RSA Conference 2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: HT-F01

Phantom Menace, Episode I? The Attack That Undressed the Mexican Banks in '18

Josu Loza

CISSP, CEH, CHFI
@josuloza

Your Company Is Ready?

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

Disclaimer:

The information, opinions, images or data expressed in this presentation, are my own personal opinions and don't represent my employers view in any way.

Agenda

- Remembering The Main Attacks On Wire Transfer Systems.
- Understanding a Payment System.
- Building A Secure Infrastructure.
- Living A Cyberattack, On First Person.
- Learned Lessons.

Not So Long Ago

The Usual Suspects

Organized Crime – 50%
Driven by profit. Often looking for personally identifiable information (PII) such as social security numbers, credit cards, and banking info.

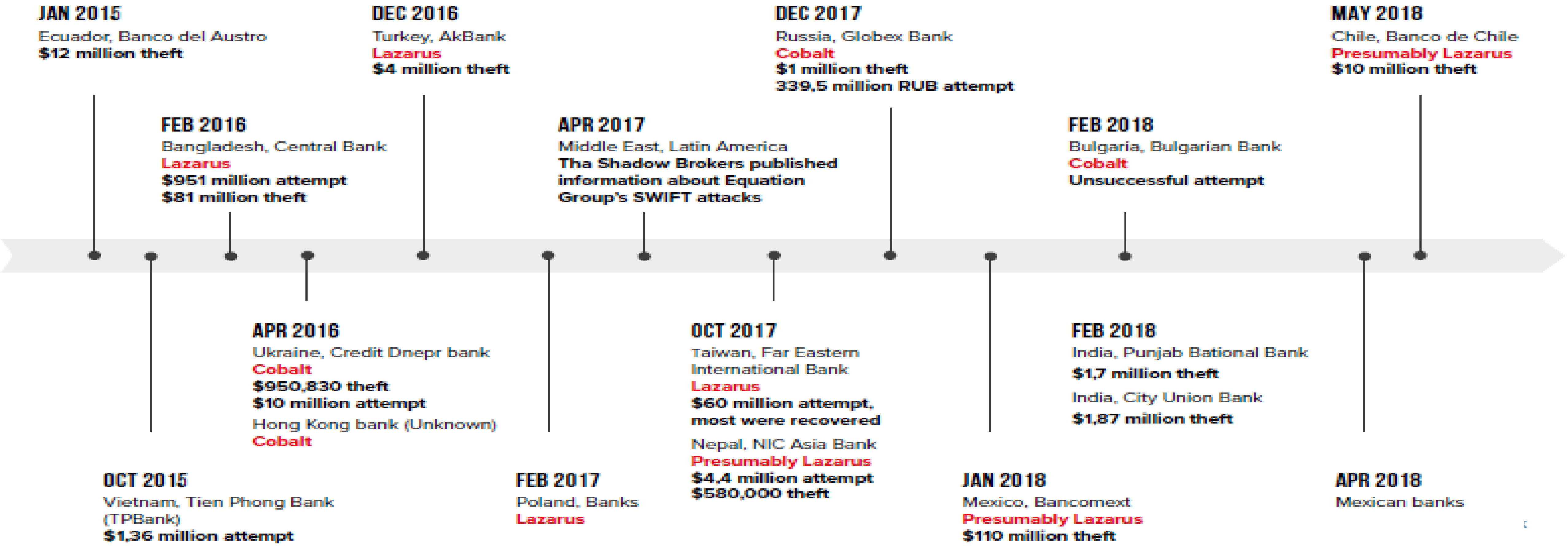
Insiders – 28%
Disgruntled employees looking for revenge or financial gain. May collaborate with other threat actors for money.

State Sponsored – 12%
Motivated by political, economic, or military agendas. Often looking for competitive information or users that can be exploited.

Hacktivists
Cause damage to disliked organizations. The ultimate goal is to gain awareness for their issue.

Opportunists
Amateur criminals, driven by desires of notoriety. Looking to exploit flaws in network systems and devices.

Main Attacks On Wire Transfers Systems



JAN 2015
Ecuador, Banco del Austro
$12 million theft

OCT 2015
Vietnam, Tien Phong Bank (TPBank)
$1,36 million attempt

FEB 2016
Bangladesh, Central Bank
Lazarus
$951 million attempt
$81 million theft

APR 2016
Ukraine, Credit Dnepr bank
Cobalt
$950,830 theft
$10 million attempt
Hong Kong bank (Unknown)
Cobalt

DEC 2016
Turkey, AkBank
Lazarus
$4 million theft

FEB 2017
Poland, Banks
Lazarus

APR 2017
Middle East, Latin America
Tha Shadow Brokers published information about Equation Group's SWIFT attacks

OCT 2017
Taiwan, Far Eastern International Bank
Lazarus
$60 million attempt, most were recovered
Nepal, NIC Asia Bank
Presumably Lazarus
$4,4 million attempt
$580,000 theft

DEC 2017
Russia, Globex Bank
Cobalt
$1 million theft
339,5 million RUB attempt

JAN 2018
Mexico, Bancomext
Presumably Lazarus
$110 million theft

FEB 2018
Bulgaria, Bulgarian Bank
Cobalt
Unsuccessful attempt

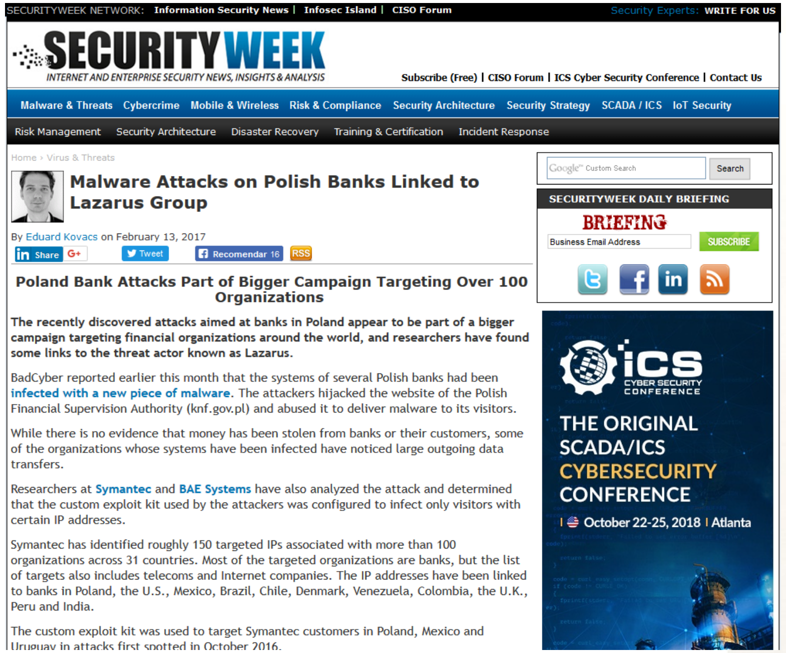
FEB 2018
India, Punjab Bational Bank
$1,7 million theft
India, City Union Bank
$1,87 million theft

APR 2018
Mexican banks

MAY 2018
Chile, Banco de Chile
Presumably Lazarus
$10 million theft

Group IB. (October 2018). Swift And Local Interbank Payment Systems. The Hi-Tech Crime Trends 2018, p.22.

