ATAQUES INFORMÁTICOS A LAS INSTITUCIONES FINANCIERAS

Dmitry Bestuzhev

Twitter.com/dimitribest

HEAD of Global Research and Analysis Team, Kaspersky Lab

GREAT

Cashing Out: ATMs Try to Stop Wave of Cyberattacks

The ATM is the newest front in the war against cyberthieves

Banks hope chip-card technology will help foil fraud at the ATM. *PHOTO: MATT ROURKE/ASSOCIATED PRESS*

Most Po

1. Vio Lew Tru
2. Sha Enc Wh
3. GO in N
4. 1M Inv the
5. Irac to F

Most Po

1. Op But Sins

SECURITY

Attackers 'Hack' ATM Security with Explosives

As U.S. ATM Operators Face EMV Deadline, Physical Attacks Surge in Europe

Mathew J. Schwartz (euroinfosec) • October 17, 2016 0 Comments

Twitter Facebook LinkedIn Credit Eligible Get Permission

Trojan-Banker

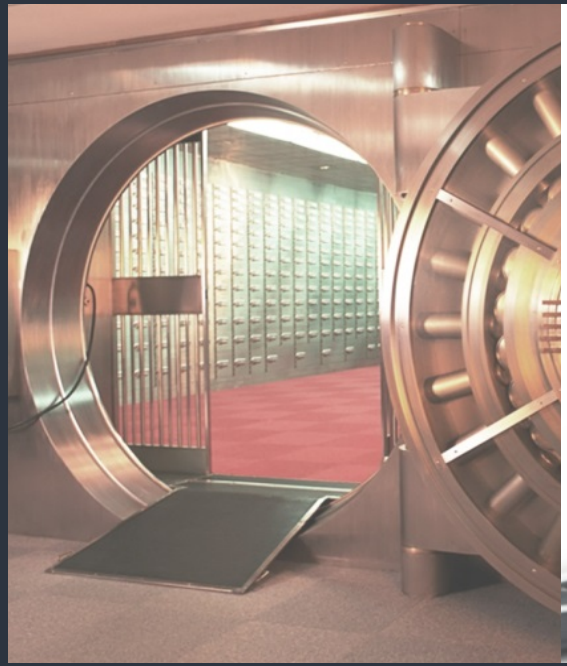
ATM

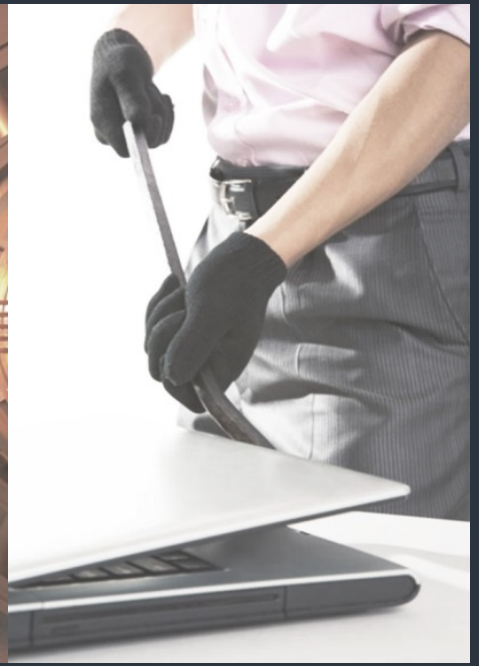
POS

Phishing

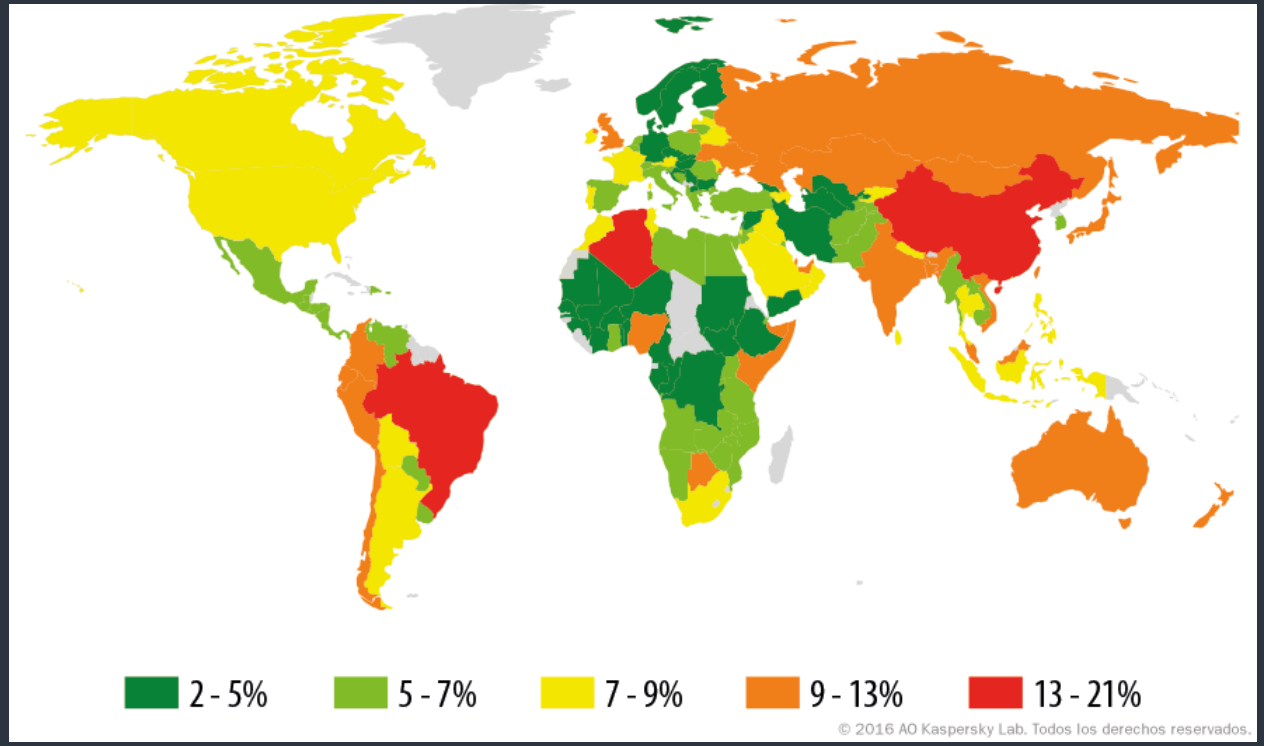
APT

A quien atacar: la banca o a sus clientes?



