International Telecommunication Union

Taller Regional sobre Ciberseguridad y Protección de la Infraestructura Crítica

Sesión 4: Supervisión, alerta y respuesta en caso de incidente.

Lic. Gastón Franco

ArCERT

Oficina Nacional de Tecnologías de Información

Subsecretaría de la Gestión Pública

ArCERT - Principales características

CREADO **Julio de 1999**

MARCO LEGAL **Resolución N° 81/1999**

Aprueba creación y establece funciones

Disposición N° 01/1999

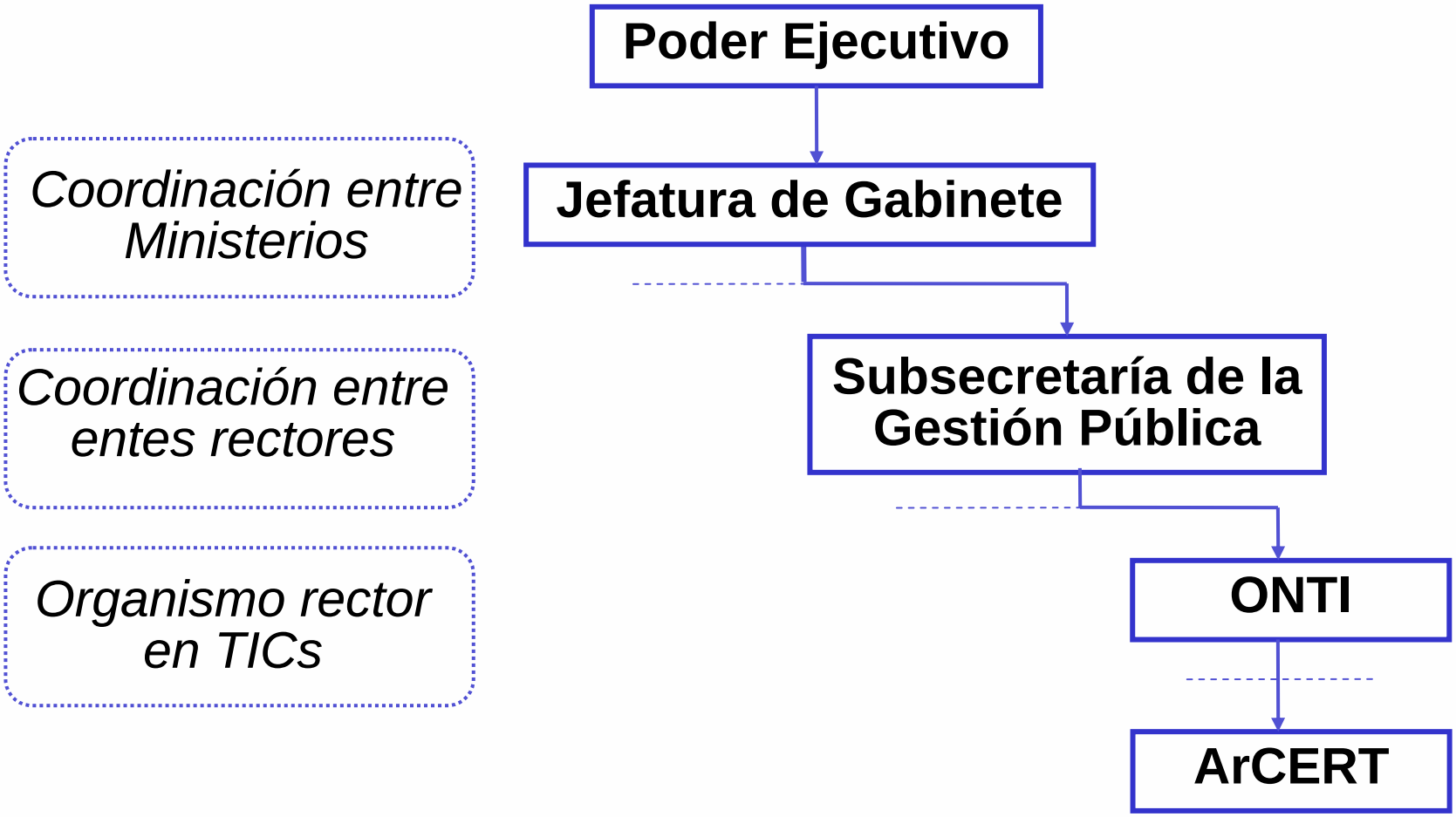
Aprueba Reglamento de Operación

Decreto N° 1028/2003

Acciones de la ONTI en materia de seguridad informática

MEMBRESIA **Miembro del FIRST desde abril de 2004**

Ubicación en la estructura del Gobierno



Principales características

Posicionamiento

Primer y único CSIRT de Argentina

Designado ante el CICTE como punto de Contacto Nacional

Promotor de creación de otros CSIRT en nuestro país y en la región

Intercambio de información con CSIRTs y otros grupos de seguridad

Participación en Iniciativas Internacionales
(ITU, Cert/cc - National CSIRTs meeting)

Principales Objetivos

OBJETIVO PRINCIPAL

Incrementar los niveles de Seguridad Informática del Sector Público

OBJETIVOS ESPECIFICOS

Atención de Incidentes de Seguridad

Actividades Preventivas

- Capacitación
- Difusión de Alertas e Información
- Servicios y Productos
