2012

Territorial behavior and the economics of Botnets

Craig S. Wright
Charles Sturt University

DOI: 10.4225/75/57b55e26cd8dd
Originally published in the Proceedings of the 10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

TERRITORIAL BEHAVIOR AND THE ECONOMICS OF BOTNETS

Craig S Wright
School of Computing and Mathematics
Charles Sturt University
Wagga Wagga, NSW, Australia
craig.wright@itmasters.edu.au

Abstract

This paper looks at the economics associated with botnets. This research can be used to calculate territorial sizes for online criminal networks. Looking at the types of systems we can compare the time required to maintain the botnet against the benefits received. In doing this it will be possible to formulate economic defence strategies that reduce the benefits received through the control of the botnet. We look at the decision to be territorial or not from the perspective of the criminal bot-herder. This is extended to an analysis of territorial size. The criminal running a botnet seeks to maximize profit. In doing this they need analyse the costs expended and benefits received against the territorial size. The result is a means to calculate the optimal size of the botnet and the expected returns. This information can be used to formulate security strategies that are designed to reduce the profitability of criminal botnets.

Keywords

Botnets, Economics, Game theory, Internet Security, Malware

INTRODUCTION

Criminals defend territories in cyberspace (Bensoussan, Kantarcioglu, & Hoe, 2010). This virtual environment is an environment where it is possible to engage in economically profitable low risk criminal activities. The boundaries are like invisible lines on the map of the Internet, but they form connected systems analogous to a real world territorial environment. The component systems that comprise the botnet are defended by aggressive displays and direct attacks, sometimes under by defenders, at times by competing criminal groups.
Several different territorial strategies exist for criminal groups running botnets. Each of these strategies has different benefits and costs associated with them and several of them are independent of the others. Some strategies involve the exploitation of high-value targets (including the exfiltration of data) whereas others involve the use of large numbers of systems to amplify low value transactions (including SPAM transmission and DDOS attacks). Territories are smaller both when they are higher in resource value as well as when they cannot be further secured by the attacker once the machine is owned because they are less defendable and are usually abandoned early when attacked (Figure 4).

EXTRA-JURISDICTIONAL TERRITORIES

One territorial strategy would be to only attack extract-jurisdictional systems. This would include machines that are located outside of the criminal's legal jurisdiction. The strategy lowers the risk of being caught and hence lowers the cost associated with engaging in this course of action.

INTRA-JURISDICTIONAL TERRITORIES

Criminal groups operate within jurisdictional boundaries when the risk of being caught is perceived as low and the rewards are perceived to exceed the risk. This can occur when the benefits of acting within a local jurisdiction exceed the increased risk of punishment that can result from being caught and more easily charged with an offense within a local jurisdiction.

NON-TERRITORIAL STRATEGIES

An alternative approach would be to compromise individual hosts and networks extract data and leave the system undetected by defenders. In this way the attacker compromises a server, gains access, obtains the resource they sought and leaves after either covering the tracks or being detected. This could be seen as a migratory strategy with the attacker moving from system to system in a constant attempt to exploit vulnerable hosts. Where sufficient vulnerable systems exist to allow the criminal to profitably move from system to system will still making an acceptable return on their investment of time and resources the non-territorial strategy can work.

The non-territorial attacker also acts as a predatory force when systems that have been compromised by territorial criminal groups are targeted. In this instance the non-territorial attacker increases the cost of maintaining access to the territorial criminal who has to expend additional time and resources maintaining their territory as well as making it more likely that the system owner will notice the compromise and respond by removing both sets of criminal groups.
Due to the time and resource requirements associated with attacking and successfully exploiting any given system, the costs associated with a non-territorial strategy limit the criminal to attacking high-value resources.

