

Organized Cybercrime

By Yuval Ben-Itzhak

Cybercrime organizations bear an uncanny resemblance to Mafia organized crime syndicates where each cybercriminal has his own well-defined role and related reward system.

As we have seen during the last year, cybercrime has developed into a fast-expanding, global industry. Its operations closely resemble the real business world, including profit-driven organized cybercrime.¹ Targeted attacks against financial institutions, enterprises, and governmental agencies have substantially grown, and the resulting financial damages keep on running into millions.

The individual hacker-for-fame, seeking the limelight, has been replaced by professional hackers and cybercriminals, deploying sophisticated cybercrime business models to maximize their profit while avoiding detection.² On the operational side, we see that they are part of hierarchical cybercrime organizations where each cybercriminal has his own well-defined role and related reward system.

The organization

The cybercrime organizations bear an uncanny resemblance to *La Cosa Nostra* or *Mafia* organized crime syndicates.³ In both cases, we see that the organization is headed by the “Boss.” He does not commit the (cyber)crimes himself, but purely operates as a business entrepreneur. Due to the nature of cybercrime, the boss is

managing an operation without borders. He also has limited or no face-to-face contact with his cybercrime workforce. He rakes in the highest revenues with the lowest risk of being caught. Similar to a legitimate business owner, he outsources, watches his profit and operational margins, and cuts costs.

Directly under him is his second in command, the “underboss.” He manages the operation, and in case of cybercrime, provides the Trojans for attacks. He also manages the Command and Control (C&C) of those Trojans similar to a business manager, operating behind the scenes.

In a Mafia family, there are several “capos” operating beneath the underboss as lieutenants leading their own section of the operation. With cybercrime, these lieutenants are called “campaign managers” and lead their own attack campaigns as part of the whole cybercrime operation. Since cybercrime is highly sensitive

to location, language and regional

economic trends, these campaigns enable them to operate locally, focusing their attacks on specific geographic locations (e.g., NYC, California) and target selected businesses (e.g., banks, health care providers). For example, the highly effective ZeuS Trojan stole \$6 million from banks in the U.S., UK, Spain and Italy. Each campaign manager was responsible for distributing the crimeware Trojan to specific “territories,” illustrating how today’s cybercriminals are deploying the “think global, act local” business strategy.

Mafia “soldiers” do the “dirty work.” A cybercrime organization works in a similar fashion, using their own “affiliation networks” to perform the attacks and steal the data. These

