National Cyber Security Centre

a part of GCHQ

Cyber crime:
understanding the online business model

Contents

Introduction....4

How an OCG is set up....5

How criminals get access to your machine or networks and steal data....7

How criminals turn data into cash....8

How profitable is cyber crime?....10

How to protect yourself from cyber crime....11

Introduction

The Internet is a major enabler for Organised Criminal Group (OCG) activity. Compared to making money from more traditional crimes, hacking individuals, SMEs and large organisations is a relatively low-cost, low-risk proposition for criminal groups - and there are many parts of the world where such activity is not actively prosecuted by the authorities.

Many of these OCGs share similar techniques and services, and communicate with each other over heavily vetted closed criminal forums on the 'dark web' where they can collaborate and advertise new services, tools and techniques.

The cyber crime threat spans different contexts, and covers a wide range of online criminal activity, from scamming activity through to sophisticated attacks against financial institutions and other large organisations. Most people are aware of phishing emails and the risk of clicking on links and attachments that could potentially result in your computer or personal device becoming infected with malware. Most people are also aware that this malware could steal your personal identifiable information, passwords, bank account and credit card numbers, or lock up your drives and databases unless you pay a ransom.

Those unfortunate enough to have been the victims of cyber crime are also familiar with that sinking feeling that accompanies the realisation that money has been stolen from your bank account, or that your credit card has been used in some distant country by a criminal to pay for a wide range of different goods and services without your knowledge.

> "Very few people are aware of the extent of the online criminal ecosystem that supports and enables cyber attacks, and the business model behind it."
>
> **Matt Carey**
>
> **HEAD OF LONDON OPERATIONS TEAM NCSC**

However, very few people are aware of the extent of the online criminal ecosystem that supports and enables these attacks, and the business model behind it. This report, which the NCSC are publishing to support our ongoing transparency agenda, briefly outlines how cyber criminals are organised, their methods, and how their activities are monetised.

Matt Carey

Head of London Operations Team, NCSC

How an OCG is set up

Most of the people within organised crime groups will have unique and valuable skill sets. Typically, these roles will comprise:

Team leader

A successful criminal group needs a team leader to oil the wheels and keep everyone in check. Sophisticated and successful cyber crime activity is managed by a co-located, or closely connected, OCG. Within any OCG there are several core criminals who are key to the success of the activity, each of whom ensure that they are keeping ahead of (and in some cases, in the pockets of) local and international law enforcement.

Coders

Coders, also known as malware developers, will write and update new code for malware, or plagiarise or modify publicly available malware. Cyber crime malware has progressed significantly in the past 10 years, from enabling basic access to a network or system to being able to:

- execute a wide range of commands on a host (including collecting screenshots, video captures and keylogs off a victim machine)
- hide from antivirus
- remotely control the victim's machine
- wiping Master Boot Records

Some forms of criminal malware are also able to hide in memory, so that even when you think you have removed them from the machine, they can re-establish themselves when it's rebooted. Increasingly, developers are deploying configuration files with their malware that look specifically for the presence of certain systems on a target system (such as salary or other payment systems like SWIFT or BACS) to maximise their access to machines most likely to provide lucrative fund-stealing opportunities.

Network administrator

Not every group will have a network administrator or bot herder, but when present, they are responsible for hijacking (compromising) hundreds of online servers and devices which, when linked together, are referred to as a 'botnet'. Having such a large network of devices within their control means bot herders have a significant network of machines to exploit. They can establish a global presence and scale their compromise of new machines, as well as execute powerful Distributed Denial of Service (DDoS) attacks if they wish to. Bot herders will also target devices that are constantly online and have good Internet bandwidth.

Bot herders are aware of the power of antivirus and other security mechanisms to remove bots from their network, as well as destroy their ability to control their networks. To add resilience to their business models, bot herders are often adding encryption to their networks to make their activity harder to detect, and using anonymisation services (like TOR) to hide the identity of their own devices on the Internet. This means researchers and law enforcement are unable to discover who they are.

Intrusion specialist

If an OCG manages to successfully install malware on a business network or other major target, then an intrusion specialist will step in with their own toolkit to ensure the malware presence is enduring and that they can exploit the network, often working to gain administrator privileges to gain access to the most valuable applications and databases.