How Many More Attacks Should Happen So That We Learn To Protect Payment Systems?



SECURITYWEEK NETWORK: Information Security News | Infosec Island | CISO Forum   Security Experts: WRITE FOR US

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Forum | ICS Cyber Security Conference | Contact Us

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Security Strategy SCADA / ICS IoT Security

Risk Management Security Architecture Disaster Recovery Training & Certification Incident Response

Home › Virus & Threats

Malware Attacks on Polish Banks Linked to Lazarus Group

By Eduard Kovacs on February 13, 2017

Share G+ Tweet Recomendar 16 RSS

Poland Bank Attacks Part of Bigger Campaign Targeting Over 100 Organizations

The recently discovered attacks aimed at banks in Poland appear to be part of a bigger campaign targeting financial organizations around the world, and researchers have found some links to the threat actor known as Lazarus.

BadCyber reported earlier this month that the systems of several Polish banks had been infected with a new piece of malware. The attackers hijacked the website of the Polish Financial Supervision Authority (knf.gov.pl) and abused it to deliver malware to its visitors.

While there is no evidence that money has been stolen from banks or their customers, some of the organizations whose systems have been infected have noticed large outgoing data transfers.

Researchers at Symantec and BAE Systems have also analyzed the attack and determined that the custom exploit kit used by the attackers was configured to infect only visitors with certain IP addresses.

Symantec has identified roughly 150 targeted IPs associated with more than 100 organizations across 31 countries. Most of the targeted organizations are banks, but the list of targets also includes telecoms and Internet companies. The IP addresses have been linked to banks in Poland, the U.S., Mexico, Brazil, Chile, Denmark, Venezuela, Colombia, the U.K., Peru and India.

The custom exploit kit was used to target Symantec customers in Poland, Mexico and Uruguay in attacks first spotted in October 2016.

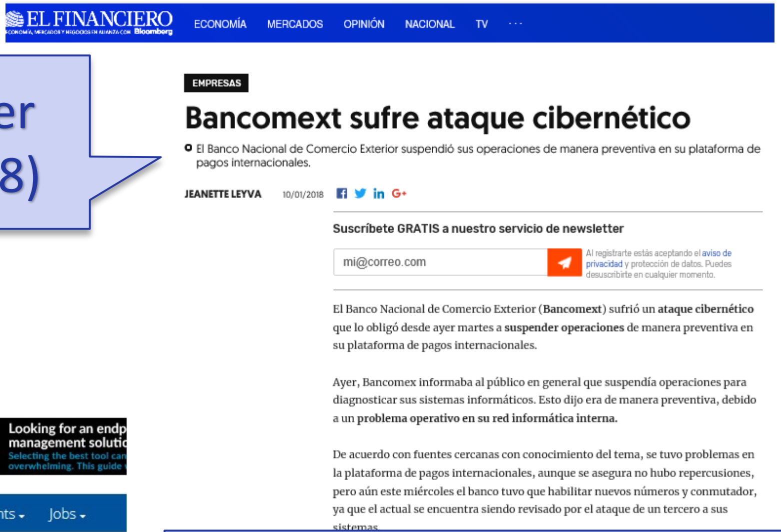
Google™ Custom Search Search

SECURITYWEEK DAILY BRIEFING

BRIEFING

Business Email Address SUBSCRIBE

Bancomext suffers cyber attack (January 10, 2018)



EL FINANCIERO ECONOMÍA MERCADOS OPINIÓN NACIONAL TV ···

EMPRESAS

Bancomext sufre ataque cibernético

- El Banco Nacional de Comercio Exterior suspendió sus operaciones de manera preventiva en su plataforma de pagos internacionales.

JEANETTE LEYVA 10/01/2018

Suscríbete GRATIS a nuestro servicio de newsletter

mi@correo.com

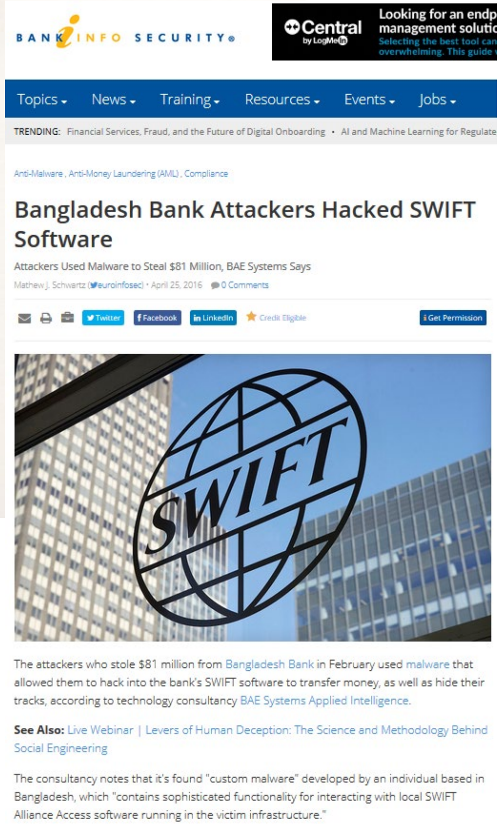
Al registrarte estás aceptando el aviso de privacidad y protección de datos. Puedes desuscribirte en cualquier momento.

El Banco Nacional de Comercio Exterior (**Bancomext**) sufrió un **ataque cibernético** que lo obligó desde ayer martes a **suspender operaciones** de manera preventiva en su plataforma de pagos internacionales.

Ayer, Bancomex informaba al público en general que suspendía operaciones para diagnosticar sus sistemas informáticos. Esto dijo era de manera preventiva, debido a un **problema operativo en su red informática interna.**

De acuerdo con fuentes cercanas con conocimiento del tema, se tuvo problemas en la plataforma de pagos internacionales, aunque se asegura no hubo repercusiones, pero aún este miércoles el banco tuvo que habilitar nuevos números y conmutador, ya que el actual se encuentra siendo revisado por el ataque de un tercero a sus sistemas.

