GESTIÓN GRCS, CONVERGENCIA & INNOVACIÓN

RADICAL

Alternativas de avanzada

Ciberseguridad y ataques dirigidos: el nuevo entorno de amenazas APT (advance persistent threats).

Casos de APT en el año 2016

14 JUN 2016 NEWS

North Korea Hacked 140,000 Computers in Cyber War Prep

Steve Evans Freelance journalist, copywriter and editorial consultant
Follow @Evans_Steve

North Korea has hacked into more than 140,000 computers belonging to 160 South Korean companies and government organizations, Seoul officials have announced. The hack was part of a long-term plan by the North to launch a huge cyber-attack on its neighbor.

The hack began back in 2014 but wasn't detected until February of this year, Reuters said. The attackers targeted a vulnerability in network management software that is widely used in South Korea. The South's cyber investigation unit told Reuters it had neutralized the malware before it could be used in a large-scale attack.

"There is a high possibility that the North aimed to cause confusion on a national scale by launching a simultaneous attack after securing many targets of cyber terror, or intended to continuously steal industrial and military secrets," an official at the cyber investigation unit told Reuters.

Some 42,000 documents were stolen before the malware was detected, with 40,000 of those being defense-related. This included blueprints for the wings of F-15 fighter jets.

White Paper
Website Security for Dummies
Download Now

Why Not Watch?

Los atacantes utilizan todos los puntos de entrada

GESTIÓN GRCS, CONVERGENCIA & INNOVACIÓN
RADICAL
Alternativas de avanzada

ELLOS ENTRARAN!

(cuestión de tiempo)

Anatomía de un APT

GESTIÓN GRCS, CONVERGENCIA & INNOVACIÓN
RADICAL
Alternativas de avanzada

1. El ciber criminal entra a través de **email**, red, archivo o aplicación vulnerable e inserta malware en la red de la organización. La red es considerada comprometida pero no hay brecha.

50%

Phishing emails opened and clicked within first hour

Anatomía de un APT

GESTIÓN GRCS, CONVERGENCIA & INNOVACIÓN
RADICAL
Alternativas de avanzada

1. El ciber criminal entra a través de email, **red**, archivo o aplicación vulnerable e inserta malware en la red de la organización. La red es considerada comprometida pero no hay brecha.

