3-12-2008

Trouble in Florida: The Genesis of Phishing attacks on Australian Banks

Stephen McCombie
Macquarie University

DOI: 10.4225/75/57b2712140cbd
6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2008.

Trouble in Florida: The Genesis of Phishing attacks on Australian Banks

Stephen McCombie
Cybercrime Research Lab, Macquarie University
mccombie@ics.mq.edu.au

Abstract

Today Phishing of Internet banks is a well know problem and globally is responsible for more than US$3 billion in fraud annually. To date there has been limited research into the individuals and groups responsible for these attacks. Considerable anecdotal evidence exists to suggest that transnational organised crime groups are involved in Phishing. The involvement of these groups, particularly those operating out of Eastern Europe, is of concern given their sophistication and resources. Earlier work by CRL@mq looked at a month of Phishing against one Australian financial institution and clustering indicative of a small number of groups being responsible was seen. To get a better picture of the nature of the groups behind Phishing we now look back to the genesis of attacks against Internet banks. The first attacks against Australian banks started in March 2003 and were in fact the first attacks of this kind against Internet banks globally. We examine these incidents as a case study and look at the individuals and organisations involved. The circumstances behind these attacks are clearer now than might be imagined given none of the perpetrators were indentified at the time. We then briefly examine how much Phishing has changed in the intervening 5 years.

KEYWORDS

Computer crime case studies, cybercrime, Phishing, money laundering, e-crime, e-fraud, Internet banking fraud.

INTRODUCTION

Phishing is a well-known problem, accounting for as much as 1 out of every 281 Internet email messages in September this year (Messagelabs 2008). Gartner estimated that annual losses from Phishing attacks in the US alone went from USD$928 Million in 2005 (Litan 2005) to USD$3.2 Billion in 2007 (Gartner 2007). APACS, the UK payments association, reported UK online banking fraud was GBP£21.4 million in the first six months of 2008 (APACS 2008). Phishing attacks today are so frequent and numerous it is difficult to understand their true scope or to understand the actors behind them except in isolation. Earlier work at the Cybercrime Research Lab @ Macquarie University (CRL@mq) looked at Phishing against one Australian financial institution in July 2006 and examined the archival data available in that case (McCombie 2008). In that case study some clear indicators of a discrete number of attackers being involved in multiple was observed. That archival study examined data that covered just one organisation in one country over one month and as such a tiny portion of the total. Given that, this work is aimed at looking at an earlier time when Phishing was not an everyday occurrence against financial institutions, was little known and therefore relatively discrete. This time is very late 2002 to the middle of 2003. Examining archival material and other work from this period we get a picture of the circumstances behind this early Phishing and some insight into how and why it began the way it did. Surprisingly the participants behind the scenes may be easier to identify than we would

expect given no one has been arrested for these early attacks. However at that time the nature of the problem was little known and certainly not well understood. What now seem rather suspicious associations may have been completely missed by responders and law enforcement at the time.

The rise of Phishing has seen the "Black Hat" hacker community in recent years transformed from a culture based largely on youthful exploration to one focused on criminal profit. With that shift markets for "Phishing" tools, for "Botnets", for zero day vulnerabilities and compromised credentials have been established to support this highly organised criminal trade. Spammers, malware writers, hackers and organised crime have come together as never before. Extensive efforts to facilitate the laundering of the illicit earnings of these crimes have also been observed with third parties known as "mules" utilised along with the services of various companies, such as Western Union, which perform international wire transfers. These mules, often unwittingly, act as agents to forward and launder proceeds of Internet banking fraud using their own accounts. The money is then drawn out in cash by the mule and then wired overseas.

Considerable anecdotal evidence exists to suggest that transnational organised crime groups are involved in this "Phishing". Their alleged involvement in these attacks has received extensive coverage in the press with headlines like "Dutch Botnet Trio Reportedly Connected To Russian Mob" (Keizer 2005), "Return of the Web Mob" (Naraine 2006). The US President's Identity Theft Task Force, set up to combat Phishing and other identity, theft reported in 2007,

"Law enforcement agencies also have seen increased involvement of foreign organized criminal groups in computer - or Internet-related identity theft schemes (The President's Identity Theft Task Force 2007)."

Groups from Russian Federation, the Ukraine and Romania were identified by the US Secret Service as being responsible for a number of the attacks (The President's Identity Theft Task Force 2007). The involvement of transnational crime groups, particularly those operating out of Eastern Europe, is of concern given their sophistication and resources. For example, Galeotti (2006) suggests that former members of the Russian Federal Agency of Governmental Communication and Information (FAPSI) - whose role was similar to that of the US National Security Agency - were recruited by organised crime groups as computer hackers when FAPSI was disbanded in 2003. Notably, this was around the same time Phishing became a significant problem and this case study relates. Galeotti also suggests other former USSR states such as Latvia are being used by Russian gangs to commit phishing attacks (2005). In February 2007, Microsoft's Chief Security Advisor in the UK, Edward Gibson (a former FBI Agent), was quoted by Viruslist.com saying, "it's not the hacker crackers you have to worry about, but the Ukrainian mafia" (Kornakov 2007).

Some of the organised crime groups are believed to use legitimate enterprises they are involved in to support illegal activities. The large Russian organised crime group Tambov was believed to have used its petrol distribution company PTK's IT division to commit phishing attacks (Galeotti 2008). Some Russian IT organisations are also suspected of being purely being vehicles for Internet crime such as the now infamous Russian Business Network (Zenz 2007).
Russian organised crime first entered the United States in numbers in the 1980s and set up significant bases in Brighton Beach New York and in Miami Florida (Friedman 2000). This case study concerns three businesses based in Florida.

To date there has been limited research into the individuals and groups behind "Phishing". To effectively combat this problem we need to better understand the disposition and motives of these criminals. This paper aims to be a further step in delivering this important analysis to help government and industry address this problem.

PHISHING HISTORY

The term Phishing originated in 1996 to refer to a practice of tricking users into giving up their America On-Line (AOL) accounts to be used to distribute warez (pirated software) and other misuse. Originally the attacker would use instant messaging and purport to be an administrator from AOL. They would then ask users to provide their credentials. Later emails were used in a similar fashion. AOL actively policed the problem and by 2000 it all but disappeared (Ramzan 2007).

A NEW TYPE OF PHISHING

Starting in late 2002 a new style of Phishing attack began. The AOL phishers in the process of taking over AOL accounts had also got access to bank credit card details and they sometimes used them to use them to pay for services on the net (Ramzan 2007). Now taking the concept one step further, the target would be the banks themselves.

In 2000 despite the significant growth of Internet banking in a number of countries Internet banking fraud was virtually non-existent. Its notable that originally Commonwealth Bank of Australia's NetBank used a fat client and National Australia Bank's Internet Banking used client side certificates. These measures had been dropped by both these organisations by 2003.

While a number of observers have spoken of this change to Phishing most seem to indicate it started in the second half of 2003 or later (Grigg 2005)(Youl 2004)(James 2005)(Harley 2007) this research shows it was clearly happening in the first six months of 2003. The below timeline by Grigg shows Phishing switching to online banks in the end of 2003. It should be noted Grigg makes mention of two earlier attacks in his paper against e-Gold but this author was unable to find any references that support this or any other material to help understand the style of those early attacks (Grigg 2005).

