

NOVEMBER 2009

SOUTH AFRICAN INSURANCE CRIME BUREAU

ISSUE 9 : 2009

INFORMATION UPDATE

Dräger:

15 Lists received
618 Records
171 Hits in Memex
23 Feedback responses from industry

Enquiries and Fraudline

55 Enquiries received
197 Feedback responses received from industry

Tracker

18 Lists received
360 Records
81 Hits on Memex
47 Feedback responses received from industry

SAPS

4 lists received
223 Records
18 Hits on Memex

INSIDE THIS ISSUE...

SAICB UPDATE	1
FRAUDLINE	1
INFORMATION UPDATE	1
ARTICLE - ISS	2
ARTICLE - ITINews	4
ARTICLE - TRACKER	5/6
CONTACT	6

SAICB UPDATE

This will be the last Newsletter for 2009, and a time to reflect on the year that has been and the year to come. It is also a time to thank those that have contributed and supported the SAICB in its endeavours which has ensured that we have had a very successful year. In addition the SAICB would like to thank all the organisations and writers who have allowed us to use their articles and contributed to our Newsletter since its inception in March. The Newsletters circulation has expanded monthly and is currently being forwarded to policing, fraud and crime prevention organizations in the UK, Europe and the US to showcase the ground breaking work being done in the fraud and crime prevention environment in the insurance industry in South Africa.

This has been an exciting and productive 12 months for the SAICB, with successes and challenges that have kept us busy and motivated. We are particularly proud of the short term industry, in particular our members—Santam, Mutual & Federal, Hollard, Zurich, Absa Insurance, MiWay, Standard Insurance, Regent, Telesure, FRSTIA and Lion of Africa, our Special Points of Contact (SPOC) committee and our Board, for their support and commitment to the SAICB. Their support has allowed us to make significant strides in the sharing of information and the fight against insurance crime and fraud in the industry and in the country.

This year has seen the company grow in staff, up to 10 at the moment and expand its partnerships and collaborations with the various stakeholders we need to effectively help with our mandate. The policing organizations have also embraced the SAICB with effective lines of communication having been established with the South African Police Service (SAPS), the National Prosecuting Authority (NPA), the various metro police departments and specialized divisions that are relevant to insurance crime.

The SAICB "Year in Review" breakfast that took place on 4 November at the Johannesburg Country Club in Auckland Park was well attended by the industry and stakeholders and showcased the progress, challenges, successes, and partnerships forged in the past year. All speeches, the media release and the presentation has been uploaded to our website—www.saicb.co.za. We thank all the attendees for their support. 2010 promises to be just as

FRAUDLINE

In October 2009, **161** reports were received of which 5 reports were for the short term insurance industry and 2 report for the life industry.

Since 2002, **25591** reports have been received of which **774** reports were for the short

term industry **120** reports for the brokers and **322** reports were for the life industry.

For the full report with all the statistics, please contact Melanie Pillay on melaniep@saicb.co.za

exciting and challenging but the lessons learned over the past year has put us in good stead to face any and all challenges.



0860 002526
insurance@fraudline.co.za

ARTICLE— ISS

MEMBERS

SANTAM
 MUTUAL & FEDERAL
 HOLLARD
 ZURICH
 LION OF AFRICA
 REGENT
 TELESURE
 ABSA INSURANCE
 STANDARD BANK
 INSURANCE
 FRSTIA
 MIWAY

PARTNERS

SOUTH AFRICAN
 INSURANCE
 ASSOCIATION (SAIA)
 TRANSUNION
 FRAUDLINE
 MEMEX
 SAFPS
 UNICODE
 BACSA
 CSFS
 DATADOT

The Politics of Organised Crime in Africa

Organised crime and corruption have existed in partnership from time immemorial. Some would argue that this has been so for as long as man has engaged in economics.

In its more outrageous forms, however, the combination is said to have manifested itself initially during the Prohibition during the 1930s in the United States of America as well as in Italy during a time of weak and often absent government structures in large parts of the country. It is from then that the general recognition emerged that organised crime and corruption could easily penetrate state structures and pose a significant threat to human and national security.