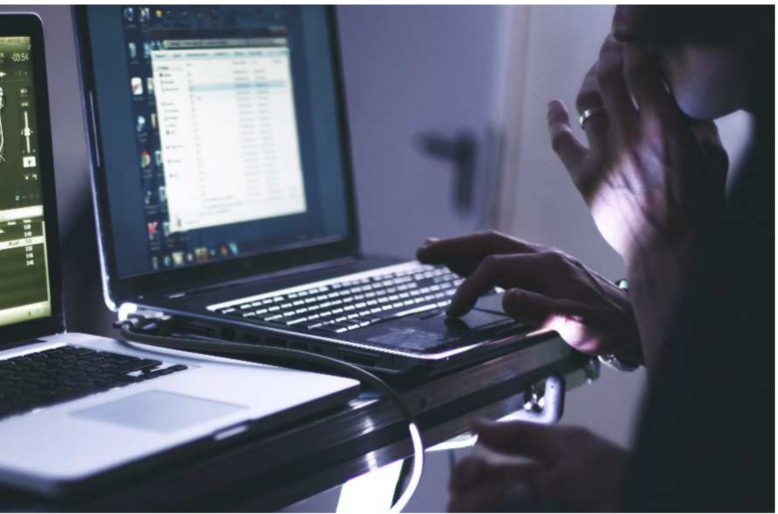
In the case of some sophisticated groups, such as the criminals behind some of the variants of financial Trojans like Carbanak and Dridex, they may spend weeks and months navigating the network to find the precise machines that they need to access to initiate and validate a large payment. They may also hijack valid administration tools on the network in order to make it look like their activity is part of normal network administration, as opposed to malicious activity.

Data miner

A cyber crime group will also often employ a data miner. Cyber criminals are now adept at stealing data in bulk. However, data is also valueless if it cannot be viewed in a format that can be easily sold on or exploited. Often, the stolen data itself is a mess and the valuable data (e.g. credit cards, passwords, bank accounts, personal details) is hidden within a mass of jumbled data strings. A skilled data miner can identify and extract the data of value so that it is ‘clean’, categorising it and presenting it in a way that can be used to make money, or sold on a criminal forum to other criminals to exploit.

Money specialist

Once an OCG has clean data, they can ‘monetise’ it. A money specialist can identify the best way to make money from each type of dataset. This could be selling in bulk to trusted criminal contacts, or by using specialist online services.



How criminals get access to your machine or networks and steal data

The most common way your computer might become infected with data stealing malware is still via spam emails which contain a malicious link or attachment. Other common ways your computer might be compromised are through visiting genuine websites that have been compromised with malicious code (known as a watering hole attack) or adverts that redirect you to a malicious server that will serve up advertisements to your computer (known as malvertising).

How phishing works

Spam emails have been used for years to deliver malware, but these have evolved significantly. Everyone with an email account in the UK will have received phishing emails in their inbox. By using interesting or concerning topics within the spam email (like fake invoices or banking security notifications), you're encouraged to open them quickly out of curiosity, or concern. When you do, malware is deployed which will attempt to exploit your device. Whether it succeeds or not is often dependent on how up-to-date your antivirus is, and how well patched your operating system and software are.

Whether malware succeeds or not is often dependent on how up-to-date your antivirus is, and how well patched your operating system and software are.

The attachment in the spam email will often only contain a basic piece of malware or a 'loader' which, when deployed to your computer, is used to determine whether or not a full exploitation is possible or worthwhile for the cyber criminal. Once this determination is made, the loader will reach back to the cyber criminal's malicious server and download a full malware package to it.

Watering holes and exploit kits

In the case of watering holes (or some spam emails containing malicious links), you will be redirected to an exploit kit - a suite of computer programmes which scan your computer for exploitable vulnerabilities. When one of these vulnerabilities is discovered, an appropriate exploit will be deployed, which will then enable the installation of *other* malware to exploit your device. Once the malware is deployed, the whole range of tools contained in its code can be used to obtain what the criminal needs, including such things as keyloggers to capture what you type - including your passwords.