TO DEFEND OR NOT DEFEND

Here, territorial refers to the context of holding a group of systems for an extended period of time. An alternative strategy would be to compromise systems for selected engagements. An example of a non-territorial criminal strategy would be to break into a targeted network, exfiltration information and abandon the system covering one's tracks. In this the attacker could remove all traces of the criminal activity before moving on to another target. Conversely where an attacker maintains access to a system in defence access to those compromised hosts they are engaging in territorial activity.
Decisions cybercriminals must make (Bensoussan, et al., 2010; Li, Liao, & Striegel, 2009):

1. Whether or not to be territorial
2. If so, what size territory to defend.

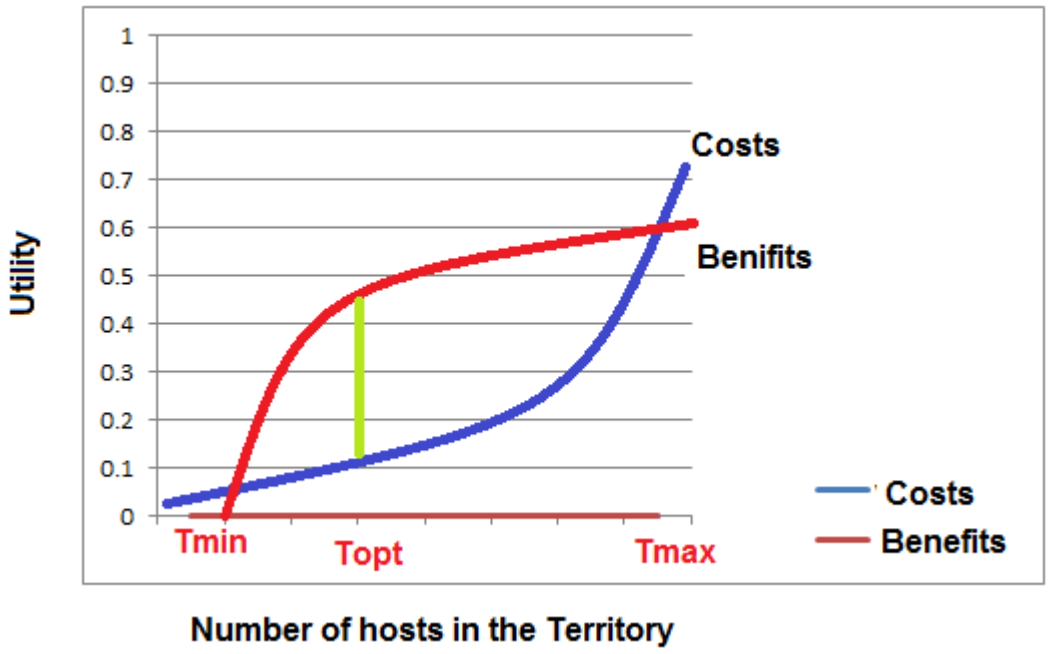

Figure 4 A cost Benefit analysis of criminal territory in cyber compromises

Cyber-criminals can engage in either pure or mixed strategies (Clarke & Cornish, 1985). The pure strategies involve either territorial a non-territorial actions where is a mixed strategy incorporates a combination of the above. In all instances where a territorial strategies involved it becomes necessary for the cyber-criminal to make decisions as to the size of territory they seek to defend.
There are multiple costs associated with the acquisition of a territory whether this is directly related to a botnet or if the system is comprised of otherwise compromised hosts. The attacker needs to not only consider the cost of initially acquiring and compromising the host (Lin, Chen, Chen, & Chien, 2009) but to the subsequent holding and maintenance of that compromised host.

THE COSTS OF ACQUIRING RESOURCES

The first cost aspect of creating a criminal territory results from the initial acquisition cost. There is several stages can be differentiated based on the strategies associated with the individual botnet. These stages can be summarised as:

- Research,

- Reconnaissance,
- Scanning,
- Exploitation,
- Maintaining access, and
- Covering tracks.