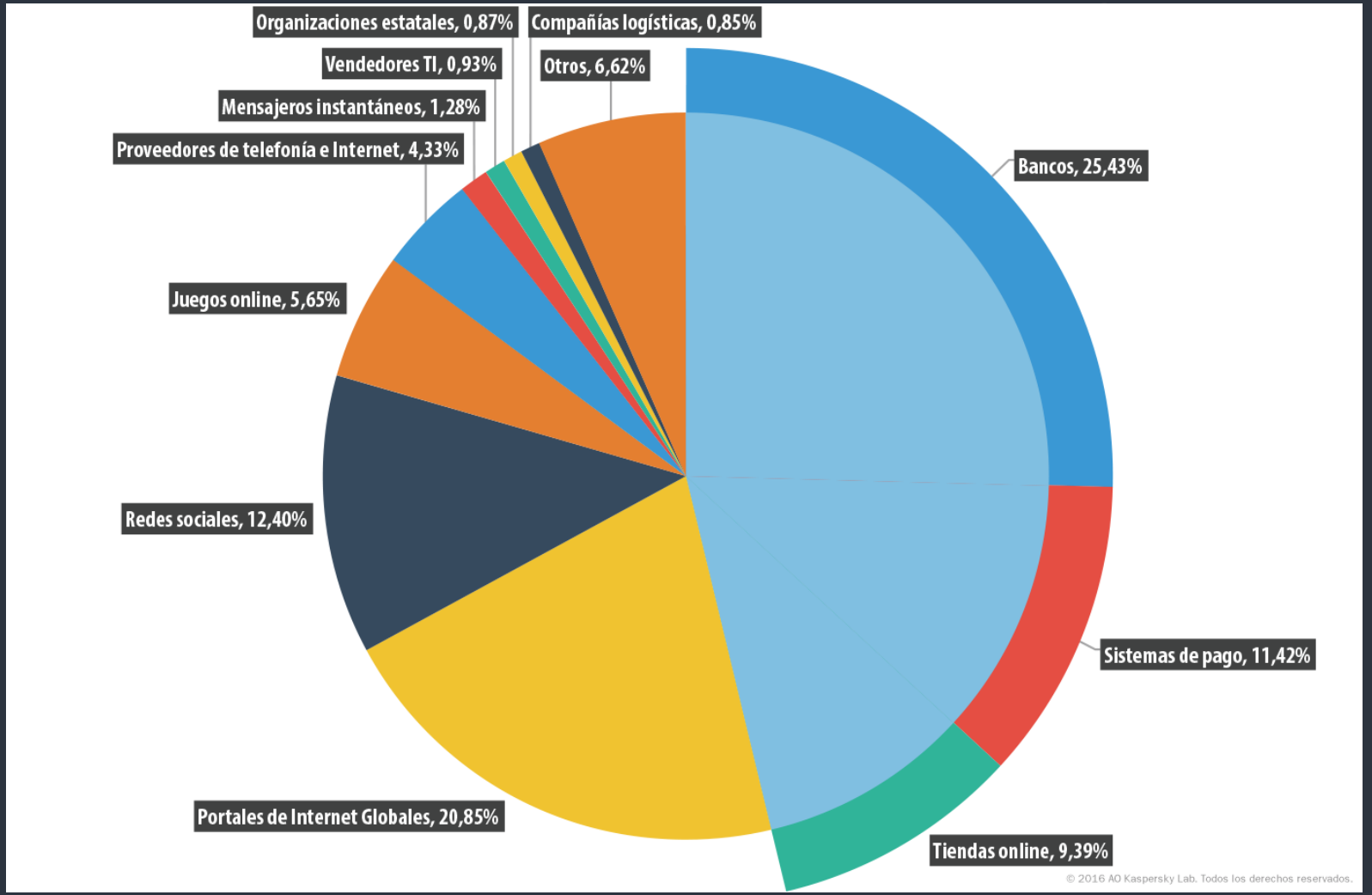


Phishing



Geografía de los ataques de Phishing*, Q2 2016

**Porcentaje de usuarios de Kaspersky Lab en el país donde el motor de Anti-Phishing haya detectado por lo menos un ataque de Phishing.*



[redacted]ndows Internet Explorer

[redacted]m

Bing

Favorites | Suggested Sites | Web Slice Gallery

[redacted]anca via Internet - Pr[redacted]

Page | Safety | Tools

PRIVATI E FAMIGLIE | GIOVANI fino a 30 anni | PRIVAT per i pass[redacted] | [redacted]G

ACCESSO A BANCA VIA INTERNET

Importanti novità sulla sicurezza e su[redacted]
Scopri di più >

CODICE
12341234

PIN
••••••••

ENTRA >

UniCredit premiat[redacted]

l Suo

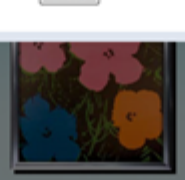
Sicurezza
- Sicurezza online
- Requisiti di sistema

Assistenza
- Visualizza la Demo di banca via Internet
- Contatta il Servizio Clienti al 800.710.710

Non hai ancora Banca Multicanale?
- Scopri i vantaggi

Per registrare la tua carta
- Registrati al Servizio Informativo UniCreditCard

è importante investire nel futuro.



[redacted]rivate Banker UniCredit hai più tempo da investire per te.

Scopri il nostro servizio >

I servizi online sono forniti da UniCredit S.p.A. tramite le Filiali contraddistinte UniCredit Private Banking.

[redacted]

Attenzione!

