Money Laundering in Cyberspace

The World Bank
Financial Sector Working Paper

November 15, 2004
Tom Kellermann, CISM
Money Laundering in Cyberspace

INTRODUCTION

On November 12, 2001 the Board of the IMF agreed to “intensify Fund activities in the international fight against money laundering, to expand these efforts to include anti-terrorist financing activities”\(^1\). The Plan recognizes that “Terrorist funds are recycled in the financial system through a variety of layering techniques which take advantage of regulatory and supervisory weaknesses.”\(^2\). In its 2002 National Money Laundering Strategy, the U.S. further acknowledged the difficulty of estimating the full magnitude of the money laundering problem, and cautioned against putting too much faith in the wide range of estimates provided by different organizations.\(^3\) Most recently the UK stated that financial crime there was 2\% of GDP. This problem is exacerbated now by use of the Internet as a means of money transmission for criminal and terrorist groups.

As of 2002, just a decade after the Internet’s introduction into the economic mainstream, the Internet boasts over 600 Million users and 10,000 Service Providers worldwide. By providing better access to information it facilitates global trade and finance in ways never thought possible just a few years ago. At the same time its unique characteristics provide an extraordinarily fertile environment for the proliferation of crime and the development of criminal alliances. In essence the Internet enables the transportation, transmission and transfer of value in an anonymous, inexpensive, tax-free and unregulated medium that portends the fluid movement of value across borders and jurisdictions with the blessing of governments worldwide. As a result, no one benefits from operating in this environment more than criminals and terrorists. Growth of the Internet as a value transfer mechanism is stressing legal, regulatory and law enforcement systems in developed countries much less weak or immature systems in emerging economies.

This Note is intended as a summary introduction to a few of the means, mechanisms and methods used by non-state actors to generate and transfer wealth over the Internet. It identifies several vehicles that the Bank could use to enhance its present services.

The relationships between criminal elements and religious entities have been well documented over time. In the 50’s and 60’s the televangelist emerged using mass communications as a way to propagate beliefs and raise phenomenal amounts of undocumented cash. Today criminal and religiously motivated groups have been early and successful adopters of the new mass communications medium:

---

1 Proposed Action Plan for Enhancing the Bank’s Ability to Respond to Clients in Their Battle Against Money Laundering and Terrorist Financing


3 In particular, it cites the extremely broad estimates provided by former IMF Director Michel Camdessus as evidence of the difficulty and wide variability associated with this task. Camdessus estimated the global volume of ML at between two to five percent of global GDP, a range encompassing $600 billion to $1.8 trillion.

Produced by Tom Kellermann, Sr. Data Risk Management Specialist, World Bank Treasury Security team
the Internet. Today, both use the Internet to solicit funds, recruit people, augment skills and assets by networking, allocate and deploy resources and perpetrate activities for their benefit. Digital technology enables the world to become increasingly interconnected as an entire economy becomes reliant upon a single, network infrastructure. While this offers tremendous opportunities to many industries, including financial, telecommunications, health, and transportation, it can also be a cause for concern if security issues are improperly addressed, or even neglected altogether. Heinous crimes such as theft, fraud and extortion can occur in great magnitude within a matter of seconds. The new network-mediated economy paradoxically presents unparalleled opportunities for the creation of good outcomes or the perpetuation of bad ones.

Trends in cyber crime reveal significant growth. Between 1999-2003 in the United States, attacks on computer servers increased by over 530% to 137,000 incidents. This is partly attributable to vulnerabilities in software code, which have grown from a total of 500 in 1995 to over 9000 in 2002 (CERT). Developing countries are also being targeted, even as leapfrog technology is implemented. Brazil has seen hacker attacks increase by at least 100% yearly since 2000. These growing numbers bear particular important on the financial sector. The International Data Corporation (www.idc.com) reported that more than 57% of all hack attacks last year were initiated in the financial sector (source and year. The FBI has corroborated this statistic. Equally troubling, FINCEN’s Suspicious Activity Reports for Computer Intrusions have shot up more than 500% over the past year. With the growing amount of financial data stored and transmitted online, the ease of computer intrusions add to the severity of traditional crimes such as identity theft; to put this in perspective for the digital age, over USD$222 billion in losses were sustained to the global economy as a result of identity theft.