Attackers will often use a tool called a 'web inject' to monitor the internet browsing of an infected user. When the victim attempts to access their normal internet banking platform, the malware will serve up a fake web page that looks exactly like their real online banking web page. It will steal the victim's login details and password, and trick the user into entering their token authentication, or SMS authentication, so that the attacker can quickly replicate the process on the genuine web page in order to get access to (and steal from) the account.

If the OCG assesses you as a high value target (such as a company or accountancy firm), once the initial infection has occurred, it may be handed over to the intrusion specialist described earlier to look for the best way to secure the highest payout, particularly if payment software like BACS or SWIFT has been identified on the victim network.

How criminals turn data into cash

Criminals have a variety of ways to 'monetise' the data they steal from you, but generally the OCG will either do it themselves, or they will sell any stolen data on to other criminals to exploit in what is known as 'secondary fraud'.

To exploit bank accounts, an OCG will employ the services of specialists (known as money mules and mule herders) to launder stolen money through a myriad of accounts, eventually overseas and into the hands of the OCG. If an OCG is going to sell the data, there are hundreds of criminal websites to facilitate this, including something called an Automated Vending Cart (AVC) where data can be bought in bulk with digital currencies such as Bitcoin.

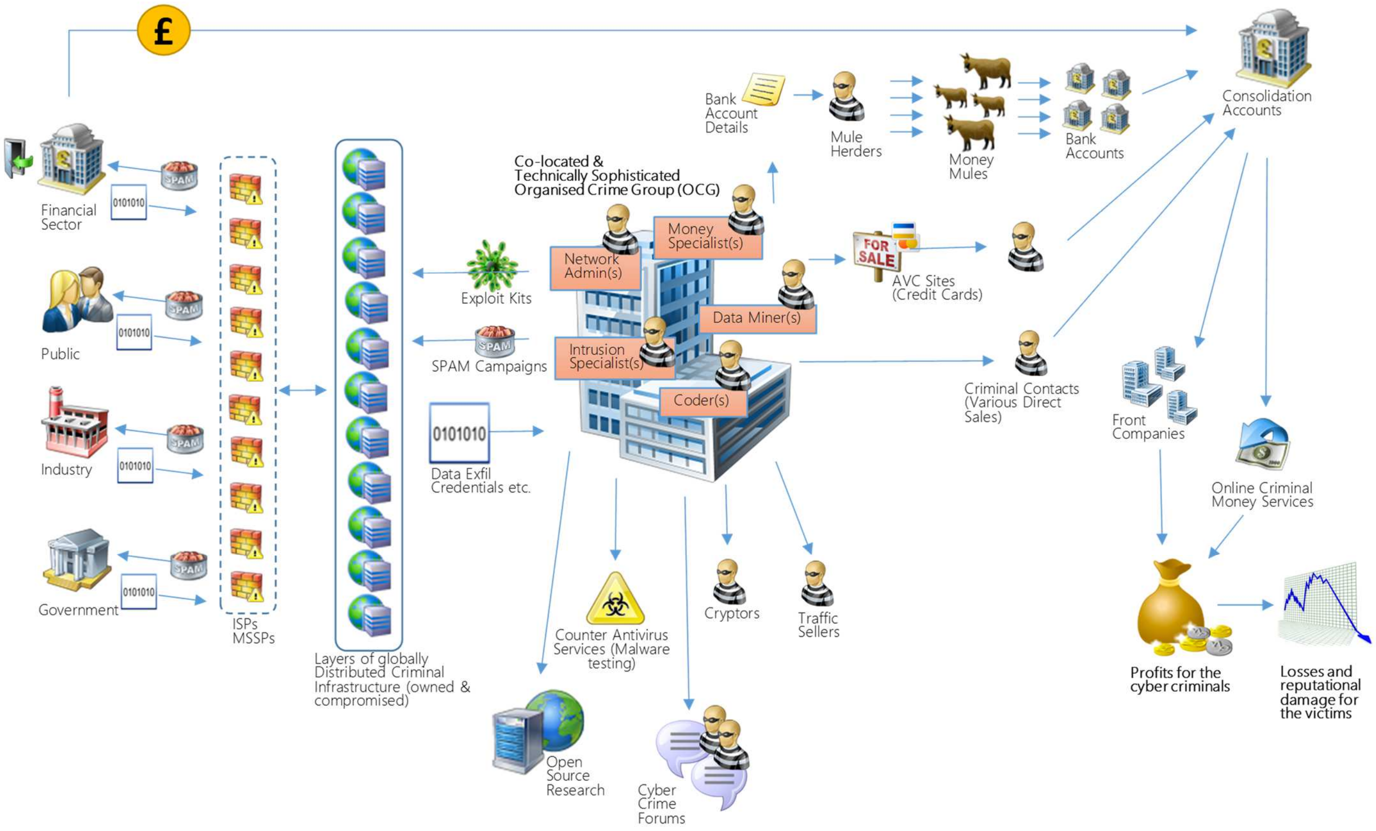
How cyber criminals use the 'online marketplace'

