3-12-2009

Cybercrime Attribution: An Eastern European Case Study

Stephen McCombie
Macquarie University

Josef Pieprzyk
Macquarie University

Paul Watters
University of Ballarat

DOI: 10.4225/75/57b2880840ccf
7th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2009.

Cybercrime Attribution: An Eastern European Case Study

Stephen McCombie[1]
Josef Pieprzyk[2]
Paul Watters[3]

Macquarie University
mccombie@science.mq.edu.au[1]
josef@science.mq.edu.au[2]
University of Ballarat
p.watters@ballarat.edu.au[3]

Abstract

Phishing and related cybercrime is responsible for billions of dollars in losses annually. Gartner reported more than 5 million U.S. consumers lost money to phishing attacks in the 12 months ending in September 2008 (Gartner 2009). This paper asks whether the majority of organised phishing and related cybercrime originates in Eastern Europe rather than elsewhere such as China or the USA. The Russian "Mafiya" in particular has been popularised by the media and entertainment industries to the point where it can be hard to separate fact from fiction but we have endeavoured to look critically at the information available on this area to produce a survey. We take a particular focus on cybercrime from an Australian perspective, as Australia was one of the first places where Phishing attacks against Internet banks were seen. It is suspected these attacks came from Ukrainian spammers. The survey is built from case studies both where individuals from Eastern Europe have been charged with related crimes or unsolved cases where there is some nexus to Eastern Europe. It also uses some earlier work done looking at those early Phishing attacks, archival analysis of Phishing attacks in July 2006 and new work looking at correlation between the Corruption Perception Index, Internet penetration and tertiary education in Russia and the Ukraine. The value of this work is to inform and educate those charged with responding to cybercrime where a large part of the problem originates and try to understand why.

Keywords
Cybercrime. Phishing. Eastern European Organised Crime.

INTRODUCTION

Phishing and related cybercrime is responsible for annual losses of billions of US dollars. Gartner reported more than 5 million U.S. consumers lost money to phishing attacks in the 12 months ending in September 2008. They have estimated the losses in the US alone were over USD$7.5 Billion between September 2005 and September 2008 (Gartner 2009). While the claims by a US treasury official that global cybercrime is more lucrative than illegal drugs and was estimating at USD$105 Billion in 2004 are rather difficult to assess (Reuters 2005) there is clearly a large illegal and successful criminal industry online. The United States Government's October 2007 International Organized Crime Threat Assessment (US Department of Justice 2008) saying, "International organized criminals use cyberspace to target U.S. victims and infrastructure, jeopardizing the security of personal information, the stability of business and government infrastructures, and the security and solvency of financial investment markets."

This paper looks at the part in this that individuals and groups based out of Eastern Europe play and whether the majority of organised phishing and related cybercrime indeed originates in Eastern Europe rather than elsewhere and why. With the end of communism, Eastern Europe has seen massive changes and with the resulting power vacuum in many countries organised crime have gained prominence. The Russian Mafiya in particular has been popularised by the media and entertainment industries to the point where it can be hard to separate fact from fiction. While hard data is limited on this phenomenon, there is considerable anecdotal evidence to suggest that transnational organised crime groups from Eastern Europe are significantly involved in Phishing and related cybercrime. Their alleged involvement in these attacks has received extensive coverage in the press with headlines like "Dutch Botnet Trio Reportedly Connected To Russian Mob" (Kreizer 2005), "Return of the Web Mob" (Naraine 2006). However a leading security researcher and vendor Eugene Kaspersky (from Russia himself) charged that the view of the Russian Mafiya and Russians more generally being behind cybercrime was a "myth" (Sturgeon 2006) and that most attacks came from China and the US. While the authors agree there is a degree of mythology around the issue there is some solid information pointing to the significant role Eastern Europeans' particularly Russians and Ukrainians play in the cybercrime world. This paper consists of a survey of information available on this area build from case studies where there is some nexus to Eastern Europe including

looking at the first phishing attacks on Internet Banks in 2003 (McCombie 2008). We also look at other indicators including the identity of leading spammers who are key part of the cybercrime business and other information such as the views of law enforcement, which also seems to support this thesis. We then re-examine some archival data on 77 phishing attacks on one Australian institution in July 2006 used in work published in 2008 (McCombie 2008). Lastly we examine the correlation of a low corruption perception index, high Internet penetration, high tertiary education levels and Eastern European cybercrime. In this work we take a particular focus on cybercrime from an Australian perspective and a lot of our data relates to the Australian experience. While this is convenient for Australia based researchers it also is relevant to understand that Australia was one of the first places where Phishing attacks against Internet banks were seen. This attack as we will discuss was, rather than a home grown problem, suspected to have originated from the Ukraine by a known spammer. To date there has been little research into the individuals and groups behind Phishing and related cybercrime. To effectively combat this problem we need to understand the disposition and nature of these criminals. This paper aims to be one step in delivering this important analysis to help government and industry address this problem.

