FUTURE OF INFORMATION SECURITY

INICTEL-UNI

Lima, September 2014

Instituto Nacional de Investigación y Capacitación de Telecomunicaciones

INICTEL-UNI

Before 70s

70 ~ 80s

90 ~ 00s

After 2010

Future?

INTERNET INCIDENT:

- emerge of malicious code, emerge of mobile malicious code, web defacement, malicious code distribution websites, zombie PC, DDoS Attack, Phishing Website, illegal spam.

KISA presentation

Internet Incident in per day
– Detected by and reports from KISA

- Emerge of Malicious Code: 1,435
  (Collected by KISA : 523,624)

- Zombie PC : 8,821
  (Average Flow in KISA sinkhole)
  (per day)

- Emerge of Mobile Malicious Code: 101
  (McAfee : 36,699)

- DDoS Attack : 1.5
  * Report from KISA : 91
  * Detected by KISA IX line : 318
  * KISA Cyber Shelter : 138

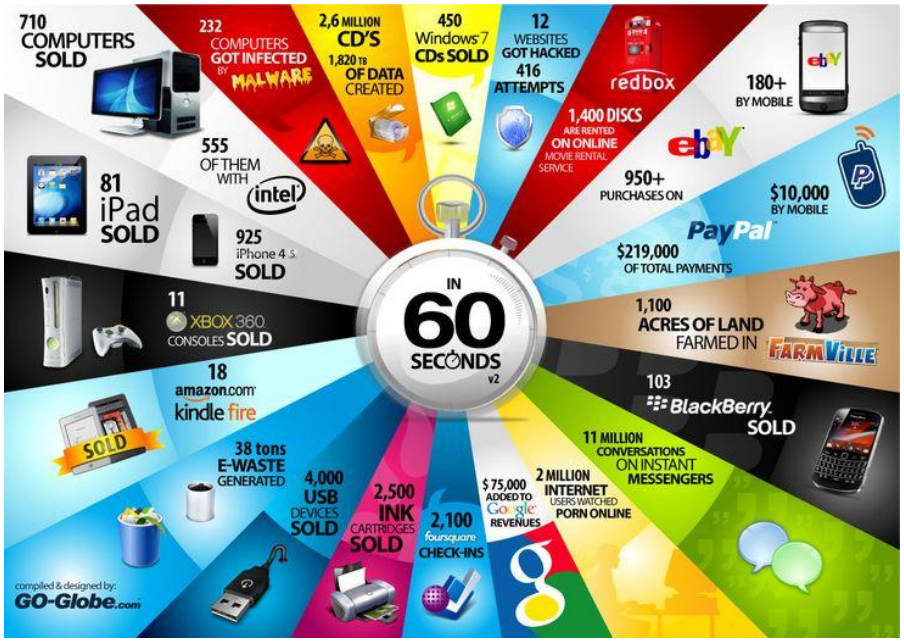
- Web Defacement : 8.7
  (Detected by KISA : 3,157)

- Phishing Website : 19
  (Responded by KISA : 6,944)

- Malicious Code Distribution Websites : 35.7
  (Detected & treated by KISA : 13,018)

- illegal Spam : 89,628
  (Responded by KISA : 32,714,062)

- What happens in Internet in 60 seconds?