Of this $222B most was laundered online through various e-channels.

The Internet’s primary attributes are speed and convenience, which in turn cuts transaction costs and float time. These attributes are doubly attractive to illegal oriented entities because it decreases exposure and risk. For example, within fifteen minutes after Slammer was introduced into the Internet, 27 million people in South Korea (the most connected country in the world) were left without cell phone or Internet access, 5 of the Internet’s 13 root servers crashed, 300,000 cables in Portugal went dark, Continental Airlines had to cancel flights because it had no Internet access, Level 3 (the major telecommunications provider in the world was shut off) and 911 in Seattle, Washington had to go to paper. This creates opportunities for disruption of business operations on a global basis for which we simply do not yet have tools to comprehend much less quantify.

---

6 Suspicious Activity Reports (SAR) for computer intrusions have grown from 419 in 2001 to over 1,293 in 2002. Over 4,713 incidents have been reported as of May 2004. http://www.fincen.gov/sarreviewissue5.pdf
7 Aberdeen Group June 2003 Report on the Economic Impact of ID Theft

Produced by Tom Kellermann, Sr. Data Risk Management Specialist, World Bank Treasury Security team
I. Overview of Electronic Money Laundering

Electronic Money Laundering — With the explosion of Internet use since 1996, and the subsequent, exponential growth in electronic finance (e-finance), organized criminal syndicates and terrorists can now launder money in cyberspace. According to Jim Savage, the Special Agent in Charge of the Financial Crimes Division of the US Secret Service: “hacking the electronic infrastructure of the world’s financial community has become a business model for both the Yokuza and the Russian Mafia.”

Estimated Annual Volume — A 1996 study entitled the Walker Model, suggests that total global Internet money laundering at that time accounted for only around $500 billion per year. It appears that no further studies have been conducted since 1996. However, today the Federal Bureau of Investigation states that the majority of illicit proceeds are laundered through electronic channels, as described in the following sections.

Means of Electronic Money Laundering — Internet based payment systems enable monetary transactions in the digital environment. While these technologies portend to be the future of payment systems, they also facilitate money laundering. Partially attributable to the lack of systems level controls, such as in the credit card industry, these new payment mechanisms are becoming a hotbed of money laundering activity.

II. Four Models of Payment Systems in Cyberspace

The characteristics of the Internet and the new cyber-based payment modalities facilitate money laundering because they provide relative anonymity, lack regulation or third party oversight and move easily across borders without detection or interception. Furthermore, money is represented by digital bits or other value propositions, and thus difficult to track or trace. The exponential growth of these models, particularly the non-bank and peer-to-peer models, perpetuate the money-laundering phenomenon by providing technological capabilities to more people, and money laundering capabilities from the convenience of a home computer.

---

8 57% of the hack attacks originated in the financial sector last year.

9 Ibid.

10 Cyberpayments and Money laundering: Problems and Promise. 1998.RAND.

11 Rather than having to launder the illicit fund through a network of front/shell companies which can take days, an individual can set up an account with an online casino or an e-gold and close it within minutes thus “washing” the money instantaneously.
i. **The Merchant Issuer Model:** In this case, both the smart card issuer and the seller of goods are the same person or entity. Example: The Creative Star farecard used by riders of the Hong Kong transit system.

ii. **The Bank Issuer Model:** The merchant and the smart card issuer are separate entities. Financial transactions are cleared through traditional financial systems, e.g. the Banksys’ Proton card in Belgium.

iii. **Non-Bank Issuer Model:** Users buy electronic cash from issuers using traditional money and then spend their e-cash at participating merchants. The merchant then redeems cash from the issuer, e.g. Cybercash’s electronic coin product. *(See Box 1, figure 3.3)*

iv. **Peer-to-Peer Model:** Bank or non-bank issued electronic cash is transferable between users. Only point of contact between traditional payments systems and initial e-cash is the initial purchase of e-cash from the issuer and redemption of electronic cash from individuals or merchants, e.g. Mondex stored value card. *(See Box 1, figure 3.4)*
Box 1: Non-Bank and Peer-to-peer issuer models