Megahack banking Mexico (May 14, 2018)



BANK INFO SECURITY®

Topics ▾ News ▾ Training ▾ Resources ▾ Events ▾ Jobs ▾

TRENDING: Financial Services, Fraud, and the Future of Digital Onboarding • AI and Machine Learning for Regulate

Anti-Malware , Anti-Money Laundering (AML) , Compliance

Bangladesh Bank Attackers Hacked SWIFT Software

Attackers Used Malware to Steal $81 Million, BAE Systems Says

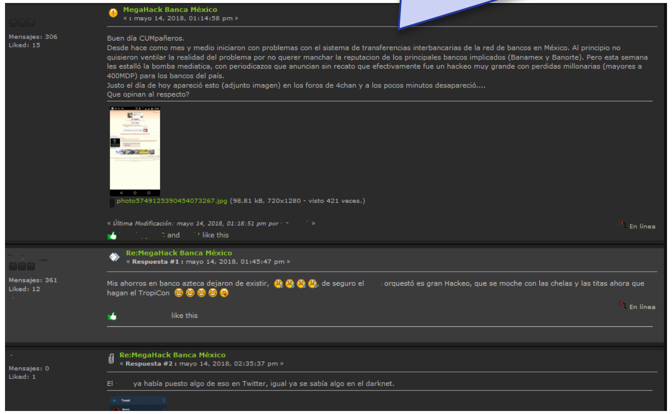
Mathew J. Schwartz (euroinfosec) • April 25, 2016 0 Comments

Twitter Facebook LinkedIn Credit Eligible Get Permission

The attackers who stole $81 million from Bangladesh Bank in February used malware that allowed them to hack into the bank's SWIFT software to transfer money, as well as hide their tracks, according to technology consultancy BAE Systems Applied Intelligence.

See Also: Live Webinar | Levers of Human Deception: The Science and Methodology Behind Social Engineering

The consultancy notes that it's found "custom malware" developed by an individual based in Bangladesh, which "contains sophisticated functionality for interacting with local SWIFT Alliance Access software running in the victim infrastructure."



Mensajes: 306
Liked: 15

MegaHack Banca México
« : mayo 14, 2018, 01:14:58 pm »

Buen día CUMpañeros.
Desde hace como mes y medio iniciaron con problemas con el sistema de transferencias interbancarias de la red de bancos en México. Al principio no quisieron ventilar la realidad del problema por no querer manchar la reputacion de los principales bancos implicados (Banamex y Banorte). Pero esta semana les estalló la bomba mediatica, con periodicazos que anuncian sin recato que efectivamente fue un hackeo muy grande con perdidas millonarias (mayores a 400MDP) para los bancos del país.
Justo el día de hoy apareció esto (adjunto imagen) en los foros de 4chan y a los pocos minutos desapareció....
Que opinan al respecto?

photo5749125390454073267.jpg (98.81 kB, 720x1280 - visto 421 veces.)

« Última Modificación: mayo 14, 2018, 01:18:51 pm por » En línea

and like this

Mensajes: 361
Liked: 12

Re:MegaHack Banca México
« **Respuesta #1 :** mayo 14, 2018, 01:45:47 pm »

Mis ahorros en banco azteca dejaron de existir, 😭😭😭😭, de seguro el orquestó es gran Hackeo, que se moche con las chelas y las titas ahora que hagan el TropiCon 😁😁😁😁😛

En línea

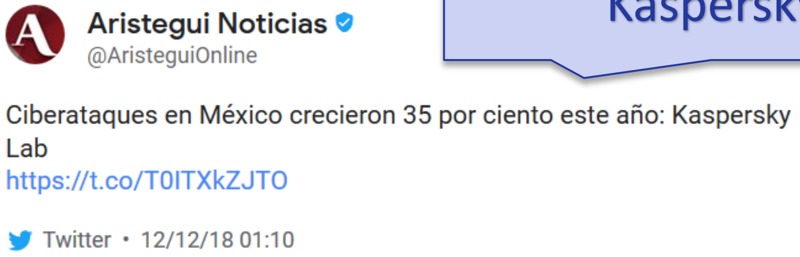
like this

Mensajes: 0
Liked: 1

Re:MegaHack Banca México
« **Respuesta #2 :** mayo 14, 2018, 02:35:37 pm »

El ya había puesto algo de eso en Twitter, igual ya se sabía algo en el darknet.

Cyber attacks in Mexico grew 35 percent this year: Kaspersky Lab.

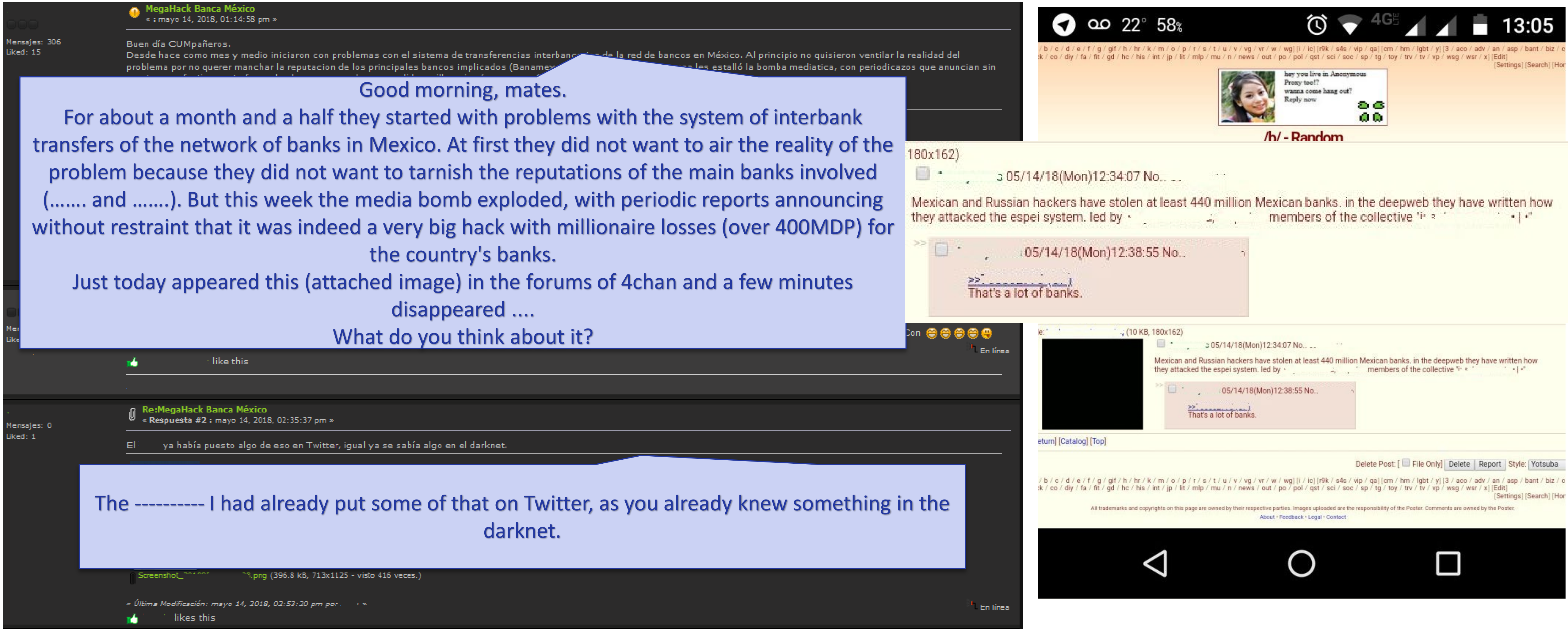


Aristegui Noticias
@AristeguiOnline

Ciberataques en México crecieron 35 por ciento este año: Kaspersky Lab
https://t.co/T0ITXkZJTO