Since that time, several countries have graphically experienced the disastrous consequences of failing to appreciate and deal with organised crime and corruption in their infancy. Colombia and Mexico have become synonymous with violent internal wars involving renowned drug lords, and their powerful, politically connected syndicates in mortal combat with state institutions. Italy and the United States, countries linked to the origins of the Mafia, have not achieved a sustainable conquest over organised crime, despite committing huge resources to fighting it.

In Africa, it is contended that the lack of sufficient resources, specifically skills and funding makes it unlikely that organised crime and grand corruption can ever be brought under control. Some researchers believe that the most powerful tool in fighting organised crime is the political will to fight it. This is something that many African governments lack.

Connections are being drawn with other parts of the world. When crime syndicates are put under pressure in Europe, Asia and the Americas, they often seek to relocate to Africa as a relatively safe haven from which to rejuvenate their activities. The result has been the rise of the African west coast as a hub for drug distribution into the rest of Africa and as a strategic stopover for drugs destined for markets in the rest of the world. Meanwhile, the African east coast is a growing entry point for counterfeit commodities, precursor chemicals for the production of narcotics and other contraband from Asia. Of late, some sections of the east coast has been affected by maritime piracy.

Weak governments cannot control organised crime. African administrations are no exception. What makes it worse for the continent is the legitimacy deficit that continues to plague a number of governments. The legacy of anti-colonial or liberation struggles is littered with military juntas and illegitimate governments, most with a violent pedigree. In quite a few countries, the state system has yet to recover from the damage wrought by decades of dictatorship.

Although it is often associated with the use of violence, organised crime only resorts to violence when strategically necessary. If it can exist in partnership rather than in competition with the political establishment, organised crime opts for friction-free co-existence. Organised crime can develop into a political vehicle through which governments or political parties stifle political rivalry. Corruption cements these alliances. International corporations back preferred candidates to guarantee access to favourable business contracts. Donations from organised criminal enterprises have been known to sustain political parties in some countries.

ARTICLE— ISS *cont....*

Many noble initiatives by African governments to install structures to deal effectively with organised crime and corruption have failed primarily due to lack of political will. A semblance of intent to probe corruption resulted in commissions of inquiry. Disappointingly, in many instances, these commissions not only fall prey to political pressure but their reports are normally inexplicably stored away to gather dust. The end result is that they become ineffective or are closed down. Both the United Nations Office on Drugs and Crime and the East and Southern African Anti Money Laundering Group (ESAAMLG) has exposed the nexus between corruption and lack of progress in implementing measures to combat money laundering. A particular factor that weakens the resolve to act against dealings with proceeds of crime is the corruption of political elites, and their circle of associates commonly referred to as "politically exposed persons". There is an almost palpable fear to establish structures that might eventually return to haunt them and/or their close associates.

It has been unequivocally established that through corruption, criminals are able to secure protection from public officials, influence political decisions and infiltrate state structures and legitimate businesses. Law enforcement operations conceived at high levels are leaked well in advance to criminals. Government procurement systems are universally inflated to accommodate the political elite or their agents who demand to be involved if any deals that are to be done. There have also been anecdotal indications of the involvement of politically exposed persons in the trafficking of contraband to or from Europe and other parts of the world.

Those in influential positions have access to evidential information and are well placed to destroy or dilute it should it implicate them. It is also not uncommon for witnesses to be haunted into exile through fear of reprisals. For this reason, convictions in grand corruption cases tend to be few and far between - despite the known prevalence of corruption scams. Much corruption in procurement occurs with deals for military or security equipment. State security issues are then brought up to stifle any investigations.

Quite a few prosecutions have been adversely affected by the taint of being selective or politically expedient. Criminal masterminds often get away with it, leaving only the proverbial small and expendable fish. Criminal justice systems are heavily compromised where they are not outright militarised or politicised. The concept of national security is only debated to the extent that it remains politically palatable.

The exploitation of natural resources is highly politicised and tainted with shady figures and unscrupulous corporate heavy weights. The world's major powers conveniently look the other way or make loud public noises while privately dining with the rogue governments and the executives of major corporations plundering Africa.