III. Examples of Money Laundering Schemes

*E-gold*\(^\text{12}\)

E-gold is an electronic currency, issued by e-gold Ltd., a Nevis corporation, allegedly 100% backed at all times by gold bullion in allocated storage. E-gold was created in response to a need for a global currency on the World Wide Web. E-gold is accounted by weight of metal, not US$ or any other national currency unit. Weight units have a precise, invariable, internationally recognized definition. Additionally, precious metals, gold in particular, enjoy a long history of monetary use around the world. Thus, e-gold is ideally suited for international transactions.\(^\text{13}\) This is not regulated and exists by reason of a trust instrument.

The problems with this type of payment system are acute. Phil Osborne Program Manager for the Department of Customs Cyber-Smuggling Center\(^\text{14}\) alluded to the following dark realities:

>This “free western union” is part of a larger trend for non-financial institutions to become money remitters/intermediaries. These companies have become money havens for the unscrupulous. No CTRs are filled out. No real records are either verified or stored and these money transmitters do not follow due diligence standards. E-gold sells the ability for people to exchange money, thus circumventing the financial institutions and their corresponding oversight/regulatory mechanisms. Intangible services like consulting are common facades for the disbursement of funds between organized criminal syndicates. At issue here is that most of the real hard data is classified. These are ongoing investigations into companies like E-gold who utilize the Internet and nations like Luxembourg and other neutral regimes to base their servers. However, there is classified evidence to suggest that organized criminal syndicates are utilizing these payment mechanisms profusely.

Appendix III depicts the modus operandi of cyber-criminals and the use of these non-bank peer to peer issuers.

*Internet Casinos*\(^\text{15}\)

A joint report by the RAND and Critical Technologies Institute (CTI) describe Internet casinos as “the provision of opportunities to play games of chance or obtain access to sports or race bookmaking via computer networks.”\(^\text{16}\) While ostensibly for amusement

\(^{12}\) For further information see: [http://www.e-gold.com/](http://www.e-gold.com/)

\(^{13}\) Copy taken from Egold’s website

\(^{14}\) In 2002 FINCEN transferred their responsibility for Cyber-money laundering to Customs

\(^{15}\) In a case settled July 25, 2003, U.S. Attorney Raymond W. Gruender went after PayPal Inc. for illegally processing online gambling transactions for customers in the district between June 2000 and November 2002. PayPal, which ceased processing for online gambling services in November 2002, agreed to pay a $10 million fine.


Produced by Tom Kellermann, Sr. Data Risk Management Specialist, World Bank Treasury Security team
purposes, online casinos have given criminal syndicates a fast and easy way to launder dirty money. In essence, dirty money is played on the cyber-casinos, quickly converted into cyber-cash, and the payment of clean money returned to criminals through various cyber-payment or funds transfer systems. This transaction is instantaneous and can be done from the convenience of a home computer. Furthermore, the borderless nature of the Internet makes it possible for users to play at any casino around the world, thereby escaping jurisdictional laws and constraints. According to Forrester Research there are over 1,400 online gambling sites in existence, most of which are based outside of the U.S..

IV. United States Initiatives to Combat Money Laundering

The Federal Bureau of Immigration and Customer Enforcement (ICE) is embarking upon a new investigation initiative called Operation Cornerstone. Its purpose is to prosecute money-laundering crimes and also engage the private sector’s cooperation to mitigate weaknesses in the financial system that allow money laundering to occur. Furthermore, by assigning a dedicated special agent to act as the private sector liaison for each of the 25 bureau field offices, ICE will share information aggregated from investigations with the private sector.

V. Proposed Action Items to Enhance Anti-E-laundering Efforts in the Bank

Despite the World Bank Group’s efforts to address money laundering and terrorist financing, further action can, and should be taken to provide financial institution supervisors and regulators as well as law enforcement with the necessary awareness and training to address the new vehicles for money laundering.

