



Evoluzione del crimine informatico nel 2010

**Evoluzione del crimine informatico:
dal fenomeno “hacking” all’ingresso del
crimine organizzato**



INDICE DELLA PRESENTAZIONE :

1. Storia dell'hacking (nascita, evoluzione, estinzione)
2. Spamming
3. Bullet proof network
4. Phishing
5. Botnet
6. Pharming
7. Identity Theft
8. Card fraud
9. Phone fraud



Panoramica del fenomeno dagli anni 80/90 ad oggi

Per comprendere bene il fenomeno è necessario conoscerne le origini e le motivazioni delle persone coinvolte.

La storia dell'hacking può essere suddivisa in due diverse ere:

- Quelle della sperimentazione e del pionierismo, dalla fine degli anni 70 agli inizi degli anni 90 quando le tecnologie di comunicazione erano poche, confuse e per pochi addetti ai lavori
- Quella dell'uso di massa, a partire dalla diffusione di Internet dal 1994 in poi



Questo era il panorama negli anni 70/80/90: molte reti, costosissime, nate per vendere tempo macchina dei mainframe o per connettere enti di ricerca/universitari, scarsamente documentante:

- X.25 psns (1975 – still alive)
- Bitnet (1981-1996)
- Comuserve (1969 – 2009*)
- GENIE (1985 – 1999)
- Prodigy (1980 – 1999)
- Decnet (1975 – ?)



- anni '70: phreaking, università e blue boxing (Steve Jobs and Steve Wozniack, Capt. Crunch)
- 1981: Captain Zap è la prima persona ad essere arrestata per reati informatici
- 1982: nasce il Chaos Computer Club
- 1983: Mitnick viene arrestato per la prima volta (1987, 1988, 1995)
- 1984/1985: the coocko's egg - hackers tedeschi accedono a siti militari usa per conto del KGB
- 1988: il primo worm su Arpanet blocca "per sbaglio" 6.000 computer (10% dei computer connessi)
- 1989: WANK worm colpisce i sistemi VMS su rete DECNET



Ian Murphy (Captain Zap) è il primo uomo ad essere incriminato ed arrestato per reati informatici



- 1990: la guerra tra due bande rivali (MOD e LOD) paralizza le reti telefoniche USA
- 1991: Kevin Poulsen, Radio contests & Porsches
- 1994: Vladimir Levin riesce a spostare 10,7 milioni di dollari da conti Citibank
- **1993 Hackers Hunter, la prima operazione di contrasto in Italia**
- **1995 operazione ICE Trap**
- **1999** due hacker vengono giustiziati in Cina per reati commessi nel 1993



- **1985** Canada Unauthorized use of computer -- s. 342.1
- **1986** USA Computer Fraud and Abuse Act
- **1988** francia
- **1990** UK Computer Misuse Act 1990
- **1991** Australia The Telecommunications Act of 1991 (sections 74 and 76)
- **23 dic 1993** Italy articolo 615 (ter, quater, quinquies) e 635 bis
- **1996** Russia Chapter 28 of the Criminal Code (article 272, 273, 274)



- Pionieri erano indistintamente presenti negli USA e nelle principali nazioni europee:
 - Germania (CCC)
 - UK (8lgm)
 - Italia (DTE222, Pier Group, Mc Link)
 - Francia
- Agli inizi degli anni 90 con l'espansione dell'economia arrivarono anche altri paesi:
 - Argentina
 - Brasile
 - Russia



- Il fenomeno “hacking” su Internet seguì invece un percorso diverso, in parte legato all’economia ed in parte casuale:
 - 1992- 1993 USA
 - 1994 - 1995 – Francia
 - 1995 – 1996 Germania
 - 1995 – 1996 Italia (anche grazie a Video on Line)
- Dal 1999 ad oggi si susseguirono in ordine cronologico
 - Brasile
 - Polonia
 - Romaniaa
 - Cina
 - recentemente i paesi islamici del medio oriente (iran, pakistan, marocco, etc.)
- La Russia è sempre stato un paese trasversale
 - Sempre presente ma silenzioso a causa di una fortissima “selezione naturale” dovuta alla difficoltà di accesso alla rete svincolata dalle risorse economiche



“La criminalità informatica è direttamente correlate alla diffusione di massa dell'informatizzazione che ha aumentato la possibilità di lucro”

- 1997 inizio dell'uso massivo di Internet in Italia
- 1998 escono i primi dialer
 - Nessuna relazione con l'hacking, puro scopo di lucro
 - C'è una recrudescenza del fenomeno applicata alla telefonia mobile

SPAMMING





- Lo spamming è l'invio di enormi quantità di email non richieste
 - Vendita di prodotti (medicinali, luxury replica, diplomi, online casinò, etc.)
 - Truffe (nigerian scam, ricerca di drop, truffe "sentimentali")
 - Phishing
 - Diffusione di worm/trojan/virus
- Lo spam è (quasi) mondialmente riconosciuto come reato
 - Esistono purtroppo dei paesi tecnologicamente avanzati (cina, russia, india) spam friendly
- Forse non tutti sanno che:
 - La prima email di spam fu inviata a 600 indirizzi email nel 1978 per pubblicizzare dei prodotti DEC
 - Già dal 2006 oltre l'80% dello spam viene inviato tramite botnet
 - Ogni giorno vengono inviate 183 miliardi di email di spam (97% del totale!)



- una discreta quantità di spam viene inviata da account di provider molto noti (gmail, yahoo, hotmail) in quanto solitamente non filtrati dagli strumenti antispam, come?
 - Tramite account rubati, generalmente da botnet o sottratti a siti compromessi (Identity Theft)
 - Tramite account registrati: esistono aziende in cina, india e bangladesh che vengono pagate dagli spammer per effettuare le registrazioni inserendo manualmente il CAPTCHA (circa un dollaro per 1000 CAPTCHA risolti)



- Uno studio del 2008 dimostra come il ritorno dello spam sia inferiore allo 0.00001% (su 350 milioni di email solamente 26 hanno portato ad un acquisto di farmaci)
 - Nonostante ciò gli introiti dovuti allo spam sono stimati in alcuni milioni di dollari l'anno
- Diversamente, lo spam mirato ha tutta un'altra economia (1-5 dollari ad email)
 - Interi database di clienti vengono trafugati su commissione



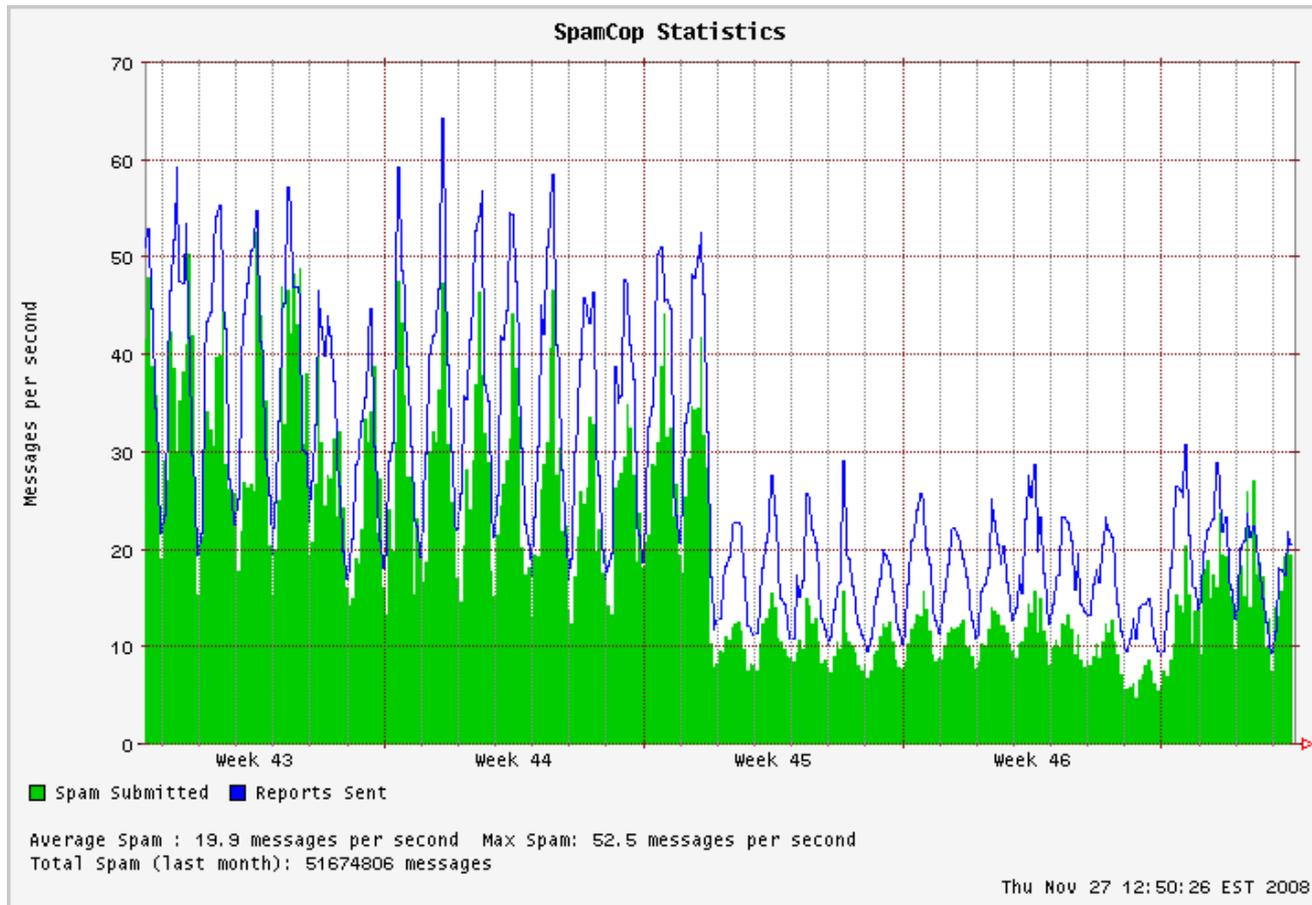
- Altre tipologie di spam sono quotidianamente applicate a:
 - Forum
 - Blog
 - Newsgroup
 - Chat (IRC, mspace, etc.)
 - Instant messaging SPIM (Skype, MSN, Yahoo! Messenger)
- Come per quello tradizionale questa forma di spam è mirata a diffondere trojan e a veicolare offerte pubblicitarie

