CONGRESO DE
PREVENCIÓN DEL FRAUDE Y SEGURIDAD

Construyendo **experiencias** desde un **entorno seguro.** ◀◀◀

FECHA 15 - 16 DE NOVIEMBRE /2018
HOTEL GRAND HYATT BOGOTÁ

Roberto Martínez

Senior Security Researcher
Global Research and Analysis Team | Kaspersky Lab

Sistemas Financieros Bajo Ataque

Inteligencia de amenazas y seguridad accionable como estrategias de defensa

Los grandes retos de los Sistemas Financieros

Estado actual del fraude

Las transacciones fraudulentas a través de aplicaciones móviles crecieron un 600 % desde 2015. *

Se identificó un nuevo ataque de phishing cada 30 segundos; pérdidas globales $10,8 mil millones. *

Las transacciones de blanqueo de dinero se estiman entre el 2 y el 5% del PIB global. Eso es aproximadamente $1-2 billones USD anualmente. * *

*RSA Q1 2018 Fraud Report
**PwC Global Economic Crime Fraud Survey 2018

https://www.plastico-bbva-bloqueo.com/

BBVA Bancomer

Cancelaciones

BBVA

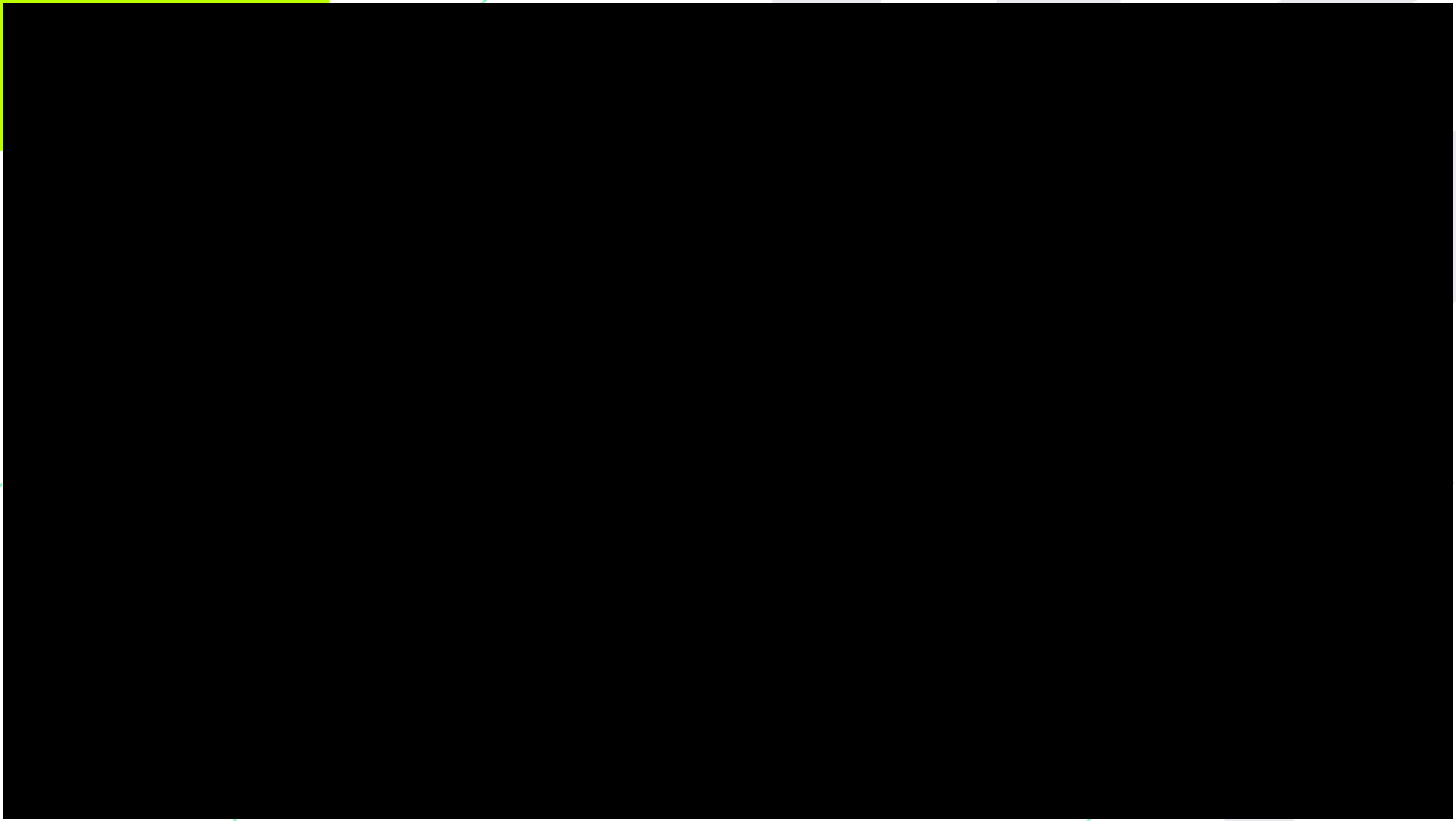
Abusos de SSL en las páginas de Phishing con el uso de **"Let's Encrypt!"**