While some civic society supported by countless international and non-governmental organisations – assuming they have no vested interests - are gallantly working towards an organised crime and grand corruption free world, the challenges remain deeply entrenched in African societies and in poor governance. Patience and persistence will be required to truly make a meaningful impact. While some patriotic and selfless men and women continue to sacrifice their lives in answering to the thankless calling of law enforcement, it is clear that their political handlers continue to determine what they successfully investigate and prosecute and that they are only sufficiently equipped and paid to stay on the job and dream of the day they will overcome the shortcomings of the system. That is not withstanding the bad apples amongst them. The criminal justice system, in its entirety, is invariably compromised and malleable to the political status quo.

It is this sad concoction of factors that feeds the belief that, for as long as African politics fail to evolve from its self-distracting predisposition of patronage, the extermination of organised crime and corruption is a pipe dream. 🖱️

Thank you to Jackson Madzima, Researcher , Organised Crime and Money Laundering, Institute of Security Studies (ISS) Cape Town Office for permission to use this article that appeared on 30 October on the ISS website -

www.issafrica.org

ARTICLE—ITNEWS

CYBER-CRIME—SYNDICATES OF THE 21ST CENTURY

The criminals play on people's lack of understanding and manipulate vulnerabilities in cyber-space, says Glen Miller, CEO of The Webcom Group.

Many people think of viruses as a nuisance, and while they are aware of the threats, they believe that ordinary anti-virus software will protect them from the ever-increasing number of attacks in the form of phishing (the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details), pharming (a hacker's attack aiming to redirect a Web site's traffic to another, bogus Web site), worms (malicious software), Trojans (malicious software), bots (collection of compromised computers) and denial of service attacks.

However, most people underestimate the tenacity of the people who perpetrate these attacks, and fail to take the threat seriously enough. The fact is, cyber-crime is an incredibly lucrative business, not only for virus writers, but for people all the way through the chain, and has already overtaken the drug trade in terms of the amount of money made through these criminal activities.

Cyber-crime has become an industry that is money-driven and has malicious intent, and people on the street need to be aware of the motivations of these criminals who play on people's lack of understanding and manipulate vulnerabilities in cyber-space in order to make a profit.

As end-users, most individuals only see parts of cyber-crime, and are unaware of what goes on behind the scenes of these attacks. The cycle begins with harvesters, whose job it is to literally harvest live e-mail addresses, which are then passed along. This happens in a number of ways. The most common way is for the harvesters to send out e-mails that encourage recipients to pass them along, such as the ones claiming that if the e-mail is sent to a certain number of people and CC'd to another address, the sender will receive some kind of reward. This confirms live e-mail addresses to all of the people to which the e-mail is forwarded, and in this way a database is built up.

Another method is robotic harvesting, which uses a program to pick a random company or organisation and builds a database of first and second names. These are then randomly matched into e-mail addresses by the program until the address stops bouncing. Once e-mail addresses are confirmed, a database is built.

These databases are then sold on to the next link in the chain, the spammers, who pay anything up to \$100 per 10 000 names. This does not sound like a lot of money, but when databases of addresses numbering in the millions are sold all the time, one begins to get a picture of just how much money changes hands simply at this first stage.

Spammers are then paid by the virus writers to send e-mails out to their databases containing viruses, Trojans or worms, which turn a laptop or PC into a zombie machine that is then effectively controlled by a third-party.

Spam e-mails also contain offers to purchase goods, commonly medication that requires a prescription to get hold of otherwise. The spammers get paid not only for every e-mail sent, but also per click for the links these mails contain and a commission of up to 50% for every product purchased.

Herders control masses of compromised PCs, known as botnets. Virus writers can hire these botnets and use the compromised machines to send out mass e-mails that do not get stopped by ISPs, because they originate from a large number of different machines and thus do not get detected as spam.

ARTICLE—ITNEWS *CONT...*

Botnets can also be used for an even more sinister purpose - straight-up blackmail. While this does not affect the majority of people, it is a real problem for organisations such as online casinos and betting agents. These businesses make a fortune from people gambling and placing bets every day, and are a prime target for denial of service attacks. Cyber blackmailers threaten to take down these sites on important days with DOS attacks, and hold them to ransom for large fees.