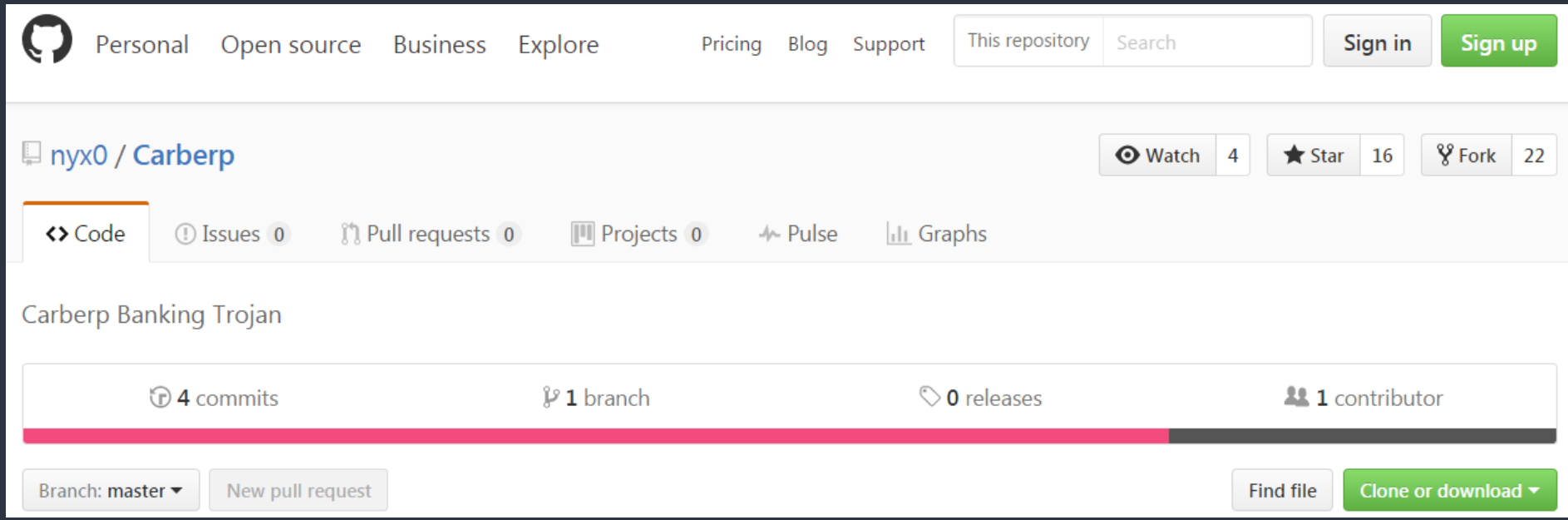
Gentile utente, Password Card associata al vostro account sara scadra tra 30 giorni. Si prega di verificare i codici in modo da poter preparare una scheda nuova Password Card. Per confermare la vostra lista, compila il modulo qui sotto e premere "Invia".

No.	Code	No.	Code
023		021	
026		032	
031		033	
035		034	
022		024	
025		036	
029		037	
040		038	
027		039	
030		028	

Invia

ZEUS en GitHub

Ahora es Open Source



Carberp también Open Source

POS

2010	Trojan-Spy.Win32.POS (CardStealer)
2011	Backdoor.Win32.Desty (Dexter)
2012	Trojan-Spy.Win32.Vskim (vSkimmer)
2013	BlackPOS (modified CardStealer)
2013	Trojan.Win32.Fsysn (Chewbacca)
2014	Backdoor.Win32.Backoff (Backoff)
2015	LogPOS, Punkey, POSeydon, FindPOS, Carbanak, MODPOS

ATM. Modelo de amanzas.

Activos a robar:
1. Dinero
2. Datos en las tarjetas

Modos de robo:
1. Skimmers
2. Robos físicos/explosivos
3. PoS malware

Métodos de ataques:
1. Desde las redes internas (Carbanak)
2. Ataques externos de alteración (Caja negra)
3. Ataques vía medios extraíbles (Todo lo demás)

ATM

Mazo 2009	**Backdoor.Win32.Skimer**
Marzo 2012	**Trojan-Spy.Win32.SPSniffer**
Octubre 2013	**Trojan-Banker.MSIL.Atmer (Ploutus)**
Noviembre 2013	**Trojan.Win32.Brob**
Diciembre 2013	**Backdoor.Win32.SkimerNC**
Marzo 2014	**Backdoor.Win32.Tyupkin**
Abril 2014	**Backdoor.Win32.NeoPacket (VB.ww)**
Diciembre 2014	**Backdoor .Win32.Atmmng**
Marzo 2015	**Backdoor.Win32.Atmdelf (Skimmer.w)**


APT

200 USD por minuto

200 USD por minuto

PSW…

2 meses de intentos
Hasta 3 intentos por cada sábado

Sonic17

Malware?

