ASSESMENT TÉCNICO “CSIRT BANCARIO”

Ing. Marco Rivadeneira, MSC.

GERENTE TÉCNICO

GRENETICS SOLUCIONES S.A

Fijo: +593 2 6034068 Cel: +593 992 795600

TEMA:

Combatiendo un **FRAUDE BANCARIO** en Latinoamérica desde un **Centro de Respuesta a Incidentes de Seguridad Informática** para el sector financiero.

Objetivo

Mostrar en un **escenario real controlado**, la forma de operar de los ciberdelicuentes que atacan a bancos de la región y cómo reacciona un Centro de Respuesta a Incidentes de Seguridad Informática frente a estas incidencias.

Escenario:

Se realizaron varias transferencias bancarias internacionales **NO AUTORIZADAS** por un valor total de **10´000.000$** desde la cuenta del **GREENBANK** ubicado en **PECUATOR** que mantiene en el **GLOBALBANK** ubicado en **U.S.B.**

La transferencia se realiza hacia la cuenta de **JOHN SMITH** del **CAIMANBAN** ubicado en **ISLAS LAGARTOS.**

Escenario:

La transferencia es solicitada aparentemente por la empresa **BARIOS S.A** de **PECUATOR** hacia la cuenta de **John Smith** de **ISLAS LAGARTOS.** Pero la empresa **BARIOS S.A** no mantiene ninguna cuenta dentro del **GREENBANK.**

En el **CAIMANBANK** inmediatamente se realizaron transacciones secundarias (500,000$,1´000.00$, 2´000.000$) a cuentas de otros bancos y de mismo **CAIMANBANK.**

GREENBANK

SITUACIÓN ACTUAL

GREENBANK

- El GREENBANK hace dos meses **incorporó** a su institución a un CSIRT financiero (G-CSIRT).
- No poseen mecanismos de monitoreo de trafico en tiempo real ni correlación de logs.
- No existe control ni manejo seguro de dispositivos móviles.

GREENBANK

- El **G-SCIRT** recientemente incorporado se encontraba realizando un inventario de los sistemas de seguridad del banco y ya implementó algunos sistema de monitoreo automáticos.
- Los aplicativos bancarios pueden ser accedidos desde la red externa (user + pass + code1 + code2).
- Instalación de equipos y aplicativos por defecto.
- Manejo de contraseñas débiles

Usted es un OFICIAL DE SEGURIDAD del G-CSIRT

¿Qué ACCIONES debemos tomar?
¿Qué información necesitamos investigar?
¿Cómo sucedió el ataque?
¿Quiénes son los responsables?
¿Dirección IP desde la cual se dio el ataque?

¿Qué ACCIONES debemos tomar?

Acciones automáticas:

- El **G-CSIRT** generó un reporte de incidente automático (Sábado 29/4/2017 - 03:00am) por un acceso remoto al aplicativo **SWIFT** perteneciente al **GREENBANK.**

- El reporte de incidente automático fue notificado (correo) inmediatamente al **GERENTE TÉCNICO** del **GREENBANK**. Posteriormente el día martes 2 de Mayo del 2017 a las 8:00 designo al **Técnico 1** del departamento de TI la revisión del dispositivo.

Acciones automáticas:

- 2 minutos después del primer incidente el **G-CSIRT** generó dos reportes de incidentes automáticos (llamada + correo) (Sábado 29/4/2017: 03:02am) por transacciones internacionales mayores a 1´000.000$ y se envió el reporte al **GERENTE DE OPERACIONES**. Estos reportes tienen la prioridad de CRÍTICA.