Twitter • 12/12/18 01:10

Let The Cat Out Of The Bag



MegaHack Banca México
« : mayo 14, 2018, 01:14:58 pm »

Mensajes: 306
Liked: 15

Buen día CUMpañeros.
Desde hace como mes y medio iniciaron con problemas con el sistema de transferencias interbanc... de la red de bancos en México. Al principio no quisieron ventilar la realidad del problema por no querer manchar la reputacion de los principales bancos implicados (Banamex ... les estalló la bomba mediatica, con periodicazos que anuncian sin

Good morning, mates.
For about a month and a half they started with problems with the system of interbank transfers of the network of banks in Mexico. At first they did not want to air the reality of the problem because they did not want to tarnish the reputations of the main banks involved (……. and …….). But this week the media bomb exploded, with periodic reports announcing without restraint that it was indeed a very big hack with millionaire losses (over 400MDP) for the country's banks.
Just today appeared this (attached image) in the forums of 4chan and a few minutes disappeared ….
What do you think about it?

like this

Re:MegaHack Banca México
« Respuesta #2 : mayo 14, 2018, 02:35:37 pm »

Mensajes: 0
Liked: 1

El ya había puesto algo de eso en Twitter, igual ya se sabía algo en el darknet.

The ---------- I had already put some of that on Twitter, as you already knew something in the darknet.

Screenshot_ .png (396.8 kB, 713x1125 - visto 416 veces.)

« Última Modificación: mayo 14, 2018, 02:53:20 pm por »

likes this

En línea

13:05

/b/ - Random

180x162)

05/14/18(Mon)12:34:07 No.

Mexican and Russian hackers have stolen at least 440 million Mexican banks. in the deepweb they have written how they attacked the espei system. led by members of the collective

05/14/18(Mon)12:38:55 No.

>>
That's a lot of banks.

(10 KB, 180x162)

05/14/18(Mon)12:34:07 No.

Mexican and Russian hackers have stolen at least 440 million Mexican banks. in the deepweb they have written how they attacked the espei system. led by members of the collective

05/14/18(Mon)12:38:55 No.

>>
That's a lot of banks.

[Return] [Catalog] [Top]
Delete Post: [File Only] Delete Report Style: Yotsuba
[Settings] [Search] [Home]
All trademarks and copyrights on this page are owned by their respective parties. Images uploaded are the responsibility of the Poster. Comments are owned by the Poster.
About • Feedback • Legal • Contact

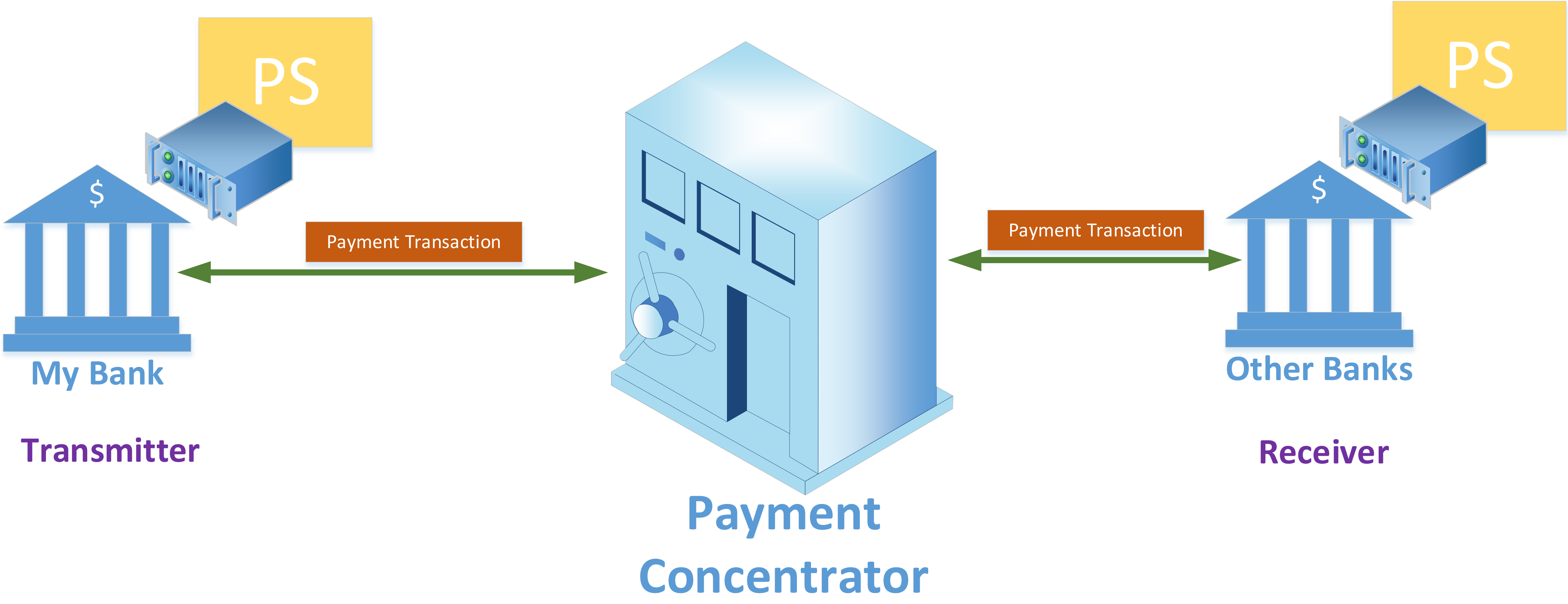
Blog. (2018). Blog. 2018, de A underground blog on internet.