Herramientas de Test de Penetración:

- Meterpreter — Powershell script
- Mimikatz — Powershell script
- Powerpreter — Powershell script
- PuTTY plink — en lista blanca

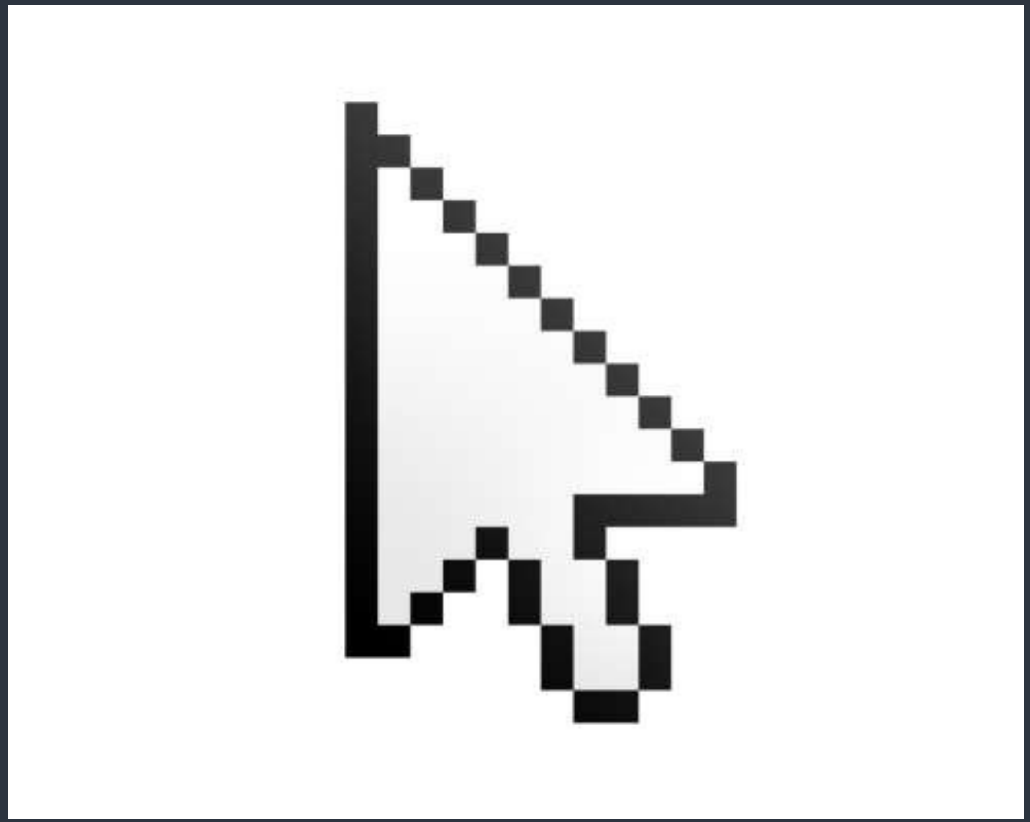
www.internet-bank.moibank.com/INFO-.ASP

INFO-.ASP

109.*.*.207 - - [May 2015] "POST /info-.asp HTTP/1.1" 200 496
109.*.*.207 - - [May 2015] "POST /info-.asp HTTP/1.1" 200 541
109.*.*.207 - - [May 2015] "POST /info-.asp HTTP/1.1" 200 496
5.*.*.132 - - [May 2015] "GET /favicon.ico HTTP/1.1" 404 2154
109.*.*.207 - - [May 2015] "POST /info-.asp HTTP/1.1" 200 496
109.*.*.207 - - [May 2015] "POST /info-.asp HTTP/1.1" 200 541
109.*.*.207 - - [May 2015] "POST /info-.asp HTTP/1.1" 200 541
109.*.*.207 - - [May 2015] "POST /info-.asp HTTP/1.1" 200 496
109.*.*.207 - - [May 2015] "POST /info-.asp HTTP/1.1" 200 541

METEL

Cómo es posible?