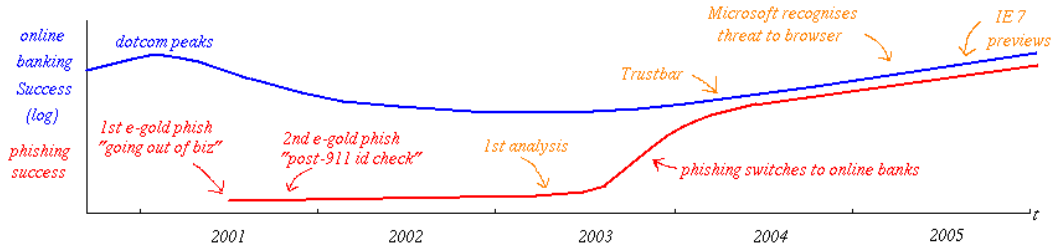


Figure 1 The Battle of Online Banking (Grigg 2005)

THE VICTIMS

E - GOLD

The first victim of new style of Phishing was Florida based E-Gold not an Internet Bank per se. E-Gold, who in recent years has seen its' directors charged with money laundering (Broache 2007), is an Internet global payment provider who backs each transaction in gold. Customers hold their balances in gold rather than currency. E-Gold is believed to have had organised crime figures as customers prior to the attack and this may be part of the reason they became the first victim of this style of phishing attack. Jeffrey Taylor, U.S. Attorney for the District of Columbia, would later characterise them as having,

"Criminals of every stripe gravitated to E-Gold as a place to move their money with impunity (Department of Justice 2007)"

On Saturday 28 December 2002 during the quiet Christmas New Year period an email purporting to be from E-Gold support was spammed out to a large number of Internet users. It's said,

"Dear Valued Customer

- Our new security system will help you to avoid frequently fraud

transactions and to keep your capitals in safety.

- Due to technical update we recommend you to reactivate your account.

Click on the link below to login and begin using

your updated e-gold account.

(Riley 2003)"

An email message like this is now a red flag to indicate a Phishing email, however despite the poor grammar, at the time it was a clever hook to get E-Gold credentials from customers. The web server hosting the Phishing page belonged to the IP range of 3d Wizards Hosting in Winter Park Florida on the address https://64.46.113.69/login.htm. The https certificate for that page belonged to cyberinvestigation.net, allegedly issued by ebizhostingsolutions.com (Riley 2003). E-Biz Hosting Solutions used some of the IP space of 3d Wizards and were also located in Winter Park Florida. One of the email samples seen by the author seems to have originated from a system at lsanca1-ar13-4-60-133-139.lsanca1.dsl-verizon.net [4.60.133.139] (Riley 2003). This appears to be a compromised system in the USA belonging to Verizon's DSL network.

COMMONWEALTH BANK OF AUSTRALIA

The next victim was as different an organisation from E-Gold as one could find. Commonwealth Bank of Australia (CBA) formerly a wholly government owned bank in Australia. It is the largest Australian bank with a $58.2 billion market capitalisation as of October 2008 (Zappone 2008). The one thing it did share in common with E-Gold is its early presence on the Internet and its more advanced functionality for users to transfer their money. On Monday 17 March 2003 an email was sent out purporting to be from "admins at Commonwealth Bank". It used much of the same text as the attack on E-Gold and was again hosted on an IP belonging to 3d

Wizards in Winter Park Florida on the address http://64.46.113.74/netbank/bankmain.htm. The Head of Security of the CBA was the former head of the Electronic Services Section of the Australian Federal Police (AFP) and he took no time in getting the AFP involved in investigating the matter. AFP agents from the Sydney office were assigned and in conjunction with NSW Police started an investigation. The law enforcement response was to follow the money. When compromised credentials were used and money transferred to a Croatian man recruited on a Croatian community website in Tasmania to be what would be later referred to as a "money mule". He was arrested by Police picking up the proceeds of one compromised account at a branch but as with money mules today was not able to identify the ultimate beneficiary of the fraud (Colley 2003). At the same time an apparent good citizen, Kevin Searle, who posted using the name Wombat to the news.admin.net-abuse.email newsgroup detailing the attack. He had contacted CBA indicating that this site was hosted on Florida and he also alerted Sydney Police and the Florida Computer Crimes Unit. Searle later told his story to Sam Varghese from the Sydney Morning Herald (Varghese 2003).

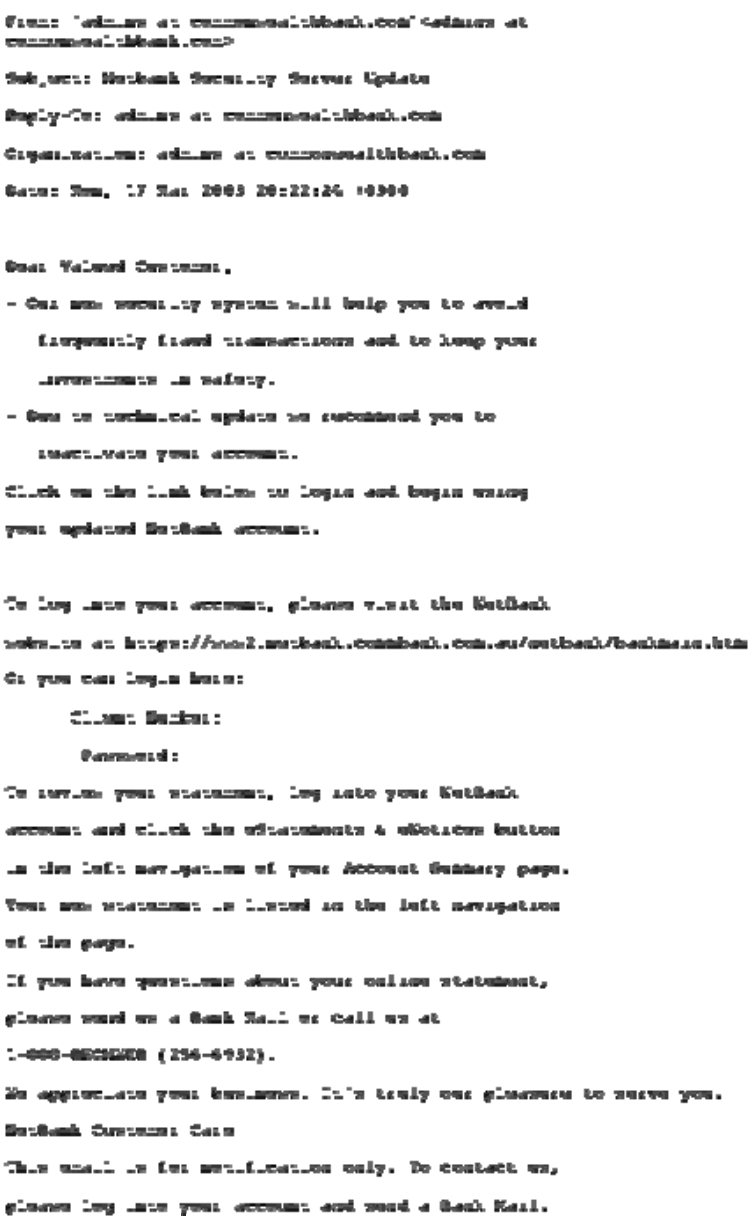
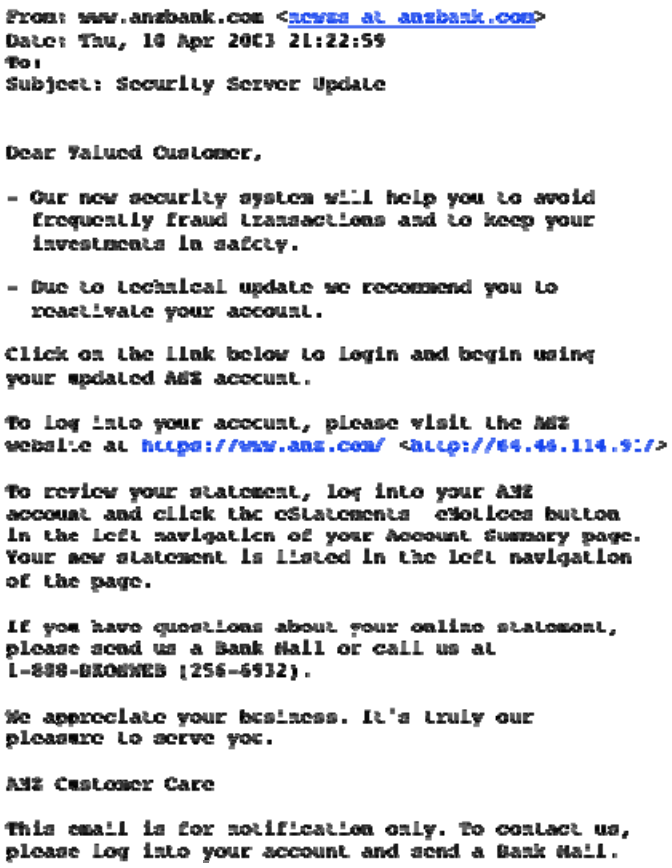