Paso 1 de 2

58%

de todos los ataques de Phishing va en contra de las instituciones financieras

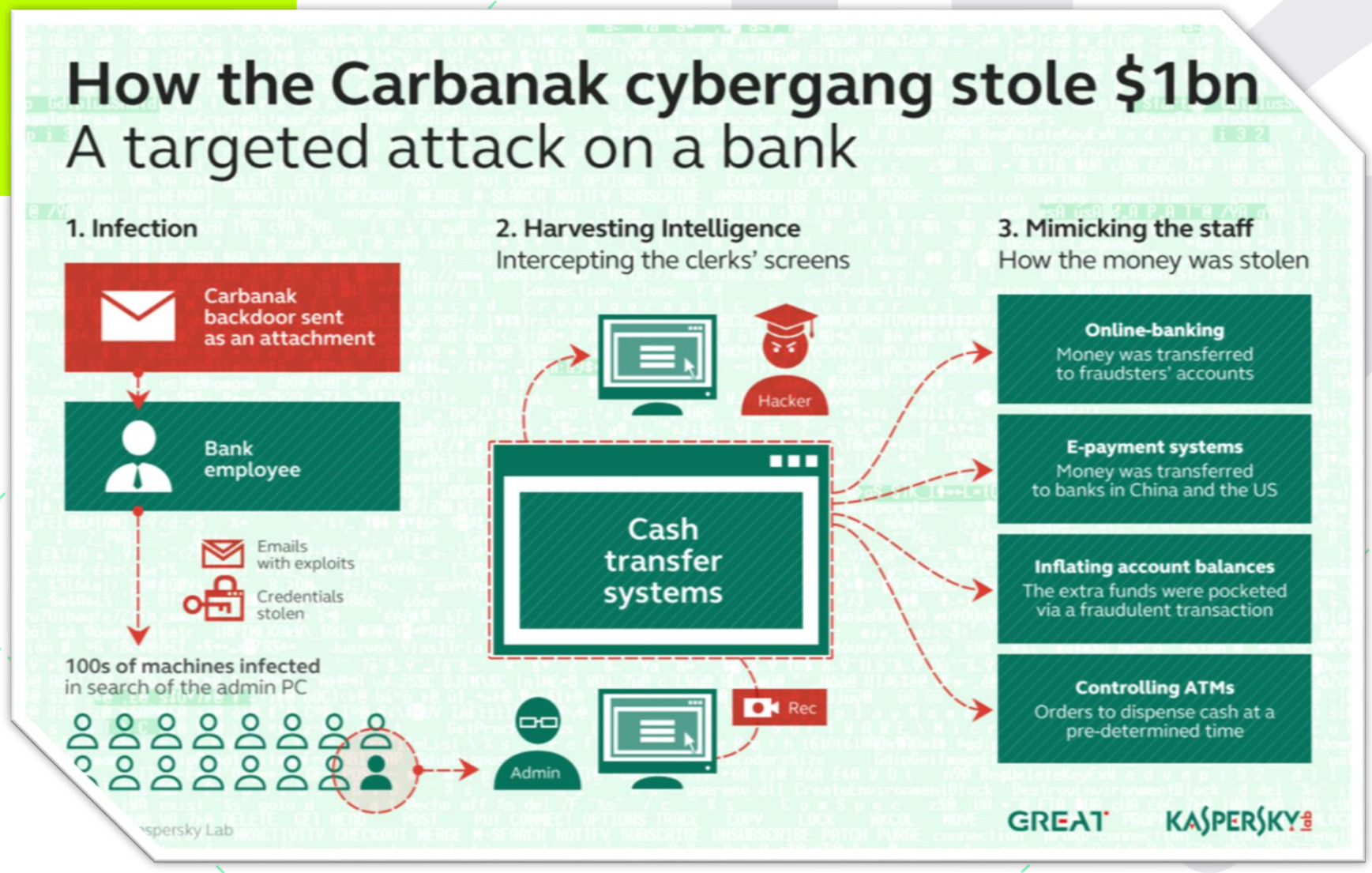
(2018)



