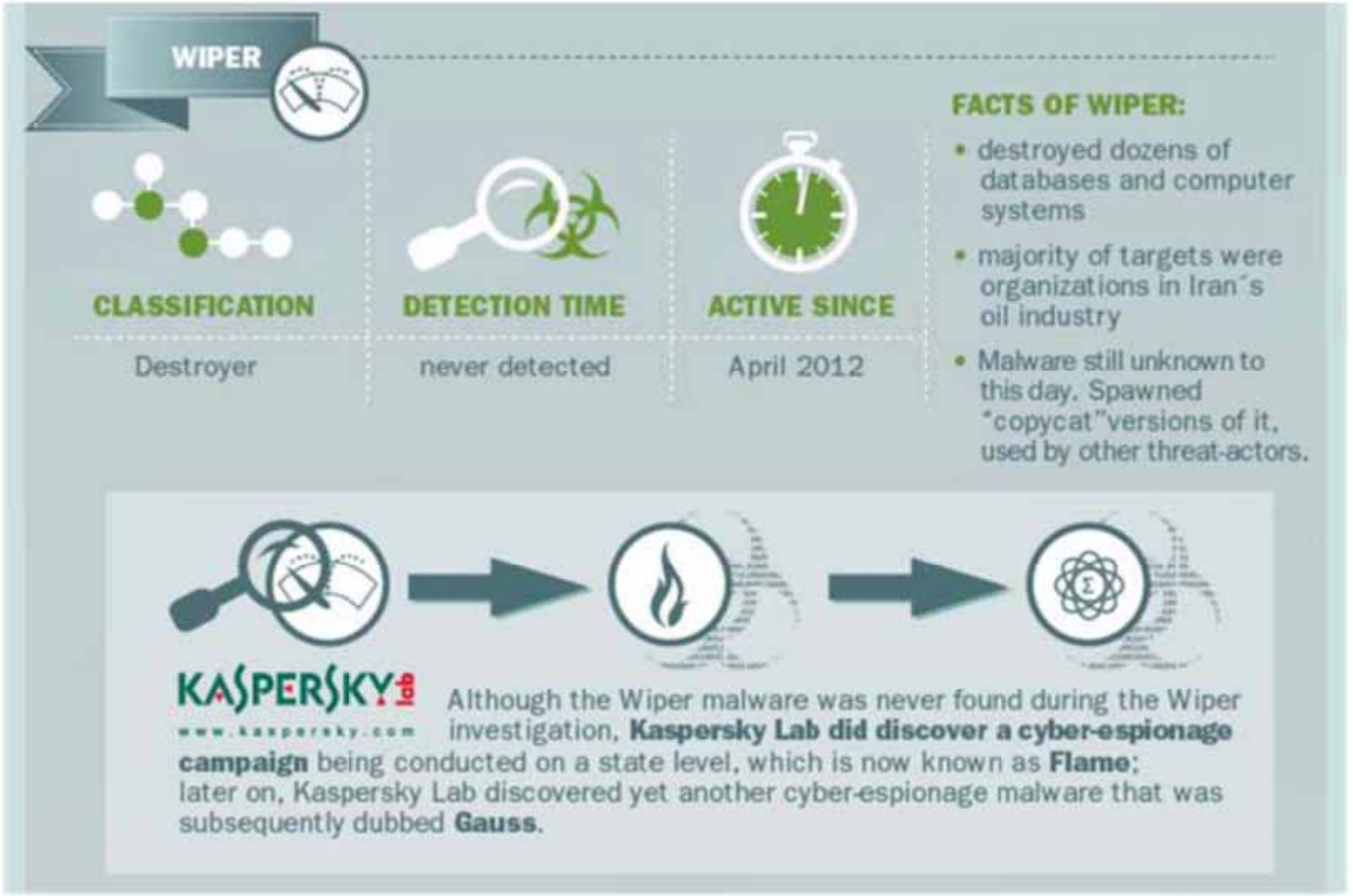
Aug./Sept. 2011

FACTS OF MINIFLAME:

- created on the Flame platform
- miniature fully-fledged spyware module
- used for highly-targeted attacks against select victims
- can be implemented as stand-alone malware or as a plug-in for Flame

Remarkably, miniFlame **can also be used in conjunction with Gauss**, another spyware program.
MiniFlame´s primary purpose is to function as a **backdoor on infected systems**, enabling attackers to directly manage them.