Acciones personal del banco:

- El **GERENTE DE OPERACIONES** del **GREENBANK** dedujo que se trata de una transacción no autorizada (por el horario de trabajo) y se contacto inmediatamente con el **GERENTE DE OPERACIONES** del **GLOBALBANK** para intentar detener la transacción. (tiempo de espera 10 minutos)

Información extra:

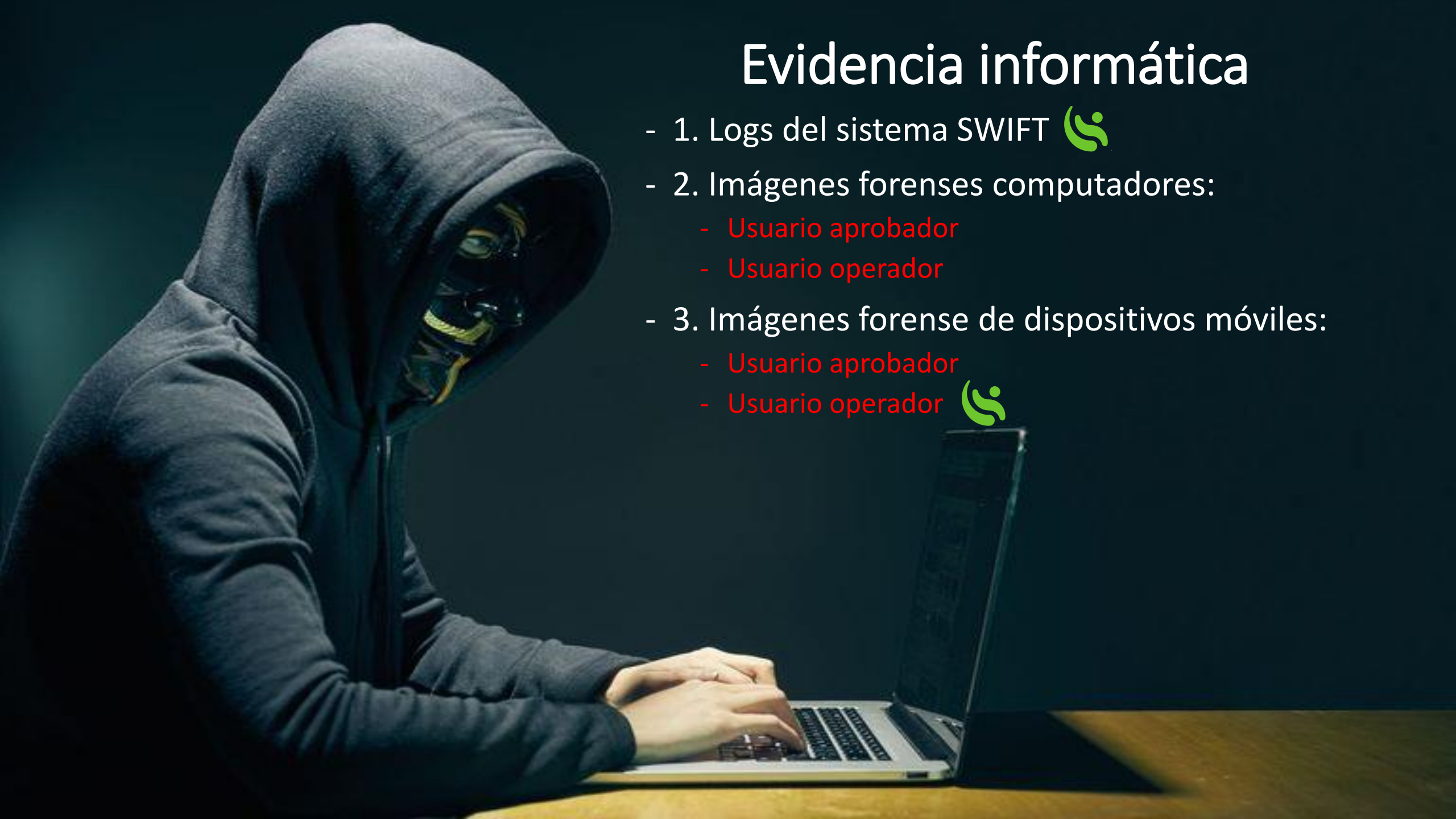
- El **GLOBALBANK** realizó una trasferencia de 5´000.000$ a la cuenta de **JOHN SMITH** del **CAIMANBAN** ubicado en **ISLAS LAGARTOS** y otra de 5´000.000$ estaba en proceso de aprobación.
- Gracias al rápido accionar de los implicados se logró detener una de las transferencias.