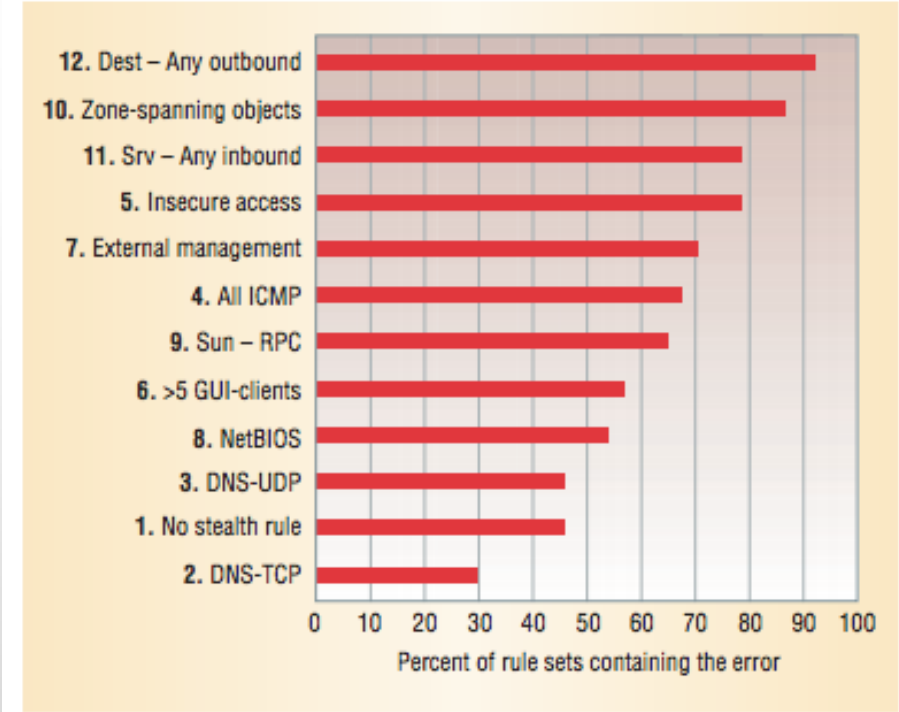
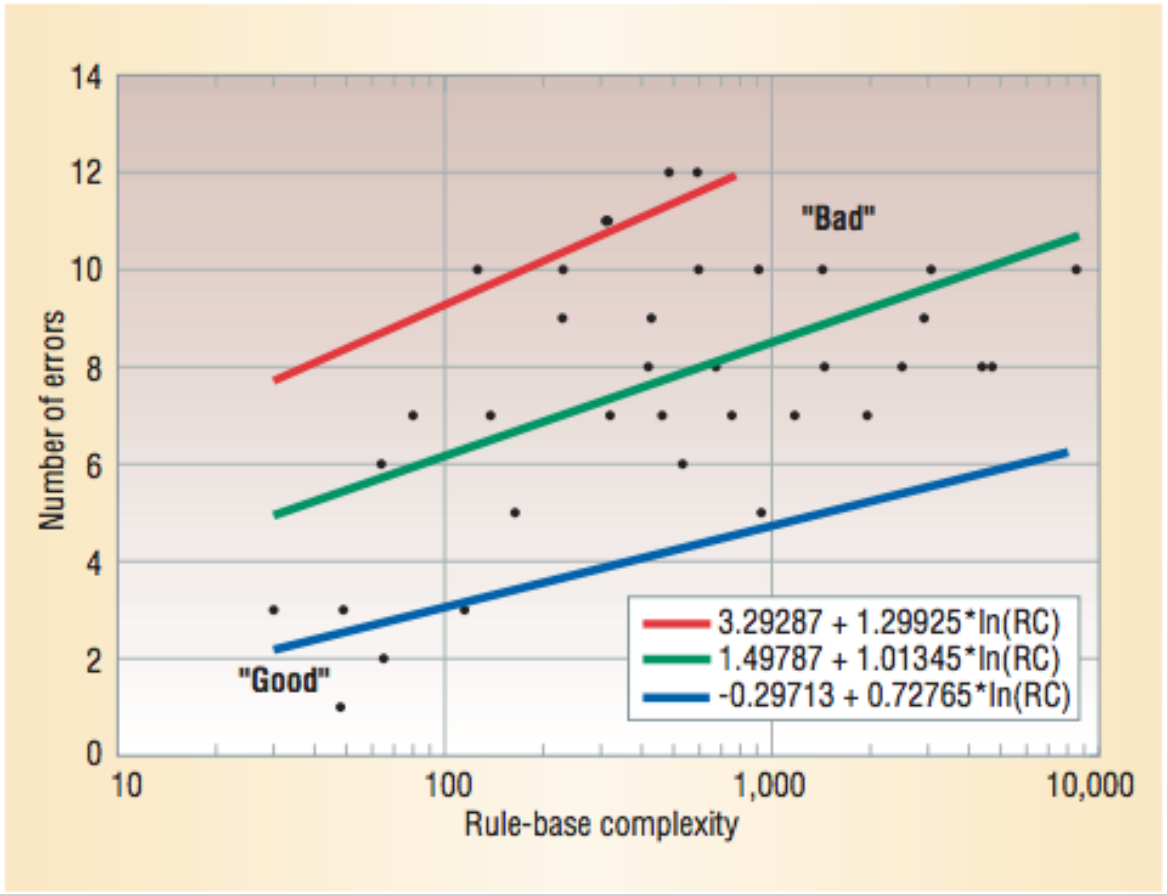