La evolución de las amenazas

Motivaciones, Actores y Objetivos

Image source: https://www.baesystems.com/en/cybersecurity/feature/the-unusual-suspects


How the Carbanak cybergang stole $1bn
A targeted attack on a bank
1. Infection
Carbanak backdoor sent as an attachment
Bank employee
Emails with exploits
Credentials stolen
100s of machines infected in search of the admin PC
2. Harvesting Intelligence
Intercepting the clerks' screens
Hacker
Cash transfer systems
Admin
Rec
3. Mimicking the staff
How the money was stolen
Online-banking
Money was transferred to fraudsters' accounts
E-payment systems
Money was transferred to banks in China and the US
Inflating account balances
The extra funds were pocketed via a fraudulent transaction
Controlling ATMs
Orders to dispense cash at a pre-determined time
GREAT
KASPERSKY

Tactics, techniques and procedures of financial attacks attributed to the Lazarus group

Lazarus is widely considered to be the group behind multiple, devastating cyberattacks including the $81 million heist of Central Bank of Bangladesh, at the beginning of 2016, and several other attacks against banks worldwide. While conducting their operations, hackers follow a set of tactics, techniques and procedures which allow them to quietly penetrate targeted systems and gain access to critical ones.

LAZARUS

Step 1

Compromise of a webserver

1. The compromised **server is used as an entry point** to the company

OR

1. **A government website is hacked** through a known vulnerability

2. The **exploit is placed on the hacked website** with a whitelist of targets to serve the exploit to

3. **The target** visits a government website and **becomes infected**

Step 2

1. A first stage, rudimentary **backdoor is deployed for reconnaissance purposes**

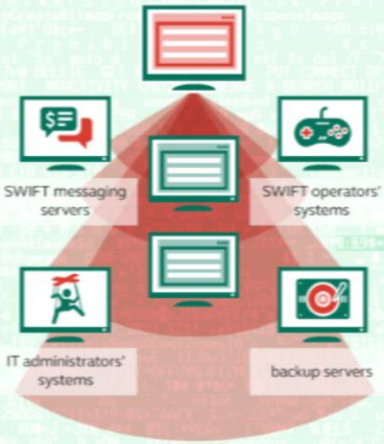
2. **The attacker** quickly **migrates to another system** in the company and **gains a foothold**

3. Additional lateral movement **tools are installed – some for privilege escalation purposes**

Admin

Step 3

Attackers analyze the network and identify critical assets in the organization including:



Step 4

1. Custom **malware is deployed**, that **disables internal security** checks of the SWIFT software

2. SWIFT message **filtering malware is integrated to hide rogue messages** created by the attackers

3. Money theft starts

While investigating Lazarus' financial attacks, Kaspersky Lab researchers were able to identify 150+ different malware samples related to recent group's activity.

Kaspersky Lab products successfully detect and block all known malware used by the Lazarus group.

GREAT KASPERSKY lab

The Geography of financial attacks by Lazarus group

The malware by Lazarus group, infamous for its theft of $81 million from Central Bank of Bangladesh, has been active since at least 2009. It has been spotted in the last couple of years in at least 18 countries.