Bulletproof Hosting e Data Heaven



- Alcune server farm in paesi privi di legislazione adeguata sono in grado di offrire protezione ai principali spammers; famoso è il caso McColo, primo a subire de-peering perché situato negli USA:
 - Riconosciuto come hosting per le principali botnet (Mega-D, Srizbi, Pushdo, Rustock e Warezov) in grado di generare il 70% dello spam mondiale
 - Nel novembre del 2008 è stato effettuato il de-peering della rete, conseguentemente si è notata una notevole riduzione dello spam
 - Il traffico spam è tornato a risalire nei mesi successivi man mano che le botnet venivano riorganizzate presso altri hosting offshore

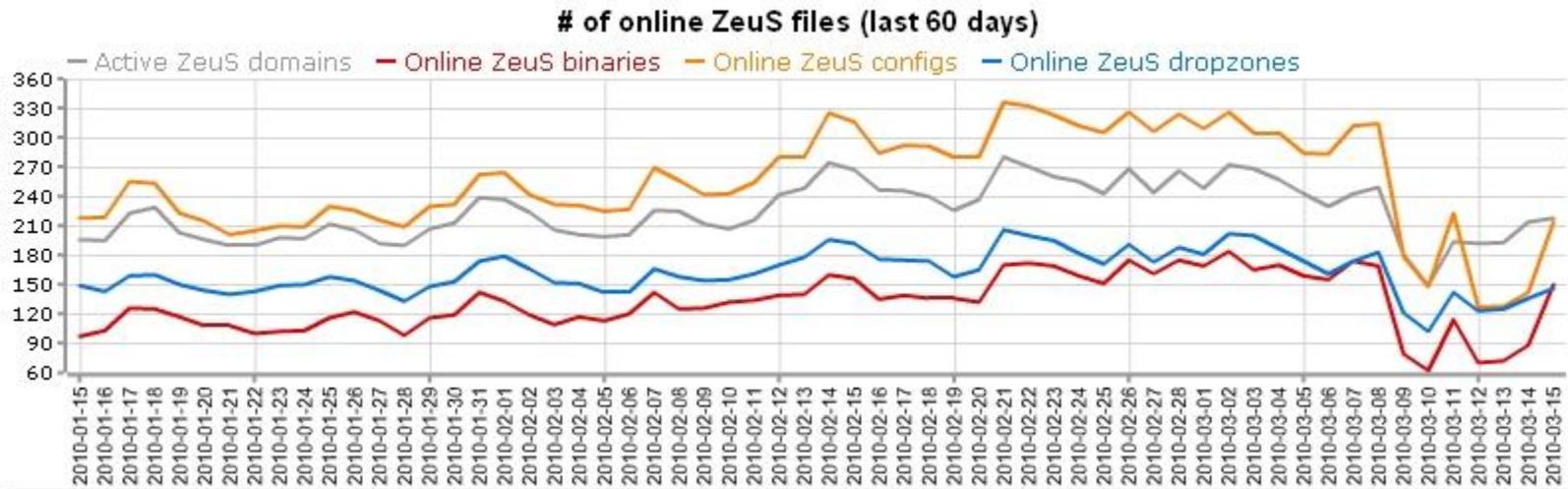
Bulletproof Hosting e Data Heaven





- Negli anni successivi anche altre reti sono state rimosse dalle tabelle BGP
 - AS 50033 (GROUP 3 LLC) de peering recente
 - AS 49365 (GROUP VERTICAL) ottobre 2009
 - Real Host (AS8206) agosto 2009 diminuzione del 38% dello spam
 - Troyak (AS50215) marzo 2010 riduzione della botnet Zeus
- Alcuni network si sono dimostrati molto resistenti in quanto dotati di connettività di backup

Bulletproof Hosting e Data Heaven



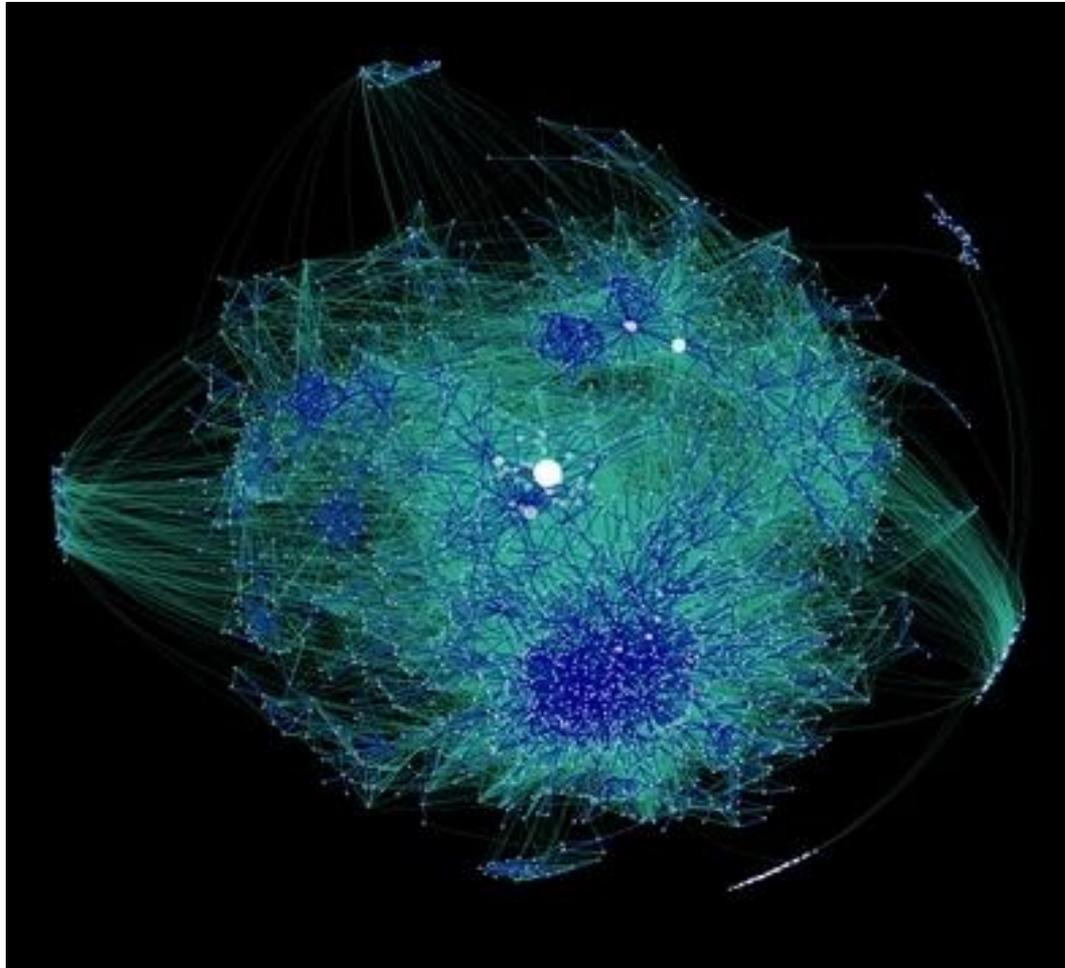
PHISHING





- C'è veramente poco da dire di nuovo sul phishing: è una tecnica fraudolenta che mira a carpire informazioni degli utenti solitamente inerenti la sfera economica (carta di credito, home banking, paypal, ebay)
 - Nonostante tutto, grazie al crescente numero di utenti poco informatizzati, riscuote ancora buoni risultati tra i cyber criminali
 - Per aumentarne l'efficacia, il phishing viene associato all'uso di attacchi XSS, laddove ne vengano individuati sui siti di interesse (c'è un consistente mercato underground per questa tipologia di vulnerabilità)
- Il termine **Whaling** indica il phishing mirato all'executive management delle aziende
- Il termine **Vishing** indica il phishing effettuato telefonicamente, di solito tramite l'uso del VoIP che permette lo spoofing del caller id

BOTNET





- Una botnet è un insieme di sistemi connessi ad Internet e pilotati remotamente da un'unica entità
 - L'entità che controlla viene definita bot master/herder
 - I computer controllati prendono nome di bot o zombie
- Le botnet comprendono diverse tipologie di sistemi:
 - Router residenziali: solitamente utilizzate per attacchi DDoS e come sistemi ponte per attacchi informatici (es. botnet Chuck Norris e psyb0t)
 - PHP hosting: queste botnet infettano i server di hosting linux in cui sono presenti applicazioni PHP vulnerabili a RFI; nonostante il numero di bot sia normalmente limitato la capacità di fuoco è elevata. Vengono solitamente utilizzate per attacchi DDoS e come sistemi ponte (es. botnet muie)
 - Client Microsoft Windows, sono le botnet più diffuse in quanto possono contare su un elevatissimo numero di zombie che possono essere controllati e sfruttati per ottenere dei vantaggi economici



- La diffusione della botnet avviene attraverso molteplici vettori:
 - Spamming di email contenente il trojan
 - Spamming contenente un link al trojan
 - Spamming con allegati contenenti exploit client side (pdf, jpeg, directX, etc)
 - Exploit per il browser contenuti dentro un iframe di un sito web compromesso
 - Network worm che fanno uso di una o più vulnerabilità remote (Conficker)
- Esistono molteplici usi per le botnet, tutti illegali:
 - Spamming/Phishing
 - Distributed Denial of Service
 - Advertising fraud (click fraud)
 - Furto di credenziali di accesso
 - Frodi (carte di credito, home banking)