Typically, it is easier for the organisations to pay the ransom than to risk millions in revenue if the sites are shut down by hackers using botnets.

These attacks are co-ordinated DOS attacks that use the zombie computers to hit the site simultaneously with meaningless queries that overload the servers and crash the sites.

Firewalls do not detect these attacks because the hits are coming from many different machines and are therefore not detected as spam.

Cyber-crime is a very profitable business, and because many people are unaware of just how prevalent it is and how vulnerable they are to threats, it is likely to continue to be so for some time to come. The best way for individuals and businesses to protect themselves from these types of attacks is to educate themselves, staff and customers with constant awareness campaigns, and ensure that systems are protected with the latest anti-malware and anti-virus toolkits with rigorous virus definition and software updates to minimise the risk of attacks.

Thank you to Marthinus Engelbrecht from CSFS who forwarded the article that originally appeared on the ITnews website on 29 October 2009— www.itnews.co.za

ARTICLE—TRACKER

TRACKER AND GAUTENG'S NEW ANTI-HIJACKING UNIT SET TO BLITZ VEHICLE CRIME

Tracker recently joined forces with the Gauteng Department of Community Safety's new Anti- Hijacking unit in a partnership that is set to dramatically increase the heat on vehicle crime syndicates operating in the province.

The new unit, officially known as The Gauteng Traffic Police Anti-Hijacking unit, consists of 40 members in 20 high-powered vehicles whose primary mandate is to patrol highways, hot spots and busy intersections throughout the province. While they also respond to a host of other crimes including traffic infringements, drug trafficking and other transport related offences, their main focus will be on countering vehicle theft and hijackings. Their presence will further boost security in the province as South Africa heads towards the World Cup in 2010. As such, Tracker has now installed its sophisticated tracking computers into each of these vehicles and has fully trained the specialist officers on how to track stolen and hijacked vehicles fitted with a Tracker.

"We are very excited by both the unit's introduction to the province as well as our partnership with them. We already have our recovery technology installed in more than 1 200 police vehicles and almost 50 aircraft and believe that our linking arms with this specialist team will be of significant benefit to both the police, Tracker's customers and the South African public at large," says Ronnie Knott-Craig, Tracker's Operations Director.

The unit's head, Control Provincial Inspector, Malose Phalane, believes that they are now ideally positioned to make significant inroads in vehicle crime in Gauteng. "With Tracker's world proven technology and a team of specialized officers patrolling our highways 24 hours a day, we are confident of making a meaningful impact on hijackings and vehicle crime syndicates. In only a few months, we have already had numerous successes and have arrested suspects for a wide variety of

ARTICLE—TRACKER

ANOTHER BLOW TO VEHICLE CRIME

As part of Tracker and the police's ongoing efforts to come up with new and innovative ways to combat vehicle crime in South Africa, Tracker's recovery technology was recently fitted to a police motorcycle as part of a pilot project.

So far the project has been an enormous success with the bike having already recovered several stolen vehicles which has resulted in numerous arrests.

"A motorcycle is highly effective in tracking down stolen and hijacked vehicles as it can travel at high speeds and is not easily held up by traffic. Given the initial success we're hoping to install more of our recovery computers in police motorcycles around the country," said Tinus Odendal, Tracker's National Manager for Operational Services.

Thank you to Gareth Crocker, Marketing and Communications Manager of Tracker Network (Pty) Ltd for permission to use these articles.

CONTACT

For further information or if you wish to reproduce any of the articles in this Newsletter, please contact :

Hugo van Zyl on
hugovz@saicb.co.za
 or Melanie Pillay on
melaniep@saicb.co.za

SEASONS GREETINGS

WISHING YOU AND YOUR LOVED ONES A SAFE AND HAPPY FESTIVE SEASON. WE LOOK FORWARD TO KEEPING YOU INFORMED AND WORKING WITH YOU AGAIN NEXT YEAR

FROM THE TEAM AT THE
 SOUTH AFRICAN INSURANCE CRIME BUREAU