GREAT KASPERSKY

citibanamex Seguros

INCOME STATEMENT

For the year ended 31 December 2016

Premium

Software Dev Mgr II

Job Description

At BBVA, we are working to make banking better for everyone. That is where you come in. We are looking for smart, team oriented people who want to be part of a first-class workforce that gives people the tools they need to meet their financial goals, all while delivering an outstanding client experience. Learn more below.

Relationship Director - Corporate Banking

Description

The Relationship Director - Corporate Banking role is based within HSBC Corporate Banking – Commercial Banking UK HSBC Corporate Banking in the UK provides both domestic and international commercial banking services to our existing and prospective clients

Business Development Executive - HSBC Insurance

Location

Asia Pacific-Hong Kong-Kowloon-Tai Kok Tsui

HSBC Insurance provides a comprehensive range of life products and services to suit the every

Finance

Engineering

Crypto Currency

Senior Esports Project Manager

The Blizzard Entertainment esports team is looking for a talented, enthusiastic, and highly organized project manager to oversee the tracking, documentation, and planning of our esports products. The ideal candidate must be a strong communicator, love the act of planning and organization, and enjoy working inside a flexible team-oriented environment. This candidate should be well versed in project management styles, methodologies, and processes. Tenacity, self-direction and follow-up skills are a must, as well as the ability to anticipate issues and find effective solutions.

CIB Operations - Warsaw Corporate Center (WCC) - Project Manager - Vice President

Req #: 170094080

Location: Warsaw, MZ, PL

Job Category: Project Management

INVESTMENT PROPOSAL

by

ABSTRACT

We analyzed and evaluated 10+ crypto currencies, the most circulated in the last four years, and expressed out company profile and investment proposal.

Katie Harris

Director at HOLLEY NETHERCOTE

Chief Financial Officer

JOB DESCRIPTION

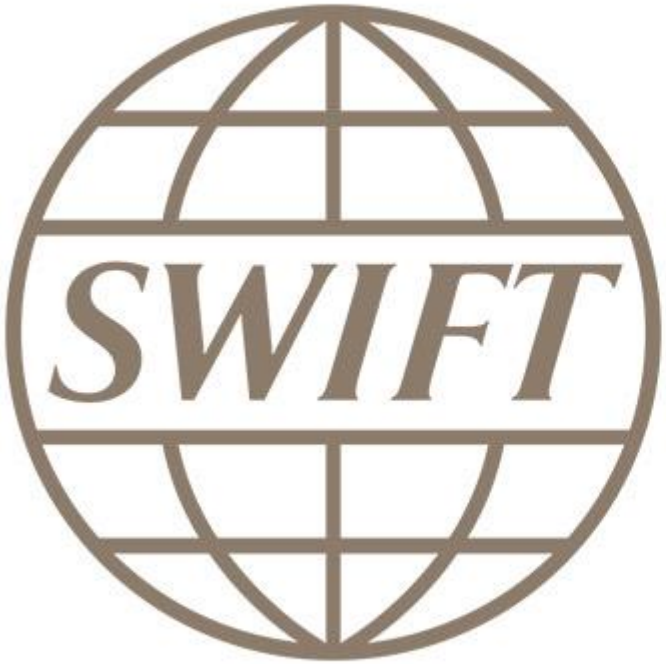
The Chief Financial Officer is one of the most important roles at Luno. As CFO you will coordinate with all business departments in providing a financial perspective to all decision making, overseeing accounting operations and ensure timely and accurate financial reporting. You will be involved in day-to-day discussions with the Executive Management team, reporting directly to the CEO and play a pivotal role in investor relations.

Engineering Manager

Job Description

Our vision is to bring more innovation, efficiency, and equality of opportunity to the world by building an open financial system. Our first step on that journey is making digital currency accessible and approachable for everyone. Two principles guide our efforts. First, be the most trusted company in our domain. Second, create user-focused products that are easier and more delightful to use.

Moving and transacting financial assets safely is core to executing on our vision and building our brand of trust. The payments team builds shared infrastructure for Coinbase and GDAX to securely store and trade billion dollars of assets. We take on hard engineering problems in cryptography, security, blockchain technology and distributed systems, with a focus on building high reliability services for product teams.


