(U//~~FOUO~~) Hacker jargon

From CIA Wiki

~~TOP SECRET//SI/TK//NOFORN~~

(U//~~FOUO~~) Overview

This page is intended to define jargon and acronyms commonly used by hackers and cyber criminals while communicating in forums in the underground economy.

(U//~~FOUO~~) Jargon and Acronyms

- **ACC** - Account
- **BIN** - Bank Identification Number, usually the first 6 numbers of a credit or debit card number. There are over 60,000 of these and each bank (no matter how small) usually is issued at least one. Large banks have several BINS. The BINS are how the hacker knows what type of cards he has. For example, if he collected 200 4430-40's he would advertise on the forums, "I've got 200 PNC Visa's for Sale."
- **Bots/Botnets** - Generally, a collection of computers (zombies) that have been compromised via worms, Trojans or backdoors, under a common command and control (C2) infrastructure, that run a variety of bot programs. Botnets are a major source of spam and can be used to deliver distributed denial of service attacks (DDoS). They usually operate without the knowledge of the computer owner. The controller may be referred to as a 'bot herder'.
- **BP Hosting** - Bullet-proof hosting
- **Carder** - Slang used to describe individuals who use stolen credit card account information to conduct fraudulent transactions.
- **Carding** - Trafficking in and fraudulent use of stolen credit card account information.
- **Cashing** - The act of obtaining money by committing fraud. This act can be committed in a variety of ways: The term can stand for cashing out Western Union wires, Postal money orders and WebMoney; using track data with PINs to obtain cash at ATMs, from PayPal accounts, or setting up a bank account with a fake ID to withdraw cash on a credit card account. Cashiers – hired to cash out an account, including Bank insiders
- **CC** - Slang for credit card.
- **Change of Billing (COB or COBs)** - Term used to describe the act of changing the billing address on a credit account to match that of a mail drop. This act allows the carder full takeover capability of the compromised credit card account and increases the probability that the account will not be rejected when being used for Internet transactions.
- **Cracking** - illegal gaining entry into a computer system or the process of discovering a password.

- **CVV2** - CVV2 stands for credit card security code. Visa, MasterCard, and Discover require this feature. It is a 3 digit number on the back of the card.
- **DDoS** - Acronym for Distributed Denial of Service Attack. The intent when conducting a DDOS attack is to shut down a targeted website, at least for a period of time, by flooding the network with an overflow of traffic.
- **DLs** - A slang term that stands for counterfeit or novelty driver's licenses.
- **Downloads** - Compromised hosts on which hackers can download their own code. Can be done through an exploit or botnet. Usually used to extract information of value from the victim computer.
- **Drop** - An intermediary used to disguise the source of a transaction. A location to which goods or cash can be sent or referred to a bank account through which money can be moved.
- **Dumps** - A collection of stolen credit card data or stolen user credentials. Includes at least Track 1 data, but usually includes both Track 1 and Track 2 data. Usually dumps are in the form of .txt files and include a long list of credit card numbers, track data (if stolen from a data processing site), or phishing data (if a product of a phishing scheme).
- **Dump checking** - Using specific software or alternatively encoding track data on plastic and using a point of sale terminal to test whether the dump is approved or declined. This provides carders a higher sense of security for obtaining quality dumps from those who offer them and also a sense of security when doing in store carding.
- **Full info(s)** - Term used to describe obtaining addresses, phone numbers, social security numbers, PIN numbers, credit history reports and so on. Full Info(s) are synonymous with carders who wish to take over the identity of a person or to sell the identity of a person.
- **Grassed** - Cheated
- **Grift** - cheat, Swindle
- **Holos** - Slang for the word Holograms. Holograms are important for those who make counterfeit plastic credit cards to emulate an existing security feature.
- **ICQ** - An abbreviation for "I Seek You". ICQ is the most widely used instant messaging system for carders. Popular among Eastern Europeans in their Internet culture, it continues to be used for carding activity.
- **IRC** - An abbreviation for "Internet Relay Chat". IRC is a global system of servers through which users can conduct real-time text-based chat, exchange files, and interact in other ways.
- **IDs** - Slang for identification documents. Carders market a variety of IDs, including bills, diplomas, driver's licenses, passports, or anything that can be used as an identity document.
- **iFrame exploit/click-by downloads**
- **Mailbombing** - Spamming
- **MSR (Magnetic Strip Reader)** - Device that can be used for skimming payment card information and/or

encoding track information on plastic.

- **Mule** – middleman used to launder money. Some are recruited through "work from home schemes" and are fooled into believing they work for a legitimate employer. Others are fully aware that they are engaging in illegal activity. Mules usually receive 10% of the transaction.
- **OS Bank** – off shore bank
- **Phishing** - The extraction of information from a target using a hook (usually an e-mail purporting to be from a legitimate company). Phishers spam the Internet with e-mails in hopes of obtaining information that can be used for fraudulent purposes.
- **Pinpads** - the 10-digit keypads on ATMS used to input PINs.
- **POS (Point of Sale)** - Acronym for a terminal through which credit cards are swiped in order to communicate with processors who approve or decline transactions.
- **Proxies** - Term used for proxy servers. The use of proxy servers to mask ones identity on the Internet is widely practiced amongst carders. Many vendors sell access to proxy servers, socks, http, https, and VPN (Virtual Private Networks), which aide in hiding the user's actual IP address when committing fraud or other illegal activity on the Internet.
- **Ransomware** - Used by criminals to encrypt documents on a victim's computer. The criminal demands money in exchange for the encryption key.
- **RAR** - a proprietary file format for data compression and archiving
- **Rippers** - Refers to individuals who steal account infrormation.
- **Roots** - refers to DNS servers that resolve Internet names and IP addresses
- **Scam/Scamming/Scammers** – refers to phishing
- **Scareware** - misleading pop-up warnings that a user's computer is infected with a virus, entising the user to click on the warning which downloads a real virus.
- **Script Kiddie/kids** - a new entrant into the hacker economy. The term does not necessarily refer to the age of the individual - just lack of hacking and other cyber crime experience and skills.
- **Shell** - a software program that provides a user interface. It enables users to interact with a system through a user-friendly interface.
- **Skimming** - thin overlays placed over legitimate keypads and card swipes on ATMS to capture account information.
- **Socks** – refers to proxies
- **Spoofed/Spoofer** - e-mail appears to come from one source when, in fact, it comes from another. Also, could refer to an attempt to mislead a search engine.
- **Track 1/Track 2 data** - Track 1 and Track 2 data is the information stored on the magnetic stripe of a

payment card that contains the account information.

- **WMZ** – Webmoney
- **WU** – Western Union

Retrieved from (b)(3)
Categories: Acronyms | Cyber Glossary

- This page has been accessed 1,908 times.
- 6 watching users
- This page was last modified 11:42, 18 February 2016 by (b)(3) Based on work by (b)(3) and others.

(b)(3)