BACK FORWARD



BACK FORWARD

A Segurança

> UM NOVO PARADIGMA

- Segurança no acesso aos Servidores
- Segurança no acesso à Internet
- Segurança no acesso às Bases de Dados
- Segurança de Dados Críticos
- Segurança nos acessos às aplicações

Perigos

- Serviços currompidos
- Roubo de informação
- Perca de privacidade
- Eliminação de dados

Vulnerabilidades

- Programas hostis
- Operadores que dão mau uso à informação
- Hackers inibindo as comunicações

-A modo de exame preliminar, vejamos como se comporta o modelo CIA (confidenciality, integrity, availability) numa infraestrutura tipo.

- **Confidentiality:** É de supor que a informação estará encriptada. Mas quem controla as chaves? O cliente ou o fornecedor do serviço?

- **Integrity**: São apenas aprovadas as modificação do dados unicamente em resposta a acessos autorizados. Se este acesso é feito através de um dispositivo móvel, sabemos quem na realidade os solicita? Para conseguir isto, são necessários standard, que hoje em dia não existem.

- **Availability**: Estarão os nossos dados disponíveis constantemente? Na Cloud?A título de exemplo, em Fevereiro de 2010 o serviço S3 da Amazon esteve em baixo durante quatro horas devido a um pico inesperado nas transações dos seus utilizadores. Se bem que a Amazon trabalhou muito para evitar que se repitam estes incidentes, a disponibilidade nunca estará de todo assegurada.

-Segurança da Informação

- Comunicação = confidencialidade e integridade
- Infraestrutura de autenticação/SSO + PKI + Certificados X.509

-Segurança de Rede

- Informação = limpa e verdadeira
- Infraestrutura que conheça e iniba a origem de ataques

-Segurança dos Dispositivos

- Isolamento das aplicações = administração + controlo de acessos
- Infraestrutura que não permita dados críticos nos dispositivos

-Pessoal IT

-Know-how

-Gestão das diversas aplicações

-Efetividade e "reportabilidade"

-Disaster Recovery

-Continuidade do negócio

-Rendimento

-Fiabilidade

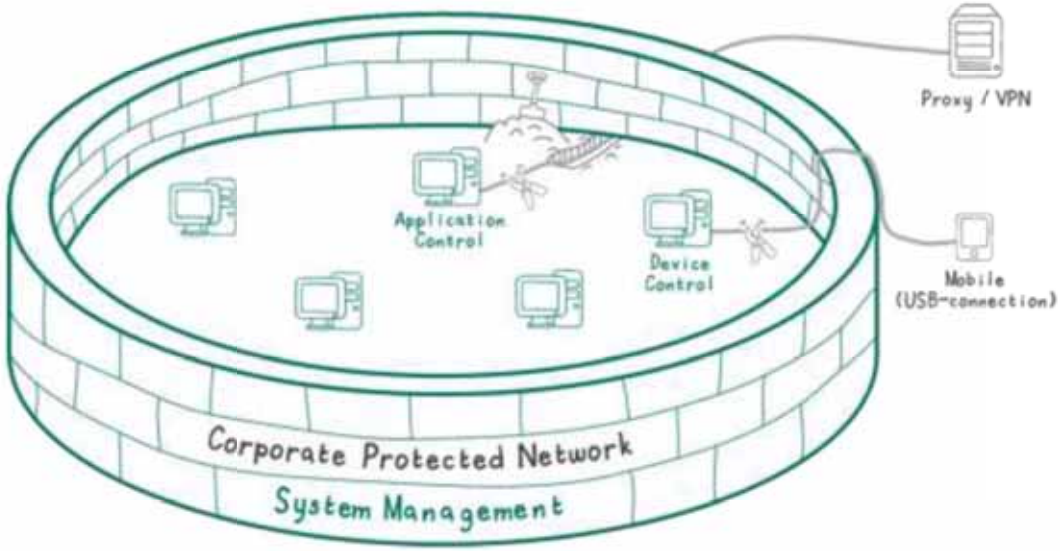
-Atualização do IT

-Custo

- Como proteger a informação? (pública, privada, sensível…)
- Como manter seguros os dispositivos? (servidores, postos, smartphones, tablets…)
- Como eliminar pontos de falha? (portas I/O, aplicações permitidas, web…)