Figure 2 CBA email 17 May 2003 (Searle 2003)

ANZ

The Commonwealth Bank incident was publicised in the Australian and International media. Other Australian banks started to look at their vulnerability to similar attacks. They did not have to wait long. On 10 April 2003 another Phishing email was sent, this time targeting ANZ bank and coming from from "newzs at anzbank.com". ANZ Bank (Australia and New Zealand Bank) is Australia's third largest bank. The samples seen by the author originated from 0x50a104ef.virnxx9.adsl-dhcp.tele.dk [80.161.4.239] and d141-107-221.home.cgocable.net (d141-107-221.home.cgocable.net [24.141.107.221], which appear to be compromised systems in Denmark and the USA. The site was again hosted by 3d Wizards in Florida at the address http://64.46.114.91/ and used similar text the attacks of CBA and E-Gold. On its ftp port the server at that IP responded as server2013.ebizhostingsolutions.com. Another good citizen informed ANZ and passed on details of the hosting company and Adam Kling from E-Biz Hosting Solutions as a contact. ANZ contacted Adam Kling and asked for the site to be removed, which happened a few days after.



From: www.anzbank.com <newzs at anzbank.com>
Date: Thu, 10 Apr 2003 21:22:59
To:
Subject: Security Server Update

Dear Valued Customer,

- Our new security system will help you to avoid
  frequently fraud transactions and to keep your
  investments in safety.

- Due to technical update we recommend you to
  reactivate your account.

Click on the link below to login and begin using
your updated ANZ account.

To log into your account, please visit the ANZ
website at https://www.anz.com/ <http://64.46.114.91/>

To review your statement, log into your ANZ
account and click the eStatements eNotices button
in the left navigation of your Account Summary page.
Your new statement is listed in the left navigation
of the page.

If you have questions about your online statement,
please send us a Bank Mail or call us at
1-888-DIGENES (256-6932).

We appreciate your business. It's truly our
pleasure to serve you.

ANZ Customer Care

This email is for notification only. To contact us,
please log into your account and send a Bank Mail.

Figure 3 ANZ Phishing Email 10 April 2003 (Scheid 2003)

BANK OF AMERICA

While other Australian Banks became increasingly concerned about a potential attack the next Phishing incident moved offshore. On 12 May 2003 a Phishing email was sent out targeting Bank of America. It again used similar text to the attacks on E-Gold, CBA and ANZ. The site this time was hosted by Verio a large hosting provider registered in Colorado and Florida at the address http://198.173.235.126/index.htm.

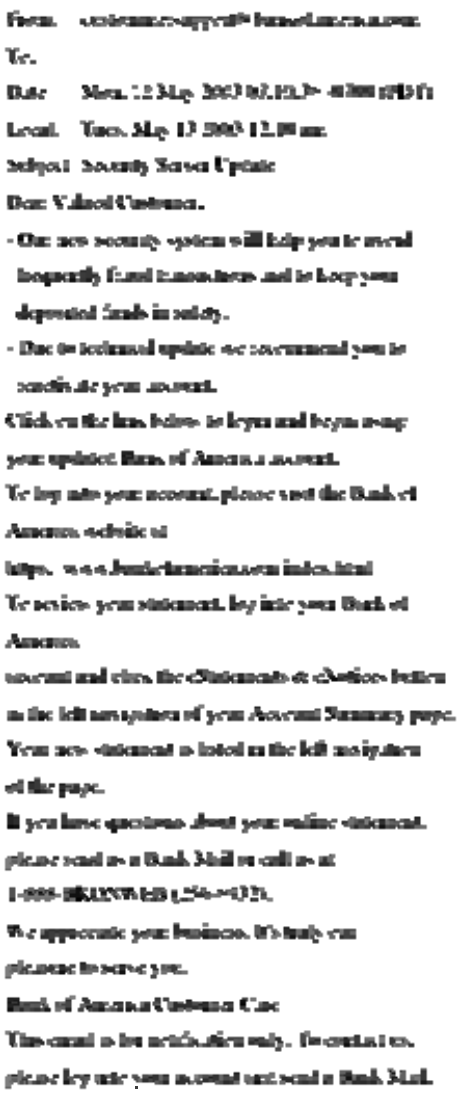


Figure 4 Bank of America Phishing Email 12 May 2003 (Jennings 2003)

WESTPAC

Australia's fourth-largest bank at this time was Westpac but was the second most popular on-line bank which had watched the recent events against its competitors Commonwealth Bank and ANZ closely. On 4 July 2003, US Independence Day they become subject of a Phishing attack. Again the same text was used as the previous banks and a site on IP space managed by 3d Wizards was involved using a domain belonging to E-Biz Hosting Solutions at the address http://d308902.website29.ebizdns.com/login.htm. A Westpac graphic was used in the html version of the email. Westpac reported the matter to the Australian Federal Police who were already engaged in the earlier ANZ and Commonwealth Bank incidents. Contact was made with E-Biz Hosting administrators via ICQ who turned out to be in Ukraine and the site was shut down after two days.