- Políticas de Seguridad de la Información

Representación en Foros Internacionales

- Miembro del FIRST desde abril de 2004
- Punto de Contacto para OEA
- Participación en iniciativas Internacionales

Reporte de Incidentes

Se reciben reportes que:

- Afecten al Sector Público o Bancario Argentino
- Estén originados desde nuestro país (no estén vinculados con SPAM)

Fuentes:

- Organismos de Gobierno
- Sector Bancario
- ISPs
- Ciudadanos
- Equipos CSIRTs y organizaciones afectadas a nivel mundial
- Fuentes de Información públicas y privadas
- Recolección y análisis de Malware
- Herramientas de Detección

Algunos casos tratados

- Sustitución de Páginas Web (Defacement)
- Phishing (engaños)
- Código malicioso (Virus, gusanos, troyanos, etc)
- Botnets y Ataques de DDoS
- Intrusiones de mayor complejidad

Casos de Phishing

Incremento considerable en los últimos meses

Casos que afectaban a clientes de Bancos de Argentina

Acciones:

- Se recibieron reportes del incidente.
- Se contactó a los Bancos afectados.
- Se informó a los responsables de los proveedores de Internet que hosteaban los sitios con contenido malicioso.
- Se notificó al CERT Nacional de competencia.

Casos de Phishing

Algunos datos interesantes:

El sitio malicioso estaba alojado en un servidor que físicamente estaba en un país del sudeste asíatico (GMT+8).