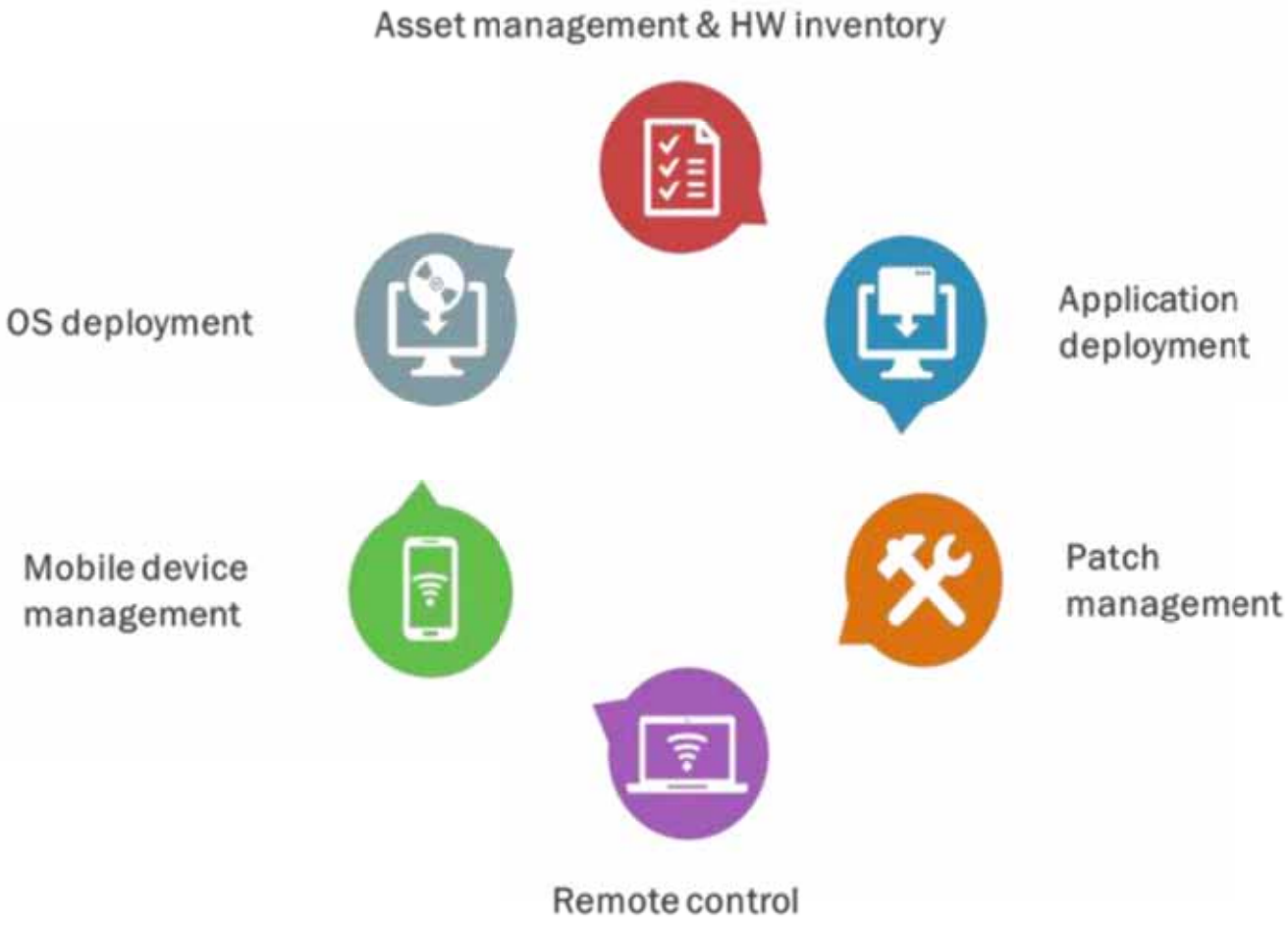
> As questões pertinentes dos profissionais IT