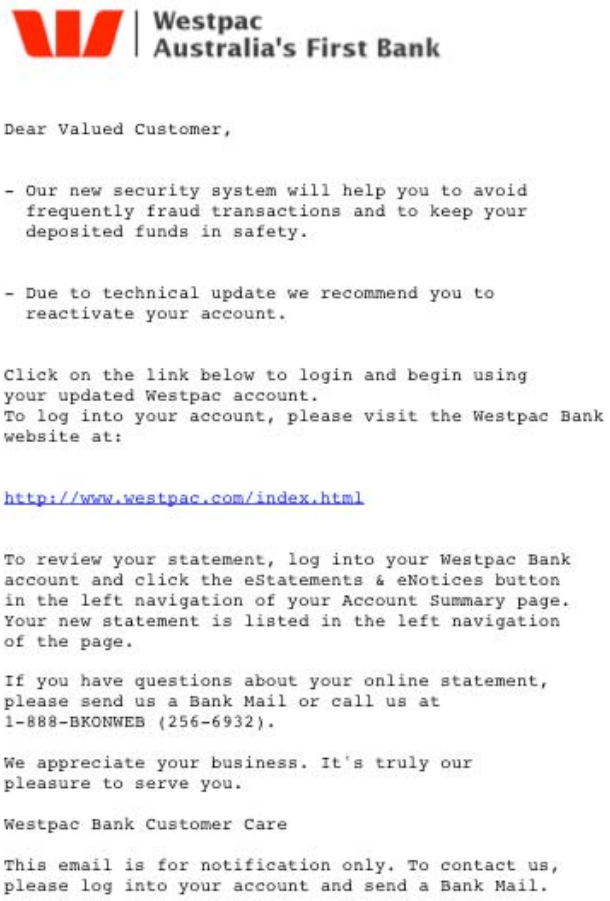


Figure 5 Westpac Phishing Email 4 July 2003 (Clapperton 2003)

Date	Victim	Subject	Phishing Site IP
28-Dec-02	e-Gold	Security Server Update	64.46.113.69
17-Mar-03	CBA	Netbank Security Server Update	64.46.113.74
11-Apr-03	ANZ	Security Server Update	64.46.114.91
12-May-03	Bank Of America	Security Server Update	198.173.235.126
4-Jul-03	Westpac	Security Server Update	64.46.100.64
4-Jul-03	ANZ	Security Server Update	64.46.113.208

Table 1 Selected List of Phishing Attacks 28/12/2002 to 4/7/2003

OTHER PHISHING ATTACKS IN THIS PERIOD

Two other Internet banks had Phishing attacks during this period. On 19 May 2003 after the Bank of America incident there was an attack on Citibank using a site at http://209.97.63.225/cgi-bin/webforms.pl (Rohrich 2003). Also in May there was an attack on First Union Bank part of Wachovia Corporation another large US Bank (Fisher 2003). There are limited details of these attacks available so it is unknown whether they are related to the six phishing attacks described above.

THE HOSTING COMPANIES

3D WIZARDS

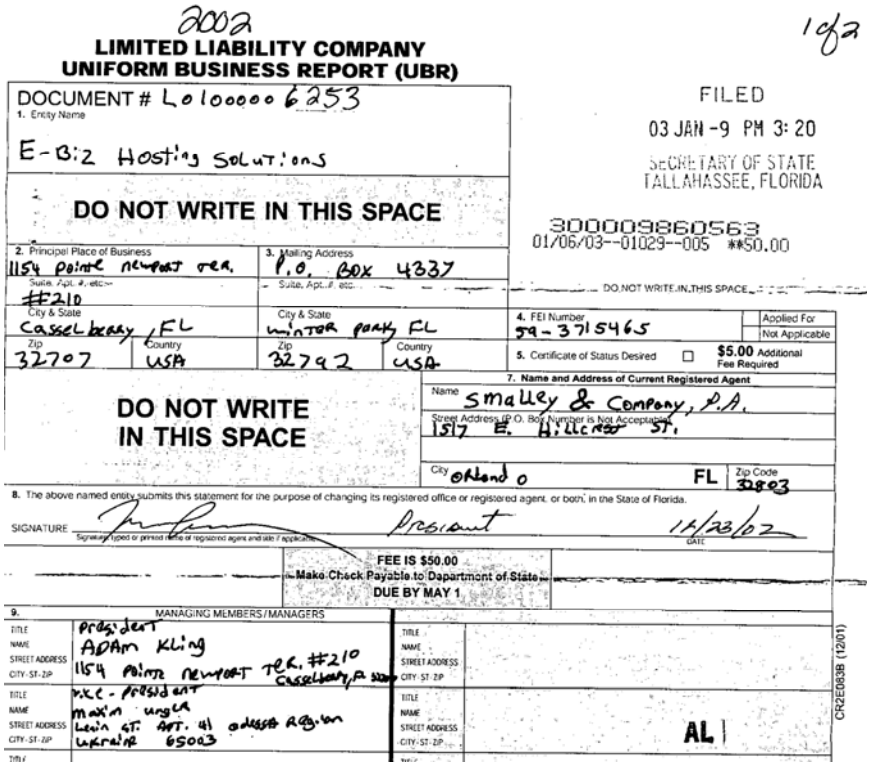
3d Wizards owned the IP space for five of the Phishing sites in this period and were part of DataColo, which was managed by Carlos Rego. The company was also known as Relio Ltd. It was based in Winter Park Florida.

DATACOLO

DataColo owned the larger block in which 3d Wizards block resided and similarly was managed by Carlos Rego. It was also based in Winter Park Florida.

E-BIZ HOSTING SOLUTIONS

E-Biz Hosting Solutions is also based in Winter Park Florida. It uses 3D Wizards IP space and was the domain owner of the domain used in the Westpac and both ANZ sites and appeared to have issued the https certificate for the e-Gold web site. It may well have used the other IPs associated the attacks that were part of 3d Wizards hosting space but this is unable to be confirmed. Adam Kling is listed in various documents as the President but the Vice-President is listed as Maxim Unger from Odessa Ukraine. Alex Mosh also from Odessa Ukraine is mentioned as CTO and employee in a number of newsgroup postings and is described in more detail below. A number of other Ukrainians or expatriate Ukrainians also seem to be associated with E-Biz Hosting Solutions in admin and sales roles according to Internet posts, including Tim Rogovets, Constantin Pogorelov and Kate Foteva.