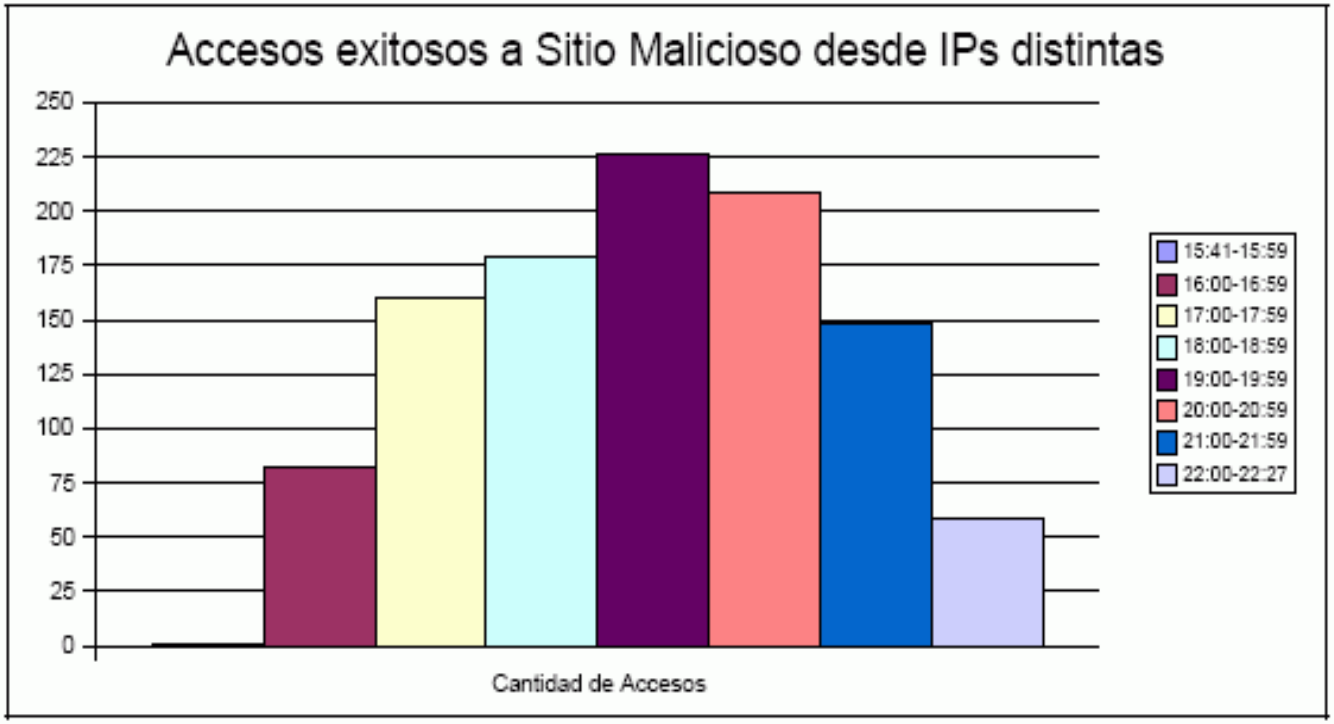
La información que los usuarios enviaban era almacenada en otro servidor, que se encontraba en un país de Europa (GMT+2).

15:41	Primer acceso al sitio malicioso desde un IP en Atlanta, USA
16:32	ArCERT recibe el primer reporte
16:58	Se contacta al Banco. Se envían pedidos de baja al ISP y al CERT Nacional
22:27	El sitio es dado de baja