METEL – Banking Trojan

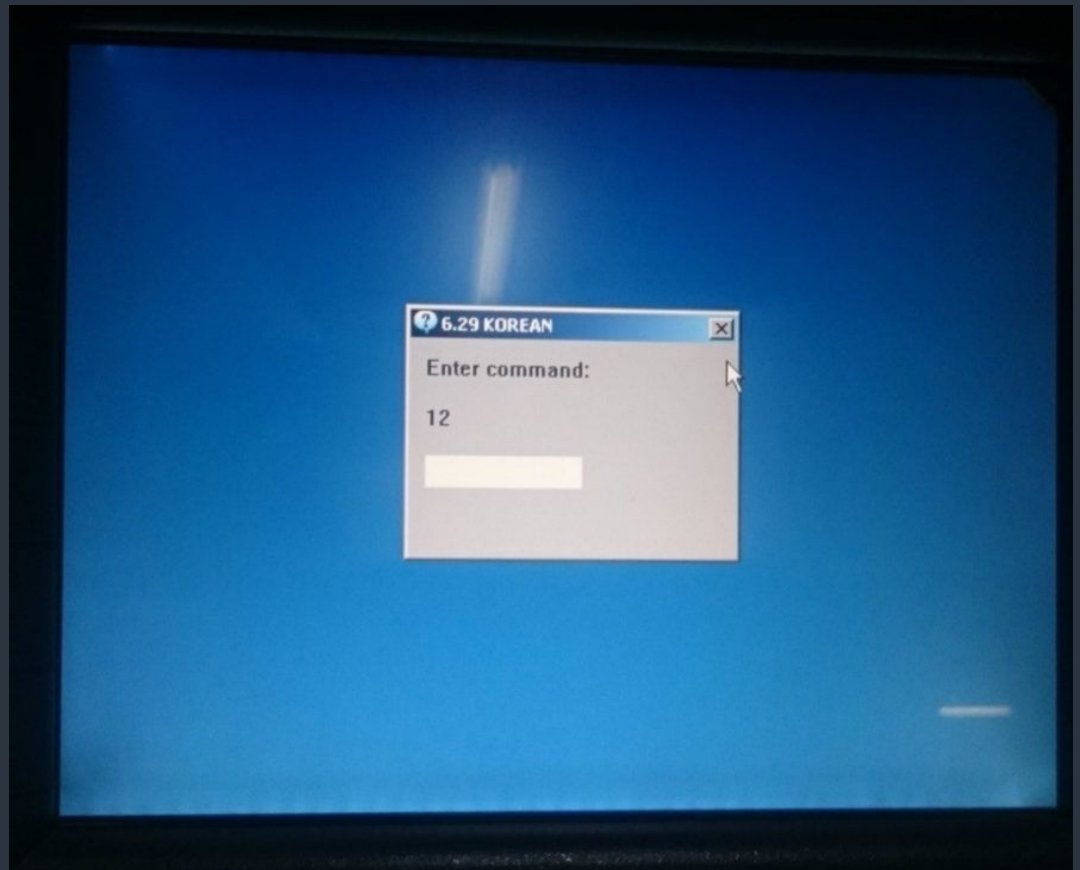
Skimmer - 2016


Turbo
BANK

Cómo funciona?

- SpiService.exe – servicio XFS (eXtensions for Financial Services). Instalado en todos los ATMs.
- Infección clásica del archivo como en caso de un “file infector”! Carga garantizada de la librería a la memoria.
- Los ATMs se infectan desde la red del Banco.

Tarjetitas “mágicas”



Tarjetitas “mágicas”

- Mostrar información detallada sobre el malware instalado;
- Entregar efectivo – 40 billetes del casete indicado;
- Comenzar la recolección de datos de otras tarjetas usadas en el ATM;
- Imprimir la información recolectada;
- Ejecutar el auto-borrado;
- Habilitar debugging;
- Ejecutar actualización (nuevo malware para actualizar se almacena en la tarjeta).

Tarjetitas “mágicas”

******446987512*=**********
******548965875*=**********
******487470138*=**********
******487470139*=**********
******000000000*=**********
******602207482*=**********
******518134828*=**********
******650680551*=**********
******466513969*=**********

Qué hacer?

1. **Educar al personal IT/Seguridad**
2. **Mejorar procesos e implementar nuevas tecnologías**
3. **Apoyarse en reportes de inteligencia!**

GRACIAS

Por su valioso tiempo y atención

Dmitry Bestuzhev, HEAD of Global Research and Analysis Team, Latinoamérica

Global Research and Analysis Team, América Latina

Dmitry.Bestuzhev@kaspersky.com, twitter.com/dimitribest