SWIFT


SONY
PICTURES

NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist

The deputy director of the NSA says he believes states have entered the bank-robbing business.

BLUENOROFF
Una unidad de Lazarus

Lazarus

- Ciber Espionaje
- Ciber Sabotaje

Bluenorroff

- Robo de dinero
- Minado de Cripto monedas

- Desarrollo Backdoors
- Exfiltración datos
- DoS
- Infiltración
- Operación C2
- Ataques de borrado

CNBV y nueve bancos han sido hackeados

Criminales han vulnerado la seguridad de instituciones financieras en México

17/02/2017 09:40 **AURA HERNÁNDEZ Y PAUL LARA**

gob.mx

› CNBV › Sanciones

ADDITIONAL WATERING HOLES

The eye-watch[.]jis domain appears to have been used in watering-hole attacks on other financial sector websites. On 2016-11-08 we observed connections to the site referred from:

hxxp://www.cnbv.gob[.]mx/Prensa/Paginas/Sanciones.aspx

This is the page for the Comisión Nacional Bancaria y de Valores (National Banking and Stock Commission of Mexico), specifically the portion of their site that details sanctions made by the Mexican National Banking Commission. This organisation is the Mexican banking supervisor and the equivalent of Poland's KNF.

ALGUNAS VÍCTIMAS

En algunos países específicos, se ha descubierto los ataques a bancos e instituciones:

RANK	COUNTRY	COUNT
1	Poland	19
2	United States	15
3	Mexico	9
4	United Kingdom	7
5	Chile	6
6	Brazil	5
7	Peru	3
7	Colombia	3
7	Denmark	3
7	India	3

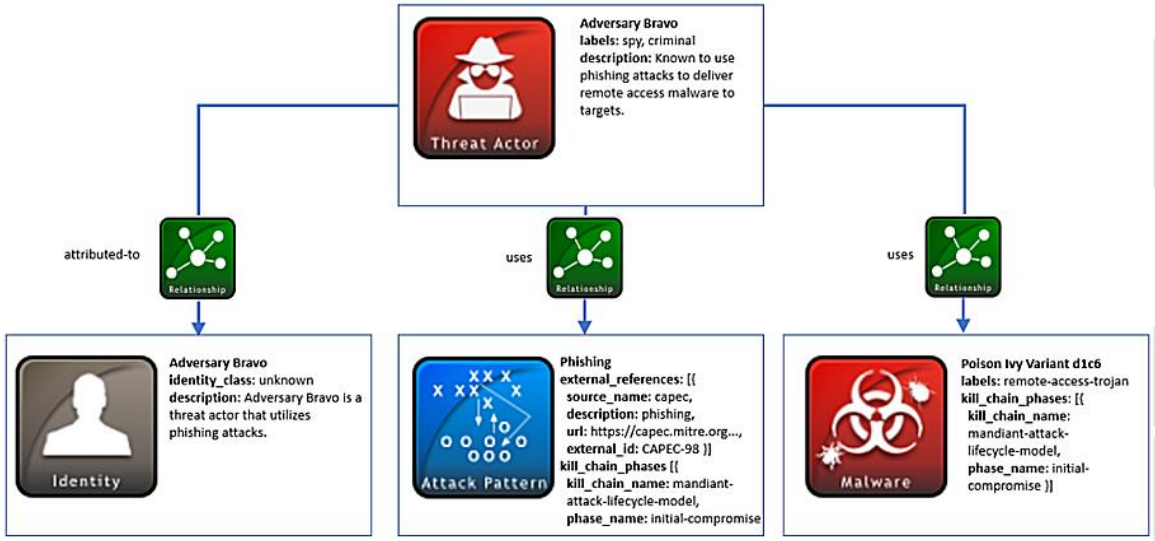
Hackers Stole Millions of Dollars From Mexico banks