A SURVEY OF EASTERN EUROPEAN ORGANISED CRIME & CYBERCRIME

A SHORT HISTORY OF EASTERN EUROPEAN ORGANISED CRIME

While this paper is focused on cybercrime, Eastern European crime is a much broader and more complex topic. However any examination of Eastern European cybercrime would be incomplete without some background of this broader issue. The Hollywood image of the ruthless Russian mafiya man who unlike the Italian Mafiosi is happy to kill not just opponents but their family members too is truly fiction but one retold so often it is almost treated as fact (Serio 2008). However there is a long history of organised crime in Russia and Eastern Europe. In the times of the Tsar well before the October Revolution of 1917 organised crime groups stole horses and moved them all over the then Russian empire for sale. After the revolution these early groups while imprisoned, sort to differentiate themselves from the political prisoners whose numbers during Bolshevik rule grew substantially. By the 1930s this Russian criminal class were known as the Vory v Zakone "Thieves in Law" and is well documented (Varese 2001). They flourished under the often corrupt Communist system where bribery and the black market were key elements of the society. With the end of communism and the privatisation of government enterprises these traditional crime gangs, along with groups of Afghan war veterans and some former state security agents became what is now collectively known as the Russian Mafiya. According to the Ministry of Internal Affairs of the Russian Federation, between 1990 and 2001 the number of organised groups and criminal societies (criminal organisations), increased almost 16-fold, from 785 to approximately 12,500 (Abramova 2007). These new groups used force where the lack of the rule of law meant this was an important business tool. They also provided real protection where law enforcement was either corrupt or simply disinterested to protect new business entities. In fact many of the leading gangs such as Tambov in St Petersburg became a legitimate security providers to business (Volkov 2002). By 2005, it was estimated by a Council of Europe Organised Crime Situation Report (2005) that there were 300–400 really important criminal groups within the Russian Federation, with 15 of them operating significant criminal network structures (Ridley 2007).

THE CRIMINALISATION OF RUSSIAN STATE SECURITY

A feature of Eastern European organised crime is the criminalisation of the state security apparatus as their influence has grown. This has occurred partly by convenience and as many former state security agents actually joined the Mafiya themselves some while keeping their day jobs. Tambov, mentioned above, is known to have close links with Prime Minister Vladmir Putin's security detail (Volkov 2002). Mark Galeotti (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. Interviews conducted by IDefense indicated that Russian and other Eastern European police had little interest in pursuing cybercriminals who commit no crimes at home (Zenz 2007). In 2000, the FBI lured two Russian hackers (who tried to blackmail Michael Bloomberg) to Seattle with job offers, then arrested them. Agents involved in the case later downloaded data from the duo's computers, located in Chelyabinsk, Russia, over the Web. Rather than assist the investigation two years after that, Russia filed charges against the FBI agents for hacking alleging the downloads were illegal (Grow 2005). The 2007 arrest of Vladimir Earsukov, aka Vladimir Kumarin, of the Tambov crime family, was handled by top-level FSB officials due to concerns about local police collusion with organised crime in St Petersburg (Overseas Security Advisory Council 2009). A high ranking member of the Ukrainian Ministry of Internal Affairs noted that although the number of Ukrainian organized crime groups had steadily decreased the remaining groups were difficult to eradicate because of their strong connections with state officials (Finckenauer and Schrock 2004).

MODERN TRADITIONAL RUSSIAN SPEAKING ORGANISED CRIME

Russian organised crime is more correctly Russian speaking organised crime. Gangs exist outside of the Russian Federation in other former Soviet Union countries such as Ukraine, Latvia and Moldova where many ethnic Russians live. With its relatively large ethnic Russian population Latvia's underworld is dominated by gangs rooted in this ethnic Russian community, typically linked with larger gangs in Moscow and St Petersburg. Latvia is reported to be an increasingly important location for computer-based criminal activities, including phishing attacks (Galeotti 2005). In Russia one of the most prominent gangs is led by Sergei Mikhailov. The Moscow-based Mikhailov's Solntsevskaya Organization owns banks, casinos, car dealerships, and even an airport. Solntsevskaya is believed to be behind many cyber-related online crime activities (Nomad 2005). In St Petersburg the Tambov, Kazan, and Malyshev crime families are the three major criminal organizations. Organised criminal activity in St. Petersburg extends into business, banking, public services, natural resources, and even art and culture. Virtually all businesses in St. Petersburg have a roof (protection scheme) provided by organised crime (Overseas Security Advisory Council 2009). Some of the organised crime groups are believed to use legitimate enterprises they are involved in to support illegal activities. Tambov is believed to have used its petrol distribution company PTK's IT division to commit phishing attacks (Galeotti 2008). PTK itself is a massive enterprise and was awarded its contract to supply St Petersburg when the current Prime Minister Vladmir Putin was Deputy Mayor of the city government such is the high level influence of Tambov (Belton 2003).