- Le botnet generano oltre l'80% dello spam mondiale

Botnet	Client infetti	SPAM Rate
Conficker	+10.000.000	10 Billions/day
Kraken	495.000	9 Billions/day
Srzbi	450.000	60 Billions/day
Rustock	150.000	30 Billions/day



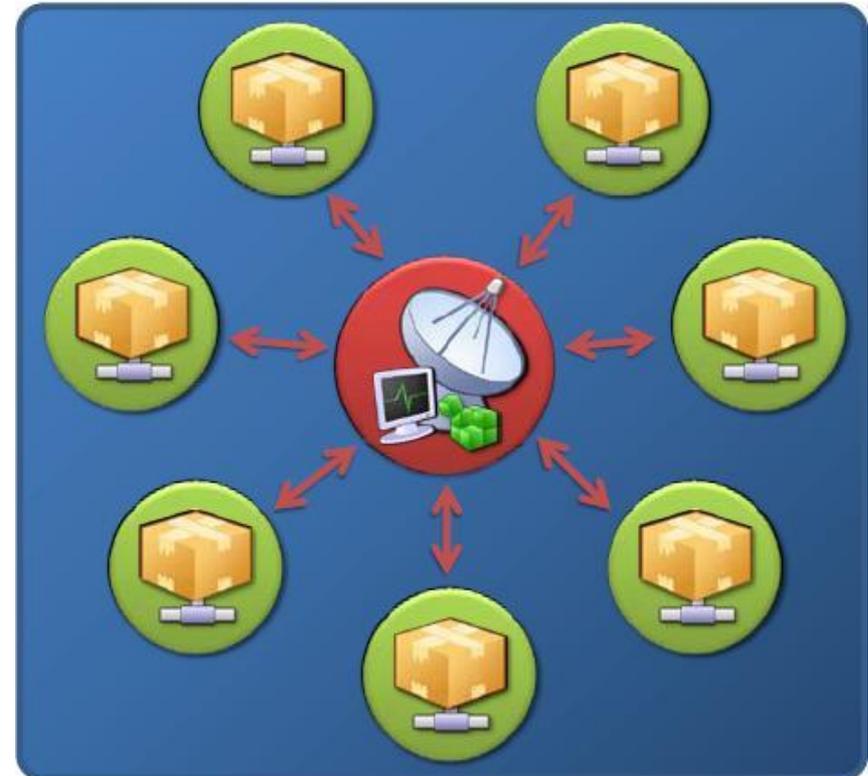
- Il mezzo utilizzato dal botmaster per pilotare i bot viene definito **Control Channel**

Botnet name	Control Channel
Botnet fino al 2007	Internet Relay Chat
Mariposa	Encrypted UDP Channel
Conficker	http pull – P2P (udp & Netbios)
Zeus	http push&pull
Grey Pigeon/Hupigon	Google Apps
?	Twitter
?	Facebook



Architettura centralizzata

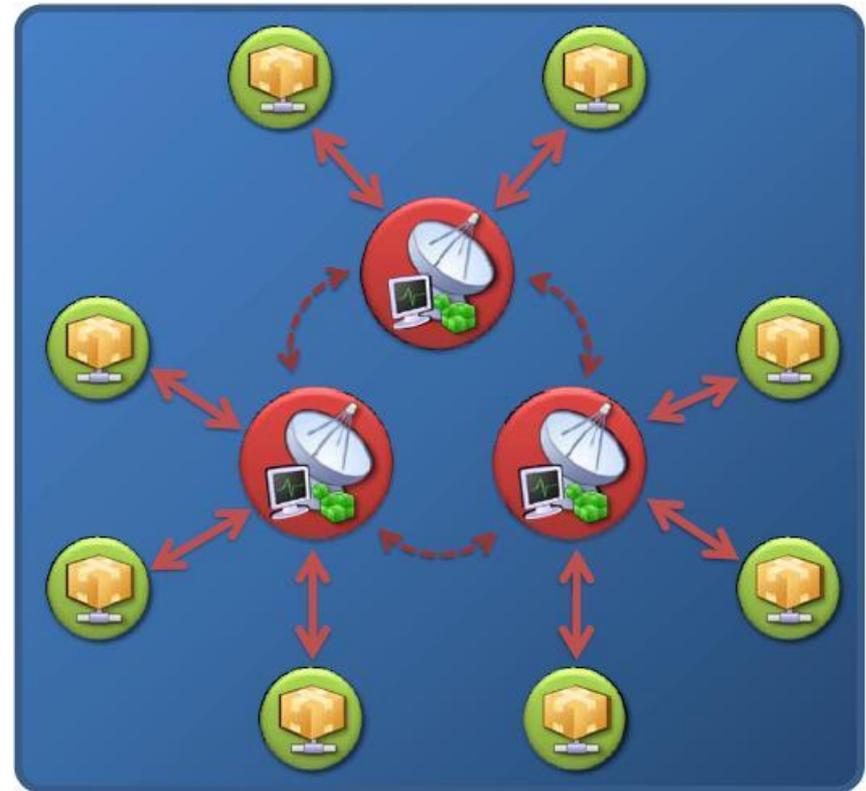
- Pro
 - La connessione tra il botmaster e gli zombie è diretta e quindi molto veloce
- Contro
 - Single Point of Failure, per bloccare la botnet basta trovare il server centrale





Architettura multiserver

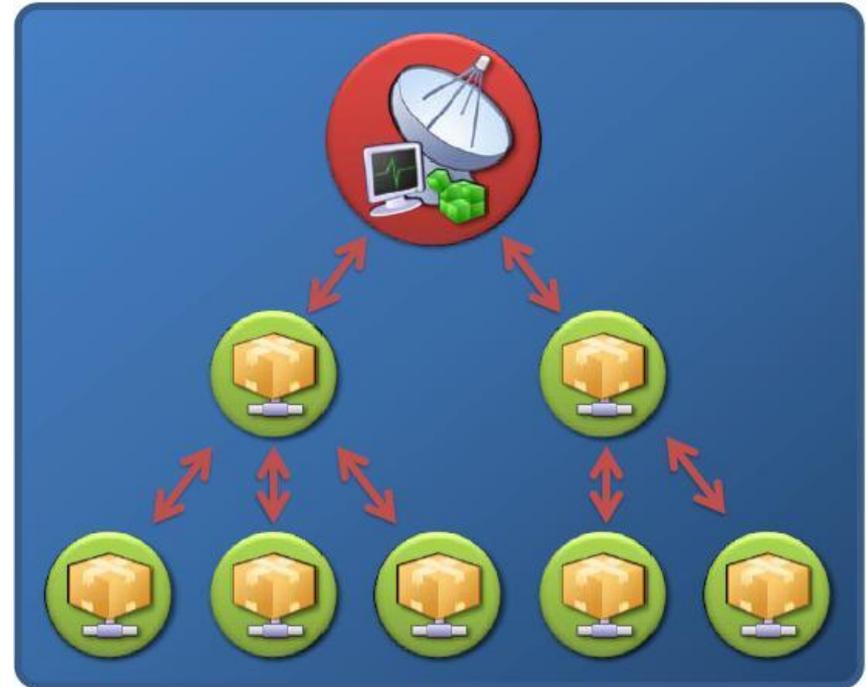
- Pro
 - Elimina i Single Point of Failure
- Contro
 - È più complicata da progettare





Architettura gerarchica

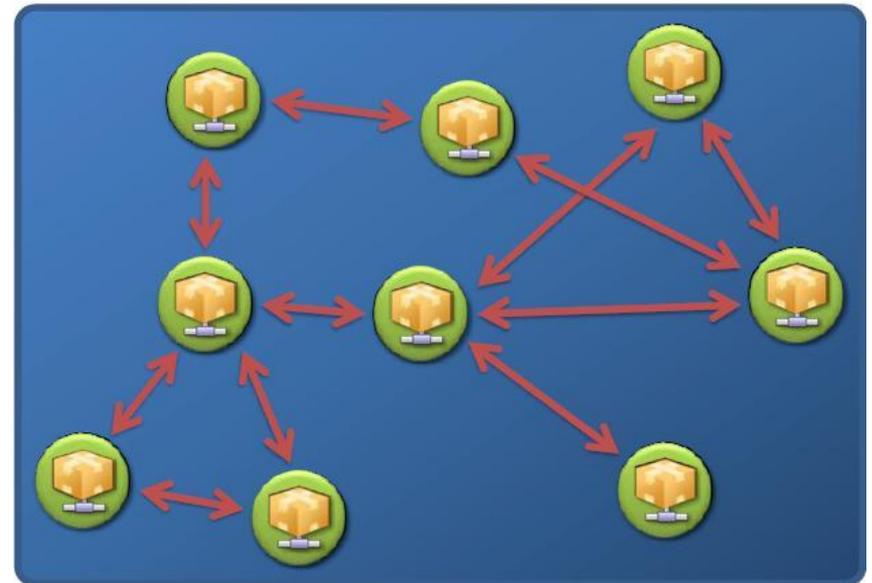
- Pro
 - L'individuazione del Control server è molto difficile
 - Permette la frammentazione della botnet (noleggio/vendita)
- Contro
 - I tempi di controllo possono dilatarsi





Architettura P2P

- Pro
 - È quasi impossibile smantellarle
- Contro
 - Analizzando un bot è possibile risalire a buona parte dei sistemi infetti





- L'offerta sul mercato nero è molteplice ed è possibile acquistare varie forme di crimeware:

Botnet name	Prezzo
Zeus Botnet	\$ 4000 – \$ 10.000
Barracuda botnet	\$ 1.600 + moduli
YES Exploit System	\$ 600
El Fiesta	\$ 1.000
Eleonore Exploit Pack	\$ 700 - \$ 1.500