RSAConference2019

Understanding a Payment System

How any wire transfer system works

General Architecture



PS

Payment Transaction

My Bank

Transmitter

Payment Concentrator

Payment Transaction

PS

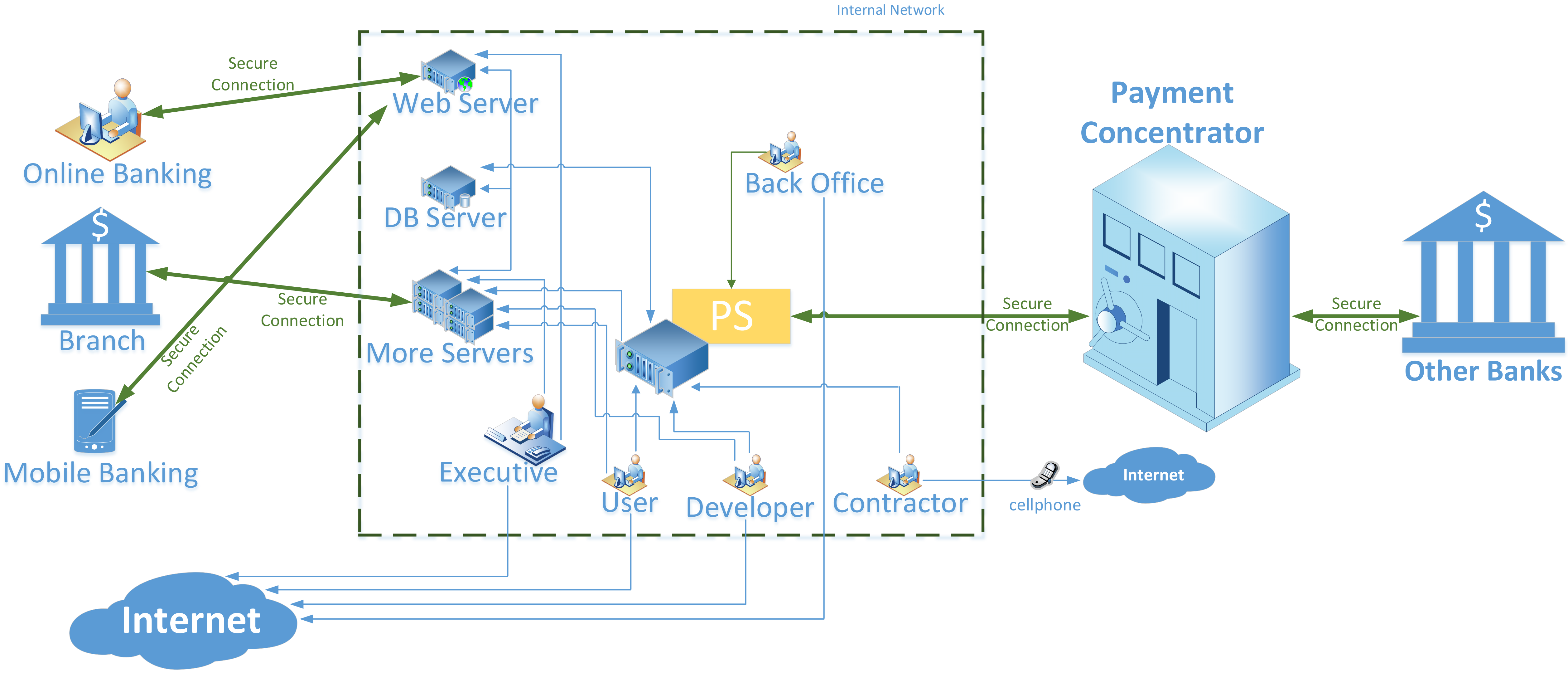
Other Banks

Receiver

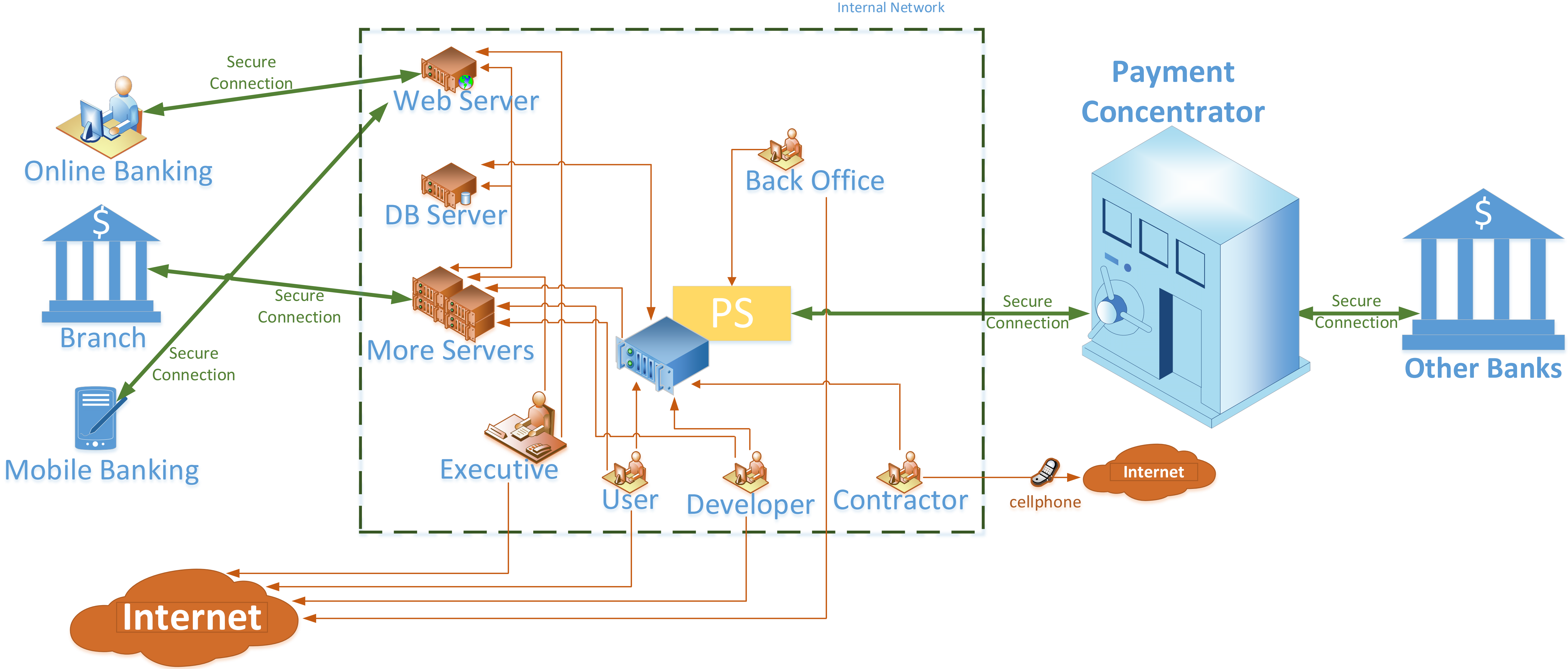
RSAConference2019

Possible Attacks to a Wire Transfer System application

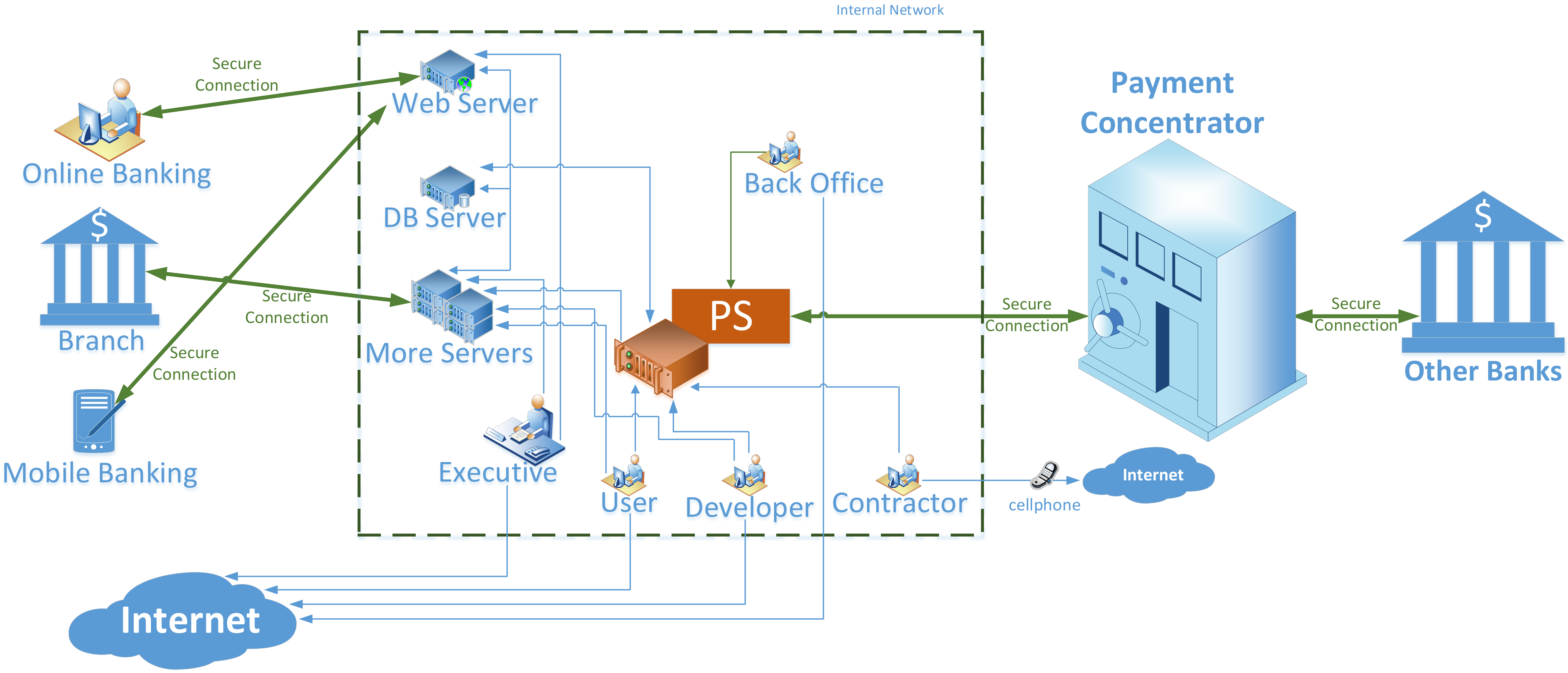
A Overview Of A Wire Transfer Architecture