2002

LIMITED LIABILITY COMPANY
UNIFORM BUSINESS REPORT (UBR)

1 of 2

DOCUMENT # L01000006253

1. Entity Name: E-Biz Hosting Solutions

FILED
03 JAN -9 PM 3:20
SECRETARY OF STATE
TALLAHASSEE, FLORIDA

300009860563
01/06/03--01029--005 **50.00

DO NOT WRITE IN THIS SPACE

2. Principal Place of Business: 1154 Pointe Newport Ter. #210, Casselberry, FL 32707, USA
3. Mailing Address: P.O. Box 4337, Winter Park FL 32792, USA
4. FEI Number: 59-3715465 (Applied For / Not Applicable)
5. Certificate of Status Desired ☐ $5.00 Additional Fee Required

DO NOT WRITE IN THIS SPACE

7. Name and Address of Current Registered Agent
Name: Smalley & Company, P.A.
Street Address (P.O. Box Number is Not Acceptable): 1517 E. Hillcrest St.
City: Orlando FL Zip Code: 32803

8. The above named entity submits this statement for the purpose of changing its registered office or registered agent, or both, in the State of Florida.
SIGNATURE: President DATE: 1/28/02

FEE IS $50.00
Make Check Payable to Department of State
DUE BY MAY 1

9. MANAGING MEMBERS/MANAGERS

TITLE: President	TITLE:
NAME: ADAM KLING	NAME:
STREET ADDRESS: 1154 Pointe Newport Ter. #210	STREET ADDRESS:
CITY-ST-ZIP: Casselberry, FL 32707	CITY-ST-ZIP:
TITLE: V.P. - President	TITLE:
NAME: maxim unger	NAME:
STREET ADDRESS: Lewa St. Apt. 41 odessa Region	STREET ADDRESS:
CITY-ST-ZIP: Ukraine 65003	CITY-ST-ZIP: AL

CR2E083B (12/01)

Figure 6 Florida Department of Commerce Filing for E-Biz Hosting Solutions (http://www.sunbiz.org)

THE INDIVIDUALS

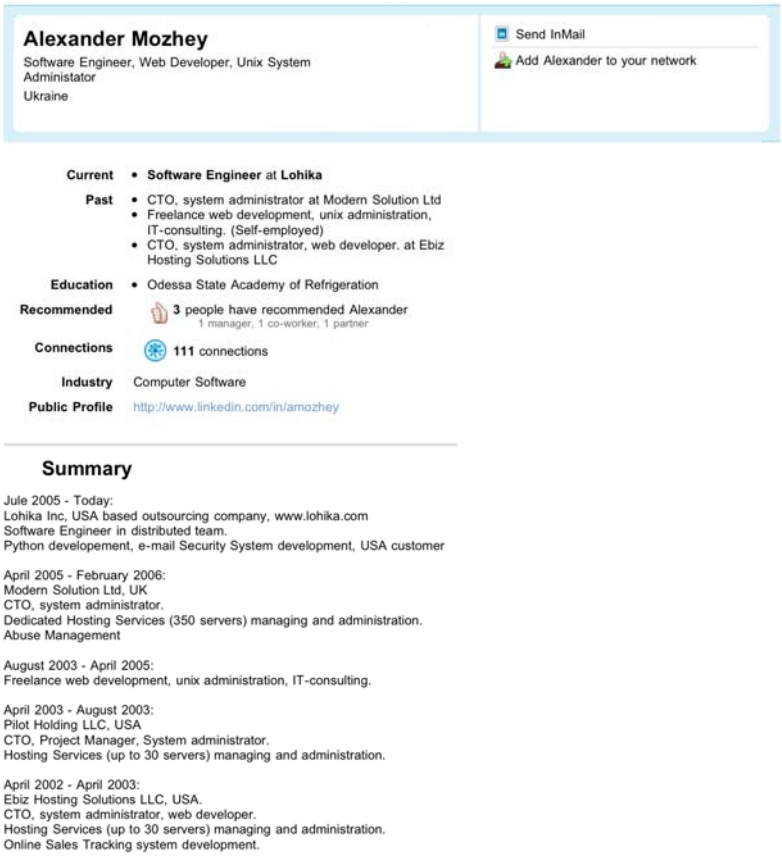
ADAM KLING

Adam Daniel Kling is listed as the President of E-Biz Hosting Solutions. On a number of the incidents 3d Wizards administrators and other upstream providers gave his name and contact number to responders and he was contacted to shut both the ANZ Phishing sites down. He appears to be a resident of Florida. How he came

to be working with Maxim Unger, Alex Mozhey (see below) and a number of others from the Ukraine is unknown.

ALEX MOZHEY, ALEX BLOOD, ALEX MOSH, ALEX POLYAKOV

Listed in a number of Internet news postings as an employee and CTO of E-Biz Hosting Solutions is Alex Mosh. Alex Mosh is listed on the spamhaus Register of Known Spam Organisations (ROKSO) top ten list as of spammers, currently No.3 as of 6 October 2008 (http://www.spamhaus.org/statistics/spammers.lasso). In 2007 he was listed No.1. He has a number of aliases including Alex Blood and Alex Polyakov. The name Alex Polyakov is a Russian spy character from John Le Carre's novel Tinker, Tailor, Spy, which may explain its use. Alex Mosh used an ICQ address when working for E-Biz Hosting Solutions, which now is used by an Alex Mozhey who lists in his linked-in profile that he indeed worked for E-Biz Hosting Solutions as CTO. In his profile Mozhey also lists being the CTO for Pilot Hosting, which is also associated with Alex Mosh and listed frequently by ROKSO in connection with spamming. Mozhey and Mosh are likely to be the same person.



Alexander Mozhey

Software Engineer, Web Developer, Unix System Administator

Ukraine

Send InMail

Add Alexander to your network

Current	• **Software Engineer** at **Lohika**
Past	• CTO, system administrator at Modern Solution Ltd • Freelance web development, unix administration, IT-consulting. (Self-employed) • CTO, system administrator, web developer. at Ebiz Hosting Solutions LLC
Education	• Odessa State Academy of Refrigeration
Recommended	**3** people have recommended Alexander 1 manager, 1 co-worker, 1 partner
Connections	**111** connections
Industry	Computer Software
Public Profile	http://www.linkedin.com/in/amozhey

Summary

Jule 2005 - Today:
Lohika Inc, USA based outsourcing company, www.lohika.com
Software Engineer in distributed team.
Python developement, e-mail Security System development, USA customer

April 2005 - February 2006:
Modern Solution Ltd, UK
CTO, system administrator.
Dedicated Hosting Services (350 servers) managing and administration.
Abuse Management

August 2003 - April 2005:
Freelance web development, unix administration, IT-consulting.

April 2003 - August 2003:
Pilot Holding LLC, USA
CTO, Project Manager, System administrator.
Hosting Services (up to 30 servers) managing and administration.

April 2002 - April 2003:
Ebiz Hosting Solutions LLC, USA.
CTO, system administrator, web developer.
Hosting Services (up to 30 servers) managing and administration.
Online Sales Tracking system development.

Figure 7 Alexander Mozhey's Linked-in profile (http://www.linkedin.com)

Mosh's ROKSO record also connects him with money laundering or money mules and now acknowledged as a key part of Phishing. Mosh's ROKSO record lists website Verimer-australia.com used in 2005 for recruiting money mules in Australia and is connected with the entities and pseudonyms used by Alex Mosh.