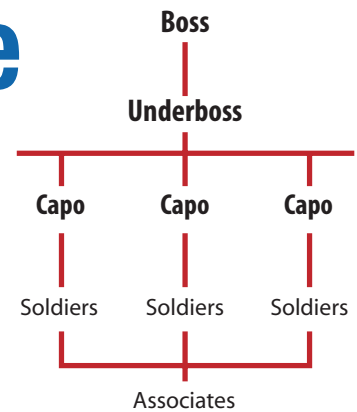


Figure 1 – Mafia organizational structure

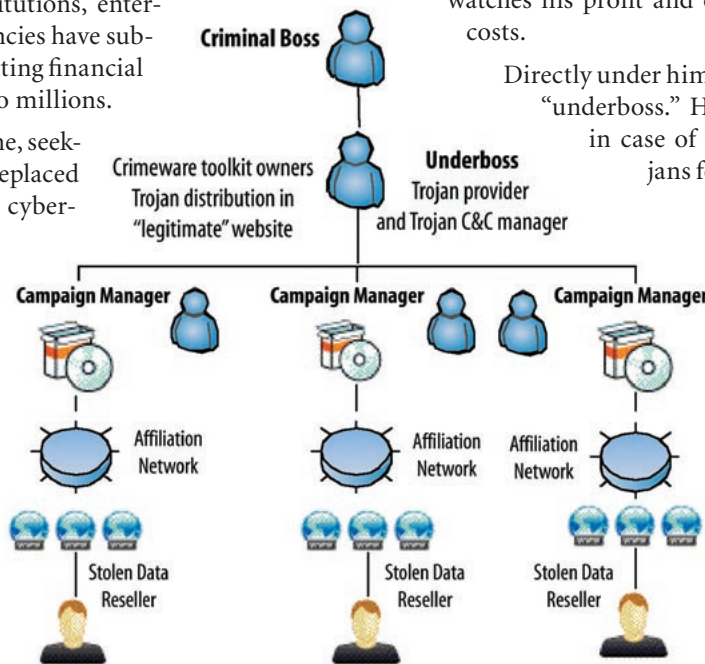


Figure 2 – Cybercrime organizational structure

1 D. Carvajal, “The evolution of CyberCrime Inc.,” *The International Herald Tribune* (April 6, 2008), <http://www.ihrt.com/articles/2008/04/04/technology/cybercrime07.php>.

2 B. Acohido, “Meet A-Z: The computer hacker behind a cybercrime wave,” *USA Today* (August 5, 2008), http://www.usatoday.com/money/industries/technology/2008-08-04-hacker-cybercrime-zeus-identity-theft_N.htm.

3 J. Kirk, “Structure of Cybercrime Gangs Unlocked,” IDG News Service - (London Bureau (July 15, 2008)), http://www.csoonline.com/article/437664/Structure_of_Cybercrime_Gangs_Unlocked.

networks act as distribution channels, especially created to promote infections. Incentives are provided to attackers to hack into legitimate sites and insert a reference to malicious code operated by other hankers. Once the malicious code runs successfully, participants are paid according to the amount of achieved infections. Their reward rate varies, depending on the country of origin of the infected computer. This structure is highly effective in avoiding the chance of detection, since multiple players are operating as stand-alones, having no contact with their “colleagues.”

Similar to the Mafia’s “associates,” “resellers” in the cybercrime organization trade the stolen data. They are not involved in the crimeware attacks themselves, but act as a “fence” dealing with stolen goods. Since credit cards and bank accounts have become commoditized, the prime targets are now health care-related information, single sign-on login credentials for organizations, email exchanges, Outlook accounts, and FTP accounts. These are considered premium goods in the criminal economy and can be sold for high prices. Similar to the legitimate business world, these resellers provide services and give guarantees to their (potential) customers. Various pricing models are used for the different kinds of products for sale. For example, stolen standard U.S. Master or Visa credit cards can be purchased for \$15 each, while a stolen EU or UK Visa credit card for sale is prized at \$90 each.

Tools of the cybercrime trade

Cybercriminals use an arsenal of highly-effective crime tools, deploying sophisticated Criminal-2-Criminal (C2C) business models for their operations, heavily borrowing and copying from the legitimate business world. A notorious example is the RBN (Russian Business Network), a multi-faceted cybercrime organization catering exclusively to cybercriminals.⁴ These kinds of crime pros also use robust and scalable crimeware that gives them maximum flexibility in terms of command and control for stealing and trading data. They are highly successful in infecting PCs and networks around the world using the latest Trojan technologies, silent installations, and drive-by downloads for their attacks.

Cybercrime attacks are made easy due to the availability of crimeware toolkits. These toolkits are “how to...” software packages that instruct users step-by-step how to infect a system, followed by how to retrieve data for financial gain. Such \$100-\$200 off-the-shelf “Do It Yourself” toolkits enable cybercriminals to easily gain access to a wide array of sensitive and valuable information.

Crimeware toolkit creators also deploy Crimeware-as-a-Service (CaaS). A classic example is the notorious NeoSploit toolkit that contained a delivery system for the Trojan upon a successful exploitation. It could be configured to provide a different version of the Trojan according to the country targeted. In mid-July 2008, the NeoSploit’s profitable business

ran into a classic business problem – it had difficulty sustaining its new customer acquisition rate, while its existing customers were not generating enough revenue to sustain its operations. The Neosploit development team was forced to abandon its product, sending an “out of business” announcement.⁵

Cybercriminals also deploy the data supplier model – customers need only log into their “data supplier” and download any information suitable for them to conduct their crime, be it financial fraud, industrial espionage, or identity theft. The availability of user data provides a “customer” service.