- Zeus è la botnet DIY al momento più diffusa
 - È in circolazione dal 2007
- Il pacchetto è composto di tre moduli:
 - Il pannello di controllo (control server), che può anche essere preso a “noleggior” ad un costo variabile a seconda dei moduli disponibili e del numero di bot controllati
 - Il builder, che consente la personalizzazione del trojan da installare sui computer infetti ad un costo base di circa 4000\$ a cui si deve sommare il costo dei singoli plugin
 - La dropzone, che può risiedere sullo stesso control server ed è il sito a cui vengono inviati i dati intercettati dal trojan
- L’installazione e l’utilizzo sono alla portata di un qualsiasi utente medio
 - Un utente con conoscenze minime può configurare ed avviare una botnet in meno di 5 minuti



- Molteplici funzionalità:
 - Capture credentials out of HTTP-, HTTPS-, FTP- and POP3-traffic or out of the bot's protected storage
 - Group the infected clients into different botnets
 - **Integrated SOCKS-Proxy**
 - Web form to search the captured credentials
 - Encrypted config file
 - Function to kill the Operating System
- Tutte le comunicazioni tra I bot ed il control server sono cifrate in RC4
- A differenza di altri trojan questo è stato specificatamente scritto con lo scopo di rubare denaro
 - JabberZeus è in grado di intercettare realtime le credenziali di accesso all'home banking bypassando multifactor authentication



- Zeus è un trojan modulare:

modulo	Prezzo
Kit base	\$ 3.000 – \$ 4.000
Backconnect	\$ 1.500
Firefox Form Grabber	\$ 2.000
Total Control/VNC	\$ 10.000
JabberZeus	\$ 500



- La propagazione avviene solitamente tramite email (quindi SPAM) oppure tramite l'ausilio di strumenti di infezione che fanno uso di exploit client side come ad esempio:
 - LuckySploit
 - El fiesta
 - Fragus
 - Liberty Exploit System
 - Eleonore Exploits Pack
- Questi pacchetti possono sfruttare vulnerabilità note e non per forzare i client a scaricare ed eseguire il binario di Zeus:
 - MS06-014
 - PDF util.printf()
 - Flash 9
 - MS009-02 per IE7
 - Many more



- Al momento dell'infezione il trojan è già stato preconfigurato dal builder con alcune opzioni base:
 - L'url da cui scaricare i nuovi aggiornamenti e configurazioni
 - L'url a cui inviare i dati (cifrati) che vengono intercettati (username, password, pin, etc.)
 - Le chiavi di cifratura
 - Alcuni timing relativi alla richiesta di nuove release del software, della configurazione e dell'invio di informazioni al server di raccolta (dropzone)
- Appena possibile il trojan contatta il Command&Control servers da cui riceve gli aggiornamenti e le nuove configurazioni del caso:
 - Nuove versioni del file eseguibile per aggirare gli antivirus
 - Domini su cui fare dns hijacking (* **pharming**)
 - Upload di plug-in (key-logger, strumenti per SPAM, DDoS)



```
<Msg ID=20002 URLLastBinary FileLen=33 RealLen=33 Type='Uncompressed'>  
http://evilzeusdomain.ru/zs/ldr.exe (Latest trojan binary)  
</Msg>  
<Msg ID=20003 URLServer0 FileLen=29 RealLen=29 Type='Uncompressed'>  
http://evilzeusdomain.ru/zs/s.php (Dropzone)  
</Msg>  
<Msg ID=20004 URLAdvServers FileLen=37 RealLen=37 Type='Uncompressed'>  
http://evilzeusdomain.ru/zs/cfg.bin (Latest config file [encrypted])  
</Msg>  
<Msg ID=20006 HTTPBotlogFilter FileLen=153 RealLen=188 Type='Compressed'> (Watching for the  
URLs below)  
!*microsoft.com/*  
!http://*myspace.com*  
</Msg>  
<Msg ID=20008 HTTPFakesList FileLen=621 RealLen=1974 Type='Compressed'> (Fake / redirect the  
URLs below)  
https://signin.ebay.com/ws/eBayISAPI.dll?co*  
https://sitekey.bankofamerica.com/sas/signon*  
https://www.paypal.com/*/cgi-bin/webscr?SESSION*  
https://onlineservices.wachovia.com/auth/AuthServ*  
https://banking.*.de/cgi/ueberweisung.cgi/*  
[...]  
</Msg>
```

Zeus: diffusione

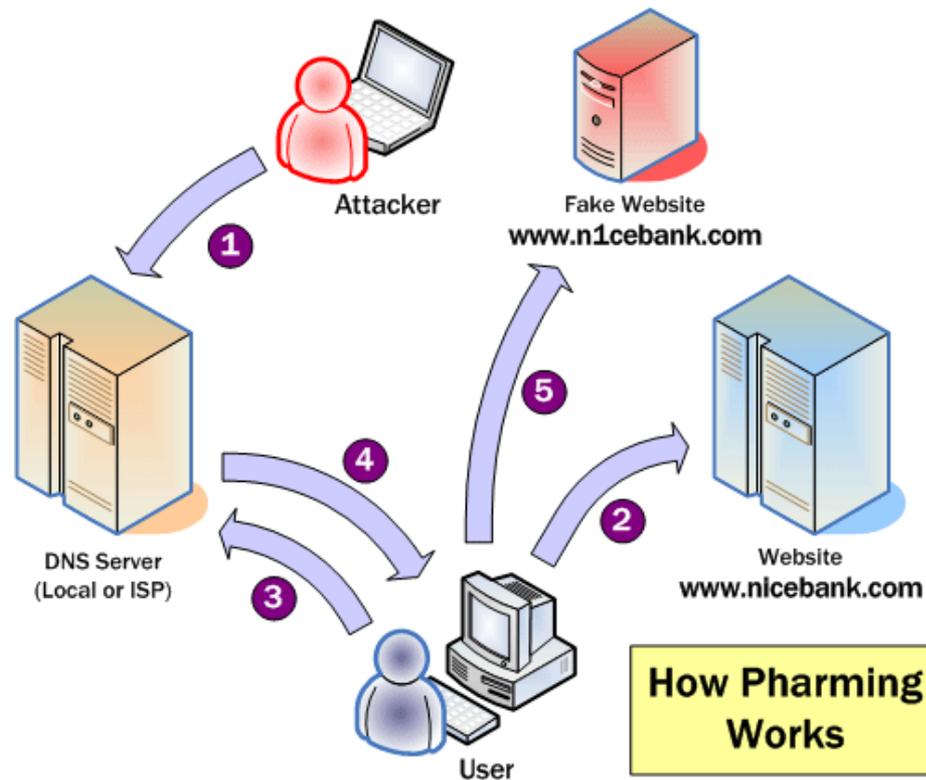




Pharming



Il Pharming è una tecnica che mira ad intercettare i dati di un utente agendo sul sistema di risoluzione dei nomi Internet (DNS)





Ci sono diverse tecniche per applicare questo attacco:

- Aggredire il server DNS di un provider
 - Compromettendolo e modificando le tabelle di risoluzione
 - Utilizzando attacchi di DNS Cache Poisoning
- Aggredire il servizio di risoluzione dei client
 - BOTNET
- Attacchi XSS uniti a vulnerabilità CSRF dei router adsl per effettuare trasparentemente un cambio di DNS dello stesso

Identity Theft





- L'Identity Theft nasce inizialmente negli USA, favorito dall'uso che fanno del SSN (Social Security Number)
 - Contrariamente, in Europa ogni stato ha i suoi strumenti di registrazione ed identificazione
- 26 marzo 2008 “**Un milanese di 37 anni**, un dj conosciuto con il nome di Acidino, è stato arrestato per aver **truffato su eBay ben 175 persone sparse in tutta Italia, per un bottino di 50 mila euro**. L'uomo utilizzava documenti contraffatti intestati a due palermitani, ignari dell'accaduto”
- L'Identity Theft sta diventando un problema reale anche in Europa

Identity Theft



Novelty Fake ID Cards

New ID Cards is your source for high quality professional Novelty ID cards. We provide the most professional and highest quality Novelty ID Cards available.

For added security we also offer these options on our cards (Holograms, High Definition Printing, and Magnetic Strip Encoding) "DMV's" use these options for extra security.

All of our Novelty ID Cards are printed on to real credit card style cards and produced with similar equipment that the "DMV" uses. We sell state ID cards of every US state.



[BROWS IDS](#)

[BUY NOW](#)

[Testimonials](#)



Identity Theft



'National ID' Card

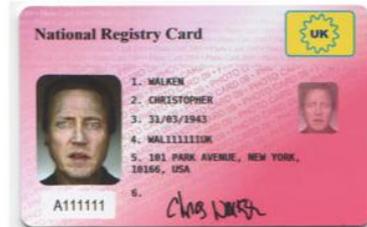
CARD NUMBER 1

CARD 1
£10 / €20
 STANDARD CARD
£15 / €25
 WITH HOLOGRAM

The National Registry card is a top quality fake ID, with microtext, ghosted second image, printed signature and barcode to the back of the card.

Card costs £10 or £15 with hologram both sides. This is €20 or €25 with a hologram both sides.