Figure 1 shows the structure of Russian Organised Crime groups as described by Vadim Volkov (Volkov 2002). This is probably more a stylised view than the strict reality as these Russian speaking organised crime groups are often known for their lack of hierarchical structure and ability to mould to the task required. However that said it is interesting to note the technical sub-divisions within the structure one for weapons and the other communications and cars etc. Such a sub-division could well include the former FAPSI hackers mentioned by Galeotti (Galeotti 2006). The involvement of these groups has been recognized by numerous governments, the US President's Identity Theft Task Force, set up to combat phishing and other identity, theft reported in 2007 (The Presidents Identity Theft Task Force 2007),

"Law enforcement agencies … have seen increased involvement of foreign organized criminal groups in computer- or Internet-related identity theft schemes."

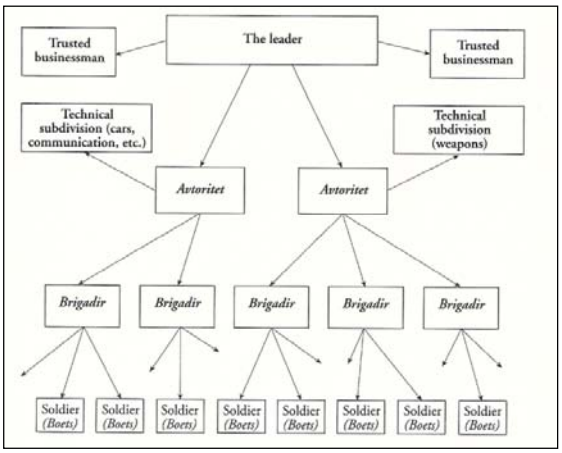

Figure 1. Structure of the (Russian) Organized Criminal Group (Volkov 2002).

Groups from the Russian Federation, the Ukraine and Romania were identified by the US Secret Service as being responsible for a number of the attacks (The Presidents Identity Theft Task Force 2007). In February 2007, Microsoft's Chief Security Advisor in the UK, Edward Gibson (a former FBI Agent), warned "it's not the hacker crackers you have to worry about, but the Ukrainian mafia" (Kornakov 2007).

INTERNET CYBERCRIME

We now look more specifically at Internet Cybercrime and Eastern Europe. In September 2009 Neil Gaughan the head of the Australian High Tech Crime Centre (AHTCC) told a parliamentary enquiry that the majority of cybercrime in Australia is driven by organised crime gangs in Russia. Nigel Phair a team leader from the AHTCC saying in his book (Phair 2007),

"A significant amount of internet-enabled crime including Phishing and denial of service attacks … is perpetrated from within the states which comprise the former Soviet Union." These views are well founded as can be seen from the following case studies.

Spam Kings

Since the expansion in usage of e-mail into the mainstream, spam or unsolicited email has been a problem. In June 2009, according to MessageLabs the global ratio of spam in email traffic was 90.4% or 1 in 1.1 emails (Messagelabs 2009). In phishing the sending of spam is essential both to compromise bank customers and to recruit Internet Monet Mules to launder the money obtained. While claims that most spam comes from the US and China are true (Sturgeon 2006), the groups behind that spam are not necessarily in those countries. Spamhaus produce the Register of Known Spam Operations (ROKSO) and they rank the top ten spamming operations based upon the ROKSO database that collates information and evidence on known professional spam operations that have been terminated by a minimum of 3 Internet Service Providers for spam offenses. If we look at this top 10 (Table 1) we see three entries for the Russian Federation, two for the Ukraine and one for Estonia. Notably Russia and the Ukraine are the only countries to have more than one entry (The Spamhaus Project 2009).

Table 1. ROKSO list of top ten spamming operations (21 July 2009) (The Spamhaus Project 2009)

Ranking	Name	Country
1	Canadian Pharmacy	United States
2	Leo Kuvayev / BadCow	Russian Federation
3	HerbalKing	India
4	Vincent Chan / yoric.net	Hong Kong
5	Alexander Mosh / Alex Polyakov	Ukraine
6	Nikhil Kumar Pragji / Dark-Mailer	Australia
7	Peter Severa / Peter Levashov	Russian Federation
8	Yambo Financials	Ukraine
9	Ruslan Ibragimov / send-safe.com	Russian Federation
10	Rove Digital	Estonia

Internet Money Mules

'Internet money mules' are those who, either knowingly or unknowingly, launder money obtained from Internet fraud and are a key part of phishing and related cybercrime. While the criminals who steal credentials can easily access Internet Banks and perform transactions from the other side of the world they cannot necessary get the money into their own hands so easily. They advertise for Internet money mules through spam email, Internet messaging and both fraudulent and legitimate employment web sites. They claim to be legitimate employment opportunities with mules receiving between 7% to 10% of funds transferred via their accounts as a commission. The cybercriminal transfers money from a compromised bank account into the mules account. The mule, simply doing what their 'job' requires, transfers the fraudulently obtained funds – minus their fee – via financial transfer services such as Western Union to an overseas address (Aston 2009). Data collected by the Australian Federal Police indicate that over 50% of these transactions relate to the former Soviet Union with Russia being the largest single recipient country (Martin 2007). Australian police have had some success in arresting Internet money mules who are aware of the illegal nature of the transactions. One of the largest investigations occurred in 2005 involving NSW and Federal Police (Walker 2006). In that particular case the recruitment method involved a company called World Transfers Incorporated. IDefense did some investigation in their profile of Internet Money Mules (iDefense 2006) and looked at this case. WHOIS data for the former World Transfers Inc. domain provides a clues as to the operation's source. Contact information for http://www.world-transfers.biz follows:

Domain Name: WORLD-TRANSFERS.BIZ
Billing Contact Name: Alex Polyakov
Billing Contact Organization: Pilot Holding LLC

The Ukrainian Polyakov is as earlier stated one of the Spamhaus top ten and allegedly the man behind the first attacks on Internet Banks in Australia (see below). This phenomenon is not just an Australian problem. In 2004 in the United Kingdom Detective Superintendent Mick Deats, Deputy Head of the National High Tech Crime Unit, said: "Organised Crime is targeting Internet users, and specifically Russian-speakers, in the UK to launder money stolen from online bank accounts where people have been duped into handing over their account details. We believe … (they have in this particular case) sent hundreds of thousands of pounds back to Russia … This is a sophisticated operation involving false identities…(Parsons 2004)"

CYBERCRIME CASE STUDIES

Russian Business Network

Some Russian IT organisations are suspected of being purely vehicles for Internet crime such as the now infamous Russian Business Network. A scan of RBN and affiliated ISPs' net space conducted by VeriSign iDefense analysts failed to locate any legitimate activity. Instead, They identified phishing, malicious code, botnet command-and-control,

denial of service attacks and child pornography on every single server owned and operated by RBN. To date, significant attacks on the financial sector continue to emanate from RBN and its affiliated organizations according to iDefense (Zenz 2007).

Hangup Gang

The HangUp Team is based in Archangelsk in Russia. In 2000 the alleged original members of the team, Alexei Galaiko, Ivan Petrichenko, and Sergei Popov, were arrested for infecting two local computer networks with malicious code. But Russian authorities let them off with suspended sentences. In 2003 the gang released the viruses Berbew and Webber. In 2004 the group infected online stores with the Scob worm. Scob waited for Web surfers to connect, then planted a key-logging trojan and relayed thousands of passwords and credit-card numbers to a server in Russia (Grow 2005).

TJ Max/Dave & Busters Restaurant

In 2007 three men have been indicted for hacking into a number of cash registers at Dave & Buster's restaurant locations in the US stealing data from thousands of credit and debit cards. That data that was later sold and caused more than $600,000 in losses. Maksym Yastremskiy of the Ukraine and Aleksandr Suvorov of Estonia hacked into cash register terminals at 11 Dave & Buster's locations and installed "sniffer" programs to steal payment data as it was being transmitted from the point-of-sale terminals to the company's corporate offices. Later the same men were charged with similar a breach at TJMax. Some Analysts estimated the losses at TJ Max at more than USD$1 Billion (Kerber 2007). Doug Bem, an inspector with the U.S. Postal Inspection Service alleged Yastremskiy was a major reseller of stolen credentials (Krebs 2008). Notably both Yastremskiy and Suvorov were arrested while visiting two countries, which actively co-operate with US law enforcement Turkey and Germany and not at home in Eastern Europe.

E-Biz Hosting Incident 2003

On Saturday 28 December 2002 during the quiet Christmas New Year period an email purporting to be from E-Gold support (an online Gold trading company) was spammed out to a large number of Internet users. The next victim of this phishing attack was Commonwealth Bank of Australia (CBA) a former government owned bank in Australia. This was the first such phishing attack against a major Internet Bank. On 10 April 2003 another Phishing email was sent, this time targeting ANZ. 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. On 4 July 2003, US Independence Day Westpac Bank become subject of a similar Phishing attack and at the same time ANZ received its second attack (McCombie 2008).

E-Biz Hosting Solutions 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 and managed the IP space for the CBA site. The Vice-President of the company was listed as Maxim Unger from Odessa Ukraine. Alex Mosh also from Odessa Ukraine was listed as CTO (McCombie 2008). Alex Mosh AKA Alex Polyakov is listed on the spamhaus Register of Known Spam Organisations (ROKSO) top ten list as of spammers above.

Ruslan Ibragimov

Ruslan Ibragimov is a Russian based in Moscow. Spamhaus credit him as “One of the largest criminal-methods/botnet/proxy hijack spamming operations around.” Apart from his own spamming operations he and his group authored the spam sending tool send-safe mailer. He is also believed to be the author of the malware Sobig in 2003 (Author Travis Group 2005). It was released in August 18, 2003 and infected hundreds of thousands of computers within just a few short hours. W32.Sobig.F@mm was a mass-mailing, network-aware worm that sent itself to all the email addresses it could find, worldwide. Within two days after Sobig was released, an estimated $50 million in damages were reported in the US alone. China had reported over 30% of email traffic had been infected by Sobig, equivalent to over 20 million users. After interrupting freight operations and grounding Air Canada, Sobig went on to cripple computing operations within even the most advanced technology companies, such as Lockheed Martin (Author Travis Group 2005).