¿Qué ACCIONES debemos tomar?

- El **G-CSIRT** de manera conjunta con la comisión de crisis bancaria y previa aprobación de la gerencia general ordenó la puesta en **OFFLINE** inmediata del servicio **SWIFT** como medida preventiva. Sábado 29/4/2017: 03:10am para lo cual se accedió remotamente y se realizó esta actividad.

- El directorio del banco autorizó el inicio de las investigaciones informáticas y forenses que serían llevadas a cargo del **G-CSIRT**.

¿Qué información necesitamos investigar?



Evidencia informática

- 1. Logs del sistema SWIFT
- 2. Imágenes forenses computadores:
  - Usuario aprobador
  - Usuario operador
- 3. Imágenes forense de dispositivos móviles:
  - Usuario aprobador
  - Usuario operador

¿Qué información necesitamos investigar?

http://green-bank.ddns.net/banco/index.html

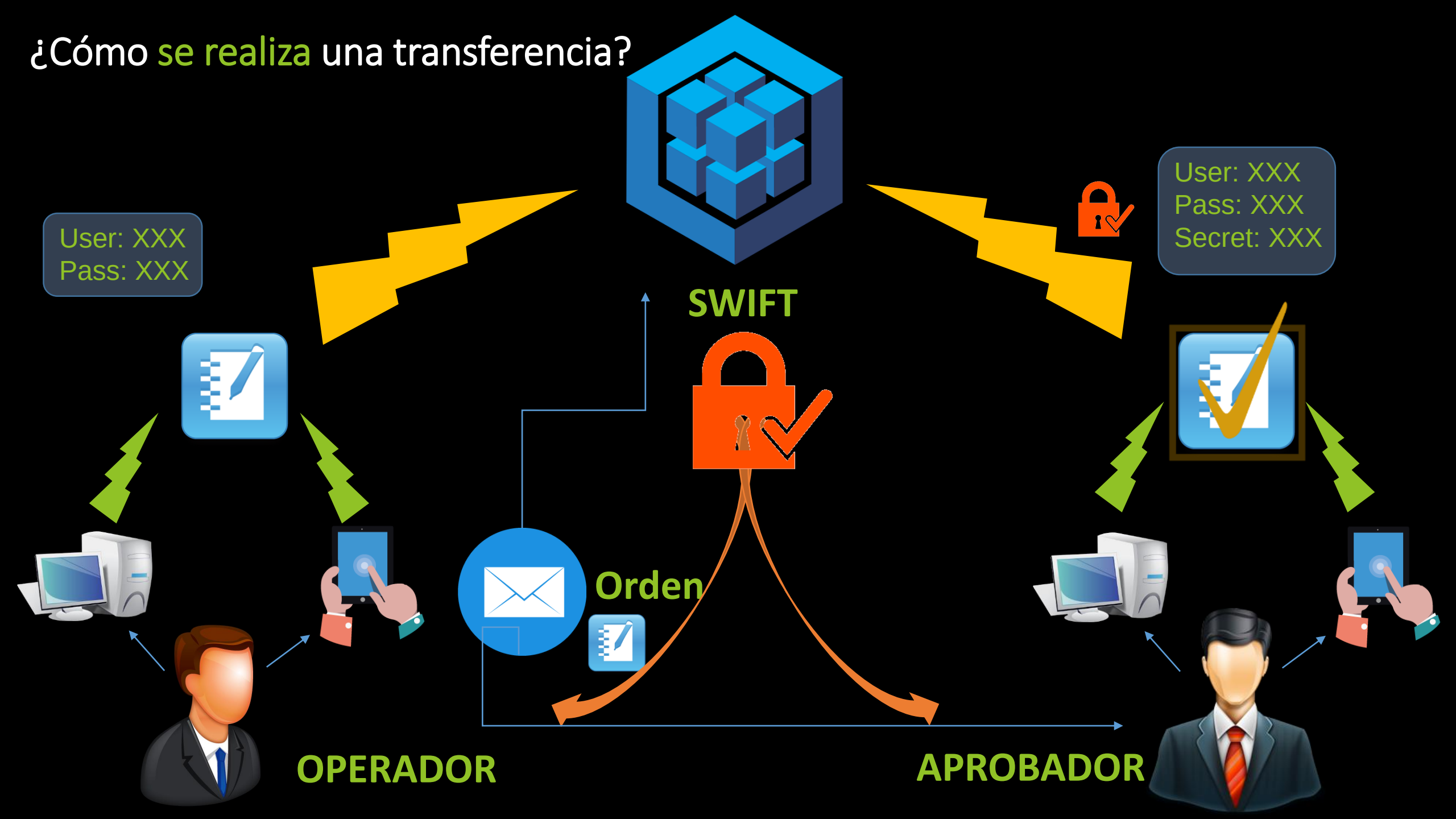
¿Cómo funciona el acceso remoto del sistema SWIFT?

