Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The Botnets have come – The Botnets have come...

In 2000, my 2nd Millennium article was titled: "*The Bots are Coming!!! The Bots are Coming!!!*"

Well... they have now arrived! Here's a short quote – then I will get into the current situation:

> *Since this is the millennium article, I thought it would be a good time to look into the future and the past and to consider the big picture. In my view, the emerging 'bots' and the remainder of the automated intelligence function as it is developing represents the killer application of the Web that will transform the society and information technology once again.*

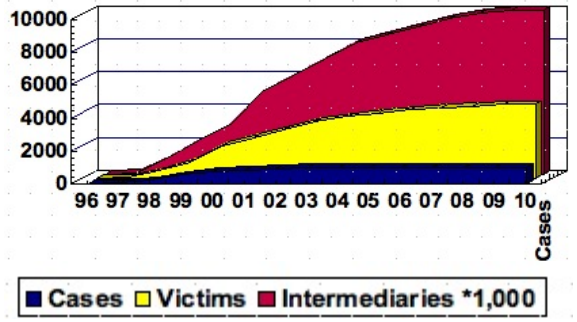

Figure 1: 1996 prediction: the future of DCAs

In 1996, I wrote another piece called: "*A Note on Distributed Coordinated Attacks*" which discussed the likely future of distributed coordinated attacks (DCAs). Somewhere in the Computer Security Institute presentation of this material, I provided the predictive graph shown in Figure 1. According to this prediction, by 2008, there would be about 400 botnets carrying out DCAs, they would be attacking about 4,000 targets per year, and there would be about 1 million intermediaries (bots) in the largest networks.

Well, this shows just how wrong I can be 12 years later. Unfortunately for me, I predicted that the curve would level out as the number of infected machines reached a level where they would be readily noticed and enough of a nuisance to cause a serious threat to network stability, become a potential information warfare weapon, and get into a high enough value level to warrant somebody in law enforcement going after the perpetrators. Foolish me. As it turns out, the largest known botnet today has something on the order of 10 million computers under control, is widely known, and yet the technical people who know what's going on don't seem to be able to get the resources or attention required to get the perpetrator in the sights of law enforcement or national security officials. There number of substantial botnets is in the order of hundreds, perhaps thousands if you get to a small enough sized network, but the number of victims, depending on what you call victims, is very large indeed. According to the folks who appear to know, just one of the botnet users sells various retail products via email and sends out billions of unsolicited commercial emails per year through an ever changing array of slave computers. They produce gross sales on the order of at least $150M/year.

It seems that botnets have become somewhat of a commercial boon to their users and to many of those whose resources they involve. For example, to rent a spam site at a high volume location within a botnet, the sellers charge on the order of $500 to $1500 per month. This is far more than a legitimate renter of the same space would pay, presumably because of

the extra costs and inconvenience of renting the space to criminals and having to resist all attempts to investigate and defend against law suits. But apparently it is worth it because these sites have continued to operate for years at the same location within the United States and elsewhere.

The effects of these networks are very widespread indeed. As an example, the people who rent these networks for sending unsolicited bulk commercial email, often in violation of laws other than just the breaking into computers associated with the creation and exploitation of botnets, sometimes get involved in contracts with legitimate businesses that wreck havoc over a longer time frames while extracting additional income from the process. Two examples of this are the sale of leads and click fraud.

In the case of click fraud, advertisers who pay for advertisements on sites like google pay based on the number of “clicks” on their advertisements. By generating large numbers of apparently clicks from different locations, the owners of the botnets are able to simulate high volumes of traffic, thus inducing large fees to advertisement service providers while not gaining the commercial benefit of real users looking at their advertisements or visiting their sites. An advertising agency reselling services might hire a click fraud producer to generate clicks so they can charge fees to their customers. In the Internet age, the advertising agency might be hiring a company that has many independent contractors carrying out many of these activities for them and be completely unaware of the fraudulent nature of what is going on.

In the case of sales leads, which is the more general version of the click-fraud example, companies pay contractors to generate sales leads for them by Internet advertising. This includes banner advertisements, placement in search engines, electronic mail, direct contracts with other providers of related services, and so forth. In the advertising business, leads are the most valuable pieces of intellectual property out there. For a good lead on a substantial valued item, advertising agencies will pay on the order of $50 or more. For example, in a car sale, the profits could be in the thousands of dollars per sale, and for a home mortgage, it could be far higher. As part of the deal, they require exclusivity, with the idea that they can sell these leads to the companies that sell the products or services for a substantial profit, perhaps $10 per lead, maybe even more. But before a company will pay $50 or more for a single sales lead, the lead needs to be qualified and offer a good change of closing a deal. Some of the criminals who take advantage of these advertisers do so by using botnets to deliver their messages, but instead of sending their leads to only one advertiser, sell them to many, turning a $25/lead commission into several times that much. When an effort is made to pursue them, they basically disappear into the ether of the Internet and find other customers, or come back under another alias. In some cases they may support many simultaneous aliases selling the same leads to the same businesses many times, depending on the safeguards in place.

I should also mention that the botnet business has become increasingly horizontal. As criminal enterprises go, they have become very big businesses and, like any other big business, they have specialized. Different individuals and groups now operate in different parts of the botnet space exploitation space. There are those who generate the malicious code that breaks into systems, those who compile this along with control and exploitation software into packaged mechanisms and maintain and update those packages over time,

those who launch these mechanisms to attack systems, and create the botnets themselves (the so-called operators), those who sell time on botnets, and who are sometimes not the botnet operators, and those who purchase capabilities of botnets directly from the operators or sales forces. While there are still a few vertical operators who do the whole set of functions, these have been largely eliminated by the commercialization of the industry. This is because different people have different skills, and teams of criminals, I suspect, tend to have a hard time fusing together because of the limited trust they tend to have for each other at larger sizes.