- Outras questões poderão ser equacionadas, mas acabam todas nas duas variáveis INFORMAÇÃO e DISPOSITIVO.



A Solução?

> PROTEGER A INFORMAÇÃO, SECURIZAR O DISPOSITIVO

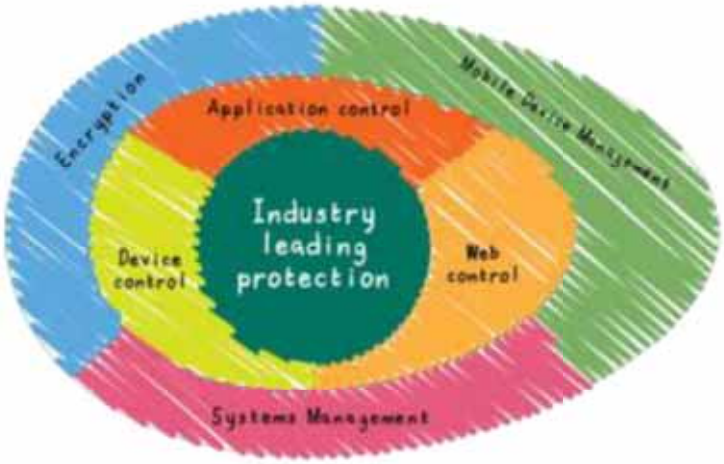


> Conseguir o exercício de poder VER, CONTROLAR e GERIR tudo de um ponto central, mantendo a coerência das políticas.

> Conseguir ter os dados Encriptados com a adição de anti malware

Resumo

> CONCLUSÕES



> Em resumo:

- Na era do 3.0, ou Cloud, ou BYOD, ter-se-á de conseguir que de um simples ponto, se possa VER, CONTROLAR e PROTEGER todos os dispositivos e toda a informação.

Aliado a tudo isso e porque cada vez mais ***a tecnologia está mais tecnológica***, é necessário canalizar os esforços corretamente para que a simplicidade e a produtividade sejam aliados

BACK FORWARD

- Geografia, redundância e backup's são importantes
- Eliminação de registo de dados ou "data sanitization"
- Focus nos dispositivos e na informação
- Sistemas de Encriptação e de Contentores (MDM)

- A Tecnologia terá de ser baseada em:
  - Listas brancas/negras para aplicações conhecidas;
  - HIPS para controlo de aplicações;
  - Ambientes Virtualizados seguros (sandbox);
  - "In-the-cloud" e "community-based" para estas tecnologias;
  - Processos automáticos de bloqueio le impeza de malware;
  - Controlo de acessos a recursos críticos;
  - Controlo de comportamento;

- Será necessário centralizadamente conseguir:

VER , CONTROLAR e PROTEGER TUDO

- Obad – the most sophisticated Android Trojan
- Exploits three vulnerabilities
  - Including one that gives it 'superuser' privileges on the device
  - So it can't be manually deleted
- Sophisticated backdoor Trojan
  - Runs silently in the background
    - No icon or other indicator of its presence
  - Remote control over compromised device
    - Receives commands from C2 server via SMS messages
    - Uploads data from device to the C2 server
  - Silently sends SMS messages to premium-rate numbers
  - Able to download and install additional malware
    - And spread to other devices via Bluetooth

> CURIOSIDADE

- [o] bad news!

Fernando Baldini Simões

Corporate Sales Manager

Kaspersky Lab Portugal

fernando.simoes@kaspersky.pt

+351 912 571 824