The Internet should be used to combat money laundering and terrorist financing by the World Bank through the following means to augment scarce resources by providing technical assistance and training, networking and information sharing and analysis:

A. FSAPs—The World Bank Group has incorporated a dedicated anti-money laundering module into the FSAP. This module can be enhanced by updating it to provide technical assistance and training on how to identify and reduce new means of money laundering, cyber-crime and terrorist financing such as the “Non-Bank Issuer Model” and the “Peer-to Peer Model”.

17 For further information see: http://www.ecommercetimes.com/story/31962.html

Produced by Tom Kellermann, Sr. Data Risk Management Specialist, World Bank Treasury Security team
B. **Global Payments Systems Mapping Project**— Operational risk is a constant of doing business in a globally interconnected environment. By mapping the various means by which money moves, it will be possible to identify patterns, trends and discrete relationships otherwise unnoticed. This project and the knowledge derived there from can grant policy makers a better understanding of the flow of money, which can in turn be converted into knowledge for helping nations craft such things as monetary policies and financial risk assessment models.

C. **International Information Sharing Vehicle**— Because of the Internet’s ability to compress time and to virulently spread cyber-crime throughout the global financial community speedily, financial regulators need an entity that can operate in this environment by augmenting and enhancing skills and knowledge quickly. Using the U.S. Financial Services Information Sharing and Analysis Center (ISAC) as a model, the Bank should initiate the creation of an International ISAC as a value added service for the Bank and its constituents. Working across financial institutions and financial service providers as a non-profit entity operated by a third party service provider, the International FS-ISAC could provide real-time information sharing, alerts, notifications, web-based education and training on e-money laundering and other cyber crimes. In addition it could provide a cyber-threat analysis center. For example, phishing is an activity that has deeply plagued financial institutions around the world this past year. Most phishing websites are active on average 2.5 days. By the time a bank is aware it has been phished the site has been closed down. With early warning, notification and information sharing banks, regulators and law enforcement could compress time and work together to assist one another on a cross border basis and multi-jurisdiction investigations.

D. **FATF Principle #13**— Knowledge of one’s customers is a fundamental requisite to prevent money laundering. The “KTC” principle is significantly hampered by online transactions where digital money and anonymity of users creates a highly stealthy environment. To increase transparency, there are many authentication solutions, including the use of biometric and public key infrastructure (PKI) for users who initiate large value transfers. Two-factor authentication\(^\text{18}\) should be mandated by law for all financial transactions.

E. **Harmonization and Coordination of Regulation**— This would mitigate the threat of non-registered and/or informal money transmitters (like E-gold.com) who continue to launder the proceeds of organized criminal syndicates in cyber-space. The provisioning of greater entry barriers, e.g. licensing and registration for such entities, will be critical to hindering the effectiveness of money laundering techniques in cyberspace.

\(^{18}\) Two-factor authentication is based on something the user knows plus something the user has or is e.g. biometric fingerprint. The user must have both factors to access the system e.g. ATM Card and Pin.
F. **Electronic Forensics**—Providing technical assistance for training and education on electronic forensics and preservation of electronic evidence is essential for both bank examiners and law enforcement in order to investigate cyber-money laundering and other cyber-crime activities. Oftentimes the most damaging evidence and that which can assist in connecting the dots is financial in nature and can only be offered up by financial institutions and financial service providers. As financial systems migrate to electronic platforms it is essential that they grow the requisite skills to process, store and protect data both to ensure the integrity and quality of the evidence.
## Appendix I: Chart on Global Anti-money Laundering Legislation