This initially starts with a research and reconnaissance phase. An attacker with a selected strategy will seek out systems to exploit and then seek possible targets.
Each step from reconnaissance to exploitation involves risk and costs to the attacker. Risk increases significantly at the scanning and exploitation stages but there costs from the initial research stage on. At the minimum cost can be counted as a time-based resource where it cannot directly be associated and accounted for in monetary terms. The reason for this is that time is a scarce resource with alternative uses. The attacker can make use of the time taken is researching and attacking one host for other uses. Whether these are the uses are attacking other systems or the pursuit of legitimate employment opportunities, the time taken could have been employed in alternative uses.
Any action taken by the potential target that results in prolonging the time needed to successfully exploit a system increases the cost to the attacker. These costs directly reduce the perceived benefits that can be obtained through an attack. In cases where the attack is not automated the attacker will become dis-incentivized when the level of perceived benefits received is reduced below an acceptable level (Bensoussan, et al., 2010). Like all rational agents, the economic criminal will seek to obtain an economic return on their investment and when this cannot be obtained will forgo the project being considered or in this case the criminal attack against other systems (Richards, 1999; Wright, 2011).
The attacker could then choose to attack a less well secured system, change their strategy or engage in non-criminal activities that produce higher returns given the time and capital investment required (Parameswaran, Rui, & Sayin, 2010). Generally speaking the Internet provides widespread opportunities to attack multiple systems with multiple vulnerabilities. In the event that the attacker is unable to attack one system economically the research and reconnaissance phases of the attack would generally be treated as lost opportunity costs as the attacker moves on to other more vulnerable targets.

THE COSTS OF DEFENDING RESOURCES

Once a system has been acquired it needs to be defended and exploited by the cyber-criminal (Li, et al., 2009). If the cyber-criminal fails to adequately take advantage of the target system (this is on average makes a profit per system compromised) they will make a loss and become less likely to attack further systems at a later point (this is shown in Figure 4 at points where the costs exceed the derived benefits.).
Any system that is not adequately defended by the attacker will eventually become a lost resource. This can be modelled as a Poisson decay function with a number of hosts held by an attacker diminishes over time. The attacker needs to actively maintain access to the compromised hosts or will in time lose access. Eventually as systems are upgraded or decommissioned by the owners the attacker will inevitably lose access.

Foraging & conflicting demands

Behaviour of cyber-criminals may be influenced by need to maintain access to compromised systems, scan for new systems, defend territories (both from system owners who will remove the criminal if detected and from predatory criminals seeking to infiltrate and take over existing botnets), defend C&C servers, and so on. While cybercriminals scan systems, the existing compromised and controlled systems are vulnerable to intruders & predators (e.g., other cybercriminals or the organisation's security personal attempting to recover the compromised site and system). The result is displayed in Figure 5.

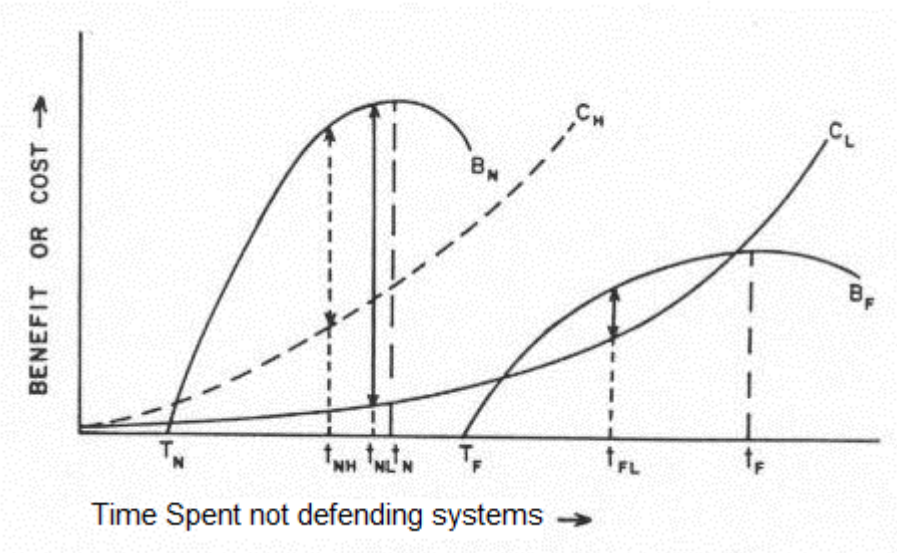

Figure 5 Defence of existing systems limits the recruitment of new compromised hosts

The terms used in the model (Figure 5) are:

- **N** & **F** = 2 sets of systems identical except for distance (Pheh, 2008) from the attacker in accessibility (N = near & F = far). A near system would be open to direct access. A far system would require access via alternate paths (such as through the use of a pivot or proxy). More low value systems (e.g. home user systems) will be considered "near" than high value corporate systems (which are more likely to be behind a firewall and other security controls).
- $\mathbf{T_N}$ & $\mathbf{T_F}$ = Scan and attack times
- $\mathbf{B_N}$ & $\mathbf{B_F}$ = benefit curves (proportional to rate at which the cybercriminal recovers costs on attacking a system)
- $\mathbf{C_H}$ & $\mathbf{C_L}$ = cost functions (proportional to probability that a successful attack on the existing compromised system occurs)
- $\mathbf{t_N}$ & $\mathbf{t_F}$ = foraging (scanning and system recruitment) times that optimize delivery rate
- $\mathbf{t_{NL}}$ & $\mathbf{t_{FL}}$= foraging times that maximize net benefit (survival of newly recruited systems into the existing network of compromised hosts) at low 'attack' rate ('far' patch affected more than 'near' patch. Here systems "deeper" inside network defences are lost first)
- $\mathbf{t_{NH}}$ = optimal time in near patch at high attack rate (far patch no longer confers positive net benefit)

Here, it can be seen that the need for system defence alters foraging behaviour. As more time is required to maintain access to high value systems (defence), less time is available to recruit more systems. We can say that investments in protecting compromised resources lower the amount of capital and time that can be used to scan for and compromise (recruit) more systems. Where an increased risk of predation impacts the market, we see the defending forager acting in a manner to defend systems "closer" to the C & C (Krogoth, 2008).
To maintain a large botnet, the exploitation of systems should be conducted faster taking valuable data in smaller loads (Kim, Lee, In, & Jeong, 2009). If the defence of the system is a goal (the value of each system is sufficient to warrant additional defence) the number of systems in the botnet will decrease due to cost pressure on maintaining the existing systems.
In order to defend the held resource territory the criminal attacker needs to maintain access to the compromised host and cover their tracks to avoid detection. There are several activities including the installation of root kits and the deletion of logs that aid the attacker in this goal.
The botnet Herder needs to be able to maintain access and control the systems they seek to take advantage of. Even with automation this takes time and resources. Each C & C (command-and-control) server can maintain limited number of compromised hosts (Pau, 2010). The process of issuing commands, updating systems and maintaining access requires an expenditure of time and effort. Each additional system added to a botnet increases the complexity and room for error or detection. Hence the larger the botnet size being maintained the greater the cost of maintenance.
In the case of high-value systems where compromised machines may be manually attacked and rigorously maintained by the cyber-criminal, the costs of maintaining additional hosts can become prohibitive quickly.

All systems contain unknown vulnerabilities that can be exploited by hostile parties. Already compromised systems can be attacked and subsequently compromised again by other attackers who act as predatory forces against other criminal groups. The difficulty in maintaining access to a compromised host increases when other attackers gain access to vulnerabilities and exploits that are unknown and undefended by both the system owner and any criminal who has already compromised the system.

THE BENEFITS OF A RESOURCE

The benefits obtained in running a set of compromised hosts will vary based on the strategy of the cyber-criminal. Some of these strategies include:

6. SPAM servers,
7. DDoS attack platforms,
8. Bitcoin currency mining,
9. Bot-For-Rent Platforms, and
10. Data exfiltration.

The economic viability of each of these platforms varies from large collections of low-value hosts (such as collections of home user machines and anonymous systems) through to targeted high-value platforms (including government and defence systems that may contain classified material). The advantages of a particular model will vary based on the ability of the attacker to maintain that system once it has been acquired.
Criminal territories can be modelled as different ecosystems. These ecosystems vary depending on resource density with the more high-value resources facing far more competition for acquisition from competing criminal elements. In order to be profitable low value systems can be seen to be components of low resource density ecosystems.