Case 1. Pwning Wire Transfer System



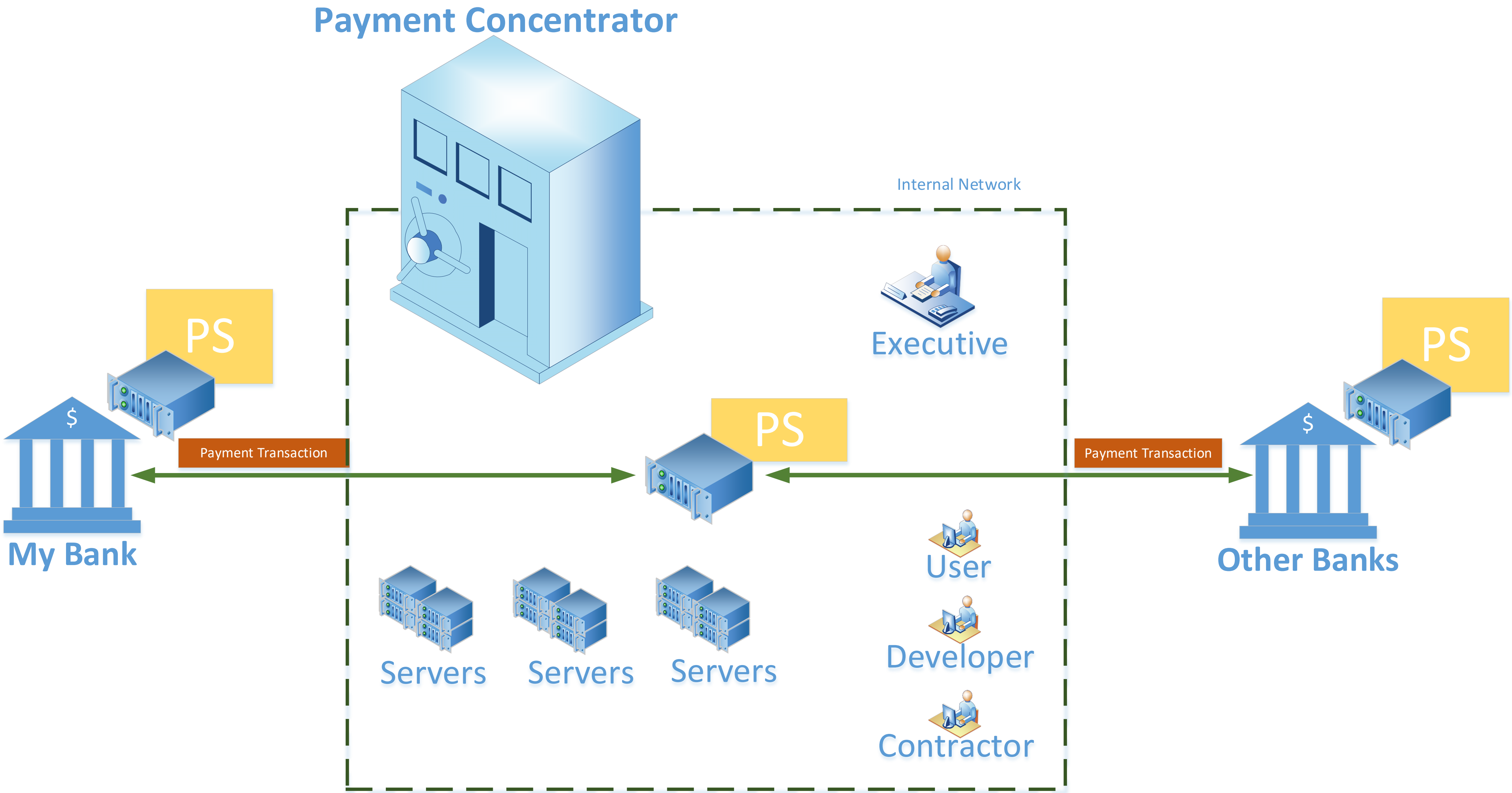
Case 2. Pwning Wire Transfer System



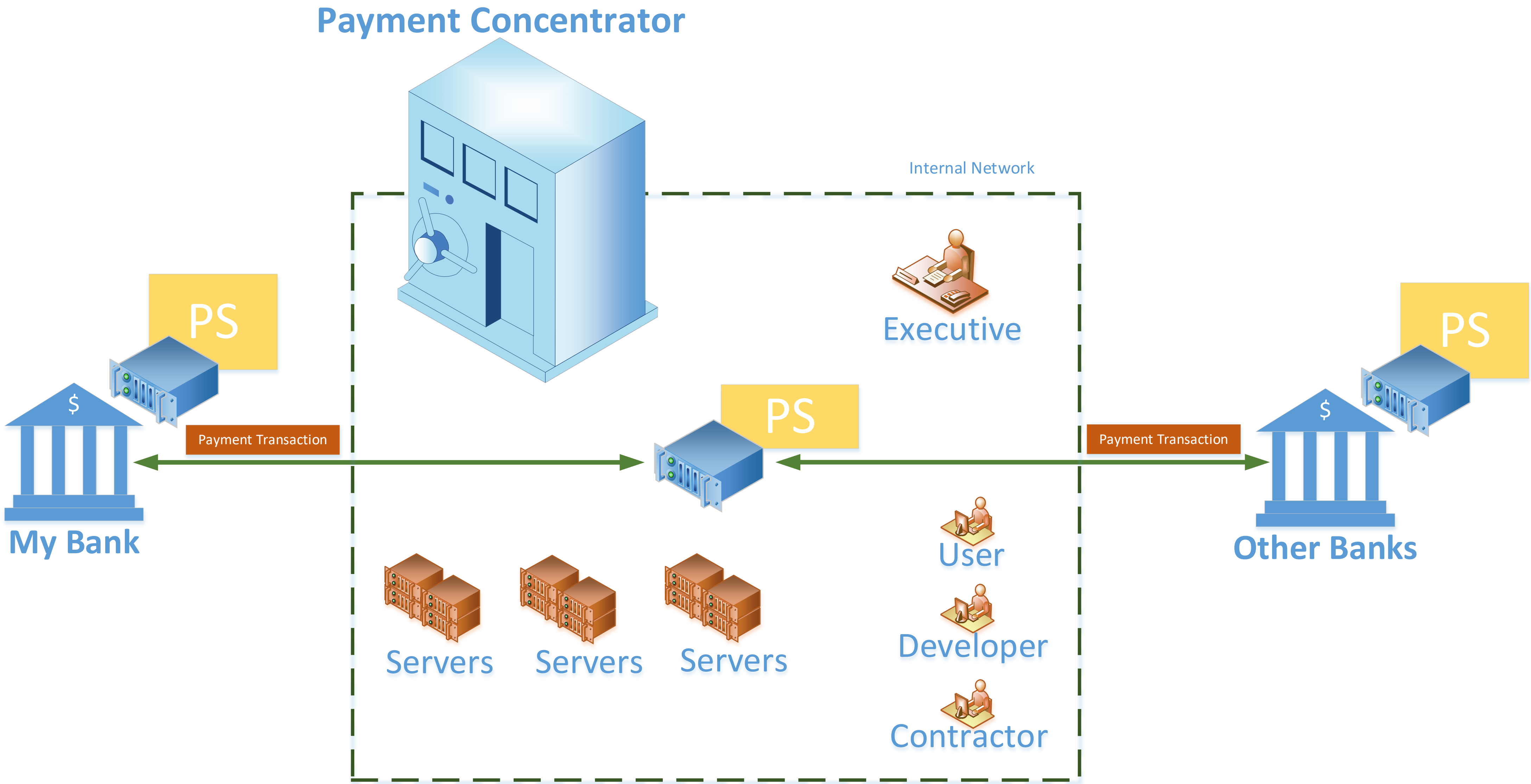
Thinking as an attacker

Imagining very bad things

Payment Concentrator Side