BlueSecurity DDoS

In 2006 Blue Security was an anti-spam company based in Israel and California. It had an original idea to stop spam. They would send requests to stop sending spam to spammers each time they sent spam to their customers. This caused a lot of problems for the spammers who found they were having serious capacity issues with Blue Security sending these messages on behalf of more than 500,000 customers. While this virtual vigilante system of spamming the spammers was controversial it was apparently quite legal. The response from the spammers was a DDoS attack. Blue Security responded effectively initially but with the time the attack grew in size and sophistication. BlueSecurity had to turn to others for support. When Blue Security got the Prolexic DDoS protection which washed their traffic the spammers merely turned their DDos on Prolexis’ DNS which shut them down and many of their customers who used their service. The result was Blue Security had to go it alone. Shortly after and as a result the CEO decided to shut the company down (Krebs 2006). Both Polyakov and Ibragimov are suspected to have been behind these attacks.

Estonia DDoS

On 26 April 2007 the Estonia government moved a Soviet WW2 memorial from the centre of its capital to a cemetery on its outskirts. To Russians at home and in Estonia it was an outrage. Russians treat the memory of the war dead from WW2 as sacred. Amongst other protests Estonian systems came under DDoS attack from large amounts of ICMP traffic. While the Estonian Government claimed the attack was lead by the Russian Government it appears more that a number of technically savvy members Russian ethnic community within Estonia and elsewhere urged on by a number of Internet posting were responsible (Lesk 2007).

NAB, Westpac, AusCERT, Malaware DDos Attacks

While the Estonian and BlueSecurity DDoS attacks would appear to have little nexus to Australia, DDoS as a tool of retribution has been seen in Australia a number of times. In October 2006 National Australia Bank (NAB) suffered a DDos as result of its efforts to frustrate phishing gangs in Eastern Europe and some claimed the infamous RBN were responsible for the attacks (Zenz 2007). Information from law enforcement officials to Janes Intelligence indicated the attacks were from Russia by groups also responsible for a number of blackmail DDoS attacks on online betting houses (Karrstrand 2007). Shortly after AusCERT and Malaware who both assist in anti-Phishing and anti-trojan efforts for Banks were DDosed. Then in September 2007 Westpac Bank suffered an attack with similar traffic patterns not long after their new cybercrime response team was established and operating against phishing gangs (Winterford 2007).

PHISHING EMAIL ANALYSIS

In work published in 2008 (McCombie 2008) email data from one month of Phishing attacks against one Australian financial institution in July 2006 were examined. This consisted of 77 discrete attacks on that organisation. Each attack involved a different URL set up at a different time and spammed out to extensive spam lists. The work examined the email source of the hooks, the phishing pages where available and other archival data stored by the organisation or otherwise archived on the Internet. The main purpose of the exercise was to see if grouping was feasible. This proved to be the case with 6 particular profiles or groups which accounting for all but 2 of the attacks (McCombie 2008). The authors using unpublished data from that work looked at timezone data in a number of the emails in that dataset.

Timezone Analysis

The timezones GMT + 3 (22 incidents) or GMT + 2 (14 incidents) were present in 36 of 62 incidents where a time zone was present. Many of these instances involved Group 1 identified in the study (McCombie 2008) who accounted for 42% of the 77 incidents. GMT +3 is the time zone of Ukraine in summer (EEST) and GMT + 2 (EET) the rest of the year. The time zone value was set by the email client in the body of the email rather than in the header by the SMTP server. The SMTP time zone value while interesting merely indicates the location of the mail server used to send the email which in most cases is a compromised system or open mail proxy and not the location of the sender which the mail client may well indicate.

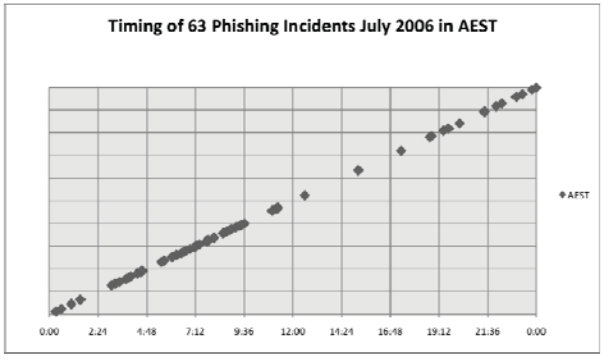

Figure 2. Timing of 63 Phishing Incidents against Australian Financial institution in July 2006.