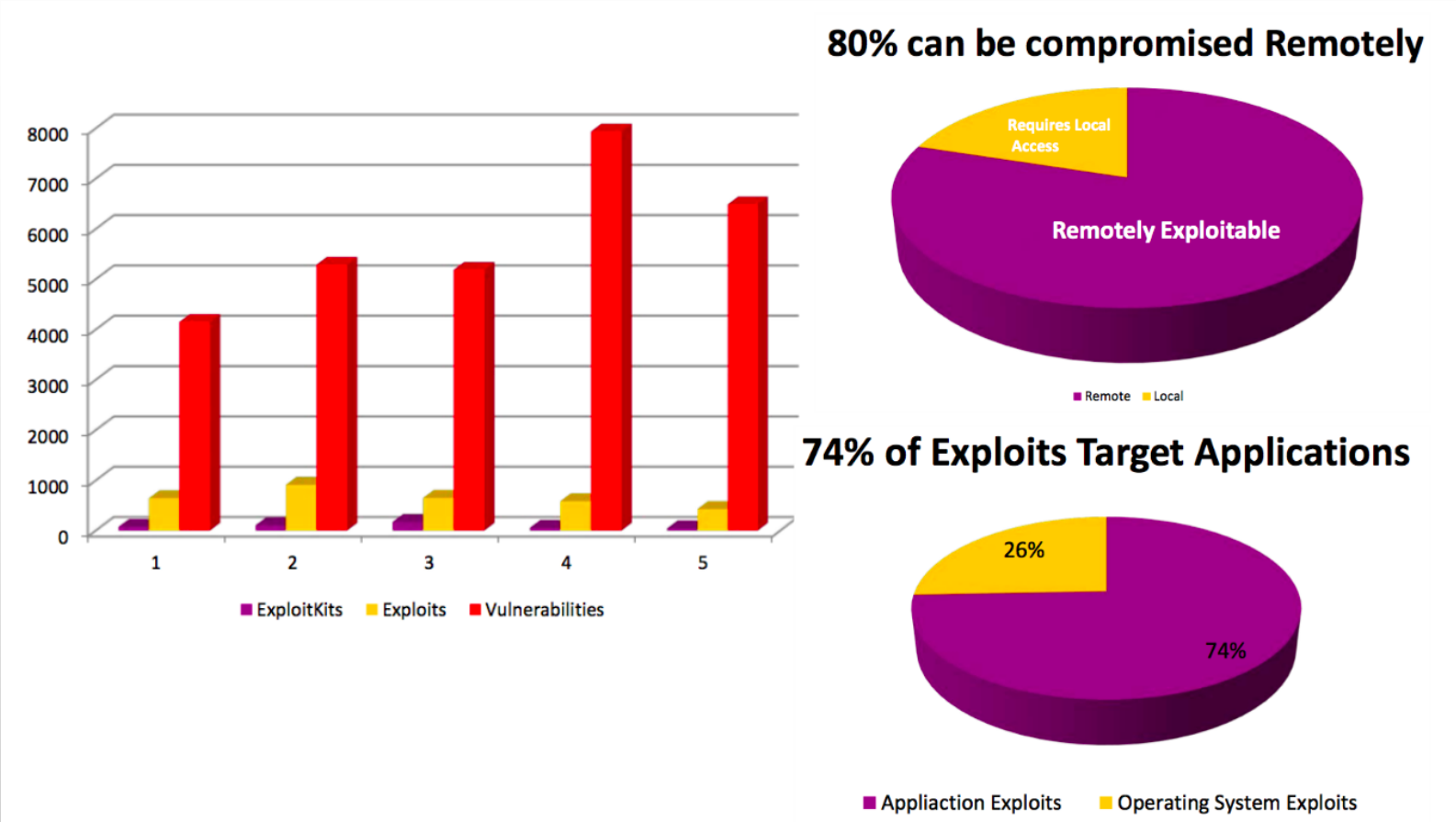