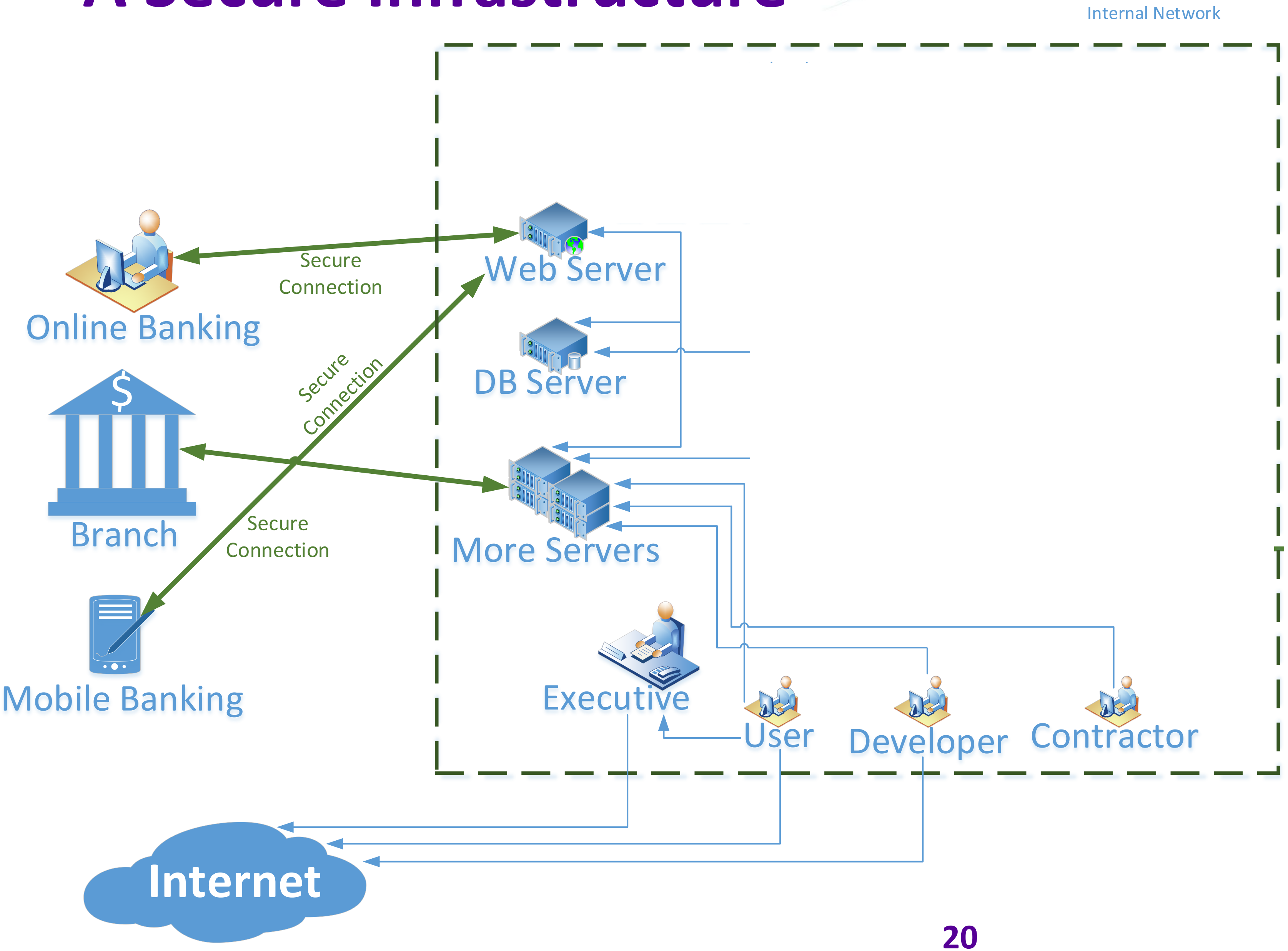
Pwning Payment Concentrator Side



RSA®Conference2019

Building A Secure Infrastructure

A Secure Infrastructure



In Sumary

- Are your data protected in?:
  - Rest.
  - In transit.
  - In use.