Once the data is stolen, hackers use crimeware servers that function as the “drop zones” of organized attacks. These servers are populated with the harvested (stolen) data and often also contain the crimeware Trojan C&C, enabling management of campaigns, remote control of the infected machine, as well as management of the stolen data itself.

Effects of cybercrime

The damage for both organizations and individuals resulting from successful crimeware attacks is widespread and long-lasting – no organization, company, enterprise or business with Internet access is safe. This vision is confirmed by Marcus Alldrick, responsible for information protection and continuity at Lloyd’s. He pointed out that targeted attacks perpetrated by organized crime are on the increase due to the high return on investment.⁶

According to the *2007 Annual Survey: Cost of Data Breach*, by the Ponemon Institute,⁷ the average cost per reported incident in 2007 amounted to \$6.3 million, while the cost of lost business per reported incident was estimated at \$4.1 million in 2007, an increase of 30% compared to 2006. The average cost of each compromised record was \$197, while the average cost of a data breach in the highly regulated financial sector was \$239 per compromised record.

The total amount of compromised records per data breach is on the rise as well. A well-documented example is the international gang of 11 cybercriminals who stole 45.7 million credit/debit cards from customers in the UK, U.S. and Canada by breaching TK Maxx’s computer systems. TJX, parent company of TK Maxx, had to increase its estimate of pre-tax charges for the compromise to nearly \$216 million from an earlier projection of approximately \$168 million. According to some experts, the company may end up spending more than \$500 million, including litigation fees and government fines.⁸

4 B. Krebs, “Shadowy Russian Firm Seen as Conduit for Cybercrime,” *The Washington Post* (October 13, 2007), <http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html>.

5 D. Danchev, “The Neosploit cybercrime group abandons its web malware exploitation kit,” *ZDNet* (July 29, 2008), <http://blogs.zdnet.com/security/?p=1598>.

6 M. Alldrick “Cyber crime provokes new security concerns,” *Lloyd’s News Center* (March 13, 2008), http://www.lloyds.com/News_Centre/Features_from_Lloyds/Cyber_crime_provokes_new_security_concerns_130308.htm.

7 “2007 Annual Survey: Cost of Data Breach,” *The Ponemon Institute* (November 29, 2007), <http://www.ponemon.org>.

8 J. Vijayan, “TJX says breach costs may exceed \$150 million,” *Central IT* (August 16, 2007), http://www.central-it.de/html/news/internationale_news/6388120/index2.html.

Cybercrime and punishment

Fighting cybercrime is problematic in many aspects. In contrast to classic crimes such as drug offences or fraud, cybercrime has a vast scope, consisting of all kinds of actions designed to steal data for profit. A legal definition of cybercrime is difficult since it should incorporate related terms such as “computer,” “access,” “authorization,” “malware,” or “spyware.”⁹ Many actions are currently not defined as illegal, such as C2C activities, writing crimeware, malicious code or Trojan programs for other criminals.

Location is a problem as well; crimeware servers are often in a different country than the criminals that operate them. The same applies to the victims as well as the buyers of stolen data – they are located all over the world and often reside in a different country than the cybercriminals who stole the

data, making law enforcement complicated since it is unclear which jurisdiction applies – the F.B.I. with its Cyber Crime Unit when the victim is located in the U.S.? or the CSIS in Canada where the cybercriminal is operating from? Even if a cybercriminal is convicted, the punishment seldom fits the crime. It is only recently that prison sentences of a few years and substantial fines have been handed out.¹⁰

About the Author

Yuval Ben-Itzhak, CTO at Finjan, has over 15 years of high-level management experience. Yuval was selected as InfoWorld's “Top 25 Most Influential CTOs of 2004” and Computerworld's “40 Innovative IT People To Watch, Under the Age of 40” for 2007. He may be reached at tel: +972-9-864 8200 or info@finjan.com.



⁹ K.C. Jones, “Congress Extends Cybercrime Laws,” *InformationWeek* (September 17, 2008), <http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=210602182>.

¹⁰ Corinne Iozzio, “The Cyber Crime Hall of Fame,” *PC Magazine* (September 8, 2008), <http://www.pcmag.com/article2/0,2817,2329605,00.asp>