<table>
<thead>
<tr>
<th>DEVELOPED COUNTRIES</th>
<th>ANTI-MONEY LAUNDERING LAW</th>
</tr>
</thead>
</table>
| **Austria**         | **Punitive Law**: Penal Code (Articles 165 and 278a)  
                      **Obligations**: Banking Law Articles 39-41 |
| **Belgium-Luxembourg** | **BELGIUM**
                      **Punitive Law**: Article 505 of the Penal Code
                      **Obligations**: Law of 11 January 1993
                      **FIU Law**: Royal Decree of 11 January 1993 (set up the Financial Intelligence Processing Unit)
                      **LUXEMBOURG**
                      **Obligations**: Act of 5 April 1993, Act of 18 December 1993 |
| **Australia**       | **Punitive Law**: Proceeds of Crime Act 1987
                      **Obligations**: Financial Transactions Report Act 1988 |
| **Denmark**         | **Punitive Law**: Danish Criminal Code
                      **Obligations**: Danish Act on Measure to Prevent Money Laundering 1993 |
| **Finland**         | **Punitive Law**: Finnish Penal Code (“money laundering” is not used, but there is a relevant offense)
                      **Obligations**: Act on Preventing and Clearing Money Laundering, latest amendment 1 June 2003 (set up a Money Laundering Clearing House at the National Bureau of Investigation) |
| **France**          | **Punitive Law**: Penal Code 324-1 to 324-9
                      **Obligations**: Monetary and Financial Code (Articles L562-1 to L562-10, L563-1 to L563-6, L564-1 to L564-3, L574-1 to L574-2) |
| **Germany**         | **Punitive Law**: Criminal Code (Section 261) |
| **Ireland**         | **Punitive Law and Obligations**: Criminal Justice Act 1994 |
| **Italy**           | **Punitive Law**: Law 328/1998 modifies articles 648bis and the of the Criminal Code to criminalize money laundering
                      **Obligations**: Law no. 197 of July 1991 |
<p>| <strong>Japan</strong>           | <strong>Punitive Law</strong>: Anti-Drug Special Law (penalizes money laundering connected to drug offenses specifically) |</p>
<table>
<thead>
<tr>
<th>Country</th>
<th>Punitive Law</th>
<th>Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands</td>
<td><strong>Criminal Code (Articles 416-417bis)</strong></td>
<td><strong>the Identification Act and the Disclosure of Unusual Transactions Act</strong></td>
</tr>
<tr>
<td>Portugal</td>
<td><strong>Decree Law 15/93</strong></td>
<td><strong>Decree Laws 325/95 and 313/93</strong></td>
</tr>
<tr>
<td>Singapore</td>
<td><strong>Drug Trafficking Act, Sections 41 and 43</strong></td>
<td><strong>Guidelines issued by the Monetary Authority of Singapore</strong></td>
</tr>
<tr>
<td>Spain</td>
<td><strong>Penal Code Article 301</strong></td>
<td><strong>Spanish Money Laundering Law of 23-12-1993</strong></td>
</tr>
<tr>
<td>Sweden</td>
<td><strong>Chapter 9 of the Swedish Penal Code (the term, “money laundering,” not specifically used)</strong></td>
<td></td>
</tr>
<tr>
<td>Switzerland</td>
<td><strong>Penal Code, Articles 305 bis and 305 ter</strong></td>
<td><strong>Money Laundering Act adopted in 1997</strong></td>
</tr>
<tr>
<td>United States</td>
<td><strong>Title 18 of the United States Code</strong></td>
<td><strong>International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, USA PATRIOT Act, Bank Secrecy Act</strong></td>
</tr>
<tr>
<td>United Kingdom</td>
<td><strong>Drug Trafficking Act 1994</strong></td>
<td><strong>Money Laundering Regulations 1993</strong></td>
</tr>
<tr>
<td>DEVELOPING COUNTRIES</td>
<td>ANTI-MONEY LAUNDERING LAW</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td><strong>Punitive Law and Obligations</strong>: Law No. 25.246</td>
<td></td>
</tr>
</tbody>
</table>
| Brazil               | **Punitive Law and Obligations**: Law No. 9.613, Law No. 2.852  
**FIU Law**: Decree No. 2.799 (established the Financial Activities Control Council, a.k.a. COAF), Order No. 330 (regulation of COAF) |
| China                | **Punitive Law**: Articles 191 and 312 of the 1997 Criminal Code  
**Obligations**: Anti-Money Laundering Regulations, RMB Reporting Measures, Forex Reporting Measures |
| Czech Republic       | **Punitive Law**: Sections 251, 251a and 252 of the Penal Code  
**Obligations**: Act No. 61 |
| Egypt                | FATF non-cooperative countries and territories (NCCT) list  
**Punitive Law and Obligations**: Law 80/2002 |
| Hong Kong, China     | **Punitive Law and Obligations**: Drug Trafficking (Recovery of Proceeds) Ordinance, Organized and Serious Crimes Ordinance |
| Hungary              | **Punitive Law**: Section 303 of the Criminal Code  
| India                | NA |
| Korea, Rep. Of       | NA |
| México               | **Punitive Law**: Article 400 bis of the Penal Code |
| Philippines          | FATF NCCT list  
**Punitive Law and Obligations**: Anti-Money Laundering Act of 2001, amended by Republic Act No. 9194 |
<p>| Poland               | <strong>Punitive Law</strong>: Article 299 of the Criminal Code |</p>
<table>
<thead>
<tr>
<th>Country</th>
<th>Punitive Law</th>
<th>Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russia</td>
<td>Articles 174 and 174.1 of the Criminal Code</td>
<td>Federal Law 115-FZ</td>
</tr>
<tr>
<td>Turkey</td>
<td>Law No. 4208 on the Prevention of Money Laundering</td>
<td></td>
</tr>
<tr>
<td>Thailand</td>
<td>Anti-Money Laundering Act 1999</td>
<td></td>
</tr>
<tr>
<td>Ukraine</td>
<td>FATF NCCT list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Punitive Law: Article 229 (12) of the Criminal Code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obligations: Law of Ukraine “On Prevention and Counteraction of Legalization (Laundering) of Proceed from Crime”</td>
<td></td>
</tr>
</tbody>
</table>
Appendix II: FINCEN/Rand Study