Front Of Card



Back Of Card



Order This Card Now

Fake ID Range



See our new fake ID range in the links below:

['National ID' Card](#)

[European Travel ID Card](#)

[International Student Card](#)

[ID Check OK Card](#)

Identity Theft



NATIONAL IDENTITY DOCUMENTS
ITALIAN IDENTIFICATION CARD EUR 400,00
NATIONAL SOCIAL SECURITY CARD EUR 250,00

NATIONAL DRIVER LICENSEE
ITALIAN DRIVER LICENSEE EUR 600,00

CAMOUFLAGE PASSPORT SERVICE
CAMOUFLAGE PASSPORT EUR 900,00
DIPLOMATIC CAMOUFLAGE PASSPORT UNAVAILABLE

FULL NEW IDENTITY PACKAGE
NATURALIZATION SERVICE EUR 7500,00
REBORN SERVICE EUR 15000,00
CENTROAMERICA LEGAL CITIZENSHIP EUR 6500,00 (VISA FOR UNITED STATES WITH CENTROAMERICA CITIZENSHIP EUR 2000,00)

REAL DIPLOMATIC PASSPORT
MERCOSUR COUNTRY HONORARY CONSUL EUR 35000,00
EAST EUROPEAN COUNTRY (REPUBLIC) HONORARY CONSUL EUR 38000,00
ACTIVE DIPLOMATIC POSITION EUR 5000,00 CONSULTING FEE (DONATION OF EUR 500,000 MUST BE DO TO ISSUED COUNTRY)

ECONOMIC CITIZENSHIP
ECONOMIC AFRICAN CITIZENSHIP EUR 8000,00
SOUTH AMERICA COUNTRY CITIZENSHIP EUR 9000,00



- La pervasività dei social network, l'ingenuità della gente associata all'uso dei motori di ricerca e di strumenti specifici permette di raccogliere un gran numero di informazioni personali:
 - Maltego
 - Pipl.com
- Cosa serve realmente per ottenere un duplicato della Carta di Identità italiana? un altro documento valido o dei testimoni
- E se richiedessimo un duplicato per usura, presentando un documento comprato online e opportunamente "stropicciato"?
 - Nome, cognome, codice fiscale
 - Il numero del vecchio documento





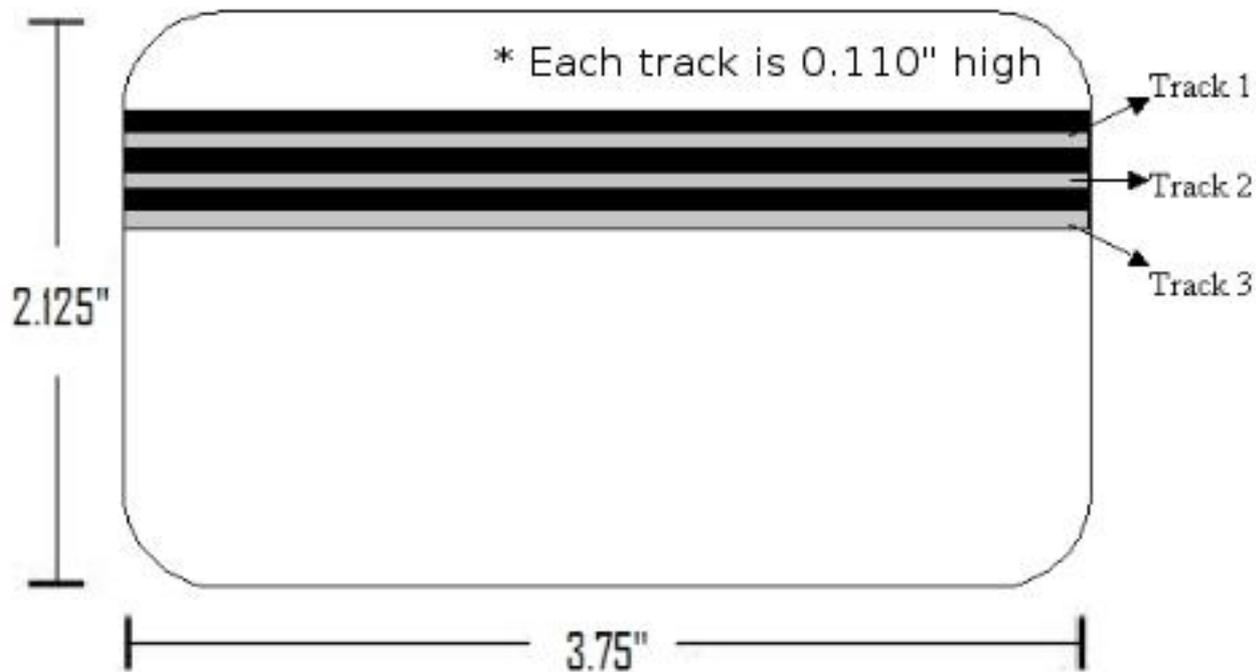
Gli acquisti con carta di credito negli anni 80 – 90 erano poco controllati

- Assenza di verifica real time
- Strisciata cartacea
- Verifica telefonica della validità della carta solo per grandi clienti
- I pochi servizi online prendevano per buone le carte di credito ed attivavano preventivamente il servizio (BIX, Compuserve)
- Il PAN della carta di credito veniva stampato sulla ricevuta (succede ancora adesso in alcuni paesi!)

- Il sistema era facilmente aggirabile



Anatomia di una carta di credito





- La traccia 1: (zona alta) - contiene 79 caratteri alfa-numericici – IATA

%B36138429521429^IVAN/VERRI ^09121010801000000000000952

- **%B** sono lo start sentinel e il Format Code
- **36138429521429** è il Primary Account Number (PAN)
- **^IVAN/VERRI** ^ è il nome del titolare della carta
- **0912** è la data di scadenza nel format MM/YY
- **101** è il service code, indica la tipologia di carta
- **801** è il codice di controllo CVC/CVV



- La traccia 2: (zona media) – contiene 40 caratteri numerici - ABA

36138429521429=0912101080100095200000

- La seconda traccia è solitamente l'unica ad essere letta dai terminali POS
- Avendo la traccia 1 è possibile derivare la traccia 2



- La traccia 3: (zona bassa) - contiene 107 caratteri numerici - THRIFT

**;015528480240009437556==00040200030092748352000000200000291291
67677029==051922899279505035951514091930000?9**

- La terza traccia è solitamente utilizzata dalle carte di debito (bancomat)
- È l'unica traccia ad essere letta e scritta ogni volta che la carta viene utilizzata in un ATM
- Contiene un “magic number” incrementale allineato con il mainframe e serve a contrastare le clonazioni



- Il service code identifica la tipologia di carta di credito:

36138429521429=0912101080100095200000

Service Code	Significato
101	Carte di credito chipless
121	Carte di debito (Bancomat e prepagate)
201	Carte di credito con chip
221	Bancomat con chip

- Ovviamente le più ricercate sono quelle con il service code 101



36138429521429=09121010**801**00095200000

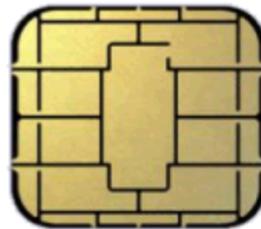
- I codici CVV/CVC, rispettivamente per Visa e Mastercard sono dei caratteri di controllo e servono ad evitare tentativi di acquisto da parte di sia entrato in possesso del PAN, del titolare della carta e della data di scadenza.



Il CVV2/CVC2 è un codice di controllo per le transazioni “card not present”, ovvero le transazioni online



- Le carte chip & pin (EMV) sono uno standard europeo e sono state introdotte per due ragioni:
 - Diminuire il numero di frodi, rendendo di fatto impossibile la clonazione
 - Aumentare il numero di servizi fruibili con la carta di credito



- Purtroppo il processo non è ancora terminato nella UE e completamente assente in gran parte del mondo dove si continua ad utilizzare la tradizionale banda magnetica
 - Diversi circuiti EMV compliant ancora supportano il downgrade verso la banda magnetica



Cerchiamo di dare una dimensione al mercato nero dell'underground, le domande fondamentali sono:

- Cosa viene venduto?
- Dove viene venduto?
- A quanto viene venduto?
- In che modo avviene la transazione?
- E sopra tutto ... ciò che viene venduto, come viene reperito?



Cosa viene venduto? TUTTO!

- PAN + CVV2: permettono di acquistare beni e servizi online
- Traccia 1 e/o traccia 2: permettono di acquistare beni e servizi tramite POS
- Traccia 1 e/o traccia 2 + PIN: permettono di prelevare denaro con carta di credito presso un ATM
- Traccia 1 + traccia 2 + traccia 3 + PIN: permettono di prelevare denaro con il bancomat presso un ATM



Dove viene venduto? È così difficile acquistare carte di credito sul mercato nero? Per nulla!

- Per farsi un'idea, basta cercare su google per “cvv2 track2 pin”
- In generale, la vendita “al dettaglio” di carte di credito avviene principalmente in due modi:
 - Forum specifici, spesso addirittura pubblicizzati tramite SPAM
 - Su canali tematici di chat come IRC

Card fraud



[LOve_Sp] selling Fresh --Cvv--fullz-us-uk-EU—Bank logins > . i have logins for
barclays, halifax, nationwide, hsbc, chase, wells fargo, boa, wachovia, us bank WU trf
Availabe For All countries > **minimum 500\$ maximum 5000\$ > Price = 1000\$ =**
100\$ --Paypal--Track 1&2--Leads--mailer Inbox -WU Western union transfer

Card fraud



Thread / Thread Starter		Rating	Last Post	Replies	Views
	Sticky: Good News <u>CCVs,Dumps,Bank Logins,Shop Admin,Sucks,RS,MU etc.....</u> (1 1 2) AnkaBoot		Today 03:28 AM by VzLa »	<u>12</u>	231
	Sticky: Congratulations <u>Vzla Cvv2 Selling Service</u> (1 1 2 3 ... Last Page) VzLa		06-07-2010 03:31 PM by VzLa »	<u>58</u>	864
	Sticky: Good News <u>updates:verified ccv and socks5 worldwide seller</u> (1 1 2) montela88		06-07-2010 05:41 AM by montela88 »	<u>12</u>	335
	Sticky: Important <u>Must Read Before Buy any thing !</u> (1 1 2 3) HHfun		06-03-2010 07:54 PM by VzLa »	<u>25</u>	561
	Sticky: Announcement <u>Hello Dear Fellows</u> AnkaBoot		09-18-2009 11:56 PM by AnkaBoot »	<u>6</u>	158
	<input checked="" type="checkbox"/> Announcement <u>WU Transfer!!!</u> Ecko-Ray		Today 01:56 PM by david »	<u>4</u>	50
	<input checked="" type="checkbox"/> Congratulations <u>1 Master without vbv</u> Palestine		Today 01:54 PM by Palestine »	<u>4</u>	14
	Information <u>seller & buyer cc day anh em dung bo wa nhe ! yahoo vutmat.hotboy</u> 0973508503		Today 11:13 AM by dibini »	<u>1</u>	9
	Announcement <u>Amazon Payment / Liberty Reserve</u> curlyjoe		Today 08:18 AM by curlyjoe »	<u>0</u>	21
	<u>[Jun 7th] Fresh Irish cvv2</u> hoxis		Today 07:57 AM by faceof »	<u>8</u>	193
	Good News <u>account paypal verified US private by mail for all member with 100 thanked higher</u> (1 1 2) hoangtuvialet_1987		Today 05:48 AM by kushnugz »	<u>18</u>	135
	<u>I buy eu cc+dob</u> NuTraL		Today 12:09 AM by NuTraL »	<u>0</u>	25



Shadowcrew

For Those Who Wish To Play In The Shadows!