Figure 1. Distribution of configuration errors. Numbers on bar descriptions correspond to the configuration error descriptions in the text.



Anatomía de un APT

1. El ciber criminal entra a través de email, red, archivo o **aplicación vulnerable** e inserta malware en la red de la organización. La red es considerada comprometida pero no hay brecha.



Anatomía de un APT

GESTIÓN GRCS, CONVERGENCIA & INNOVACIÓN
RADICAL
Alternativas de avanzada

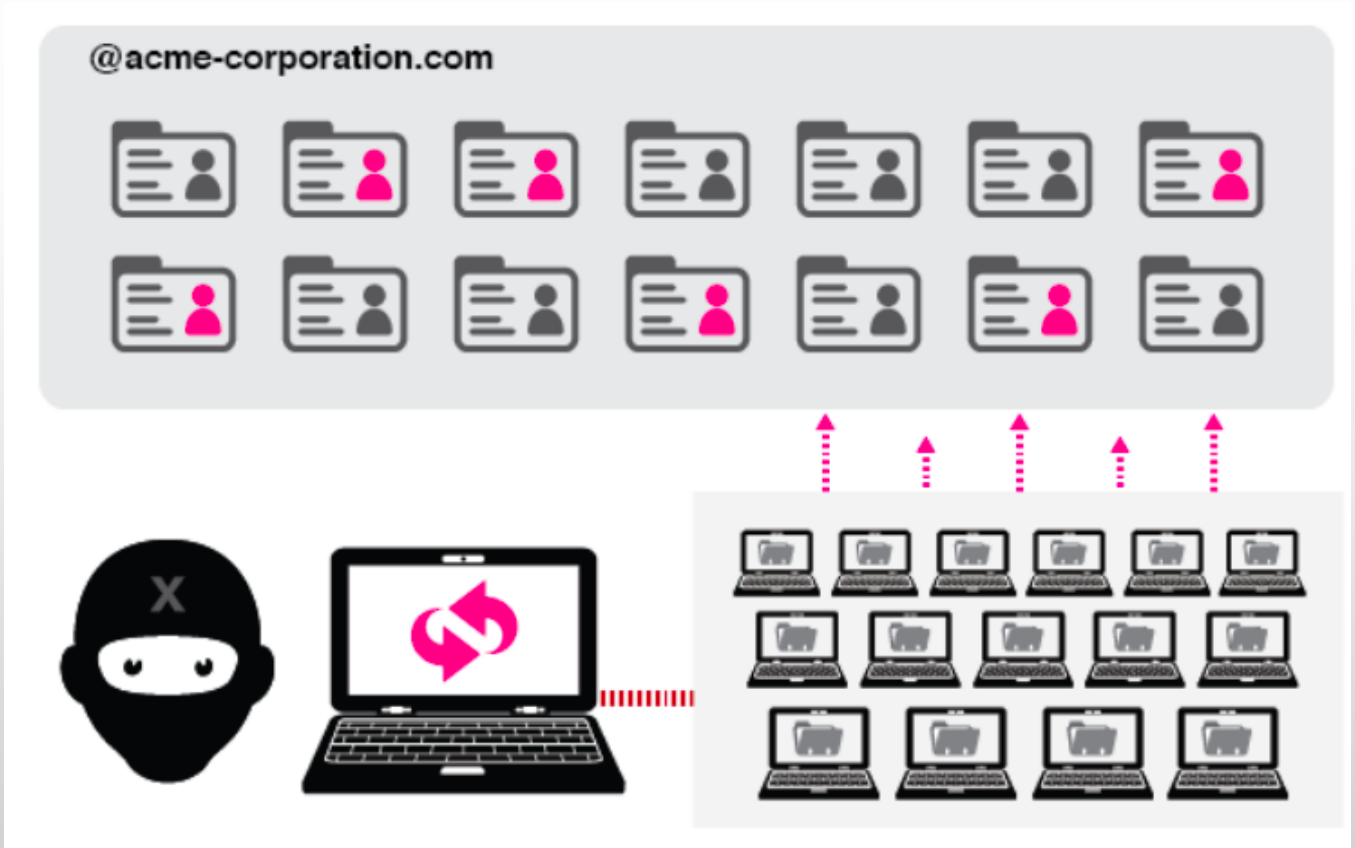
2. El malware avanzado busca accesos adicionales a la red y vulnerabilidades o se comunica con un centro de mando y control C&C para recibir instrucciones adicionales y/o código malicioso.

Protocolos utilizados para comunicación de los hackers: SSH, SNMP, SIP2, SMTP, POP3, IRC, DNS Response, HTTP, FTP, TFTP, SMB, RDP, DHCP, TELNET, HTTPS, UDP, ARP, IGMP, etc.