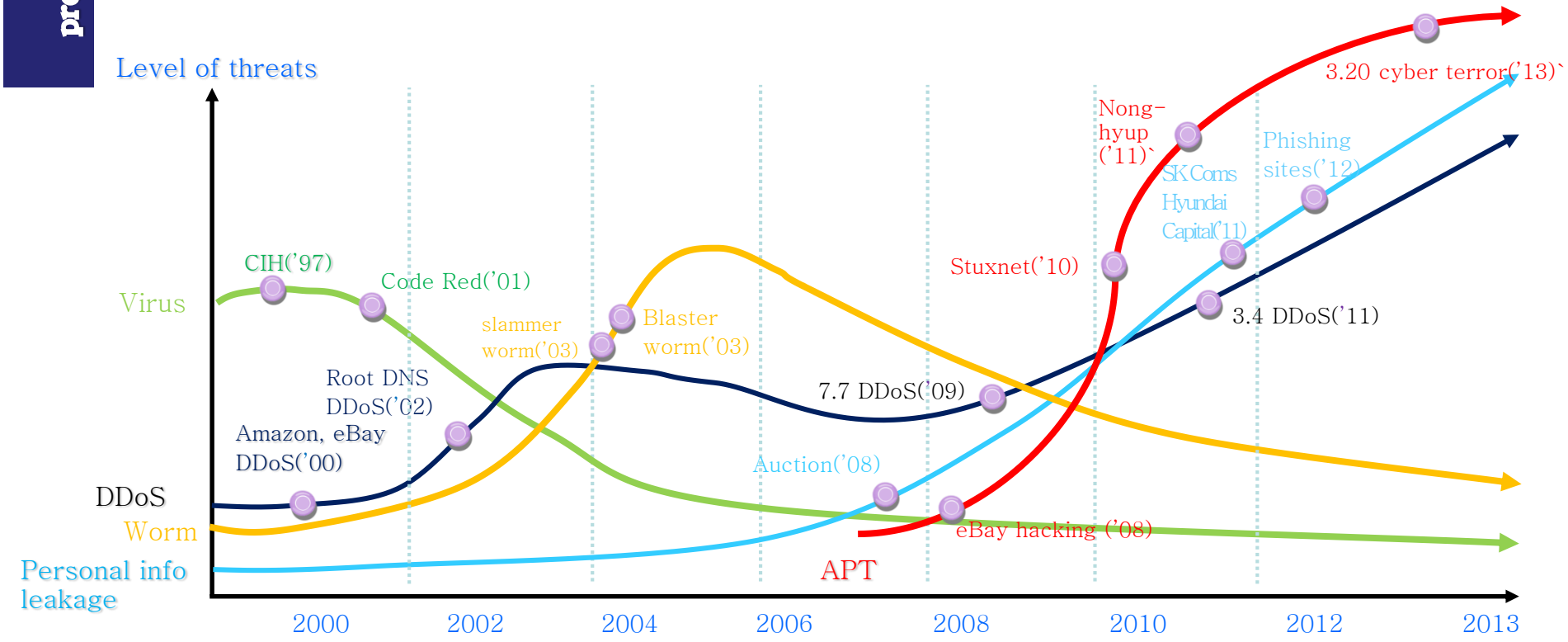


Instituto Nacional de Investigación y Capacitación de Telecomunicaciones

TENDENCIA DE LOS CIBERATAQUES

KISA presentation

- Purpose : self display ➡ money extortion ➡ cyber terror(social chaos)
- Technique : manual ➡ hide, automatic ➡ systematic, intelligent
- Target : individual system ➡ large scale, network ➡ social infra, nation