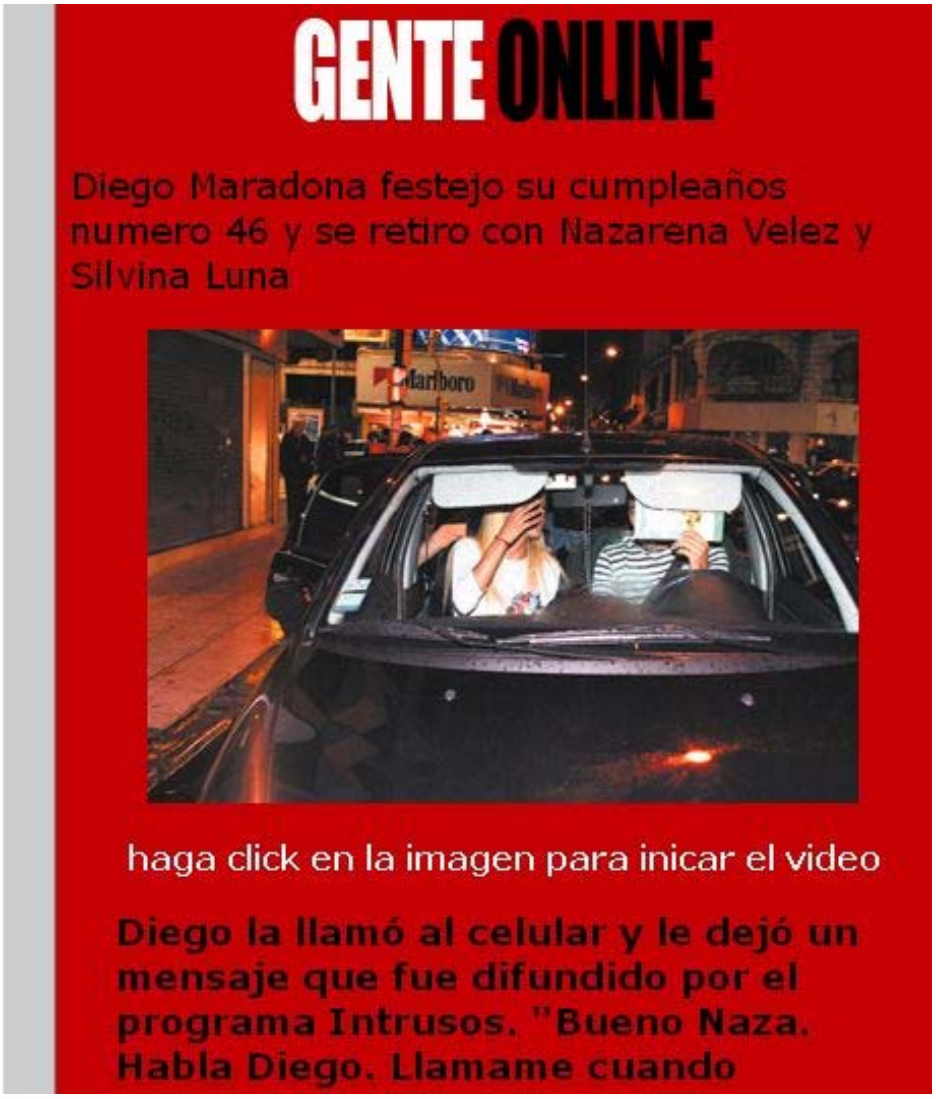
Casos de Phishing

Accesos al sitio malicioso:

- Tiempo de vida: 6 horas, 46 minutos
- Más de 1000 IPs distintas



Código Malicioso distribuido por Mail



Código Malicioso distribuido por Mail

Caso de potencial servidor DNS vulnerable

- **13/4/07 se hace pública una vulnerabilidad que podría producir DoS contra la interfaz de administración remota del servicio de DNS de MS Windows 2000 y 2003.**

- **18/4/07 se recibe un reporte que informa de 111000 potenciales servidores públicos vulnerables.**

En Argentina:

- **700 servidores potencialmente afectados**
- **32 entidades involucradas (ISPs y otras organizaciones)**
- **se les notificó el potencial impacto indicando posibles soluciones.**
- **La actividad se realizó el mismo dia de recibido el reporte.**

Ataque DDoS utilizando DNS recursivos

Reporte de ataque DDoS contra un ISP de EEUU

- Tráfico DNS superior 1Gbps
- Utilizaba 175.000 DNS distribuidos que permitían consultas recursivas

En Argentina:

- 2600 servidores estaban afectados
- 62 entidades involucradas (ISPs y otras organizaciones)
- Se les notificó el incidente indicando posibles soluciones al problema
- Duración aproximada: 5 horas

Algunos productos de monitoreo y alerta

- DNSar – Análisis de Servidores y Dominios DNS
- CAL - Sistema de Sensores (en desarrollo)
- RAM – Recolección y Análisis de Malware (en desarrollo)

DNSar

¿QUE ES? **Sistema de análisis de servidores y dominios DNS**

OBJETIVO **Detectar y alertar sobre falencias en los servidores DNS de los Organismos**

Mantener una base de datos histórica con dicha información

Generar información estadística

DNSar


Reporte DNSAR - dominio
DNSar
Sistema de Control de Configuración para Servicios DNS
Reporte del dominio: .gov.ar
Reporte generado con los datos obtenidos el día: 16 - 09 - 2006.
::Información general del dominio
Entidad Registrante
Email Responsable
.gov.ar
Contacto Técnico
Email Contacto Técnico
.gov.ar
::Información de los servidores de nombres definidos en la zona padre
FQDN
IP
Estado
¿Acepta consultas recursivas?
ns3. .gov.ar
200.
No responde
No
server2. .gov.ar
200.
No responde
No
ns1 .gov.ar
200.
OK
Si
ns2 .gov.ar
200.
OK
Si

ALGUNOS DATOS

2282 dominios - 1203 servidores

- ✓**39%** servidores **aceptan consultas recursivas**
- ✓**37%** dominios con algún servidor que permite **transferencia de zona**
- ✓**48%** tienen **sólo 1 registro mx**
- ✓**41%** dominios tienen, al menos, un **NS que no responde**
- ✓**5,6%** dominios con, al menos, un ***lame delegation***
- ✓**2,6%** utilizan **cnames en MX o NS** (RFC 2181)
- ✓**0,5%** incluyen **direcciones IP privadas** (RFC 1918)