A MODEL OF TERRITORIAL CYBERCRIME

The process of actively defending a set of resources requires time and effort on the part of the attacker. The more valuable the system is, the more likely it will be attacked. This results in multiple attacks occurring against high-value targets. The result is active defence from the owner of the system coupled with increased competition from other criminal groups also seeking to exploit high-value resources. The necessity to defend territories (or those systems that have been compromised by the attacker) limits the attacker's ability to recruit (attack and compromise) other systems. It can thus be shown that the requirement to defend a system limits the size of the territory. As such, the more valuable a system is the more it will be attacked and hence the requirements for defence of existing systems will limit the attacker's ability to grow their territory.
Compromised systems can be lost from the criminal’s territory through combination of defensive strategies from the system owner and predation from competing criminal groups. Competing criminal groups may have differing strategies and reasons for obtaining a system. In some cases, the predation of criminals in taking over already compromised hosts can be an active strategy designed to reduce the risk associated with the attack. In compromising a system that is already maintained by another criminal group the predatory criminal can use the existing compromise to cover their own tracks. In this way the risk of their own detection and possible prosecution is minimized.
The necessity of defending a territory requires time and resources. This time taken in actively or passively defending the territory currently held is time that cannot be used to expand the territory further. As such, as activity defence can be shown to limit the access to new systems. The more time required to defend existing territory the less time there is to acquire new territory. For this reason there is an upper limit on the size of a territory that can be held with systems requiring a good deal of active maintenance necessitating more resources to defend the no systems that are not sought by many others.
The holding a system requires the exclusion of other parties. In doing this the attacker can more successfully and fully exploit a resource. Thus the ability to exclude competitors increases the returns available to the criminal holding the system. For the rational criminal (Wright, 2011), it is worth expending time and effort in these activities to the extent where the additional returns gained from holding the territory exceed the expenditure of time and energy is associated with the territorial behaviour.
In order to be defendable, a territory as comprised of compromised systems must necessarily return a greater net benefit to the attacker or other criminal party then would be available if a non-territorial approach was undertaken.
Where resource density and availability have been lowered through either increased criminal predation on hosts or through improved defence through the system owner, it becomes more likely that the criminal that has already obtained the territory will maintain access to that set of systems. In this instance defence becomes more likely as a strategy.

In these situations it becomes necessary to consider the resource renewal rate.
In cases where a high depletion rate is coupled with a low renewal rate it becomes more costly and hence less likely to defend a territory. That is as large a territories become economically more costly to defend, the size of criminal systems such as botnets will become smaller. A high depletion rate will come about when the attacker is unable to maintain access to existing systems and loses access to systems that have been compromised. A low renewal rate will come about when systems are more difficult to acquire. In this case the cost of compromising a system exceeds the amount of time and resources available to the attacker. An attacker with no zero day exploits and whose current arsenal of attacks are becoming less likely to result in compromising a system successfully will not be able to maintain and renew those systems in their territory.
Where a high depletion rate is coupled with a high renewal rate, the territory may still be economically defensible. In this instance the territory is likely to come to equilibrium in size at a point where the depletion rate of losing systems and renewal rate of recruiting new systems into the botnet approximately equal one another.
Hypothesis 1 - Criminal groups adjust the territory size to the density of the critical resources (such as access to systems, bandwidth or data) such that the resulting territory contains sufficient benefits to offset the costs of obtaining and maintaining the component systems.
Our first hypothesis can be demonstrated in the variation in botnet sizes and has been modelled by Bensoussan et. al (2010)
Hypothesis 2 - Variation in territory size occurs because more competitors are attracted to networks that are rich in resources, and such areas are, therefore, more costly to defend per unit host.
Although intuitive, preliminary investigations [such as those reported by Kaspersky (Kaspersky reveals price list for botnet attacks, 2009) and iDefense (Danchev, 2010)] support this thesis.

