



# Control Essentials

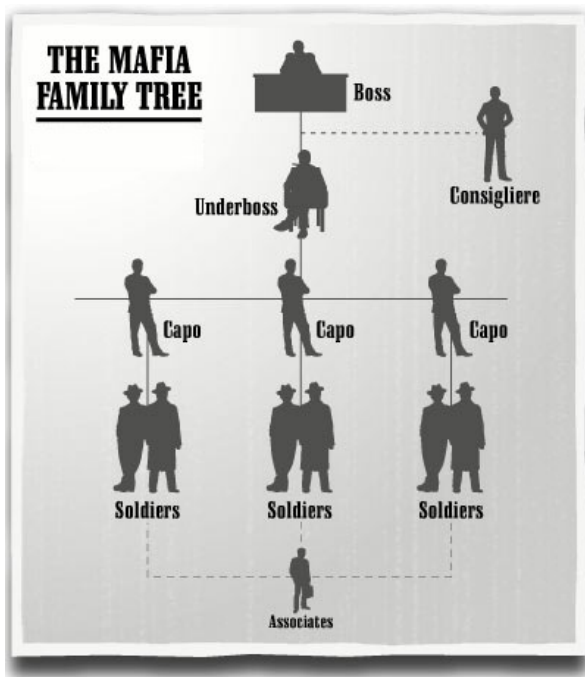
## Commercial Hacking: The Mafia Returns



Hacking is no longer just for fun any more. These days it is big business. In 2004, cyber-crime became more lucrative than drug trade as a \$105 billion business<sup>1</sup>. So how, exactly, does cyber-crime differ from individual hackers, and how has it grown to be so strong?

### My Respects, Godfather

The meteoric rise of cyber-crime to become a highly lucrative—if illegal—business proposition can be directly attributed to its business model. This model is a tried and tested one, once used by the highly successful mafia. The mafia used a disciplined, premeditated, and well-structured approach to crime. Many cyber-criminals today operate exactly like the mafia with a sophisticated approach involving an organizational chart that would almost fool you into believing that this was a beauty products company or a car manufacturer.



The picture on the left portrays the organizational chart of the traditional mafia. The new-age cyber-crime mafia operates under a very similar structure. The boss is the quintessential CEO. The boss never gets his or her hands dirty and thus has, technically, never committed a cyber-crime. The person who carries out the orders is the underboss who works in conjunction with the *consigliere* or the boss' right-hand-man. The underboss works as the control center and could be called on for provision of attack tools such as Trojans, Keyloggers, Formloggers, and other malicious software.

There are several Capos or the *caporegimes*, each commanding his own network of soldiers who carry out the actual attacks and mine all the personal information that they can hack. The soldiers, in the cyber-crime sense, form an entire network, interdependent for spare resources.

Image Source: HowStuffWorks.com



Associates, or salespeople, make up the bottom tier of the organizational structure. They make their money by reselling personal information, including credit card numbers, social security numbers, bank account details, and other data. Since they obtain this information from the various soldier networks, they do not know exactly how this information was obtained but they do have all related “product knowledge,” such as the tightness of a particular bank or credit card company’s rules on withdrawals or overdrafts, or if any particular stolen information (e.g. credit card number) has been already reported as stolen. These associates are very similar to a salesperson at your favorite electronics store who has detailed knowledge of the features of a product on sale but not as much on its origin or wholesale cost.

Internet chat rooms and forums are the marketplace where buying and selling take place. The pricing structure is highly interesting and one that you can relate to. Fast moving consumer goods like credit card numbers, ATM/Debit card numbers, PINs, and social security numbers, are available at economical rates, ranging from as low as \$10 to a few thousand dollars. Luxury goods like corporate espionage information from competitor companies, healthcare records, corporate e-mail and file transfer accounts, are pricier given the higher stakes involved.

Even with all these similarities, there is one important aspect that sets the cyber-crime mafia a long step ahead of the traditional mafia. The traditional mafia operated in the real world while the cyber-crime mafia works within the comfortable cushion of the internet. Geography does not limit the structure, as the boss can be located in Russia while the underboss is in Indonesia and the capos do the legwork in Venezuela, China, Brazil, and Nigeria. The soldiers can dot the entire globe with their presence and the associates can pitch their products virtually anywhere and anytime.