RAM

- **Arquitectura de honeypots de baja interacción para captura de malware (especialmente gusanos).**
- **Implementación de nepenthes y surfnetIDS, con mejoras y adaptaciones a nuestras necesidades.**
- **Las capturas se envían a diversos fabricantes antivirus, y a grupos de análisis y seguimiento de botnets.**
- **Se monitorea la evolución en la detección por parte de diversos motores de antivirus.**

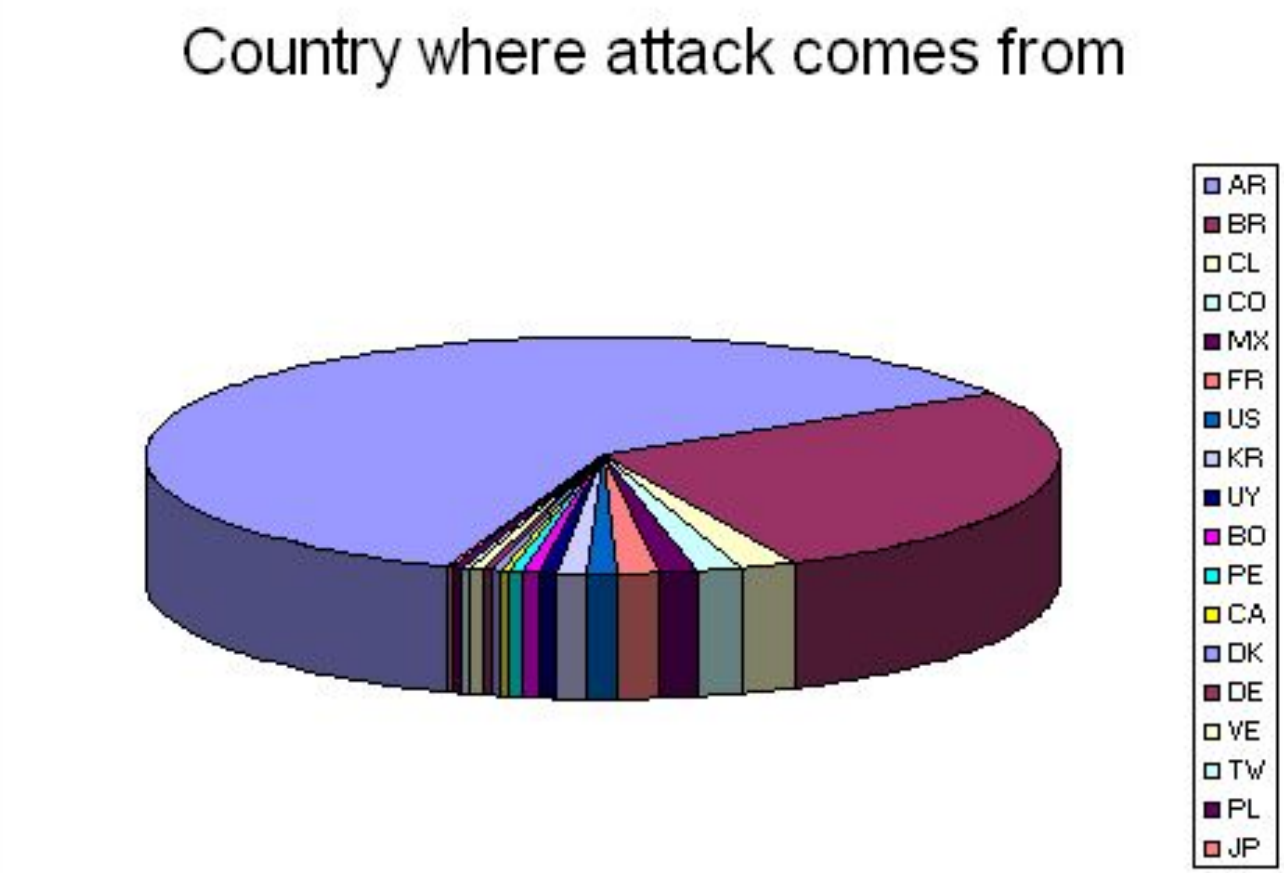
RAM

- **Se obtienen reportes automatizados acerca de algunas de las características de comportamiento de los programas maliciosos.**

