The Underground Economy

Aditya Chopra

08 November 2017

1 The underground economy

The underground economy refers to economic activity surrounding illegal goods or services. In the past years, we've seen a shift from teenagers hacking to make a name for themselves, to organized criminals hacking for profit. These hackers take part in the underground economy. We describe some of the common ways criminals make money with hacking skills today.

Blackmail

By infecting computers, hackers have access to victims' data, including sensitive private data such as browsing habits. These hackers can then make money by forcing victims to pay them in exchange for not having their information released.

Ransomware

Ransomware is malicious software that hackers place on victims' computers which encrypts the victims' hard drives and sells the user the decryption key in exchange for some money.

Stealing credentials

Hackers can also garner victim's credentials to banking websites by infecting their computers. These credentials can be used in a number of ways including stealing and laundering money.

Botnets

Botnets are groups of infected computers under the control of a central authority. These can be used for a variety of purposes, including services such as DDoS or performing computational tasks such as mining bitcoin.

DDoS

DDoS is distributed denial of service, or an attack that focuses on using the power of a large number of computers to deny users access to a particular service. This attack is powerful and can often bring down entire websites by hitting them with a large amount of traffic. It is difficult to defend against when the attacker is using a botnet because the machines are distributed across the world and do not necessarily share any characteristics that can be used to mitigate the attack.

Bitcoin

Botnets can also be used to mine bitcoin using the computational resources in the botnet. Experts[1] suggest that using botnets to mine for bitcoin is not worth it, however.

Selling services

Hackers also make money by hacking for hire. Large companies often pay these hackers to attack their software and report exploits.

Selling spam

Hackers often also sell spamming services that can leverage compromised computers to send spam emails to users. The spam market is complicated, and we go into more detail in section 5.

2 Credit cards

We now look into a specific case study. In the underground market, one can often find lists of credit card numbers in which each card is being sold for a couple of dollars each. This raises the question of why credit cards with thousands of dollars in credit limits are being sold for such a discount.

Risk tax

First off, there is an inherent risk associated with using stolen credit cards. Any buyer in the underground economy would need to take precautionary measures that take extra effort and money. This reduces the amount that a buyer is willing to pay for each credit card.

Ripper tax

Furthermore, not every card number sold is legitimate. Buyers attempt to counteract scammers by only buying from trusted sellers with good reputations. However, in the end, the cards may not be fresh, or could have been sold to other buyers too. There is no guarantee on the cards' authenticity.

3 Combating the underground economy

Given the huge underground economy, one may ask themselves what law enforcement can do to combat this illicit activity. We describe two approaches.

Fight monetization

The first approach is to fight criminals' monetization methods, which is their primary bottleneck. There are a few select banks in the U.S. which criminals use to launder their money. Law enforcement agencies can target these banks and force them to tighten their policies to affect a large number of criminals.

Infiltration

We have seen law enforcement agencies gain control of underground forums and slowly extract the information of numerous key players who they can pursue offline. For example, law enforcement once infiltrated a large forum by creating an account, gaining reputation, and passively gathering information. Once they had

[1] https://www.theregister.co.uk/2014/06/24/bad_news_malware_infections_are_mining_bitcoin_good_news_theyre_not_making_any_money/

enough information to pursue a key sysadmin, they offered a deal to the sysadmin, which allowed them to take control of the sysadmin's account. They then used this highly trusted account's reputation to convince the site to move onto another hosting service (one owned by the law enforcement agency). Then, after continuing operations for a year to gather data, the agency suddenly shut the website down and simultaneously raided hundreds of criminals worldwide.

4 Security economics

In this section, we consider an example about security software and game theory. Imagine a scenario where the IT department of a company is responsible for protecting their computers from malicious hackers. Suppose that this company owns 900 PCs and 100 Macs. Now, we assume that the department must make a choice of protecting either PCs or Macs. Furthermore, the attackers must make a choice of attacking either PCs or Macs.

In order to solve for the optimal strategy for both parties, we must assume that they employ probabilistic strategies. We include the payoff matrix to describe this problem below:

$$\begin{array}{cc} & \text{Defender} \\ & \begin{array}{cc} \text{PC} & \text{Mac} \end{array} \\ \text{Attacker} \begin{array}{c} \text{PC} \\ \text{Mac} \end{array} & \begin{bmatrix} 0 & 900 \\ 100 & 0 \end{bmatrix} \end{array}$$

If we solve for the optimal strategies, attackers should attack PCs with 90% probability, and the defender should also defend PCs with a 90% probability.

Now we consider the situation where the attacker's success rate is only 50%:

$$\begin{array}{cc} & \text{Defender} \\ & \begin{array}{cc} \text{PC} & \text{Mac} \end{array} \\ \text{Attacker} \begin{array}{c} \text{PC} \\ \text{Mac} \end{array} & \begin{bmatrix} 0 & 450 \\ 50 & 0 \end{bmatrix} \end{array}$$

The optimal strategies, in this case are the same, since the payoffs were simply scaled by a factor of 2.

Finally we consider the situation where the defender's defense rate is only 50%:

$$\begin{array}{cc} & \text{Defender} \\ & \begin{array}{cc} \text{PC} & \text{Mac} \end{array} \\ \text{Attacker} \begin{array}{c} \text{PC} \\ \text{Mac} \end{array} & \begin{bmatrix} 450 & 900 \\ 100 & 50 \end{bmatrix} \end{array}$$

In this case, in contrast to the last one, the attacker's optimal strategy is now to always attack PCs since the payoff will always be higher for them.