Also during that study a virtual work day was established based on the header time set by the receiving SMTP server. That study examined Tuesday 18 July 2006 in detail when 12 phishing incidents were observed, starting at 4.01am and continuing to 8.59am, then followed by a break of about ten hours, followed again by three attacks from 6.44pm to 7.39pm. This may be deliberate targeting of the victim users when they access their systems in the morning and first thing in the evening, or may again indicate the working schedule of the phishers themselves (McCombie 2008). The authors examined unpublished header data for 63 of 77 incidents from that study. If we know look at those 63 incidents across July we see a similar pattern of activity. In the time from midnight to 9.37am AEST and we see 45 incidents. From 6.37pm to midnight AEST we see 12 further incidents. However from 9.37am to 6.37pm AEST we see only 6

incidents (3 of which occur within 17 minutes). Clearly in this period there is significantly less activity. If we convert to EEST these 63 incidents we can see how busy times map to mid morning and to very early morning for EEST, potentially the waking hours of the perpetrators. An argument also could also be made for later timezones such as GMT but clearly the timing does not match the waking hours in Australia.

Windows-1251

Unpublished character set data was also examined from the July 2006 study. The Windows-1251 character set is associated with the Cyrillic character set used in Russia and Eastern Europe. In the 5 instances where any value was seen, 4 were Windows-1251 (the remaining was Windows-1252 the standard Latin text). All these instances involved Group 3, which accounted for 18% of the 77 incidents. We then looked at a different Phishing Corpus, which has made available by Jose Nazario of phishing incidents from 7 August 2006 to 7 August 2007 (Nazario 2007) to see if we could see this value. In that corpus there were 2279 different phishing attacks, of those 904 had a value for the Windows character set and for 693 of these the value was Windows-1251. Future research will look at this and other larger email corpus of Phishing attacks to further assess this value to see its pre-eminence.

CORRUPTION PERCEPTION INDEX, INTERNET PENETRATION, TERTIARY EDUCATION AND CYBERCRIME

Russia and other parts of the former Soviet Union have suffered from a high level of corruption for some time. The Transparency International Corruption Perceptions Index (CPI) is based on a number of surveys conducted globally (Transparency International 2008). When trying to understand why Russia and Ukraine in particular seem to figure in cybercrime incidents we decided to look for a possible correlation between high corruption, high Internet penetration and high levels of tertiary education. As you will see this certainly shows the unique position of Russia and the Ukraine both on in terms of absolute numbers and per capita in these areas when compared with other countries with poor (low) CPI scores.

The Transparency International CPI ranks countries in terms of the degree to which corruption is perceived to exist among public officials and politicians. It is a composite index, a poll of polls, drawing on corruption-related data from expert and business surveys carried out by a variety of independent and reputable institutions. The CPI reflects views from around the world, including those of experts who are living in the countries evaluated. The lower the score the worse the perception of corruption in that country (Transparency International 2008). We then added information relating to Internet penetration gathered by International Telecommunications Union (International Telecommunication Union 2008) for each country for listed in the CPI ranking. We then added data relating to the level of Tertiary Education from the World Bank (World Bank 2007). The CPI rating and Internet data relate to 2008 and the Tertiary education data relates to 2007.

In 2008 Russia has more than 30 million Internet subscribers with a penetration of over 20 users in 100. Ukraine while considerably smaller still has over 6 million Internet users and penetration of over 13 users in 100. At the same time they are both listed in bottom 25% of countries by corruption perception, Russia scoring 2.2 being 147/181 and Ukraine scoring 2.5 being 134/181. They also have very high levels of enrolment in tertiary education. Russia having over 9 million enrolled and 72.3% of students enrolled of the relevant age group or Gross Enrolment Ratio (GER). Ukraine has nearly 3 million and 72.8% GER.

While countries like China have far higher numbers of Internet subscribers (150 million) their CPI sits a lot better at 3.6 at 72/181 with a GER of a mere 21.6%. This makes Russia and Ukraine relatively unique. Even Nigeria with its reputation as the home of the 419 scams and West African Crime actually sits higher on the CPI at 121/181 scoring 2.5 but with only 115 thousand Internet subscribers and a tiny penetration of 0.08 users in 100 and a GER of 10.2%. In Table 2 shows all countries ranked by CPI score with greater than 1.5 million Internet Subscribers by CPI including tertiary figures. This shows the unique position of Russia and the Ukraine.

Table 2. Countries ranked by CPI Score (lowest to highest), Internet Subscribers (>1.5 Million) showing enrolment in Tertiary Education