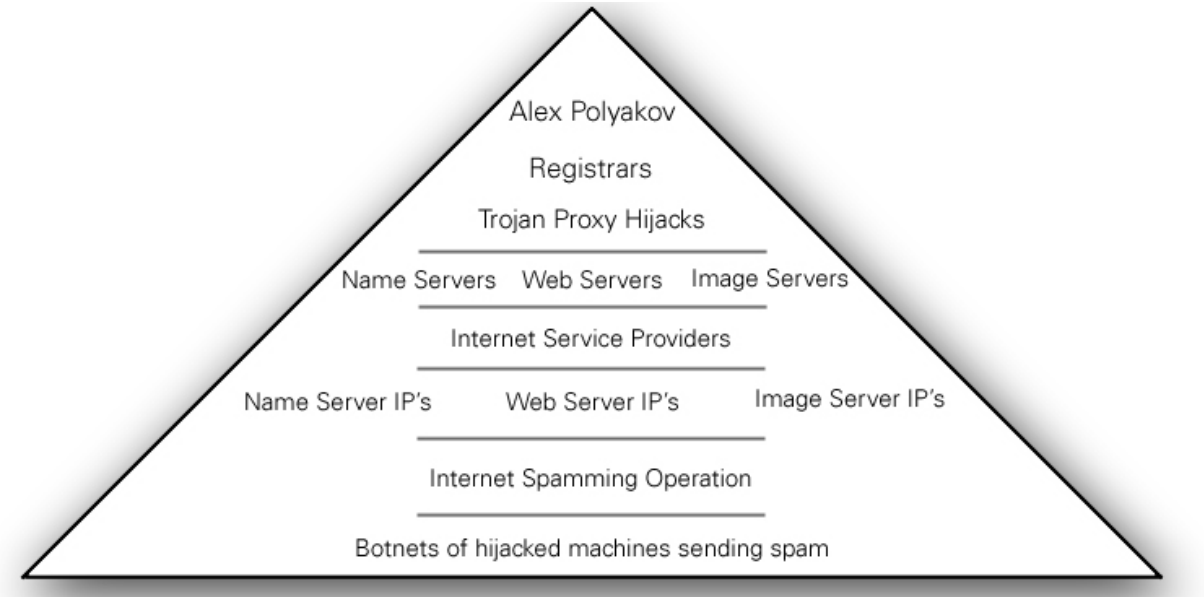


Figure 8 Alex Polyakov Internet Operation (http://spamtrackers.eu/wiki/index.php?title=Alex_Polyakov)

Mozhey in his linked-in profile amongst his skills are, "Good knowledge of Payment/Billing Systems, CC (credit card) processing, Merchant Gateways". He also indicates past experience in "Abuse management". Both he names Alex Mozhey and Alex Mosh are also connected with the nickname Deir that uses the same ICQ address and in some places Mozhey's actual name. Deir is a member a Parallels Forum. Below Deir signs himself as Alex Mosh CTO Ebiz Hosting Solutions LLC in that forum.

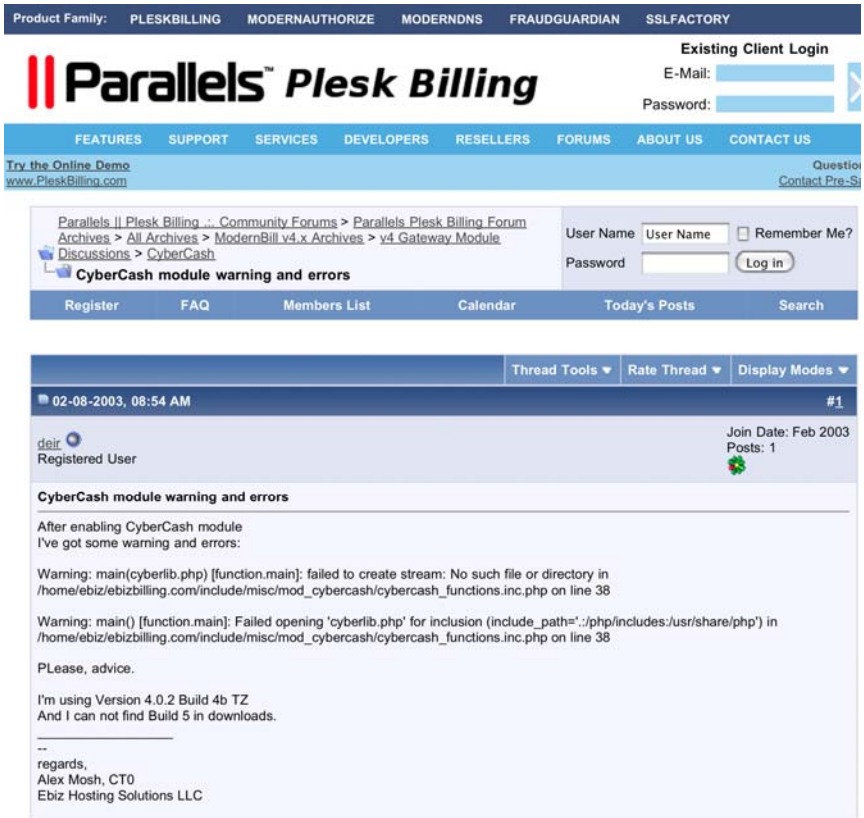


Figure 9 Posting by Alex Mosh to Parallels Forum (http://forums.modernbill.com/member.php?u=757)

CARLOS REGO

Carlos Rego was the CEO of 3dWizards Hosting and DataColo and in 2003 lived in Florida. He has a blog and uses the handle nullmind. Amongst his postings he refers to the day in September 2003 when the FBI came to the DataColo office apparently in connection with the aforementioned Phishing incidents.

"Today the FBI came by the office to pickup some logs on a scammer that was hosting with us, after taking his site down we kept all the info and logs on him .. I hope they catch the sucker. Basically the user had a fake e-gold site, he would send emails out to people saying they need to verify their e-gold accounts, people then would go to HIS site and enter their details and pin numbers :p ouch ..

Null (http://nullmind.com/2003/09/)"

Rego only mentions E-Gold but it is believed this FBI visit was also a result of an international mutual assistance application from the AFP on behalf of the Australian banks impacted by these early Phishing attacks. According to Carlos's linked-in profile and Internet news items since leaving DataColo he has worked for Comodo, Positive Software and successful virtualisation software maker Parallels. All these organisations seem to have strong links to Russia and/or Ukraine. For instance Parallels CEO Serguei Beloussov studied for his Ph.D. in Computer Science at the Moscow Institute of Physics and Technology and the company has development centres in Russia and Ukraine. There is nothing suspicious in this but clearly Rego has a large degree of contact with Ukrainians and Russians in his business life.

Again it is not known how Rego who was born in Portugal and now lives in the United Kingdom came to be working with these individuals from Eastern Europe.

