SEVENET

Trendy w atakach cybernetycznych na instytucje finansowe

Forum Technologii Bankowej, Jachranka 27.04.2016

Andrzej Nowodworski
Architekt Bezpieczeństwa IT

O czym będzie mowa?

SEVENET

1. Czy to się naprawdę dzieje?
2. Ataki skierowane na klientów banków
3. Ataki skierowane na infrastrukturę banków
4. Socjotechnika
5. Podsumowanie

Czy to się naprawdę dzieje?

SEVENET

The Hacker News™
Security in a serious way

Here's How Hackers Stole $80 Million from Bangladesh Bank

Monday, March 14, 2016 Swati Khandelwal

The recent cyber attack on Bangladesh's central bank tha
from the Institutes' Federal Reserve bank account was re
installed on the Bank's computer systems.

Few days ago, reports emerged of a group of unknown ha
central bank, obtained credentials needed for payment tr
New York and then transferred large sums to fraudulent
Sri Lanka.

EUROPE

How 100 Banks Got Hacked And Lost $900 Million

By PYMNTS

Posted on February 16, 2015

TWEET SHARE SHARE EMAIL

ldwide have been hit in a cyberheist that Russian cybersecurity firm **Kaspersky Lab** estimates could have netted as
n in stolen funds.

ras discovered in late 2013 when an ATM in Kiev went crazy and started dispensing cash at apparently random intervals
despite the fact that no one had touched the machine. Further investigation by Kaspersky indicated that a cash machine
ing piles of cash with little-to-no prompting was actually the absolute least of the bank's problems. The bank's real
ternal computers had been compromised by malware.

l on the back end of the bank's computer systems for months, sending back video feeds and images that gave a gang of
alth of information about how the bank carried out its daily routines, according to the investigators.

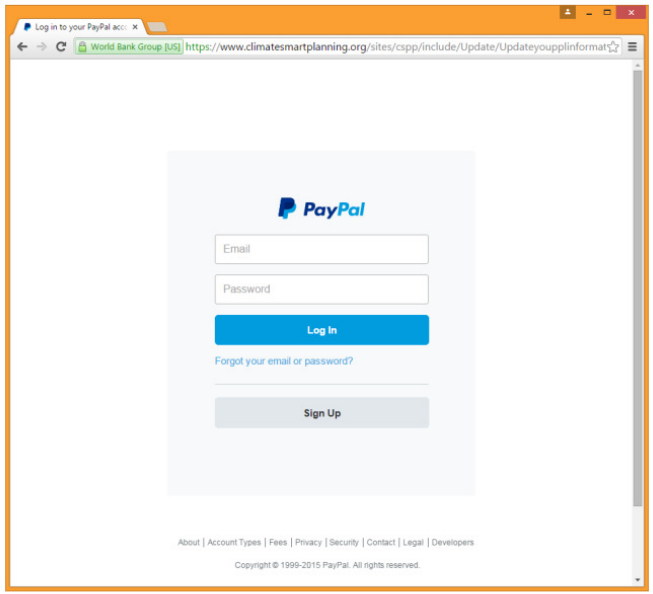
World Bank Site Hacked to Serve a Convincing PayPal Phishing Page

SECURITY 5 months ago by Shaikh Rafia

Tweet Like Share 14

Twitter
Facebook

The website of a World Bank's project site has been hacked and then exploited to host a very convincing PayPal phishing page.



World Bank project site hacked by two malicious actors:

Reports have revealed that the official website for the World Bank's Climate Smart Planning Platform was penetrated by hackers and then exploited to host a PayPal phishing site. The Climate Smart Planning project focuses on helping developing countries create and implement climate-smart policies.

Czy to się naprawdę dzieje?

SEVENET

Trash 2397 total Show: All Messages Search: pko in Current Folder

From	Subject	Date
Bank PKO BP <zoee@interlinegroup.com>	Nowa wiadomosc PKOBP	01/04/2016 15:47
PKO Bank Polski <jerry@mail.manti.com>	Wazna wiadomosc PKOBP	01/14/2016 18:25
Marek Wojciechowski Profes <biuro@najlepszydruk.com.pl>	Kupony zdrapkowe - zorganizuj loterię dla swoich klientów.	02/16/2016 13:04
Bank PKO BP <nbyegrjgjyqt@klampfer.com.ua>	***SPAM*** Autoryzacja konta iPKO	02/17/2016 17:32

DaTu
Inbox

From: Bank PKO BP <nbyegrjgjyqt@klampfer.com.ua>
To: a.nowodworski@datu.pl
Subject: ***SPAM*** Autoryzacja konta iPKO
Date: Wed, 17 Feb 2016 18:32:43 +0200 (*02/17/2016 05:32:43 PM*)

Data: 17.02.2016 r.