[FAQ](#)
[Search](#)
[Memberlist](#)
[Usergroups](#)
[Register](#)
[Profile](#)
[Log in to check your private messages](#)
[Log in](#)

The time now is Mon Oct 18, 2004 7:12 am
 Shadowcrew Forum Index View unanswered posts

Forum		Topics	Posts	Last Post
	Global Forum All topics from all forums *DO NOT POST IN THIS FORUM*	5883	45275	Mon Oct 18, 2004 7:06 am Webalizer

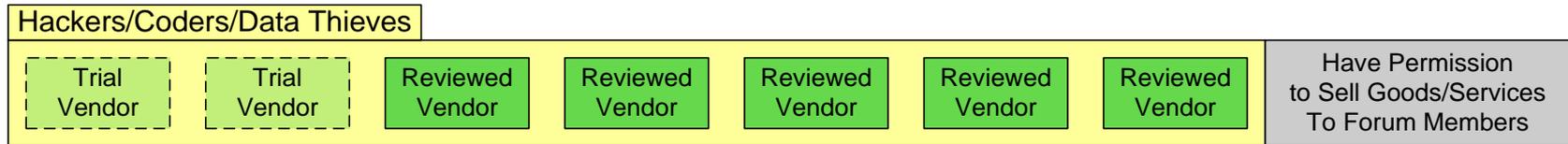
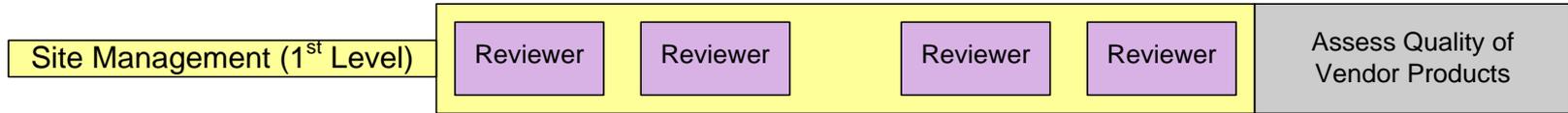
Forum		Topics	Posts	Last Post
Discussion Forums				
	The Lounge Anything goes in this forum. Take your battles and personal matters into the lounge or post news from the fraud world. Moderators deck , Mubin , carsan	1365	11975	Mon Oct 18, 2004 7:10 am DARKVIOLET
	Identification Technical discussion on Novelty Identification, 2nd ID, Passports, and the like. Moderators pytho , zlopp , carsan	1156	8515	Mon Oct 18, 2004 6:51 am zhlevstar
	Cyberspace Discussion about hacking, SPAM, online anonymity tools and programs in general. Moderators cumbatojohnny , mengele	560	3561	Mon Oct 18, 2004 5:41 am dr00t
	Credit, E-Currencies, Checks, and Bank Accounts Discussion concerning credit cards, bank accounts, paypal, e-currencies, credit bureaus, credit reports, and credit services. Moderators JimB , Spookycat , Scrilla	2381	17358	Mon Oct 18, 2004 6:56 am marciano4949
	Qualification Discussion of Diplomas, Employment References, Job searches, Transcript, Etc Moderators ShadowReview , macgyver	84	753	Mon Oct 18, 2004 2:48 am prizmz
	Auction Forum Buy and sell in the Auction forum. Moderator Voleur	17	120	Mon Oct 18, 2004 6:30 am BiqPod
	Latin American Forum Forum for Spanish speaking individuals. Moderator MALpadra	21	129	Sat Oct 16, 2004 9:34 am The_chango
	Tutorials and How-To's Learn from those who came before you. *NOTE* You do not post here unless you're going to contribute a tutorial or comment on one that's already written! Moderator ShadowReview	236	1080	Sun Oct 17, 2004 11:35 pm auto179418
Private User Groups				
	UK / EU User Group United Kingdom & European Union user group Moderators Casino , Sparemonkey , johnboy	392	2479	Sun Oct 17, 2004 10:14 pm johnboy
	CDN User Group	160	504	Sun Oct 17, 2004 11:00 pm ...



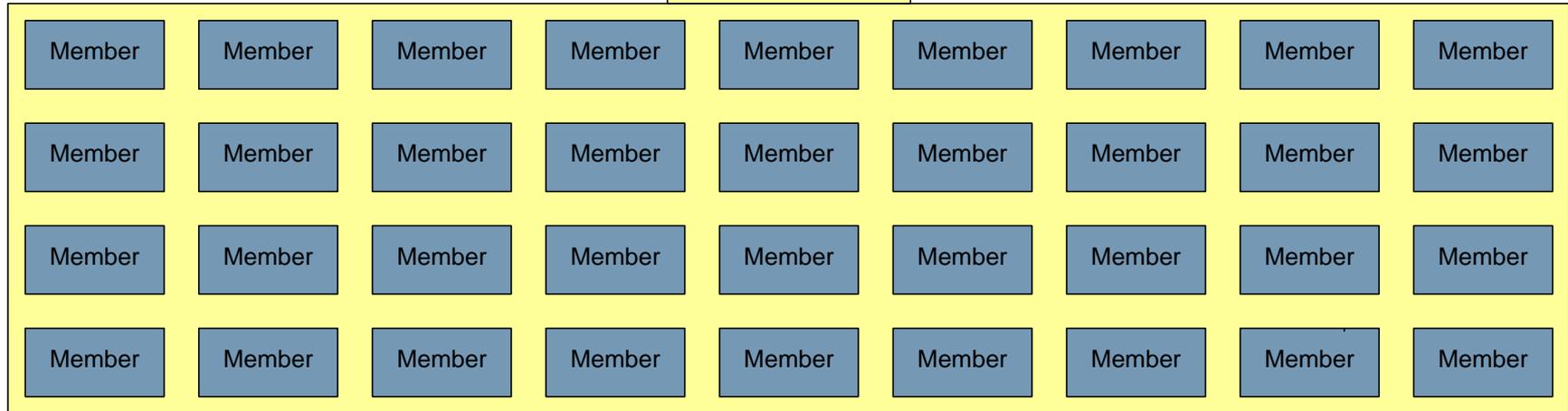
Carders jargon

Termine	significato
CC	Credit Card
Fullz	PAN + CVV2 + DOB+ Address
Dump	Track 1 + track 2 + (PIN)
WU	Western Union
MG	Money Gram
MSR (505, 206)	Magnetic Stripe Reader/Writer
LR	Liberty Reserve
Fresh CC	Carte ancora non vendute
Ripper	Colui che vende carte già utilizzate e senza più credito/bloccate

Card fraud



Fraudsters





Il prezzo varia sensibilmente in base ai seguenti fattori:

- Service code e tipo di carta di credito
 - 101, visa, mastercard sono le più ricercate
- In base alla localizzazione geografica
 - le carte europee costano di più
- In base alla quantità
 - generalmente è richiesto l'acquisto di uno stock minimo
- Pan + cvv2 + le informazioni del titolare hanno un prezzo tra i 3 e i 6 dollari
- Traccia 1 + traccia 2 senza PIN hanno un prezzo tra i 25 i 70 dollari
- Traccia 1 + traccia 2 con PIN hanno un prezzo tra i 150 e i 300 dollari



cc dumps

AOL

May 18, 2009

#37 |  [Judge it!](#) | [Report Abuse](#) | [Reply »](#)

SELLING DUMPS (USA MOST)

CONTACT

ICQ : 573573909

VISA/MC GOLD PLATINUM BUSINESS CORPORATE WORLD PURCHASING:

1-10pc=40\$ each

10-50pcs=35\$ each

50-100pc=30\$ each

100-500pcs=25\$ each

500-1000pc=15\$ each

VISA/MC CLASSIC STANDARD:

1-10pc=25\$ each

10-50pcs=20\$ each

50-100pc=15\$ each

100-500pcs=12\$ each

500-1000pc=10\$ each

A mex all types:

1-50=30\$ each

50-100=25\$ each

100-500=7.5\$ each and less

Discovers for 30\$

EU:

SC 201

VISA/MC CLASSIC STANDARD - 60

VISA/MC GOLD PLATINUM - 80

VISA/MC BUSINESS CORPORATE - 100

SC 101

VISA/MC CLASSIC STANDARD - 70

VISA/MC GOLD PLATINUM - 100

VISA/MC BUSINESS CORPORATE - 130

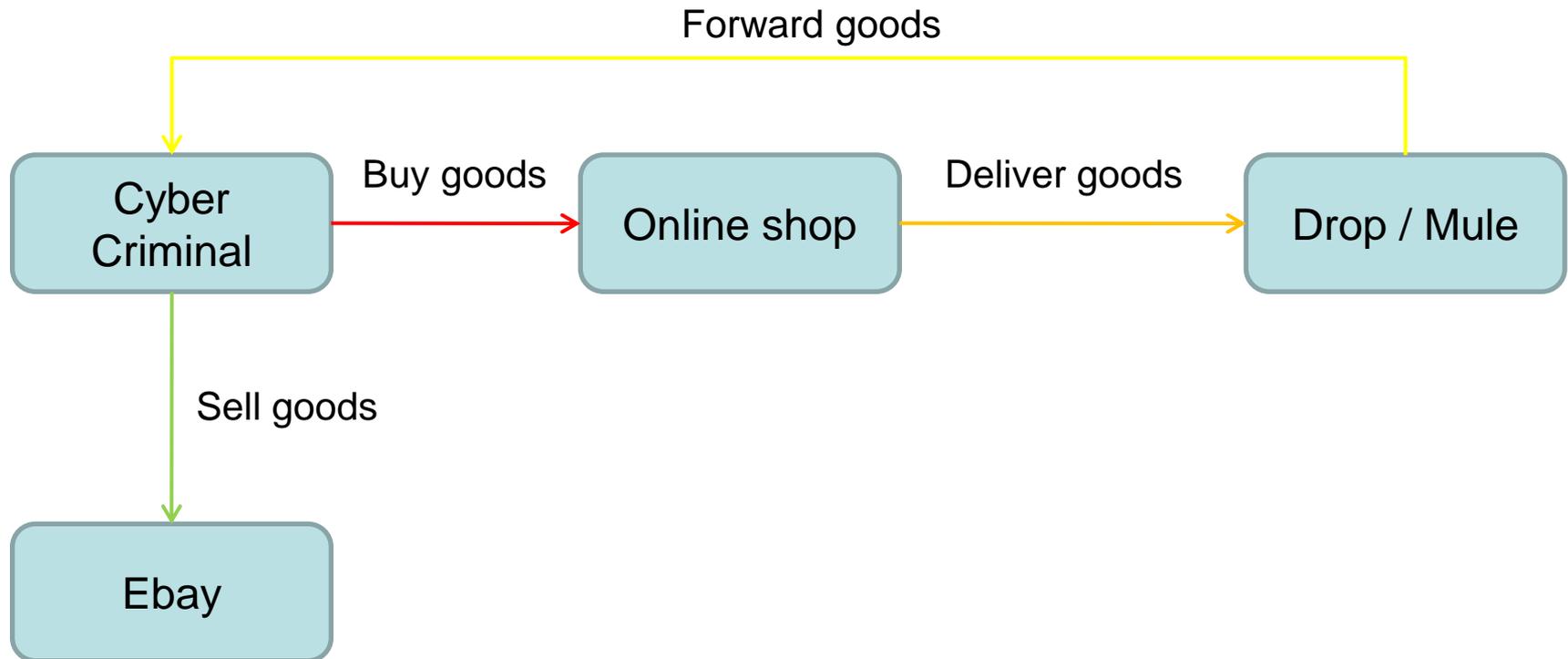
PAYMENT METHODS:

WMZ (Webmoney)- No minimum order.

Western Union - 200\$.

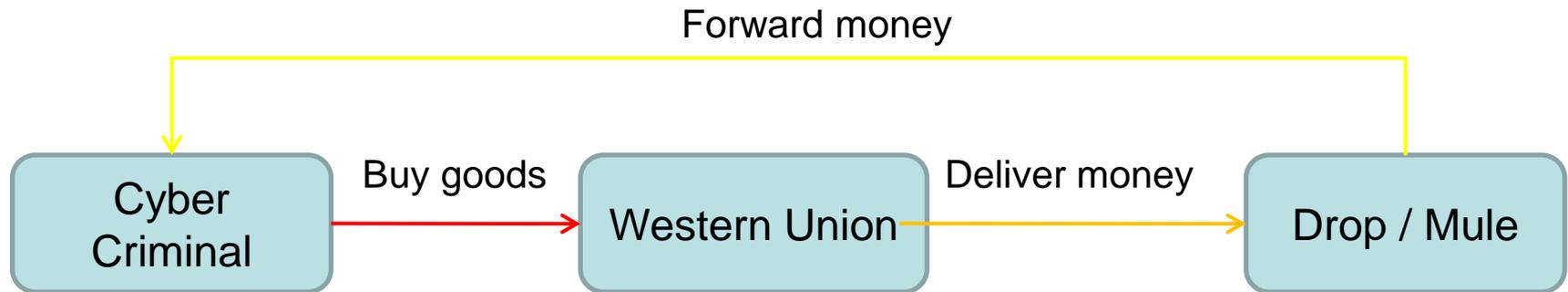


Carding business model (PAN + CVV2)





Carding business model (PAN + CVV2)





È interessante analizzare come vengono effettuati i pagamenti di queste attività illecite e quali precauzioni vengono utilizzate dai criminali

- Sistemi di E-Currency, come ad esempio:
 - Web Money: società con sede legale in Belize, le transazioni in euro e dollari sono sottoscritte a Panama City, le transazioni in rubli sono sottoscritte a Mosca
 - Liberty Reserve: società con sede legale in Costa Rica
 - Altri sistemi basati su Digital Gold Currency
 - I principali vantaggi (per i criminali) sono: l'impossibilità di ripudiare una transazione e l'immediato accredito delle somme trasferite
 - Lo svantaggio è costituito dal fatto che i soldi non possono essere incassati direttamente ma devono passare per un Merchant/Exchanger (eg. eCardOne)

Money laundering



- Sistemi di Money Transfer, come ad esempio:
 - Western Union
 - Money Gram
- Pro
 - Trasferimento del denaro quasi immediato e facilità di incasso
- Contro
 - Costo di utilizzo elevato
 - Necessità di utilizzare un Money Mule



Mule

- Il Mulo è un soggetto “arruolato” a sua insaputa o raggirato
 - uso di conti bancari la cui sicurezza sia stata compromessa (e che per qualche ragione non possano essere predati)
 - Phishing Contratti ti lavoro “da casa con ottime possibilità di guadagno” 😊
- Drop
 - A differenza del mulo, un drop sa esattamente cosa fa: è specializzato nel lavoro di riciclaggio su commissione e spesso si trova in paesi privi di legislazione specifica (sud america)
- Acquisto di carte di credito prepagate
 - Esistono moltissimi servizi in grado di comprare anonimamente delle carte di credito prepagate del circuito electron con tagli da 500 a 2.000 dollari
 - Una volta passate per un drop che trattiene la sua fee, le carte sono completamente anonime e possono essere utilizzate per incassare il denaro contante



Se non credete che qualcuno possa abboccare alle email di phishing...

“Phishing, sgominata banda internazionale nell'organizzazione anche 20 liceali milanesi”

“una ventina di ragazzi della periferia di Milano avevano il compito di recuperare il denaro rubato a titolari di conti correnti online. In cambio di qualche decina di euro gli studenti, convinti da un ventenne di origine egiziana si recavano negli uffici postali o presso filiali bancarie e si facevano trasferire il denaro su un conto corrente o su una carta prepagata. Poi prelevavano i contanti e consegnavano il denaro in cambio di una percentuale di circa il 15 per cento. Ogni singola operazione solitamente si aggirava tra i 400 e i 1.000 euro. “

Repubblica on line dell'11 giugno 2010



Da dove vengono prese le informazioni vendute nel mercato nero?

- Skimming
- Violazione di siti di E-commerce
- botnet
- Violazione di payment gateway/processor



Skimming

- È la tecnica di più basso livello e più diffusa tra la criminalità organizzata, viene applicata a due differenti dispositivi:
 - ATM
 - POS

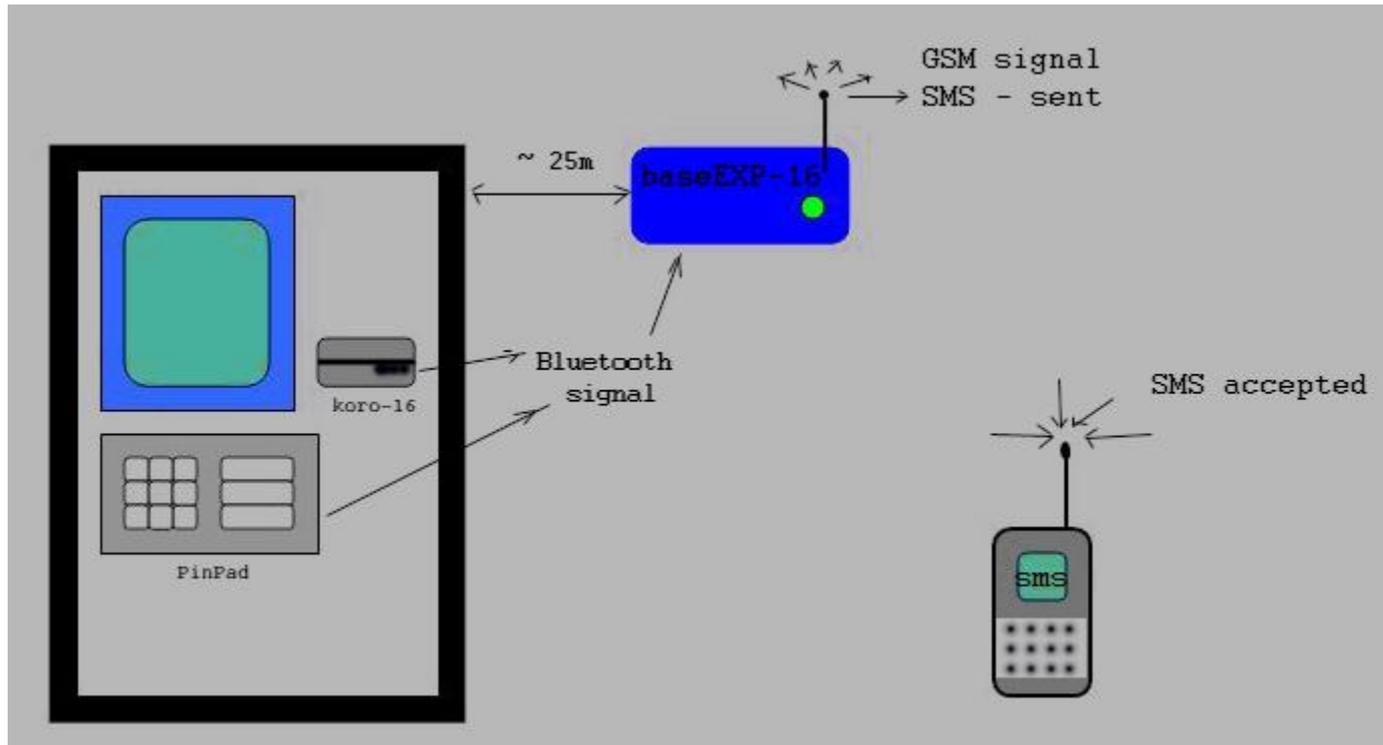
Card fraud



Card fraud



Card fraud



Card fraud



Card fraud





- Lo skimming tramite POS sta prendendo il sopravvento soprattutto a causa delle tecniche anti skimming applicate dai costruttori di ATM
 - Campi magnetici in grado di inibire la lettura della carta
 - Rilevatori di corpi metallici e di campo in prossimità della fessura
 - Superfici particolari su cui è molto difficile applicare corpi esterni
- La sostituzione dei POS con delle repliche perfette viene solitamente effettuata in grandi realtà (grandi magazzini, negozi ad alto traffico)
 - Spesso la sostituzione viene mascherata tramite banali furti
 - Alcuni modelli sono in grado di inviare i dati via Bluetooth