In 1998 a RAND Study entitled *Emerging Cyberspace Vulnerabilities Through Emerging Cyberspace Technologies* was produced for the Financial Crimes Enforcement Network (FINCEN) of the U.S. Department of Treasury to examine potential money laundering and financial crime concerns raised by the emergence of cyber-payments and E-banking. It states that “Due to advanced computing and communications technologies organized criminal syndicates utilize this existing medium—the Internet to facilitate and enhance the efficiency and anonymity of today’s money laundering operations.”

The study concluded that:

1. **Record keeping systems**: collecting the information on the nature of network traffic. Profiling techniques through artificial intelligence. Data mining would be useful.
2. **Authentication measures**: Digital signatures/PKI and biometrics
3. **Tracking Systems**: Classifier systems and software agents utilizing Artificial Intelligence.
4. **Enhanced sharing of information amongst Financial Intelligence Units (FIUs)**. The creation of such a database necessitates security for both authenticating authorized users and the layered security of the database to keep potential criminals from spying upon law enforcement activities.

The combination of record keeping systems, authentication measures and tracking systems yields infrastructure that is useful to the law enforcement community for mitigation of this threat. All of these technological solutions are an integral part of proper E-security as well. The Technology Risk Checklist 7.3 and 8.1 dissects each one of these elements in detail.
Appendix III: A birds eye view on how cyber criminals obtain and launder funds

The following excerpts detail conversations that routinely take place in an Internet Relay Chat room (IRC).

Of course the usual sort of activity continues unabated. It is a boom time for the underground economy. This is particularly true in the Middle East, with most of the underground economy IRC networks run by Middle Eastern crews. While some of these networks are run by Middle Eastern crews, the denizens of these networks come from all over the world. Think of it as a very cosmopolitan bazaar.

<A> got verified paypal......worth $894.39 and $598...
need fresh visa mastercard or discover or active
master aol accounts..........msg me for trade i ver
1st or dont msg me i dont have time playin with
rippers

<A> i need cvv2 virgin i have root & shell & i can send
money

<A> Need Stormpay,PayPal and other offers, MSG ME! Need
good partners!