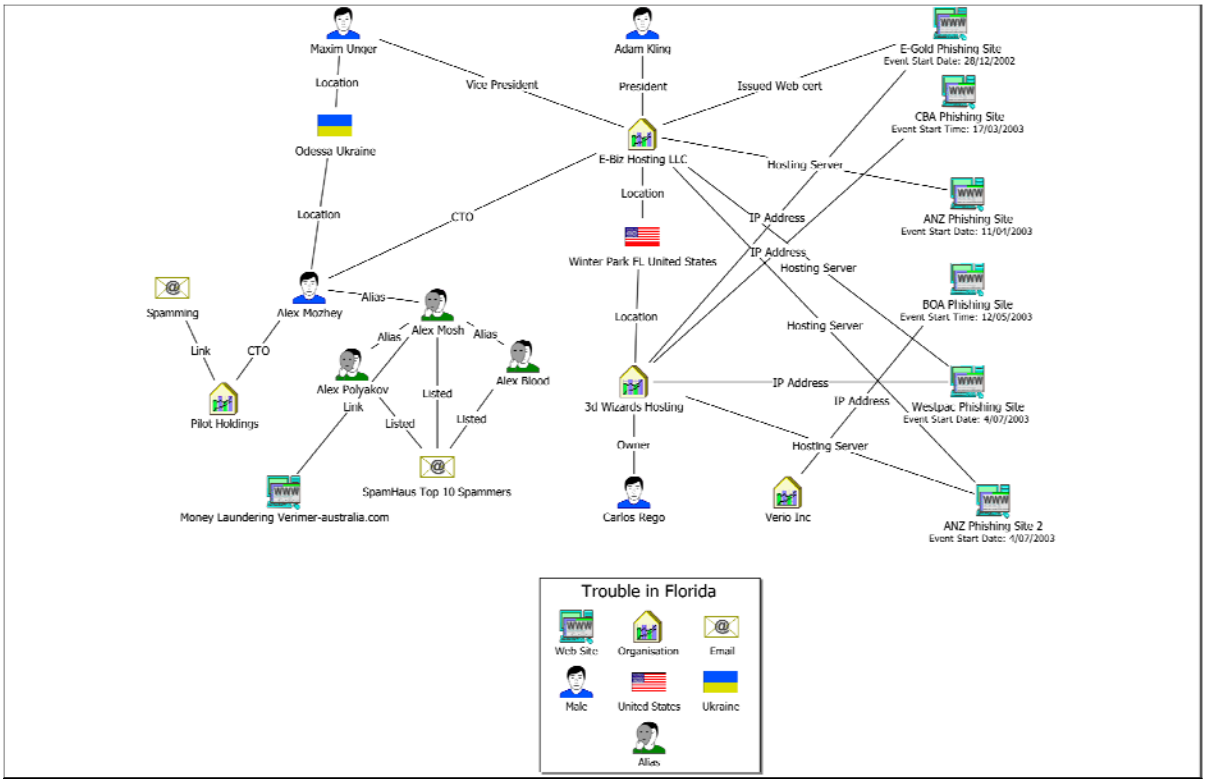


Figure 10 Relationships with Internet Bank Phishing Attacks Late 2002 to July 2003

WHAT HAPPENED AFTER JULY 2003?

Detailed figures on Phishing attacks were only collected towards the end of 2003. Judging from press reports and the documented histories of Phishing attacks; they did increase in numbers from August to the end of 2003 with more brands being targeted, including numerous UK and US Internet Banks. The earliest statistics from APWG Anti Phishing Working Group (APWG) show 21 phishing incidents in the month of November 2003

(APWG 2004). The phishing sites at this time were primarily located at large web hosting providers whose systems were apparently compromised and used to set up the sites. This method continued for some years even being the main method observed during the examination of phishing attacks in July 2006 on one Australian financial institution (McCombie 2008). The number of attacks increased into 2004 and has continued to increase to date, see below for the most recent figures.

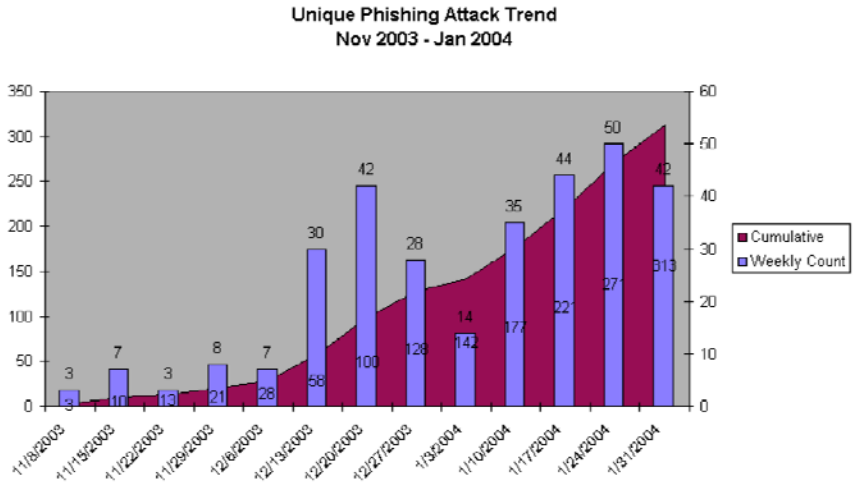


Figure 11 Unique Phishing Attack Trend Nov 2003 to Jan 2003 (APWG 2004)

HOW IS PHISHING DIFFERENT IN 2008?

Today many aspects of Phishing have changed. Phishing sites are now almost always found on Botnets. While Botnets certainly existed in 2003 they were far less common. Their use provides greater redundancy and is also more resilient to take down requests by the victim banks and their service providers. There is also a greater use of password stealing malware (crimeware as it is now described) to compromise users of Internet banks, which is again delivered using Botnets. Since 2004 the significance of crimeware has grown. For the month of March 2008 APWG reported 356 new unique password stealing malicious code applications (APWG 2008).

The ability of the Phishing sites to dupe unwitting users has reduced over time as user education and the shear volume of Phishing emails made knowledge of Phishing mainstream. However the attacks continue as they rely on only a small rate of success. In 2006 APACS the UK payments association working on behalf of the banking industry commissioned research agency Canvasse Opinion from Experian to poll a representative sample of 1,835 adults aged 18 and over, who have access to the Internet across the United Kingdom. Their results were,

"If we extrapolate for the 15.7 million people (in the UK) who regularly use the Internet to access their current, savings and credit card accounts as:

- 3.8% (an estimated half a million people) said they would still respond to an unsolicited email asking them to follow a link and re-enter personal security details, supposedly from their bank, unwittingly giving fraudsters access to their account (this is slightly down from 4% in 2004)."

Despite the fact that at the time of this survey Phishing had been widely known for 3 years a return of 3.8% shows us why Phishing sites still appear, in fact, APWG reported over 25,000 unique Phishing attacks attacking 139 different brands in February 2008 alone (APWG 2008).

WHAT CAN WE LEARN FROM THIS CASE STUDY

While not conclusive this case study shows there is some evidence to support the thesis that East European groups involved in spamming branched into Phishing and other online crime in 2003. Further research into the involvement of East European IT companies in on-line crime is needed. The trend in traditional Eastern European organised crime and indeed other transnational organised crime to move illegal profits into legitimate enterprises may well have extended to the cybercrime area but further work is needed to confirm this. Regardless there is clearly availability of IT skills within Eastern Europe to support both legal and illegal IT

businesses and the challenge for those countries and the broader European community is to ensure organised cybercrime groups do not get a foot hold in legitimate industries.