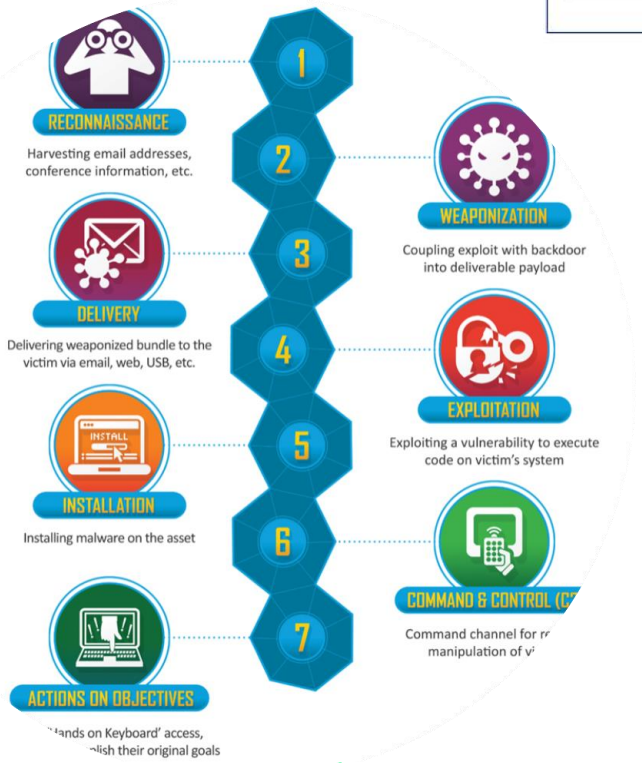
SPEI®
SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS

Pagos más rápidos y seguros

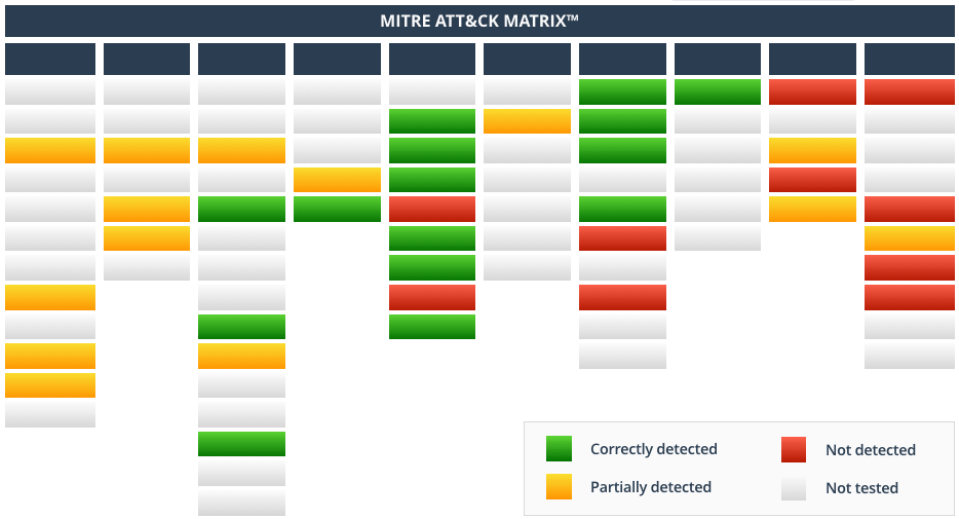
Defensa proactiva ante las amenazas

Seguridad basada en estrategias, no solo en herramientas y cumplimiento de normativas