Hogar

SWIFT

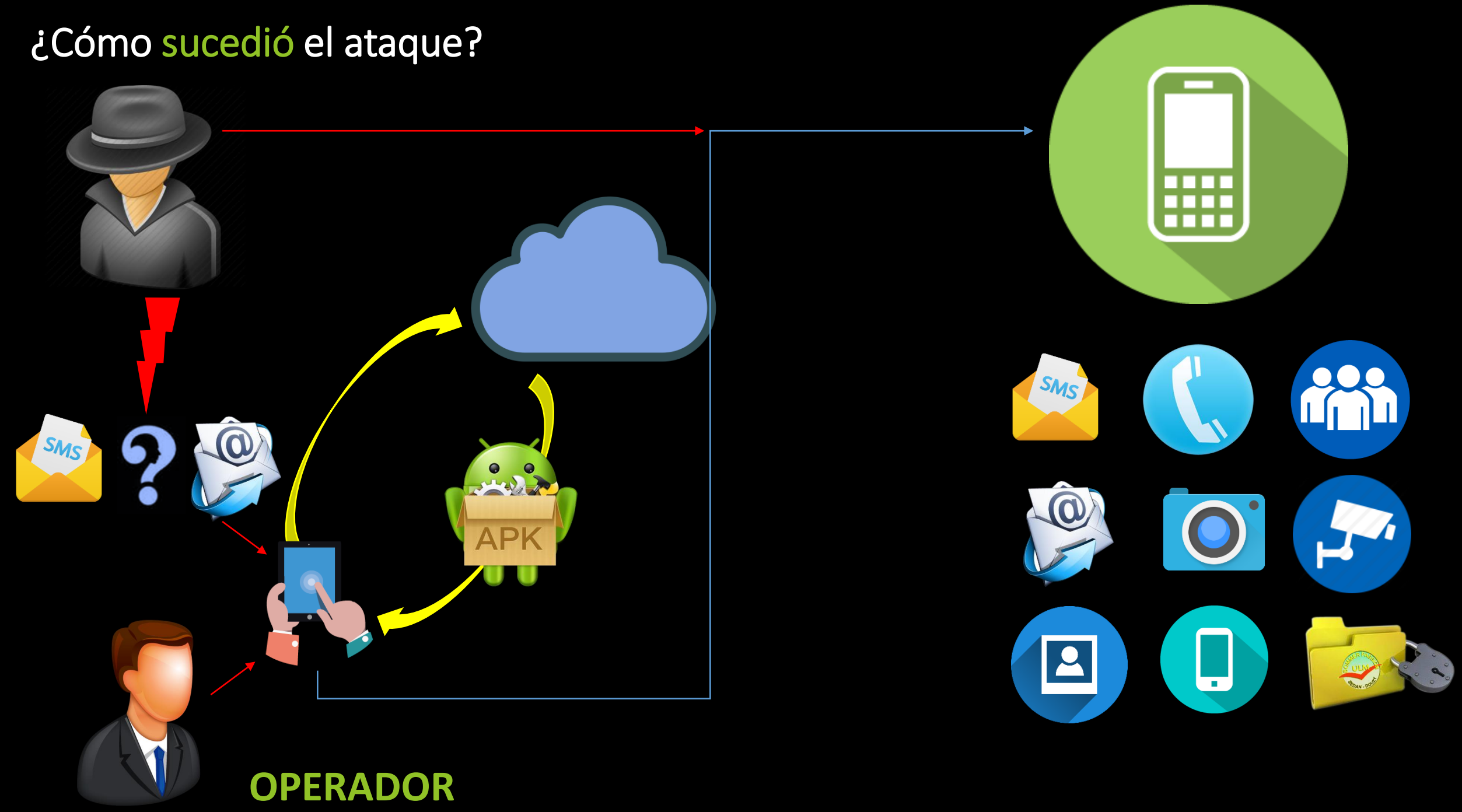
OPERADOR

¿Cómo se realiza una transferencia?