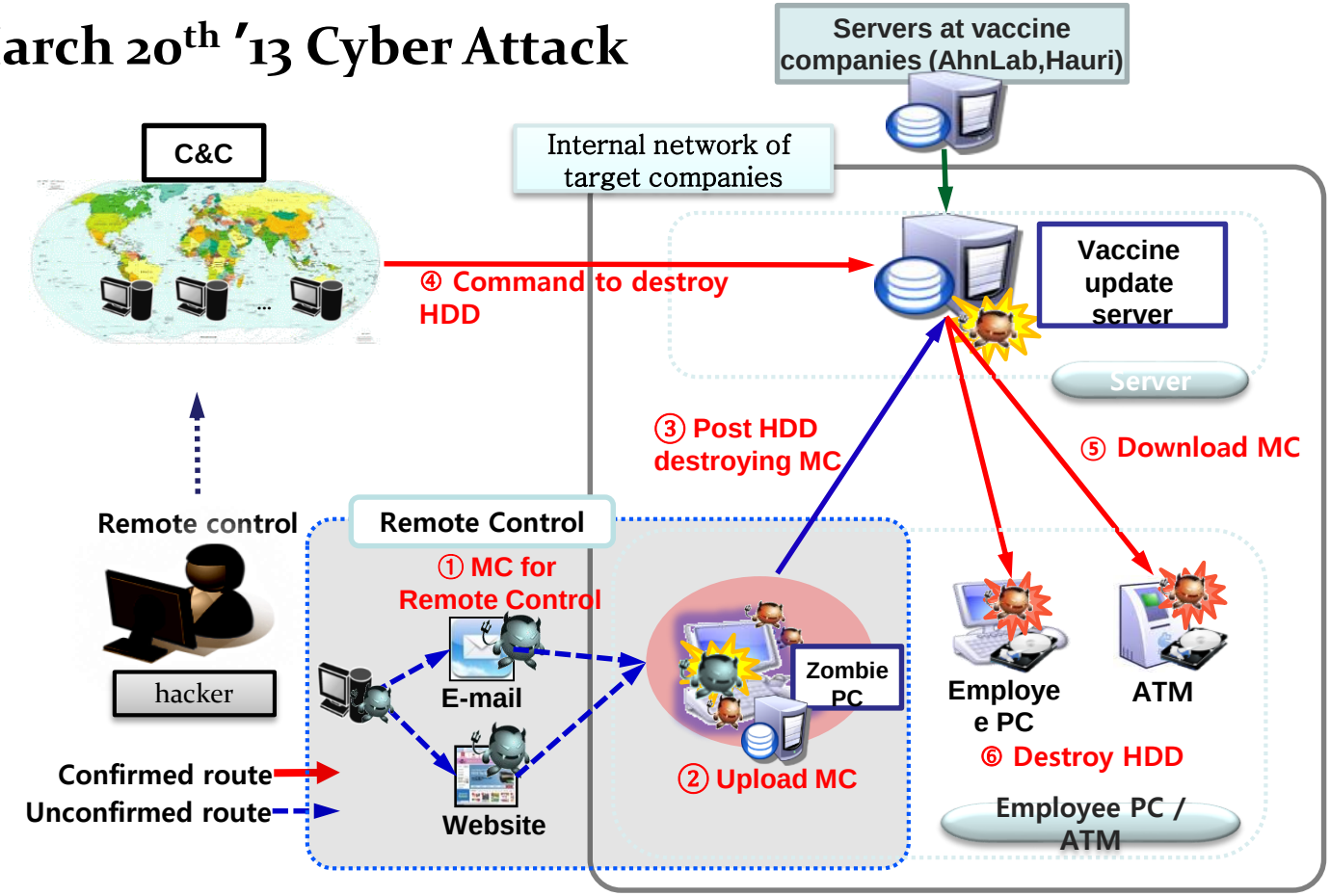
KISA presentation

Overview of 3. 20 Cyber Terror

- **Destroyed 48,700 PC, servers and ATMs of 6 broadcasting, Financial institutes were damaged by cyber (March 20th)**
  - Using "www.nalsee.com" website as distribution point to infect users PC (about 800 PCs) (March 25th)
  - destroyed 58 Digital YTN website server's hard disk(main website service unavailable)(March 26th)
  - Wiped out the data of 14 North Korea(related) · conservative group's webpage (March 26th)
- **Number of 6 broadcasting · Financial institutes 'damaged systems were completely recovered (March 29)**
  - Digital YTN's 58 webservers are recovered(100%) (April 12)

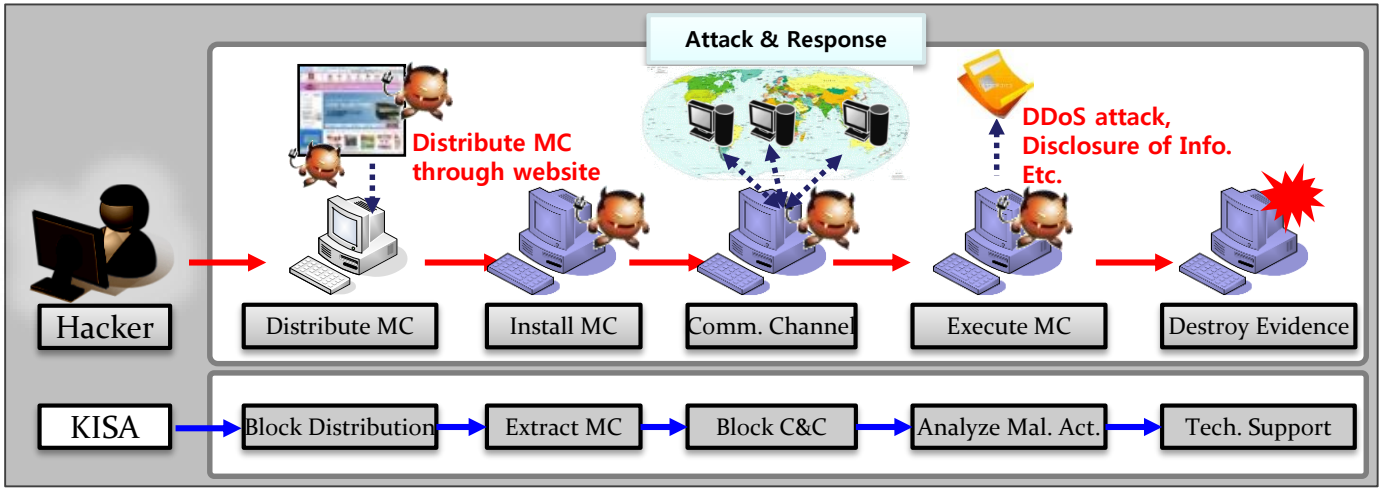
KISA presentation

March 20th '13 Cyber Attack



Responses to the Incident

KISA presentation



- Visit KBS, MBC, YTN, Nonghyup, Shinhan bank 25 times
- Distract MC and confirm attack route
  - Develop and distribute dedicated vaccine to detect 76 MCs

    ※ March 21, 0100 started to distribute and 360,000 download (April 16)
- Analyze vulnerability and issue security advisory

  ※ Security Measures : Delete MC, Revise Firewall security policy, etc.