Technical solutions to large botnets are not that hard to come up with, but it turns out that technology is not getting the job done. The technologists are able to track control channels between bots and eventually are able to decode all of the controls being sent. The masters of these networks evolve the networks over time and improve them, making it more and more challenging, but the defenders are able to see what's going on and counter it. The problem is that the defenders are not allowed to do what they are able to do. They cannot attack the botnet because it is not under their legitimate zone of control. They cannot cut off botnet computers because they don't have management permission. They cannot map out the whole network because they cannot get cooperation across ISPs, especially from the small and low priced ones that support botnets and refuse to answer support calls or coordinate defenses. As the defenders sit there not allowed to defend the networks of the world, the attackers continue to evolve, grow their networks, and learn how to do things better. As a result, the attackers are getting better and better and the defenders are having a harder and harder time dealing with them. And the defenders are starting to move toward vigilante behaviors.

Finally, there is the lack of real attention by law enforcement and government agencies, the seeming indifference or inability of Internet Service Providers, and the careless attitude of and unwillingness of enterprises to act against these criminal organizations.

- Law enforcement has limited resources and they are spent elsewhere, largely because their executive management doesn't understand that these are criminal enterprises of such magnitude or because there is no clear benefit to them in focussing significant resources on them. Law enforcement is also hand-strung because it takes so long to do the necessary formalities surrounding meeting legal mandates while the botnet masters move from place to place with ease and speed and go through many jurisdictions along the way. The chances of getting arrested for such crimes is indeed very small, as it always has been.
- Internet Service Providers are also in a bind. The botnets are largely exploiting the ISP's customers, who are, for the most part, innocent victims and generally have no idea of what is being done with their computers. The notion that an ISP who is getting, in some cases, as little as a few dollars a month per customer, will somehow educate their customers to a level of knowledge where they can defend their own systems, supply systems administration services to the customers, or shut down their customer connectivity pending mitigation seems hard to fathom. But even if this were something they could do, that would also mean that they might become legally responsible for any failure to do so, responsible for damage to their customers' systems, and no longer be common carriers and protected by common carrier law.

- Enterprises of all sizes are often, in my view, the most neglectful of botnet master victims, because they should have the knowledge and wherewithal to defend their systems and mitigate the issues, but they very often don't do anything about these sorts of problems. Generally, enterprises seek to minimize costs associated with information technology, tend to turn a blind eye on any systems issues that don't prevent them from doing business or significantly damage their customer reputation. Most CIOs I have encountered give lip service to security but spend almost nothing on it, and cut competent chief information security officers who get too pushy about removal os botnets and similar things from their computers. They will often choose the simplest momentary fix, such as blocking the most commonly used ports of these bots, rather than fixing the underlying problem, resulting in ongoing infestations of, in many cases, thousands of computers within their networks that are used to transit from place to place concealed and protected by the enterprise boundaries.

Cooperation is required to fight off substantial botnets. The botnet masters tend to operate across national boundaries, go through and involve many ISPs and enterprises, commit the financially damaging crimes indirectly based on what is gleaned from the botnets, have limited effect on each endpoint they exploit, and conceal themselves and their overall infrastructures, using multiple hops between locations to obfuscate their actual sources, embedding encryption in many of their control channels, and exploiting the least controlled regions of the Internet to make them harder to trace. But cooperation is also hard to get. ISPs are highly competitive, and while the larger and well known ones often ask and give cooperation in this area, some refuse to talk to other ISPs, don't cooperate or have significant technical capabilities or knowledge, and don't see benefit in helping others. Some ISPs are, in essence, part of the criminal enterprises, while other vendors make most of their money from high volume low cost sales of throw-away items that are of use to the botnet operators. Some ISPs are operated by nation-states that may support the botnet masters either directly or through intentional inaction against them. Enterprises may cooperate, depending on who the chief information security officer is and their relationship with others, but if they spend substantial resources cooperating, they may get into internal trouble and be forced to stop. They have limits on what they can do because of regulations, contracts, policies, and so forth. Even if they have management support, very few have budgets that allow substantial cooperation. They may also believe that they risk retribution of the botnet master if they get too aggressive. Extortion based on denial of services, wiping out of computer system content, and other similar acts have been undertaken by botnet operators against systems when the botnets are threatened. When ISPs or enterprises send information to law enforcement, they often get no feedback because of investigative issues, and nothing may happen that is visible for months to years. The ISPs and enterprises cannot wait for years to act, so this also hinders cooperative efforts. So as a result, we are allowing global criminal enterprises to grow to billion dollar fraud, extortion, and theft groups, to perfect their methods of concealment and build up their criminal organizations and capabilities, and to do so with relative impunity.

Upcoming Events

April 7, 2008 - MiniMetriCon will be held near the RSA conference for the security metrics community to work on issues surrounding measurement of security. FCA is a sponsor and

Fred Cohen will be participating in the discussions.

April 11, 2008 – RSA conference – Fred Cohen will present “Improving Security Decisions“ to the management track. This will show how tools help executives better understand security-related decisions and how decisions can be clarified and justified to make business sense.