Anatomía de un APT

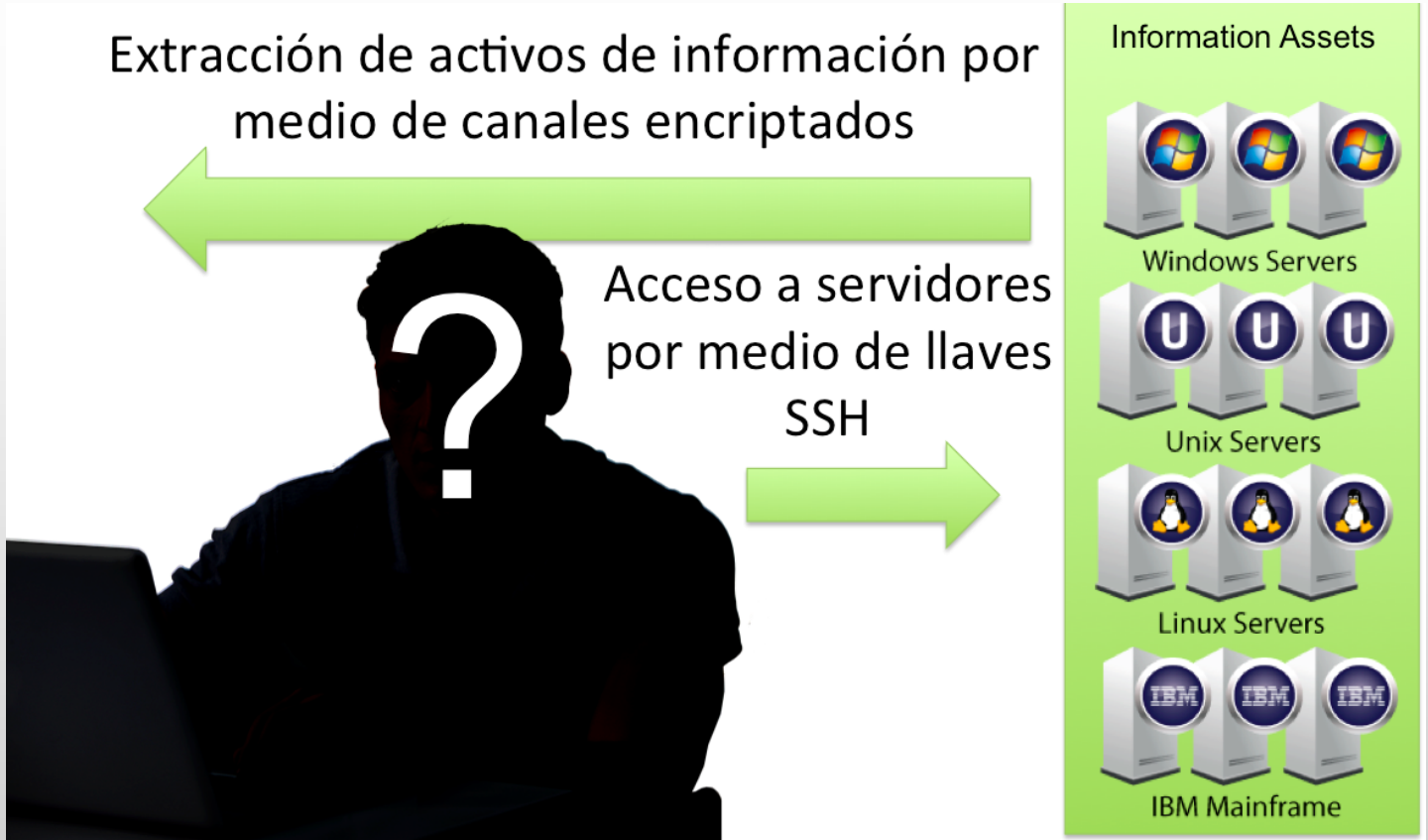
GESTIÓN GRCS, CONVERGENCIA & INNOVACIÓN
RADICAL
Alternativas de avanzada

3. El malware establece puntos adicionales de compromiso para garantizar que el ciberataque continúa si un punto es cerrado. Realiza movimientos laterales en busca de usuarios privilegiados



Anatomía de un APT

4. Obtienen información como usuarios, contraseñas, llaves, identifican y acceden a la información. Aprovechan las vulnerabilidades para hacer escalamientos de privilegios, inyectar código arbitrario, etc.



Anatomía de un APT

5. Exfiltración de la información, en este punto se considera una brecha

Avg. 229 Days
Compromise goes without notice

by Tom Spring

April 7, 2016 , 3:54 pm

The FBI issued a rare bulletin admitting that a group named Advanced Persistent Threat 6 (APT6) hacked into US government computer systems as far back as 2011 and for years stole sensitive data.

Protección ante Ataques Dirigidos y Amenazas Desconocidas

GESTIÓN GRCS, CONVERGENCIA & INNOVACIÓN
RADICAL
Alternativas de avanzada

¿Cómo puede protegerse si no son detectados?

Porqué un sistema de detección de brechas?