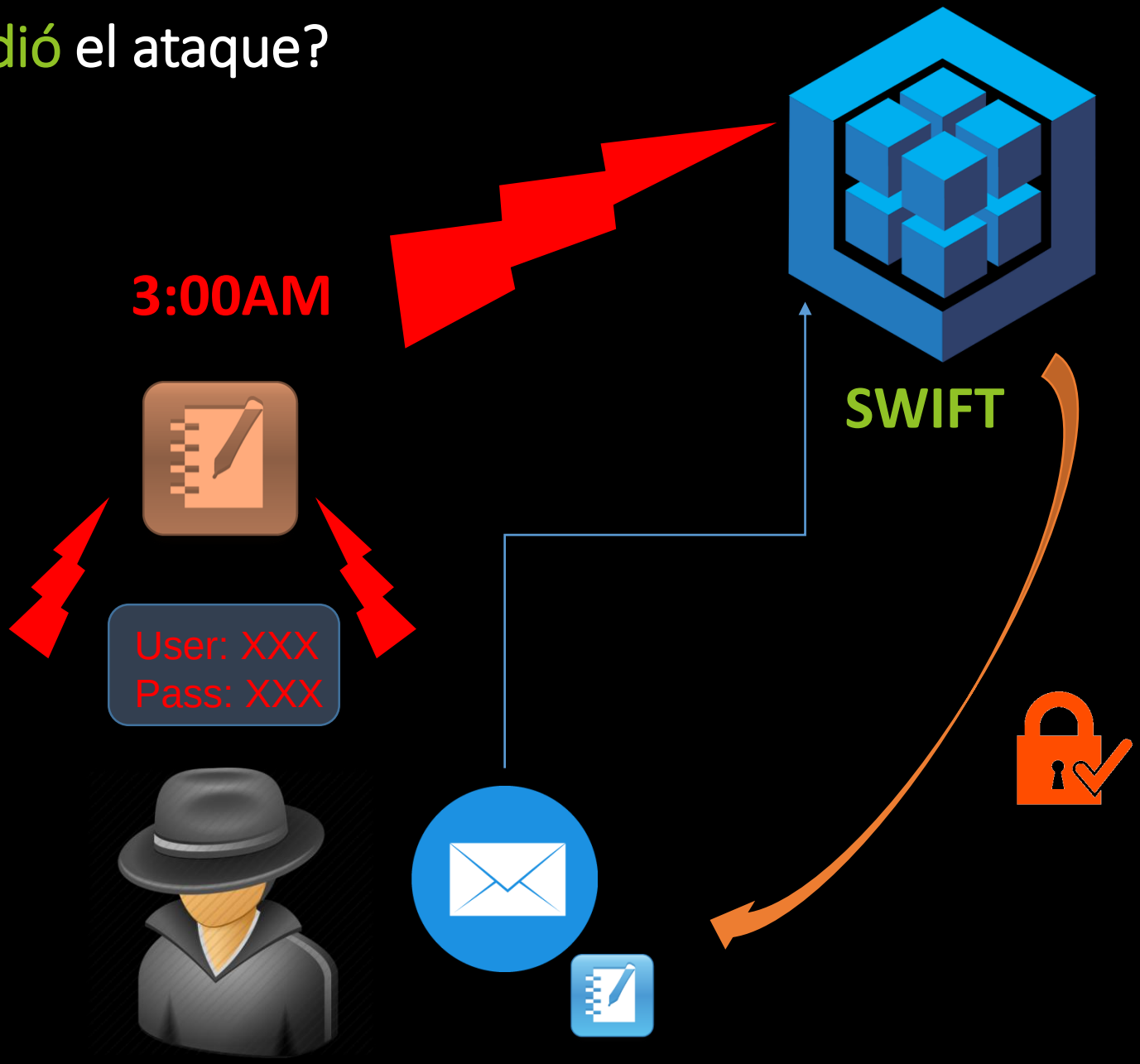


¿Cómo sucedió el ataque?

¿Cómo sucedió el ataque?



¿Cómo sucedió el ataque?

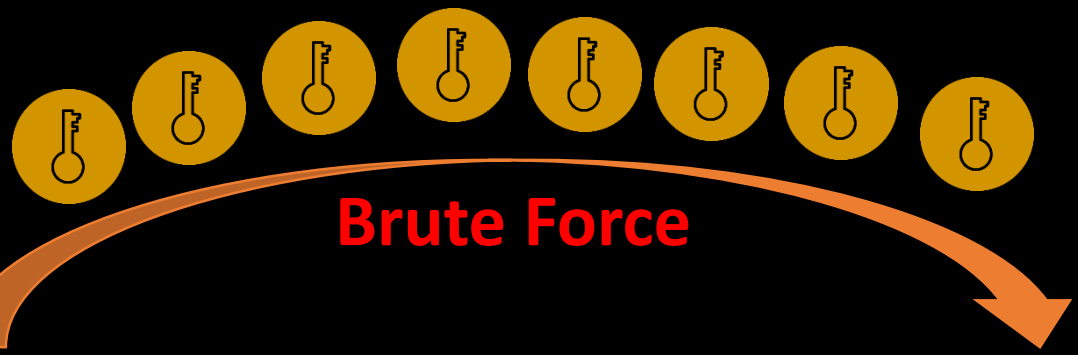


¿Cómo sucedió el ataque?

SWIFT

GLOBALBANK

User: XXX
Pass: YYY
Secret: XXX



Brute Force

APROBADOR

APROBADOR

¿Quiénes son los responsables?

CIBERDELINCUENTE

OPERADOR

APROBADOR

¿Dirección IP desde la cual se dio el ataque?

CIBERDELINCUENTE

Dirección IP: 117.34.70.143
País: China
Empresa: Shangay Shop LDTA.
Representante: Wan Yoing Se
Dirección: Shangay 7640, Av. Terika 67-7 y Tsu Tsu
Mail: wan.yoing@shangayshop.com
Phone: + 86 65 523647

Recomendaciones CSIRT

- Presentar una denuncia por el delito de **APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS**, tipificado en articulo 2 de la Ley Cibernética de **PECUATOR.**
- Emitir **informe forense** sobre la investigación realizada, validar el informe fiscalmente.

greenetics

Recomendaciones CSIRT

El **G-CSIRT** dispuso e implementó nuevas medidas de seguridad y el refuerzo extremo de las seguridades existentes sobre:

- **SWIFT**
- Equipos de **Protección Perimetral**
- Equipos de **Red**
- Usuarios **Aprobador y Operador**
- Dispositivos **Móviles**
- **Computadores**

Recomendaciones CSIRT

Investigación:

G-CSIRT

FIRST
Improving Security Together

CNCERT/CC
国家互联网应急中心

Gracias!

Ing. Marco Rivadeneira, MSC.
GERENTE TÉCNICO
GRENETICS SOLUCIONES S.A
Fijo: +593 2 6034068 Cel: +593 992 795600
Mail: mrivadeneira@greenetics.com.ec