For the most organised and technically advanced groups, many of the services described are carried out 'in-house' as part of their own business model. For smaller groups or individual criminals, these services can be hired on the cyber criminal 'online marketplace' using a plug-and-play approach to crime. Most of these services will be openly advertised in criminal forums. Some of the other typical services that are also regularly used by cyber criminals include:

- Counter Anti-Virus (CAV) Services, which scan malware against all of the Anti-Virus packages currently on the market to ensure it goes unnoticed when it is deployed against a victim's device.
- Bullet Proof Hosting Services, which rent servers to host online criminal activity, but will not co-operate with local or international law enforcement (hence 'bullet proof').
- Escrow Services, which will act as a 3rd party during transactions between untrustworthy criminals, holding onto their payments until they are happy with the quality of the service provided.
- Cryptor Services, which put an encryption 'wrapper' around your malicious code to give it the best chance of being undetected.
- Drop Services, which help any criminal business translate ill-gotten gains into cash. This service helps multiple crime types (including cyber criminals) transfer money between bank accounts, or physically move currency across international borders, or into other less traceable currencies such as Bitcoin.

These services form part of the financial trojan business model, as shown in Figure 1 below.

Figure 1 The financial trojan business model


£
Financial Sector
Public
Industry
Government
SPAM
0101010
ISPs
MSSPs
Layers of globally Distributed Criminal Infrastructure (owned & compromised)
Exploit Kits
SPAM Campaigns
Data Exfil Credentials etc.
Co-located & Technically Sophisticated Organised Crime Group (OCG)
Network Admin(s)
Money Specialist(s)
Data Miner(s)
Intrusion Specialist(s)
Coder(s)
Counter Antivirus Services (Malware testing)
Open Source Research
Cyber Crime Forums
Cryptors
Traffic Sellers
Bank Account Details
Mule Herders
Money Mules
Bank Accounts
Consolidation Accounts
FOR SALE
AVC Sites (Credit Cards)
Criminal Contacts (Various Direct Sales)
Front Companies
Online Criminal Money Services
Profits for the cyber criminals
Losses and reputational damage for the victims

How profitable is cyber crime?

The interesting thing is that all the services used by cyber criminals cost money, from malware development all the way through to money muling. All the individuals involved in the criminal ecosystem that supports fraud through a malware campaign require payment. This means that unless the criminals are able to access large numbers of bulk payment systems, and get high value payouts on each occasion, each individual criminal is relying on small profit margins from each hack just to keep their business going.

They then need to reinvest these profits into developing their botnets and campaigns further in order to have continued success. They are constantly developing the next new malware and attack, so that if their current malware campaign gets taken out by law enforcement or industry interventions, they are ready with a new campaign to ensure the continuity of their cashflows.

Therefore, while it is a low risk enterprise for many of those criminals operating in places where law enforcement is unable or unwilling to prosecute them, in order to make a good living out of this form of crime, most of the criminals involved in maintaining criminal marketplace services and running financial trojan campaigns have to work full time in order to turn a decent profit.

How to protect yourself from cyber crime

NCSC publishes two key products covering how best to protect individuals and businesses from cyber crime, including the best route to report incidents if you have been a victim:

- Cyber Aware: (https://www.cyberaware.gov.uk/) cyber security advice for individuals and small businesses, including software updates and information on creating effective passwords
- Cyber Essentials: (https://www.cyberstreetwise.com/cyberessentials/) industry-supported scheme to guide businesses in protecting themselves against cyber threats

National Cyber Security Centre
a part of GCHQ

Cyber crime: understanding the online business model