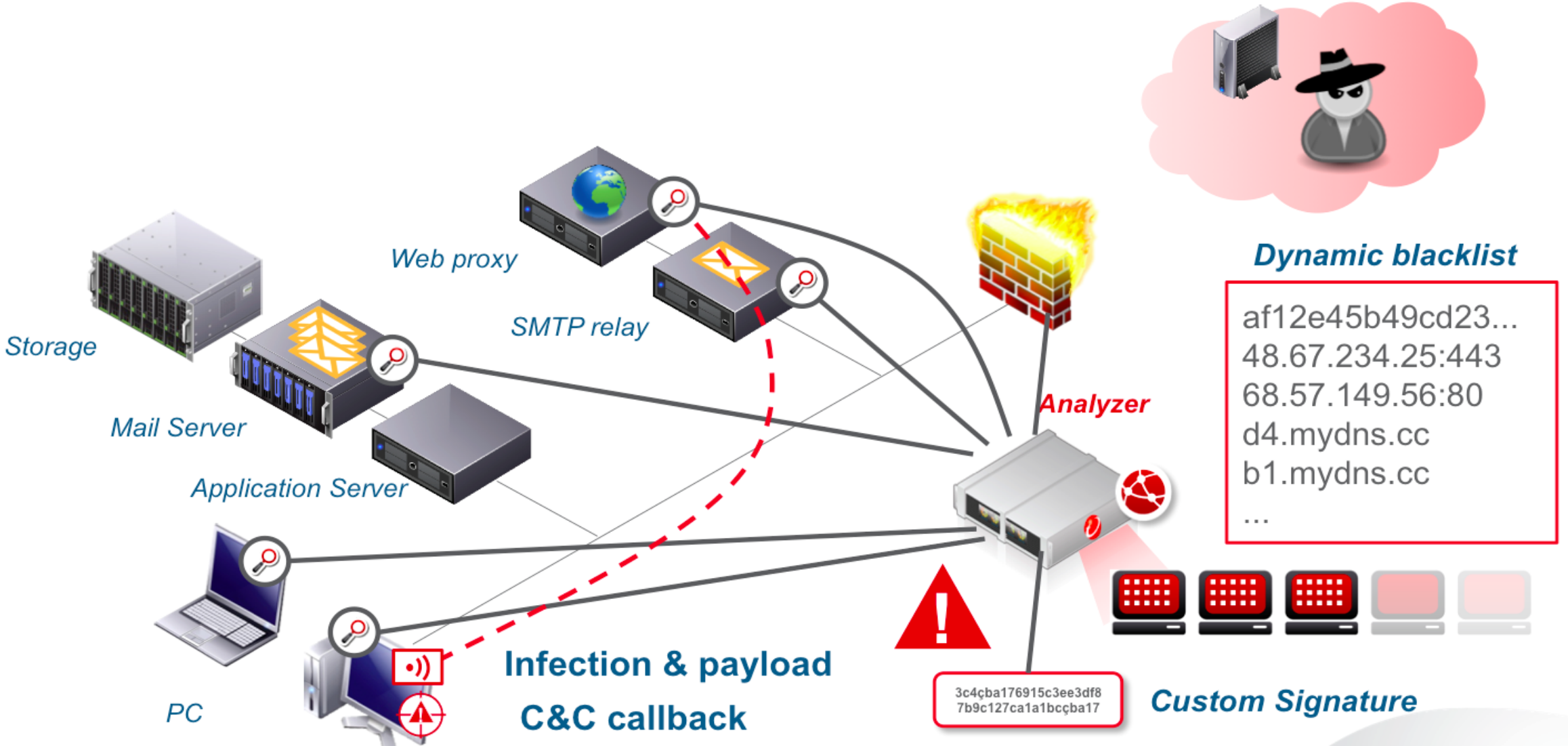
- Para descubrir si están en la mira o ya han sido comprometidos
- Para entender el nivel del impacto
- Para definir cuan sofisticado el ataque es
  - Oportunístico or Dirigido
  - Fue el ataque diseñado para evadir la detección ?

Obtenga visibilidad para resolverlo

- **Quién** está atacando la organización?
- Que **profundo** es el ataque?
- Que **información** han logrado sacar?
- **Cuánto tiempo** ha pasado el ataque?
- Soy **el único** que enfrenta éste ataque?
- Cómo lo **detengo** si sucede otra vez?

Qué debe soportar un BPS (BREACH PREVENTION SYSTEM)

GESTIÓN GRCS, CONVERGENCIA & INNOVACIÓN
RADICAL
Alternativas de avanzada



Pasos a seguir

RADICAL
Alternativas de avanzada

Muchas Gracias

Preguntas