<A> i sell cvv2 and track 2 cc's (just hacked)------
message me for a good deal

<A> have paypal,root,shell,psybnc.I need virgin cc. Only
cc nr,exp and date of birth of the cardholder.
(mastercard or visa) or aol scam page...I ver 1st or
no trade

<A> has psybnc vhosted (255 vhosts), bnc vhosted (295
vhosts), shell (vhosted and eggable), roots, exploits,
and ebay! I need a site c-a-r-d-e-d! msg me!

We must ask why a miscreant located in the Middle East needs drop sites and bank accounts in the USA.
There is a lot of chatter about visas in several Middle Eastern miscreant channels. Most of it is centered on Australian visas for some reason.

The latest rage in the Middle Eastern chat channels are I.T. certifications. The offers pour in at a rapid rate.

{ MCSE , CCA , CCNP , CCNA ,MCSA ,CCIE , A+ , CIW ,
CCA , A+ , and Tofel , Iltes }
With 100% Gaurantee

The usual sorts of trades take place 24x7x365, becoming a sort of background noise in the logs.

need http proxies msg me

i need exploits of gsm phone hacking

have shell, bnc, root, hacking hotmail account,
paypal $2000 , i need valid cc anyone interested
MSG me and he will verify first

i have alot of hacked ebay accounts, msg me if you are intrested

want to Trade bots

I need cvv2s with 9,000$ Visa or Master. MSG Me For Trade.

I need European Mastercard/Visa. MSG Me For Trade.

trade shell 4 shell! uptime 210 days!

i need one root linux , i have root sun0s , or psyBNC sun0s owner ... prv me !
<J> trade psybnc or Bots Channel to Channel ; msg me in pv

<K> i have shell very stable , i need root or shell msg me for good deal!! Ripper died!

<L> i have 2 laptops at a cheap prise if you are inrested msg me for more details . Thanl You!

<M> trade vhosted shell with uptime 490 days I add u shell in my server if u give me other shell or root on ssh22! /msg me for nice trade (u can ver first!)

<N> need fast shell i give psybnc shells roots apache ciscos and much more BUT i Ver 1st Or No Bye Bye!!

<O> Have exploit 0days ! I need 2 shells , I ver 1st or bye !

<P> Need id on adultbouncer.com .....i have vhosted shelll....vhosted psybnc.....rh roots .....sunos shells....i verify FIRST or no TRADE!!!!

<Q> can card items to ur drop or mine, msg me for business, also if u have ebay seller accts msg me

<R> Anyone here tht can card templatemonster.com msg me i pay u e-gold money

<S> i have 400 cvv2 full info/200 ebay accouts with email acces /paypal verified with email acces msg me if u wanna buy some :P

<T> (Have) Root/Shell/Psybnc/Bnc/Ebay/CC/E-Gold/Domain/ Paypal Verified (Need) Vhosted Shell Msg Me For Trade Good (lammers no msg me).

<U> I have virgin ccs need E-gold or cvv2
<V> I NEED EGOLD. I HAVE 400$ STORMPAY! MSG ME!

<W> Got E-Gold Accounts, PayPal Accounts, Vhosted
    Shells (ushells.net), Vhosts (ipv4 - ipv6), Full
    Domin, Root, Root Scan, Root Nuke, Proxy Serv,
    Fresh CC's, Fresh Cvv2 (Need Root) I Verify 1st!!!

<X> has psybnc vhosted, bnc vhosted, shells, roots,
    exploits, scanner (ssh), ebays, domains, and bots!
    I need a site c-a-r-d-ed! pm me!

<Y> i need cc for europe , i have cc for usa , i verify
    first , thanks

<Z> SELLS FULL INFOS, THEY ARE ALSO COBs AND WILL GIVE
    A SAMPLE TO PROVE THAT HE'S LEGIT . THEN WHEN I
    SHOW YOU THE SAMPLE YOU SEND MONEY. MSG ME NOT
    THOSE I'M NOT GIVING A SAPLE FIRST RIPPERS

<AA> have shell, root, vhosted psybnc, psybnc owner(users)
    proxy list (sock 4/5, https), program to check proxys.
    need bank account or cc with fool information

Pulling real currency out of the underground economy is no longer a
challenge of risk or logistics. There are plenty of brokers willing to help
out, for a price.