Country	CPI Score	Internet Subscribers (000)	Internet Subscribers per 100	Enrolment in tertiary education, Total (000)	GER in tertiary education (%), Total
Russia	2.1	30500.0	21.4	9167.3	72.3
Philippines	2.3	2500.0	2.8	2484.0	28.5
Pakistan	2.5	3700.0	2.2	820.3	4.5
Ukraine	2.5	6400.0	13.9	2740.3	72.8
Indonesia	2.6	3126.0	1.4	3657.4	17.0
Viet Nam	2.7	5240.6	6.0	1354.5	
Egypt	2.8	2968.6	3.9	2594.2	34.7
Argentina	2.9	3737.4	9.4	2082.6	63.8
India	3.4	12850.0	1.1	12852.7	11.8
Brazil	3.5	11401.9	5.9	4572.3	25.5
Saudi Arabia	3.5	3000.0	11.9	614.9	29.2
China	3.6	150264.0	11.3	23360.5	21.6
Mexico	3.6	8273.1	7.7	2446.7	26.1
Colombia	3.8	2023.3	4.3	1315.0	30.8
Romania	3.8	2520.0	11.8	835.0	52.2
Poland	4.6	3987.3	10.5	2145.7	65.6
Turkey	4.6	5829.2	7.7	2342.9	34.6
Greece	4.7	1744.1	15.6	653.0	94.9
Italy	4.8	12199.1	20.7	2029.0	67.0
South Africa	4.9	3566.0	7.6	741.4	15.4
Hungary	5.1	1584.3	15.8	438.7	68.6
Malaysia	5.1	5221.6	19.3	696.8	28.6
South Korea	5.6	15474.9	32.0	3204.0	92.6
Taiwan	5.7	6026.5	26.2		
Israel	6.0	1714.9	24.3	310.0	57.6
Portugal	6.1	1733.3	16.3	367.3	54.5
Spain	6.5	9311.8	20.9	1789.3	67.4
France	6.9	18700.0	30.2	2201.2	56.2
Belgium	7.3	3055.7	29.2	394.4	62.8
USA	7.3	72721	23.78	17487.5	81.8
United Kingdom	7.7	19380.0	31.8	2336.1	59.3
Germany	7.9	20000.0	24.2		
Norway	7.9	1606.1	34.2	214.7	77.5
Austria	8.1	2127.0	25.4	253.1	49.9
Hong Kong	8.1	2905.3	39.9		
Australia	8.7	7996.0	38.2	1040.2	72.7
Canada	8.7	10163.0	30.9	1326.7	62.4
Netherlands	8.9	5886.0	35.8	579.6	59.8
Switzerland	9.0	2750.0	36.6	205.0	45.8
Denmark	9.3	2158.9	39.6	228.9	79.9
New Zealand	9.3	1504.0	35.7	237.8	79.7
Sweden	9.3	4054.0	44.5	422.6	79.0

CONCLUSION

It is acknowledged that the above discussed data analysis work is not alone conclusive as to the source of phishing and related cybercrime. However if viewed in conjunction with the survey information and other supporting material it certainly presents a compelling argument of the major role played in Phishing and related cybercrime by Eastern European individuals and groups. Eastern Europe's situation has made it particularly suited to the development of cybercrime groups. High levels of technical education reflected in the high GER, a period economic uncertainty and downturn, a breakdown of state institutions, and an established tradition of criminal gangs have all contributed. It is interesting to note Romania, which was identified in association with EBay auction fraud (Warne 2007), has now improved its situation with the prosecution of a number of cybercriminals in that country (Goodin 2008). Romania now has a healthy CPI of 3.8, by Eastern European standards, up from 2.8 in 2003. Both these developments seem to have been a result of the closer ties with the European Union, the USA and the west generally. It however seems that as long as Ukraine and Russia remain outside of this type of influence it is going to be difficult for western governments and more particularly western law enforcement to have much impact on individuals and groups in these countries committing cybercrime. The Russian and Ukrainian Governments would appear to have the capacity to deal with the problem just not the incentive.

REFERENCES

Abramova, I. (2007). "The Funding of Traditional Organised Crime in Russia." Economic Affairs 27(No.1): 18-21.

Aston, M., McCombie S., Reardon B., and Watters P. (2009). A Preliminary Profiling of Internet Money Mules: An Australian Perspective. Cybercrime and Trustworthy Computing. Brisbane.

Author Travis Group. (2005, September 2005). "Who Wrote Sobig? ." from http://authortravis.tripod.com/.

Belton, C. (2003, 2003). "New Book Poses Question of Putin's Links with Underworld." from http://www.sptimes.ru/index.php?action_id=2&story_id=11164.

Finckenauer, J. O. and J. L. Schrock (2004). The prediction and control of organized crime : the experience of post-Soviet Ukraine. New Brunswick, N.J., Transaction Publishers.

Galeotti, M. (2005, 24 May 2005). "Russian mafiya become more active in Eastern Europe." from http://www.janes.com/security/law_enforcement/news/jir/jir050524_1_n.shtml.

Galeotti, M. (2006). "The Criminalisation of Russian State Security." Global Crime 7(Number 3-4).

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

Gartner. (2009). "Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008." from http://www.gartner.com/it/page.jsp?id=936913.

Goodin, D. (2008). "Notorious eBay hacker arrested in Romania." from http://www.theregister.co.uk/2008/04/18/vladuz_arrested/.

Grow, B. (2005). "Hacker Hunters: An elite force takes on the dark side of computing " Retrieved 20 August, 2009, from http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm.

iDefense (2006). Money Mules: Sophisticated Global Cyber Criminal Operations Verisign.
International Telecommunication Union. (2008). "Internet indicators: subscribers, users and broadband subscribers: 2008." from http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP_intYear=2008&RP_intLanguageID=1.