SUPERTERRITORIES

The notion of superterritories (Verner, 1977) can be used in modelling criminal behaviour in the creation of large-scale botnets.
In this the notion of selection can be used to compare the fitness of a particular criminal strategy. The use of various types of malware can be seen as competing against one another as separate criminal groups vie for resources. In ecology, selection acts on an individual's performance relative to that of all others. When used in the context of competing criminal groups, individual criminals form either predatory or parasitic strategies against the host they seek to compromise as well as other criminal groups. An individual criminal group can enhance overall fitness either by improving their own absolute performance all through reducing the effectiveness of other criminal groups.
One strategy that can be used to reduce the fitness of competing criminal groups comes from the difficulties seen in maintaining a superterritory. The maintenance of such a territory consisting of botnets of greater than 1 million compromised hosts reduces the fitness of other attackers. In maintaining such a large territory and the incumbent criminal restricts access to vital resources and increases the cost of acquisition to other criminal actors (Pau, 2010). This increase in acquisition cost becomes a barrier to entry for new criminal groups. The fitness of those criminals that defend superterritories is only increased where it is still possible to gain profit whilst holding such a territory. The majority use of such territories would be in high-volume low value transactions such as SPAM.

CONCLUSION

The overall size of criminal territory results from a compromise between the following factors:

- Acquisition needs,
- Resource maintenance needs,
- Defence costs,
- Predation pressure.

Each of these factors comes with an economic cost. Increasing any of those costs results in reduced benefits to the criminal organization and hence the reduced crime. Modelling the economic costs of cybercrime allows for the better allocation of resources designed to minimize loss. In making a system more difficult to attack in the first instance, increasing the cost of maintaining access to a compromised system or reducing the amount of time that an attacker can hold access to a compromise system it becomes possible to increase the cost to the attacker. Additionally we see that predation from both territorial a non-territorial criminals increases the cost associated with cybercrime. For this reason high resource density targets become more expensive to acquire and maintain leading to smaller territory sizes associated with this criminal strategy. Conversely, low value targets that are likely to be resource poor are more likely to formulate parts of a larger botnet territory.

REFERENCES

Bensoussan, A., Kantarcioglu, M., & Hoe, S. (2010). *A game-theoretical approach for finding optimal strategies in a botnet defense model*. Paper presented at the Proceedings of the First international conference on Decision and game theory for security, Berlin, Germany.

Clarke, R., & Cornish, D. (Eds.). (1985). *Modelling offender's decisions: A framework for research and policy*: Chicago: University of Chicago Press.

Danchev, D. (2010). Study finds the average price for renting a botnet. *Zero Day* Retrieved 10 Aug 2012, from http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528

. Kaspersky reveals price list for botnet attacks. (2009), from http://www.computerweekly.com/news/1280090242/Kaspersky-reveals-price-list-for-botnet-attacks

Kim, D.-H., Lee, T., In, H. P., & Jeong, H.-C. (2009). *Bonet Damage Propagation Estimation Model*. Paper presented at the KSII The first International Conference on Internet (ICONI) http://embedded.korea.ac.kr/esel/paper/international/2009/1200910.pdf

Krogoth. (2008). *Botnet constuction, control and concealment.* MSc. Retrieved from https://www.botnets.fr/index.php/Botnet_construction,_control_and_concealment

Li, Z., Liao, Q., & Striegel, A. (2009). Botnet Economics: Uncertainty Matters *Managing Information Risk and the Economics of Security* (pp. 245-267): Springer US.

Lin, J.-C., Chen, J.-M., Chen, C.-C., & Chien, Y.-S. (2009). *A Game Theoretic Approach to Decision and Analysis in Strategies of Attack and Defense*. Paper presented at the Proceedings of the 2009 Third IEEE International Conference on Secure Software Integration and Reliability Improvement.

Parameswaran, M., Rui, H., & Sayin, S. (2010). *A game theoretic model and empirical analysis of spammer strategies.* Paper presented at the CEAS 2010: Collaboration, Electronic messaging, Anti-Abuse and Spam Conference.

Pau, L.-F. (2010). Botnet economics and devising defence schemes from attackers' own reward processes: University Library of Munich, Germany.

Pheh. (2008). *RBN As a Business Network - Clarifying the guesswork of Criminal Activity*. The ShadowServer Foundation.

Richards, J. R. (1999). *Transnational Criminal Organizations, Cybercrime, and Money Laundering*. Boca Raton, Florida: CRC Press LLC.

Verner, J. (1977). On the adaptive significance of territoriality. *American Nature, 111*, 769-775.

Wright, C. S. (2011). *Criminal Specialization as a corollary of Rational Choice.* Paper presented at the ICBIFE, HK, China.