<A> anyone have a login to the defcon proxy site? msg me
<B> ah man A about 2 days ago i did
<B> man
<B> i would have given it to you
<B> Im gonna buy it again
<B> i have had a good month cashing out cvv2s
<B> pm me and ill hook yah up
<B> providing cashout to ops mainly as they messarround,
    will offer to cashout cvv2s to others but only for
    either a small amount from the cashout or another
    arrangement ( all heavy carders, welcome, no newbies
thanks)

<C> Cann cash out e-gold in 24h, and send you in WU money!
Cann take Wu money and send you back (i dont care from
were are they), Cann take wire and send you back in Wu
or e-gold money! for more info msg me!

<D> have many paypal/e-gold/stormpay/etc verified, i want
to cash out it with the check/send money, who have
bank account in USA, to cash it or receive the money,
msg me for a good deal.. it's no trade!!

Having US-based bank drops is becoming a common trend.

<A> I have U.S. Banks to drop, if you can do Wire
Transfers /msg genius`

<A> genius if you have bank drop wit bank acc victim
we can something happen
<B> learn english..
<B> then something could happen
<C> hehe
<B> ;)
<D> lol
<D> A its not that easy
<D> it requires you having a offshore account, merchant
account and software

Obtaining Social Security Numbers isn't as difficult as it should be. In
fact a miscreant can too easily obtain the complete details, to include the
driver's license number, of innocent victims.

<A> Am selling full info CCs include [ssn, dob, mmn, cvv2,
bankinfo, pincode, dlnumber,...etc] --- EBAY seller
id/pass with mail access ---- verified paypal
accounts with mail access /msg me now for a good
deal

As previously mentioned, a great many Middle Eastern miscreants shop in the
underground economy. Some of them have resources in the US.

<A> has U.S Bank Drop, i could cashout Full Infos,Paypal, Wire Transfers,Stormpay,Bidpay, and iKobo.../msg me for deal
<A> acool
<A> u making any money lately?
<A> lol
<A> i'll buy you a house
<A> nah
<B> lol
<A> i wana makke some money
<A> but i need a good partner
<A> all i want is 35%
<A> acool
<A> ur arabic?
<C> yes
<C> iraqi
<D> nice
<D> :
<C> nice?
<C> MAN im not gay
<E> :
<A> im palestinian
<C> i hate palestina
<C> I love israel
<C> :D
<D> why acool
<D> :|
<D> hehehehe
<A> hes an idiot

Thanks to the use of keylogging and data extraction bots, which is just about every bot now installed, the miscreants have ready access to bank accounts and other financial accounts.

<A> selling Bank Of America online access with $10.000 and other with $900 balance. Payment : Western Union
who can cashout Bank Of America/Washington Mutual without pin but with online access msg me and lets make a great deal!

can cashout verified paypals in 2 days. $2000 every couple of days. 75/25. Msg me for deal

Payee: Centennial Bank
Centennial -5541
4605 Harrison Blvd.
Ogden, UT 84403
914-528-5626 Confirmation Number: XXX-YYY
To edit this payment, change the payment information and click Save Changes
Payee Amount Send Action
Centennial...
Centennial $2,500.0 05/05
i am w8 for new found hehe:D
ey they just founded 2 transfers and i said why not try again
this is my online acc:Payee: Centennial Bank
i just send from a bank of america
they sended checks to my acc lol
2 checks for 2.500
lol
gotta to go to italy to cash

I SELL PAYPAL VALID AND VERIFIED WITH BALANCE 50$++++
MSG ME U GOT username/pw email acces ,pw!!ONLY WU!
rippers dont waste my time

have some 2k in Wells Fargo can transfer it in a form of check and can send paypal cash ....msg me if you can i perfer do deal with OPS@

--- snip snip ---

** SENSITIVE INFORMATION**