- Have you already done your annual pentest?
- Have you already done your annual threat and risk analysis?
- Do you know the architecture of your applications?

RSAConference2019

Living A Cyberattack, On First Person

Are You Ready To Face A Security Incident?

- First question:
  - Do you have already thought about what you should do to attendant a security incident?

- In the following scenarios, imagine that you are in the position mentioned and you must attend to what is being requested.

- Let's start the security incident.

CEO

- The reporters are at the principal entrance, you are ready to give a speech?.
- The company has already lost 20% of its value, shareholders want to know what happens.
- The regulator is on the phone and wants to know what's going on.
- You need to urgently call other CEOs.

CIO

- You have a reporter waiting on the cellphone for an interview for a local channel.
- The board are waiting for actions.
- The CFO is texting you and reporting the multi-million dollar losses of the company.
- Your work team is waiting for instructions and doesn't understand what's happening.
- The regulator awaits the report on the unavailability of services.

CISO

- Social networks demand the resignation of the CISO.
- The Board wants to understand what's happening through a video call and in terms that they understand (they do not understand technological terms and less security terms).
- Marketing requests your help to write an official statement.
- The CEO are very upset and are asking for immediate actions.
- Can you perform all these actions while you're attending a security conference in another country?

The Company in General

- All employees know how to face an attack?, they know what to do?.
- There are different communication plans, ready to face the most common threats?
- The CEO, CIO, CISO, CFO, CTO etc. Are ready to answer an interview?. -Now-
- Your infrastructure is ready to be resilient for a cyber attack.

We’re On Time

- At night, on the weekend or back to our house, let's take 10 minutes to reflect on the following:
  - What points caught my attention?
  - With what points can I help my company?
  - What points can't my company cover today?
  - What actions should we take to be ready for a cyber attack?

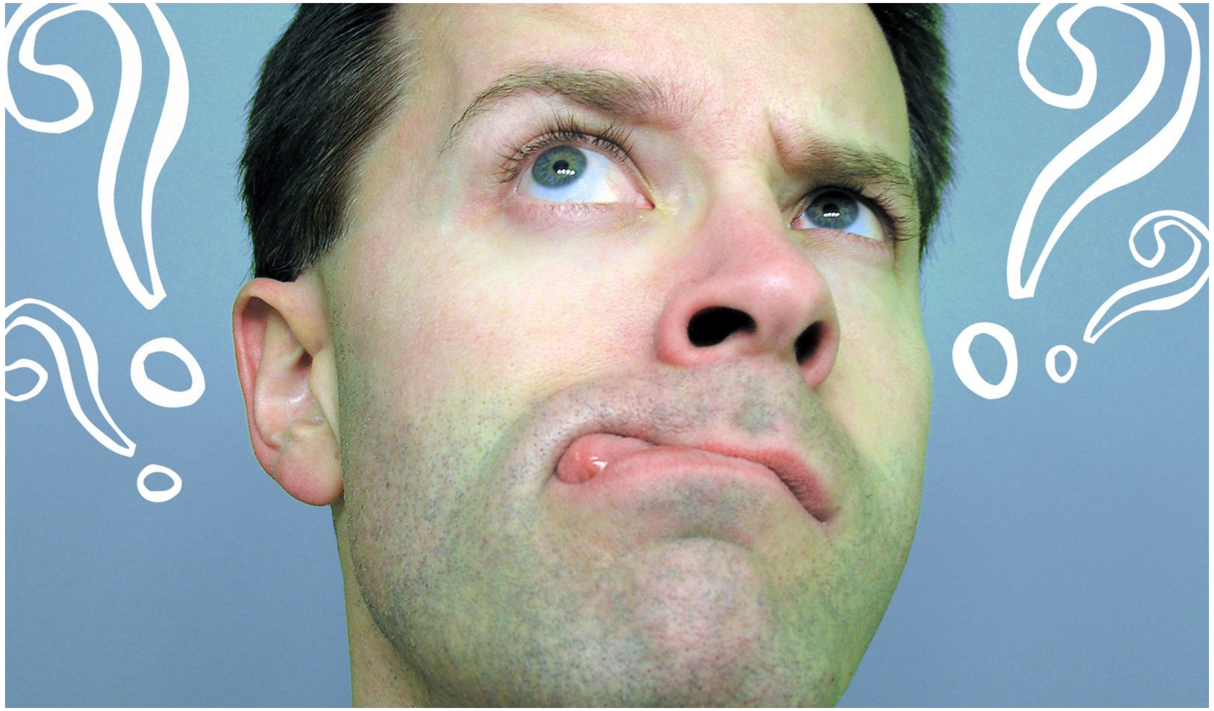
- On Monday, as the first task, let's start the first activities.
- Remember, the timer is running.

RSAConference2019

Learned Lessons

The Big Question Is:

- The question isn't whether my payment systems will be compromised, is when someone tries to compromise them?, or how many times they tried to compromise them?



What We Can Do

- Place the wire transfer systems servers and personal computers that operates the wire transfer system in an isolated network.
- Dedicate exclusive personal computers to wire transfer systems.

*** The above points are less expensive than any incident.***

- Implement transaction validation mechanisms in all systems.
- Scan the application code.

What We Can Do

- Protect wire transfer systems isn't a rocket science and doesn't require a large investment.
- Place the wire transfer applications on physical servers.
- Performs an annual audit by a specialist payment systems firm.
- There must be constant internal reviews of payment media applications.

PLEASE! Don't be a statistic

Year	Bank	Amount
2018	State Bank of Mauritius (NEW)	$14MM
	Banco De Chile (NEW)	$10MM ($100MM attempted)
	City Union Bank (NEW)	$2MM
	Punjab National Bank (NEW)	$1.77B
	Bank Negara Malaysia (NEW)	Unsuccessful
2017	EastNets Bureau (Middle East)	No impact
	Far Eastern International (Taiwan)	$500K
	NIC Asia	$580K ($4.4MM Attempted)
2016	Bangladesh Central Bank	$81MM ($1B attempted)
	Unnamed Bank (Ukraine)	$10MM
	First Bank of Nigeria	$100MM
	Union Bank of India	$171MM
	Central Bank of Malaysia	Unsuccessful
	P.T. Bank Bumi Arta Tbk (India)	Unsuccessful
	Akbank (Turkey)	$4MM
	Russian Central Bank	$31MM
2015	Banco del Austro (Ecuador)	$12MM
	Central Bank of the Philippines	Undisclosed
	Tien Phon Bank (Thailand)	$1.3M Attempted

$3.2B attempted

$2.19B stolen

The Most Important

- The **AWARENESS** is the most important action.

@josuloza

Add to Network Josu Loza