Why did Australian Banks figure so significantly in these attacks? One likely reason is that Australian Internet banks had much greater functionality for payments than those in the US and most of the rest of the world at that time. Westpac for instance actually allowed Overseas Telegraphic Transfers (OTTs) to overseas banks direct from their Internet Banking in 2003. This allowed phishers to move the money straight from compromised accounts to banks in Eastern Europe. So Australian Internet banks were indeed world leading but in ways that were not intended.

CONCLUSION

Further work is required to better understand these early attacks but we hope this will start further research in this area. The author would have liked to interview more individuals involved but many were either unreachable or unable to comment on the events so this case study has been developed looking mostly at news reports and archival material available on the Internet from a number of sources and from the author's personal knowledge of events. While this approach has its shortcomings it was felt this case study was worth relating even on this limited information. We hope in future research to conduct further interviews with those involved and obtain more archival data on the organisations involved for more in depth analysis of these events.

REFERENCES

APACS (2008) *APACS announces latest fraud figures*. Retrieved 20 March 2007 from http://www.apacs.org.uk/APACSannounceslatestfraudfigures.htm

APWG (2004) *Phishing Attack Trends Report January, 2004.* Retrieved 9 October 2008 from http://www.antiphishing.org/reports/APWG.Phishing.Attack.Report.Jan2004.pdf

APWG (2008) *Phishing Activity Trends Report Q1/2008.* Retrieved 9 October 2008 from http://www.antiphishing.org/reports/apwg_report_Q1_2008.pdf

Broache, A. (2007) *E-Gold charged with money.* Retrieved 9 October 2008 from http://news.cnet.com/2100-1017_3-6180302.html

Clapperton, D. (2003) *[Oz-ISP] Westpac online banking scam in progress.* Retrieved 15 October 2008 from http://archive.humbug.org.au/aussie-isp/1057285342.54415.28.camel%40inferno

Colley, A. (2003) *NetBank suspect nabbed in Sydney.* ZDnet Australia. Retrieved 9 October 2008 from http://m.zdnet.com.au/120273072.htm

Department of Justice (2007) *Digital Currency Business E-Gold Indicted For Money Laundering And Illegal Money Transmitting.* DOJ press release. Retrieved 9 October 2008 from http://www.usdoj.gov/criminal/cybercrime/egoldIndict.htm

Fisher, D. (2003) *First Union Hoax on the Loose.* Retrieved 15 October 2008 from http://www.eweek.com/c/a/Messaging-and-Collaboration/First-Union-Hoax-on-the-Loose/

Friedman, R. (2000) Red Mafiya: How the Russian Mob has invaded America, New York. Penguin Putnam

Gartner (2007) *Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks*. Retrieved 9 October 2008 from http://www.gartner.com/it/page.jsp?id=565125

Galeotti, M. (2005). *Russian mafiya become more active in Eastern Europe*. Jane's Intelligence Review - June 01, 2005

Galeotti, M. (2006). *The Criminalisation of Russian State Security*. Global Crime Volume 7 (Number 3-4): August-November 2006.

Galeotti, M. (2008) Interview with the Author.

Grigg, I. (2005) *GP4.3 - Growth and Fraud - Case #3 – Phishing.* Retrieved 9 October 2008 from http://www.financialcryptography.com/mt/archives/000609.html

Harley, D. (2007) *A Pretty Kettle of Phish*. Retrieved 9 October 2008 from http://www.eset.com/download/whitepapers/Phishing(June2007)Online.pdf

James, L. (2005). Phishing Exposed, Rockland MA Syngress Publishing.

Jennings, I. (2003) [fraud?] Security Server Update. Retrieved 15 October 2008 from http://groups.google.com.au/group/news.admin.net-abuse.sightings/browse_thread/thread/b2cbf3154a916d14/41aabb11fdcc8067?hl=en)aabb11fdcc8067

Keizer, G. (2005). *Dutch Botnet Trio Reportedly Connected To Russian Mob.* Retrieved 24 January 2007 from http://www.techweb.com/article/showArticle.jhtml?articleId=173600331&pgno=1

Kornakov (2007) *Gibson offers sneak peek into his world.* Retrieved 2 March 2007 from http://www.cambridge-news.co.uk/business/news/2007/02/06/ca10f0fb-fa50-4e49-b8d4-51b8c359075a.lpf

Litan, A. (2005). *Increased Phishing and Online Attacks Cause Dip in Consumer Confidence.* Gartner Research. Gartner.

McCombie, S., Watters, P.A., Ng, A. & Watson, B. (2008) *Forensic Characteristics Of Phishing – Petty Theft or Organized Crime?*, Proceedings of the 4th International Conference on Web Information Systems and Technologies (WEBIST), Madeira, Portugal.

Naraine, R. (2006) *Return of the Web Mob.* Retrieved 20 March 2007 from http://www.eweek.com/article2/0,1895,1947561,00.asp

Ramzan Z. (2007) *A Brief History of Phishing: Part I*, Retrieved 9 October 2008 from https://forums.symantec.com/syment/blog/article?message.uid=306505

Rohrich R. (2003) *CRIME Fwd: Your account is On Hold.* Retrieved 15 October 2008 from http://lists.jammed.com/crime/2003/05/0044.html

Riley D. (2003) *Security Server Update.* Retrieved 15 October 2008 from http://groups.google.com/group/news.admin.net-abuse.sightings/browse_thread/thread/c3c46036499f48f7/95565cf69675334d?hl=encf69675334d

Searle, K. (2003) Netbank Security Server Update (Commonwealth Bank scam Australia) host in FL. Retrieved 15 October 2008 from http://groups.google.com/group/news.admin.net-abuse.email/msg/11f128a770befb15?hl=en

Scheid E., (2003) *FW: Security Server Update.* Retrieved 15 October 2008 from http://mailman.anu.edu.au/pipermail/link/2003-April/049438.html

Schultz, E. (2003) *Email hoaxes continue to deceive users*. In Computers & Security,Volume 22, Issue 5, July 2003, Pages 368-377

The Presidents Identity Theft Task Force. (2007) *Combating Identity Theft: A Strategic Plan.* Retrieved 10 May 2007 from: http://www.idtheft.gov/reports/StrategicPlan.pdf.

Varghese, S. (2003) *NetBank scam: why didn't Commonwealth Bank do the obvious?* Sydney Morning Herald. Retrieved 9 October 2008 from: http://www.smh.com.au/articles/2003/03/19/1047749811735.html

Youl, T. (2004) *Phishing Scams: Understanding the latest trends.* Retrieved 9 October 2008 from http://www.fraudwatchinternational.com/pdf/report.pdf

Zenz, K. (2007) *Uncovering Online Fraud Rings: The Russian Business Network.* Retrieved 9 October 2008 from http://labs.idefense.com/intelligence/researchpapers.php

COPYRIGHT