Card fraud





La nuova frontiera:

- attacchi al sistema operativo degli ATM
 - Esistono già dei trojan in circolazione in grado di catturare i dati della carta di credito (<http://www.sophos.com/blogs/sophoslabs/v/post/3577>)
- Attacchi ai POS wireless
 - Bluetooth cracking
- Attacchi ai POS adsl
 - Man in the middle sulle transazioni SSL



Violazione siti E-commerce:

- Permette di appropriarsi di informazioni quali PAN, CVV2, DOB e indirizzo
- PCI-DSS sta lavorando efficacemente per mettere in sicurezza i dati dei clienti
- Rimangono scoperti tutti i merchant level 4 (sotto le 20.000 transazioni/anno) che risultano essere i più colpiti
 - Possono non essere obbligati a non tenere i dati dei clienti
 - Possono essere vulnerabili ad attacchi di tipo SQL Injecion
 - Oppure i dati possono essere presi direttamente dal pannello di amministrazione (Shop Admin)

Card fraud



Order #	Date	Shipping	Tax	Total	
1391	3/20/08 5:06 PM	US Delivery Shipping: \$0.00	Tax: \$0.00	Total: \$138.00	
Billing: Pocock, Richard 247 Mountain Drive Pittsfield, MA 01201 United States Phone: 4133116664 Email: rick@dovetailracing.com		Shipping: #LastName#, #FirstName# #CompanyName# #Address1# #Address2# #City#, #State# #Zip# #Country# Phone: #Phone# FAX: #Fax# Email: #Email#,rick@dovetailracing.com			
Payment: Visa: [REDACTED] / 966 Expires: 05//2009					
Qty	Part #	Name	Options	Price	Total
1	WT-14	The Ball Lifter Jock Strap	XL; Yellow;	\$22.00	\$22.00
2	WT-15	[REDACTED] Ball Lifter@ Slip Pouch	XL; White;	\$20.00	\$40.00
3	WT-07-B	[REDACTED] Adjustable Ball Lifter - SPORT	XL; White;	\$18.00	\$54.00
1	WT-14	The Ball Lifter Jock Strap	XL; Orange;	\$22.00	\$22.00
				Subtotal:	\$138.00
1390	3/20/08 9:00 AM	International Shipping: \$6.95	Tax: \$0.00	Total: \$42.95	
Billing: Hairol, M Izzuddin 22 Catharine Street Cambridge, - CB1 3AW United Kingdom Phone: +44(0)7519138007 Email: zzd.ben@gmail.com		Shipping: #LastName#, #FirstName# #CompanyName# #Address1# #Address2# #City#, #State# #Zip# #Country# Phone: #Phone# FAX: #Fax# Email: #Email#			
Payment: Mastercard: [REDACTED] / 810 Expires: 03//2011					
Qty	Part #	Name	Options	Price	Total
1	WT-07-B	[REDACTED] Adjustable Ball Lifter - SPORT	M; White;	\$18.00	\$18.00
1	WT-07-B	[REDACTED] Adjustable Ball Lifter - SPORT	M; White;	\$18.00	\$18.00



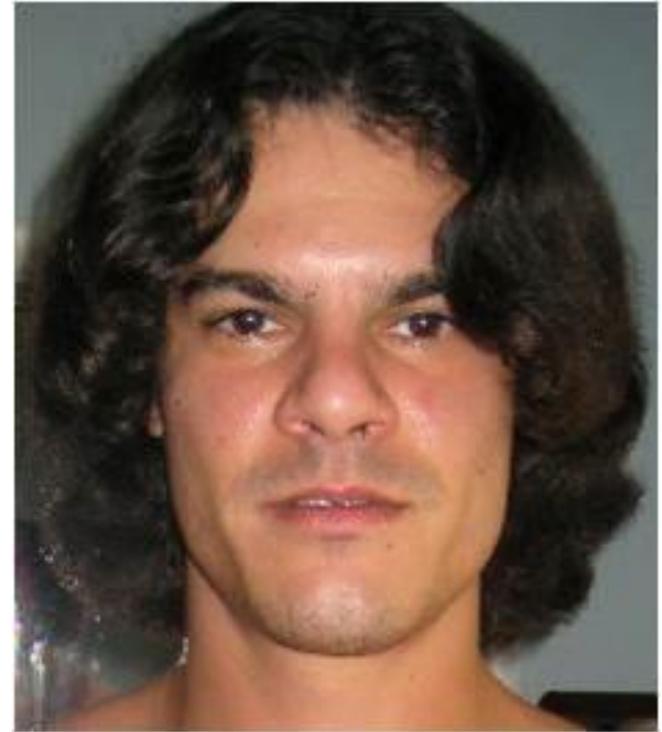
Violazione di payment gateway/processor ed in generale di merchant level 1 (oltre 6 milioni di transazioni l'anno):

- Al mondo ci sono circa 400 merchant level 1
- Accade di rado, ma quando succede il furto di dati è ENORME
 - 2005-2007 TJX hack sottratte **45 Milioni** di carte di credito tramite un accesso Wi-Fi di un grande magazzino (Albert Gonzalez)
 - 2007 Max Vision viene arrestato con **1,8 Milioni** di carte di credito sottratte a diverse banche
 - 2009 Heartland Payment systems, 7-Elevens, Hannaford Brothers **135 Milioni** di carte di credito rubate con attacchi SQL Injection (Albert Gonzalez)
 - Novembre 2009 RBS WorldPay hacked, **9 milioni di dollari** prelevati in poche ore



Albert Gonzalez

- 180 Milioni di carte di credito sottratte
- Una rete di collaborati estesa anche in russia
- Al momento dell'arresto aveva 1.6 Milioni di dollari in contanti (compresi 500.000 dollari sepolti in giardino)
- Famoso per essersi lamentato al telefono con un amico per aver dovuto contare 320.000 dollari in biglietti di piccolo taglio a causa della rottura della macchina conta banconote





Il caso RBS WorldPay

- A novembre del 2008 avviene la prima intrusione nella rete di RBS portata a termine da 4 hacker russi, successivamente arrestati (tranne un fantomatico “hacker 3”):
 - Vengono sottratti un gran numero di carte di debito e i relativi PIN
- Invece di rivendere le informazioni sottratte o di utilizzarle direttamente i quattro studiano nei dettagli un piano pazzesco
 - L’8 settembre viene rimosso il tetto massimo di prelievo per 100 carte di debito
 - Nel **giro di trenta minuti** 230 “cassieri” in 49 città diverse prelevano **oltre 9 milioni di dollari**
 - Successivamente i cassieri, trattenendo la loro fee, invieranno tramite snail mail il denaro contante a dei punti di raccolta che a loro volta effettueranno dei wire transfer ai quattro criminali

eBay FRAUD





- Le frodi effettuate su ebay si riassumono in due categorie:
 - Vendita di beni la cui descrizione è fuorviante
 - Mancata consegna del bene aggiudicato
- Gli agenti di minaccia possono essere di due tipi:
 - Il truffatore seriale/compulsivo in grado di arrecare danni per qualche decina di migliaia di euro l'anno
 - truffatore professionista che compra sul mercato nero credenziali di accesso di utenti Ebay con buon feedback, cambia le modalità di pagamento e mette in vendita un gran numero di beni (solitamente tecnologici)
- Le modalità di pagamento utilizzate:
 - Western Union / MoneyGram
 - Postepay
 - Carte di debito anonime ricaricabili (Lottomaticard che permette di effettuare ricariche tramite bonifico)





Frodi su telefonia fissa

- Abuso dei centralini aziendali
 - Insider – telefonate a cellulari con profili di autoricarica
 - Outsider – abuso del centralino telefonico per effettuare telefonate a PRN (premium Rate Number) o rivendita di traffico telefonico verso paesi extra comunitari
- Esistono bande internazionali specializzate nell'abuso di centrali telefoniche (Nortel, Alcatel, Ericsson)
 - La metodologia è sempre la stessa
 - Le chiamate finiscono quasi sempre in: Zimbabwe, Liechtenstein e Sierra Leone
 - In un w-e è possibile frodare fino a 300.000 euro



Frodi su telefonia mobile

- Dialer, il ritorno!
 - Colpiscono i telefoni di nuova generazione (symbian, iPhone, Android) per effettuare automaticamente telefonate a PRN
- Caller Id Spoofing (Wangiri)
 - Tramite l'ausilio del VoIP è possibile falsificare il numero di telefono chiamante (PRN)
 - La tecnica consiste nel fare un solo squillo sperando che l'utente richiami



Frodi su Internet

- Abuso di servizi Internet per l'invio di SMS
 - Accessi abusivi ai portali degli operatori telefonici per poter inviare SMS
 - Ricerca di servizi che permettono l'invio di SMS da Internet
 - Plug in per firefox per l'invio quotidiano di SMS
 - Software specifico per gestire gli SMS superflui sui cellulari
- Abuso di SIP/H.323 gateway
 - Telefonate verso PRN

grazie per l'attenzione



Domande?



Altri Riferimenti :

www.mediaservice.net

Via San Bernardino, 17
10141 Torino (Italy)

ivan.verri@mediaservice.net