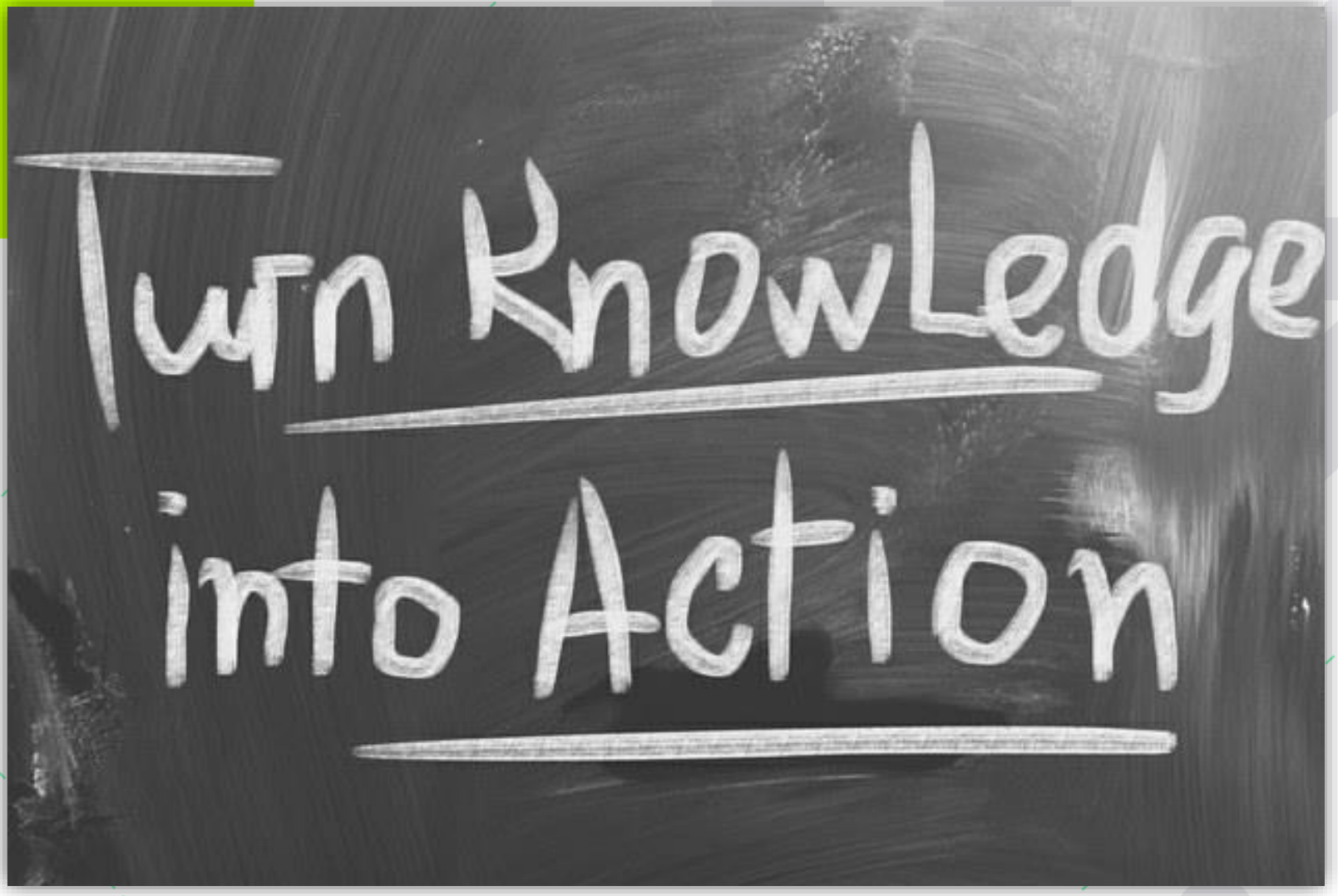
Herramientas, técnicas y actores



Cacería de Amenazas (Threat Hunting)

Inteligencia de Amenazas (Threat Intelligence) y Colaboración

Respuesta a Incidentes (IR)