5 Spam value chains[2]

The spam value chain describes the infrastructure and parties of the spam ecosystem responsible for monetization. There are three distinct stages:

1. **Advertising** is responsible for getting the spam URL to the target user and getting them to click it.

[2]Student presentation by Won Park

2. **Click support** is responsible for redirecting the user's click through redirection sites, owning domains, provisioning name servers, running web servers, and operating affiliate programs[3].

3. **Realization** is responsible for fulfilling the customer's order. This involves payment and delivery infrastructure.

In the paper[4], the authors study the bottlenecks in the value chain in order to determine where law enforcement can do the most damage. They specifically study three parts of the chain:

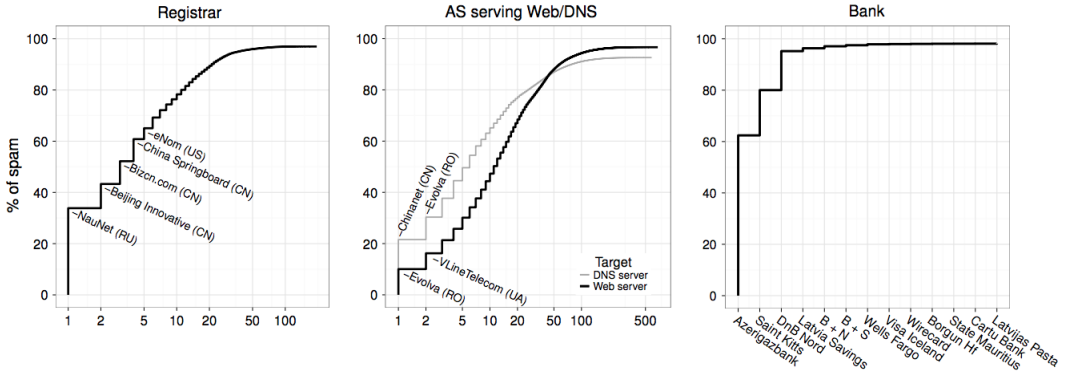

Figure 5: Takedown effectiveness when considering domain registrars (left), DNS and Web hosters (center) and acquiring banks (right).

1. **Registrars** As one can see in the graph, the sharing amongst registrars is low. Furthermore, it is easy to switch registrars, so this is not an effective way to target spam value chains.

2. **DNS and Web hosters** We can see that there is even less sharing amongst hosting services, which are also easy to switch.

3. **Acquiring banks** Banks are harder to switch in the case of a bank's policies becoming more restrictive, making them a better target. Also, we can see that there is a large amount of sharing, meaning that even by targeting one bank, authorities can hurt 60% of spam supply chains.

6 Research ethics[5]

In this paper[6], the authors describe four guiding principles that they believe researchers ought to follow when conducting ethical research, citing reviewed and accepted papers that they believe violate these tenets.

6.1 Do not harm humans actively

This principle, while seemingly straightforward, deserves mention. Some studies in the past such the Tuskegee syphilis experiment have violated it. In this experiment, the researchers were studying the progression of syphilis. However, the researchers did not inform any of the infected that they had the disease, nor did they inform the subjects about the cure once it was discovered.

[3]Affiliate programs storefronts, analytics, and advertising in addition to taking responsibility for contracting payment and fulfillment services.

[4]Click Trajectories: End-to-End Analysis of the Spam Value Chain, Levchenko et al.

[5]Student presentation by Aisha Mushtaq

[6]Ethics in Security Research: Which Lines Should Not Be Crossed?, Schrittwieser et al.

6.2 Do not watch bad things happening

This principle suggests that the authors believe that researchers performing an experiment have an ethical duty to stop or report harm if they observe it. Does this mean that we shouldn't study criminal activities to gain deeper understanding? One of the case studies cited is *Spamalytics: An Empirical Analysis of Spam Marketing Conversion*[7]. In this example, the researchers infiltrated a botnet and analyze two spam campaigns that the botnet was running. However, the researchers then gathered data from the users that were infected by the botnet. Were the researchers justified in utilizing an illegal botnet to gather data, without users' consent, for their own purposes?

6.3 Do not perform illegal activities to harm illegal activities

For this principle, the authors consider a case study *Your Botnet is My Botnet: Analysis of a Botnet Takeover*[8]. They argue that breaking into a botnet, regardless of the botnets function is unethical. To back up their claim, they consider distributed computing projects to be in the same class. They draw an analogy to breaking into a thief's home. Can we justify breaking in just because the home belongs to a criminal?

6.4 Do not conduct undercover research

The idea behind this principle is best explained with an example. The authors consider *Is the Internet for Porn? An Insight Into the Online Adult Industry*[9]. In this paper, the authors actively participate in the adult content industry by setting up their own website serving mature content. The authors of this study argue that it is necessary to perform a realistic experiment in order to estimate the success of attacks in the real world. The ethics of this study are questionable, and thus the authors (of the paper criticizing this study) argue that we should avoid such ethical gray areas by not conducting undercover research.

[7] Kanich et al.
[8] Stone-Gross et al.
[9] Wondracek et al.