Karrstrand, K., Jonsson, M. (2007). "The Baltic connection - Money laundering in the Baltic region ." Janes Intelligence Review.

Kerber, R. (2007). "Suspect named in TJX credit card probe: Ukrainian's arrest seen as break in record fraud case." from http://www.boston.com/business/globe/articles/2007/08/21/suspect_named_in_tjx_credit_card_probe/.

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

Krebs, B. (2006). "In the Fight Against Spam E-Mail, Goliath Wins Again." from http://www.washingtonpost.com/wp-dyn/content/article/2006/05/16/AR2006051601873.html.
Krebs, B. (2008). "Three Charged With Hacking Dave & Buster's Chain ", from http://voices.washingtonpost.com/securityfix/2008/05/three_charged_with_hacking_dav.html.

Kreizer, G. (2005). "Dutch Botnet Trio Reportedly Connected To Russian Mob."

Lesk, M. (2007). "The New Front Line: Estonia under Cyberassault." IEEE Security and Privacy 5(No.4 July/Aug. 2007): pp.76-79.

Martin, S. (2007). International Field Report : Australia. 2007 APWG General Members Meeting. Pittsburgh PA.

McCombie, S. (2008). Trouble in Florida: The Genesis of Phishing attacks on Australian Banks. 6th Australian Digital Forensics Conference. Perth.

McCombie, S., Watters, P. , Watson, B. & Ng, A. (2008). Forensic Characteristics of Phishing - Petty Theft or Organized Crime. WEBIST Conference Funchal Portugal pp149-157

Messagelabs. (2009). "MessageLabs Intelligence: July 2009." from http://www.messagelabs.com/resources/mlireports.

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

Nazario, J. (2007). "Phishing Corpus." from http://monkey.org/~jose/wiki/doku.php?id=PhishingCorpus.

Nomad, S. (2005). "Organized Cybercrime." from http://www.dc214.org/notes/june_2005/dc214_sn_orgcrime.ppt.

Overseas Security Advisory Council (2009). Russia 2009 Crime & Safety Report: St. Petersburg, Overseas Security Advisory Council.

Parsons, M. (2004). "Twelve arrested for laundering phished funds." Retrieved 1 September, 2009, from http://news.zdnet.co.uk/security/0,1000000189,39153687,00.htm.

Phair, N. (2007). Cybercrime : the reality of the threat. Kambah, A.C.T., Nigel Phair.

Reuters. (2005, November 29, 2005). "Cybercrime now bigger than the drug trade." from http://www.smh.com.au/news/technology/cybercrime-now-bigger-than-the-drug-trade/2005/11/29/1133026443366.html.

Ridley, N. (2007). "Financial Crime Trends in Central and Eastern Europe." Economic Affairs 27(No. 1 March 2007): pp. 22-26.

Serio, J. D. (2008). Investigating The Russian Mafia. Durham NC, Carolina Academic Press.

Sturgeon, W. (2006). "Analysis: A globetrotter's guide to cyber crime." Retrieved 30 July, 2009, from http://www.silicon.com/research/specialreports/ecrime/0,3800011283,39158777,00.htm.

The Presidents Identity Theft Task Force (2007). Combating Identity Theft: A Strategic Plan. 2007.

The Spamhaus Project. (2009). "The 10 Worst ROKSO Spammers." Retrieved 21 July, 2009, from http://www.spamhaus.org/statistics/spammers.lasso.

Transparency International. (2008). "Corruption Perceptions Index 2008." from http://www.transparency.org/policy_research/surveys_indices/cpi/2008.

US Department of Justice (2008). Strategy to Combat International Organized Crime.

Varese, F. (2001). The Russian mafia : private protection in a new market economy. Oxford, England ; New York, Oxford University Press.

Volkov, V. (2002). Violent entrepreneurs : the use of force in the making of Russian capitalism. Ithaca, Cornell University Press.
Walker, F. (2006). Gone phishing ... gangs using Aussie kids to steal millions. Sydney Morning Herald. Sydney.

Warne, D. (2007). "Romania a global hotspot for eBay fraud." APC Magazine May 2007. from http://apcmag.com/romania_a_global_hotspot_for_ebay_fraud.htm.

Winterford, B. (2007, 19 June 2007). "Westpac hit by DoS attacks." from http://www.zdnet.com.au/news/security/soa/Westpac-hit-by-DoS-attacks/0,130061744,339278748,00.htm.

World Bank. (2007). "Education Statistics 2007 Version 5.3." 2007. from http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTEDUCATION/EXTDATASTATISTICS/EXTEDSTATS/0,,menuPK:3232818~pagePK:64168427~piPK:64168435~theSitePK:3232764,00.html.

Zenz, K. (2007). Global Threat Research Report: Russia. iDefense Security Report. iDefense, Verisign.

Zenz, K. (2007). Uncovering Online Fraud Rings: The Russian Business Network. iDefense Security Report. IDefense, Verisign.

COPYRIGHT