Nearly 40 years after the first Godfather movie, the mafia has returned and its members are even harder to catch.

## **Operational Groups**

With the advent of the cyber-crime mafia and its modus operandi, some organized groups have reached the pinnacles of cyber-crime. One in particular, the most notorious known, is discussed below.

### **Russian Business Network**

Known as the RBN, this organization is a multi-faceted cyber-crime mafia. Their well-known activities include child pornography, corporate blackmail, spam attacks, and in some cases the group has monopolized personal identity theft for resale. The RBN’s individual activities are pegged at earnings of up to \$150 million a year.

The RBN, allegedly, is said to have good connections in Russia’s political sphere and it has also been alleged that cyber-terrorism incidents directed at Georgia and Azerbaijan were linked to the RBN<sup>3</sup>. The fact that the organization operates under 19 different known names out of more than six different known countries indicates the measure of their resolve and sophistication.



## **Extortion...With A Discount!**

To conclude, an excerpt from an actual DDoS (Distributed Denial of Service) extortion letter<sup>4</sup> would be most apt – *Hello. If you want to continue having your site operational, you must pay us 10,000 rubles monthly. Attention! Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us. The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and they begin to block our bots, we will increase the number of bots to 50,000, and the protection of 50,000 bots is very, very expensive.*

*You will also receive several bonuses.*

*1. 30% discount if you request DDoS attack on your competitors/enemies. Fair market value ddos attacks a simple site is about \$ 100 per night, for you it will cost only 70 \$ per day.*

*2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them.*

## **References**

<http://www.foxnews.com/story/0,2933,177016,00.html>

[http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/the\\_web/article2844031.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2844031.ece)

<http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html>

<http://m.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528>

## ***ERM wants to hear from YOU....***

With this edition of our newsletter, we're rolling out a new format and new features. Tell us what you think!

What features or topics would you like to see covered in future issues? Who else should receive this newsletter?

Your feedback is welcome and encouraged. Please send your comments to [editor@emrisk.com](mailto:editor@emrisk.com).

## **Enterprise Risk Management: *At a Glance***

ERM brings clients the highest level of expertise to assess and address risks, comply with standards and regulations and mitigate risks, using integrated and reasonably priced security services and solutions.

Our practice provides organizations with the tools they need to address the compliance and risk management issues of today, as well as the broader and ever-increasing security challenges of the future.

### **Services**

IT Security  
Regulatory Compliance  
IT Audit  
Computer Forensics  
Risk Management  
Attestation

### **Certifications**

Certified Public Accountant (CPA)  
Certified Information Systems Security  
Professional (CISSP)  
Certified Information Systems Auditor (CISA)  
Certified Information Systems Manager (CISM)  
Certified Information Technology  
Professional (CITP)  
GIAC Security Essentials Certification  
GIAC Systems and Network Auditor  
Qualified Security Assessor (QSA)  
Approved Scanning Vendor (ASV)

### **Some of our Clients**

ABN-AMRO Private Banking  
Bacardi-Martini, Inc.  
Bancafe International  
Banco Industrial de Venezuela  
Banco ITAU  
Bank United  
Caja Madrid Bank  
Carnival Cruise Lines, LLC  
CitiBank  
Coconut Grove Bank  
Commerce Bank  
E-data Financial  
Florida International University  
Florida Power & Light Company  
Heico Aerospace  
Helm Bank  
Knight Ridder  
Nova Southeastern University  
Rinker Materials  
Rudy, Exelrod & Zieff, LLP  
Seabourn Cruise Line  
TecniCard, Inc.  
The International Bank of Miami  
TransAtlantic Bank  
U.S. Century Bank

For more information, visit [www.emrisk.com](http://www.emrisk.com)

E-mail: [info@emrisk.com](mailto:info@emrisk.com)

Phone: 305-447-6750

800 Douglas Road  
North Tower, Suite 835  
Coral Gables, FL 33134

**enterprise risk management**

*The Control Professionals*