Dostęp do Twojego konta iPKO został zablokowany!

W trosce o bezpieczeństwo naszych klientów zablokowaliśmy konto w systemie iPKO, powodem jest nieautoryzowany dostęp do konta.
W celu odzyskania dostępu prosimy o weryfikację właściciela rachunku, logując się na:

www.ipko.pl

Serdecznie pozdrawiamy,
Zespół PKO Bank Polski

W przypadku jakichkolwiek pytań prosimy o kontakt z Infolinia 801 307 307

Ten e-mail został wygenerowany automatycznie. Prosimy na niego nie odpowiadać. Powszechna Kasa Oszczędności Bank Polski Spó
Rejonowym dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000026438;

Trash
Immunity
Mail
Contacts Calendar
Tasks Memos
Click to open http://iipko.ru/?email=a.nowodworski@datu.pl

Włamywacz spełnił groźbę i publikuje dane klientów Plus Banku

Adam dodał 12 czerwca 2015 o 23:04 w kategorii Włamania z tagami: Plus Bank • Polsilver • ToRepublic • włamanie • wyciek

Dzisiaj upłynął termin ultimatum przedstawionego Plus Bankowi, okradzionemu przez przestępców. Włamywacz, który najwyraźniej nie otrzymał okupu, opublikował dane pochodzące z kilkuset kont firmowych klientów Plus Banku.

To był tydzień, który na długo zapisze się w historii polskiej bankowości. Najpierw w poniedziałek ujawniliśmy, że polski bank padł ofiarą poważnego włamania, na skutek którego przestępcy mogli ukraść około miliona złotych oraz dane klientów banku. We wtorek przestępca ukrywający się pod pseudonimem Polsilver ogłosił, że ofiarą był Plus Bank i przedstawił ultimatum – albo do piątku otrzyma ofertę od banku (proponował 200 tysięcy złotych za milczenie), albo opublikuje dane klientów banku. Bank zapowiedział, że okupu nie zapłaci a przed chwilą na forum w sieci Tor pojawił się kolejny wpis Polsilvera zawierający zmodyfikowane żądania, fragmenty skradzionych danych oraz obietnicę przyszłych wycieków.

1. Phishing

2. Malware bankowy wstrzykujący swoje dane w kod strony banku (MitB)

3. Malware bankowy podmieniający numery rachunków w schowku, bądź pamięci komputera

Szybkie i krótkie demo
–
panel zarządzania Zeus'a.

1. Ataki profilowane
2. Zorganizowana przestępczość
3. Przykłady

“Łamałem ludzi, nie hasła”

Kevin Mitnick

Podsumowanie.

SEVENET

1. Nadal najłatwiejszym celem są klienci
2. Pomału ciężar ataków przenosi się także na banki
3. Ciągłe podnoszenie świadomości pracowników jest kluczem do skutecznego wykrywania incydentów
4. Sama technologia nie wystarcza
5. Bezpieczeństwo to proces, nie stan

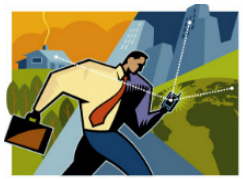
Kim jestem?

SEVENET

- **8 lat** doświadczenia w bezpieczeństwie teleinformatycznym
- **17 lat** doświadczenia w IT (sieci, telekomunikacja, bezpieczeństwo)
- Certified Ethical Hacker (**CEH**)
- Licensed Penetration Tester (**LPT**)
- Offensive-Security Cerified Expert (**OSCE**)
- Członek zespołów Red-Team'owych
- Penetration Tester
- Architekt, analityk systemów antyfraudowych
- Główny architekt systemu Web Fraud Protector
- Pasjonat zagadnień związanych z inżynierią odwrotną, IoT

C|EH Certified Ethical Hacker

OFFENSIVE SECURITY OSCE



L|PT Licensed Penetration Tester

?

SEVENET

DZIĘKUJĘ ZA UWAGĘ!