Seguridad Accionable

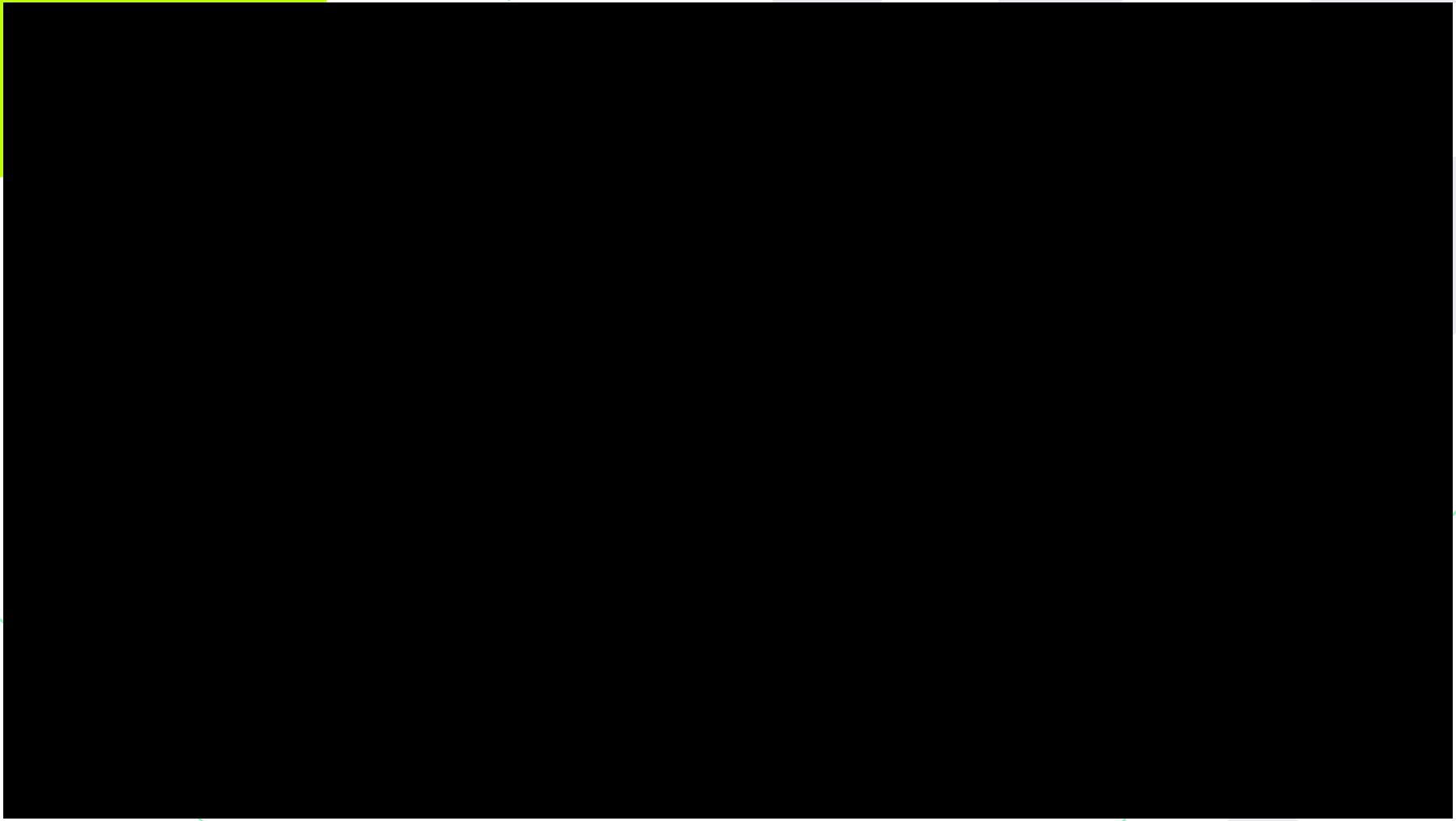
GReAT - Investigación élite de amenazas

- Equipo global de investigación y análisis
- Fundado en 2008
- Inteligencia de amenazas, liderazgo en investigación e inovación
- Enfoque: APTs, amenazas a infraestructuras críticas, amenazas a sistemas financieros, ataques dirigidos, búsqueda de vulnerabilidades de día cero programas y sistemas.

Ataques dirigidos

GREAT

Descubrimos y diseccionamos las amenazas más sofisticadas del mundo



“Fundamentalmente, si alguien quiere comprometer su red o dispositivo, seguramente lo va a hacer…… asumámoslo

Debemos entender que estamos en medio de una batalla, lo queramos o no y seguramente su red ya fue comprometida de alguna manera”

Michael Hyden
Ex-director CIA, NSA
Microsoft Enterprise Cloud Teaming Whitepaper

Gracias

Roberto Martinez

Senior Security Researcher | Global Research and Analysis Team

@r0bertmart1nez | roberto.martinez@kaspersky.com