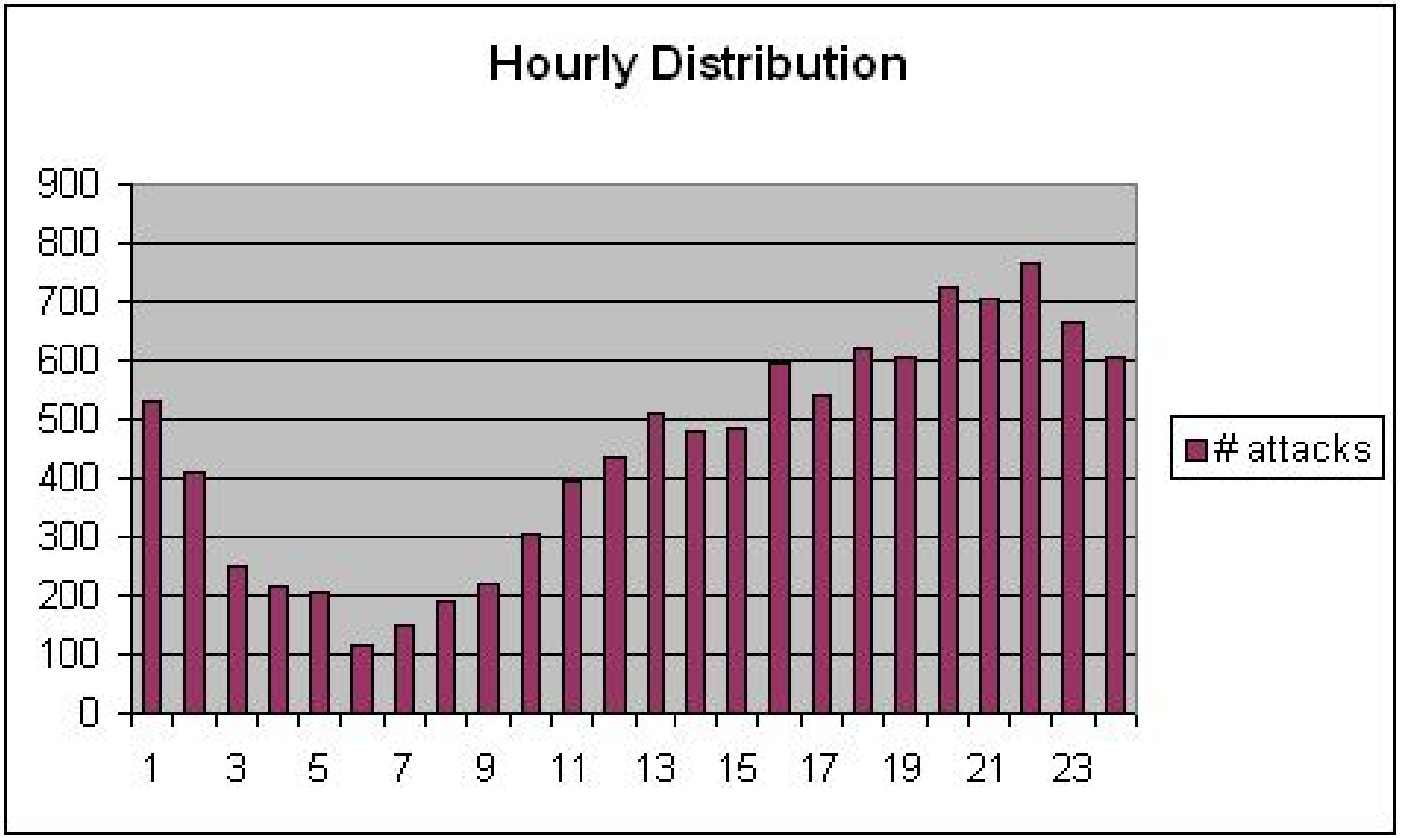
- **Promedio de 10 malwares nuevos capturados por día.**

- **Detección promedio (Virustotal): 69% de los motores detectan el programa como malicioso.**

RAM - Origen de los ataques



RAM – Distribución horaria



International Telecommunication Union

¡Muchas Gracias!

Preguntas y Comentarios

www.arcert.gov.ar

info@arcert.gov.ar