What about ?

- ✓ The cloud, Bring your own device, Internet of Things
- ✓ What happens with our lifestyle
- ✓ What about our right to privacy
- ✓ Body area network and wearables
- ✓ Borders in cyberspace
- ✓ Democracy and Citizen ¿cyber security?
- ✓ Cybersecurity in Smartcities
- ✓ Law and Regulation of cyberspace
- ✓ cyber espionaje, cybercrime, cyberactivism, cyberterrorism

RETOS

Proteger el ciberentorno : Ciberseguridad

Lograr el uso seguro de las tecnologías de la información y la comunicación

- ✓ Para ello se requiere primero el Fortalecimiento de Capacidades:
  - ❖ Prevención
  - ❖ Defensa
  - ❖ Detección
  - ❖ Análisis
  - ❖ Investigación
  - ❖ Recuperación
  - ❖ Respuesta a los ciberataques

Physical Security

Technical Security

Managerial Security

- ✓ Colaboración nacional, regional, internacional

RETOS

1. Efectividad de la Política y Estrategia Nacional/Regional de Ciberseguridad
2. Establecer un esquema u organización específica para la ciberseguridad
3. Desarrollo Ciberseguro de la Sociedad de la Información
4. Mejorar las capacidades en aspectos de ciberseguridad a nivel gerencial, técnico y de los ciudadanos en general, así cómo a nivel del Estado.
5. Modernización, certificación, auditoría y mejora continua de la seguridad de la infraestructura crítica para la seguridad y defensa nacional (Gobierno, agua, alimentación, energía, espacio, instalaciones de investigación, salud, sistema financiero y tributario, transporte, TIC, industria química)
6. Modernización, certificación, auditoría y mejora continua de la seguridad de la infraestructura de tecnologías de la información y comunicación de las Entidades Públicas y Privadas.
7. Mejora de la regulación, normas legales, normativa específica y estándares para la ciberseguridad

RETOS del INICTEL-UNI

1. Promover la ciberseguridad y alcanzar un rol protagónico en el país y en la Región
2. Conocer las ciber amenazas, gestionar los riesgos y articular una adecuada capacidad de prevención, defensa, análisis, investigación, recuperación y respuesta ante incidentes.
3. Promover que las Entidades Públicas posean un adecuado nivel de seguridad
4. Promover la cultura de la ciberseguridad en el sector privado y los operadores
5. Promover la creación de normativa y asegurar su cumplimiento
6. Promover que las autoridades brinden una respuesta adecuada contra el cibercrimen
7. Crear conciencia en los ciudadanos acerca de los riesgos seguridad para que se involucren y fomente el uso seguro de las TIC
8. Realizar capacitación necesaria para un adecuado índice de ciberseguridad
9. Promover la implementación y mejora de la infraestructura de seguridad, incluyendo sus procesos
10. Sensibilizar a las autoridades para la mejora de la organización (esquema) de la ciberseguridad nacional

PROYECTO
CENTRO DE EXCELENCIA DE CIBERSEGURIDAD

Ser un nodo especializado de excelencia en ciberseguridad a nivel regional, generador de sinergia entre el Estado, la comunidad, el sector productivo nacional e internacional.

PROYECTO
CENTRO DE EXCELENCIA DE CIBERSEGURIDAD

ENTRENAMIENTO ALTAMENTE ESPECIALIZADO
DIPLOMADOS, CURSOS INTERNACIONALES, CONFERENCIAS, COMUNIDADES DE EXPERTOS…

CREACIÓN DE MASA CRÍTICA A NIVEL NACIONAL Y REGIONAL

INVESTIGACIÓN Y DESARROLLO: GOBIERNO, GESTIÓN Y TECNOLOGÍA

UNIVERSIDAD NACIONAL DE INGENIERIA

Instituto Nacional de Investigación y Capacitación de Telecomunicaciones

INICTEL-UNI

PROYECTO

EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA

Contar con el grupo de expertos de mayor reconocimiento para desarrollar medidas preventivas y respuestas coordinadas ante incidentes de seguridad en el ciberespacio nacional.

Divulgar de las mejores prácticas para la ciberseguridad.
Colaborar activamente en la ciberseguridad global.

THANK YOU FOR YOUR ATTENTION

WE EXPECT TO RECEIVE YOU SOON IN OUR CENTRE OF EXCELLENCE OF CYBER SECURITY