Diary of a Professional Botmaster

June 20, 2009

I've decided to restart the diary. I used to keep one many years ago, but stopped when I moved down to London and started my MSc in Computing & Security at King's College - much use that degree ever turned out to be!

I found out yesterday that me and most of the team are going to be made redundant at the end of the month. It appears that the company doesn't need so many developers after they decided to sell off the Private Banking division to some German brokerage and they ditched those annoying trader guys up on the 18th floor a couple of months back.

Anyhow, I'd better start looking for a new job. The markets pretty tight at the moment. It seems that all the banks are laying off folks and the developers are the first to go. Not surprising really. I've been thinking about setting up my own business for a while though. Perhaps it's time to bite the bullet and just do it. Take that redundancy cheque and invest it in myself?

June 22, 2009

Was down at the pub for most of the afternoon with Bill & Ted. We were tossing around ideas of businesses I could start - in particular, businesses that could make me a millionaire in a year's time. Granted, most of the ideas were completely off the wall and would be destined to fail or end in my bankruptcy within weeks of starting them (or would likely land me in prison within short order) but some of the grey areas look like they could be pretty exciting.

Ted was going on about botnets and how they're not really illegal. Sounds like rubbish to me, but I'll check it out anyway.

Last year when we had that worm go around the office and the Ops guys spent a couple of weeks chasing it down and cleaning up systems - that was pretty cool, and I can see how the authors of that worm could make quite a bit of money from it with a little banking knowledge. I don't think they ever got caught either. Ted told me that James - the lardy guy over in second-level helpdesk - said that they were still having outbreaks of that very same worm and uncovering other infected computers almost every day (after an entire year). How cool is that!

June 25, 2009

I've been reading up on botnets. The Internet is full of great information about them. YouTube even has tutorials on how to create the malware, deliver the bot agents, manage the Command and Control (CnC) and turn the stolen data into real money.

I did some digging on these hacker forums too. They're pretty cool. Most are well organized and there are bundles of tutorials, guides and discussion threads on all aspects of the botnet business. There's even entire forums dedicated to matching buyers with sellers - Craigslist style!

June 26, 2009

Had a great session with Demitri over IRC today. He's been running a handful of botnets over the last couple of years and seems to know what he's talking about. Came across his advertisement on one of the boards and was offering a free 2-hour test-drive of his botnet CnC console - so I got to play with a couple hundred computers. Some of the functionality was grayed out, but I got a chance to DDoS the companies' website - from the comfort of my desk ☺

I spoke with a couple of the company Internet ops guys afterwards - being careful in what I said of course - to see if they noticed. Apparently they did. It didn't bring down the site, but they were alerted from their IPS. Supposedly this is a common enough occurrence and happens most weeks. I guess I'm a little disappointed with that. I wonder how many bots I'd need to take down the webserver?

Dimitri said that he normally uses about 5,000 bots to take down big websites - but 200 is more than enough to wipe out corporate VPN appliances. Handy to know!

June 27, 2009

Sat down with Jim the lawyer this afternoon. I wanted to go over the details of setting up my own contracting business. Since I haven't had much luck on the replacement job front looking for permanent roles, I figured I'd just go down the contracting route - since there are more opportunities going for temporary software engineering positions.

There's not much to creating your own business. Jim helped me with all the forms - so I just need to mail them off tomorrow, and I'll be on the way to creating my first business. He also explained some of the nuances to setting up a company in some other countries and the possibilities of "offshore accounts" and tax havens. I took plenty of notes. You never know when that'll come in useful.

June 28, 2009

Spent all day harvesting hacker boards for tools and playing with them on a couple of old laptops. This stuff really is easy.

I even came across this guy(?) on one of the chat forums (who can't have been more than 14 years old) who was selling a botnet of 2,000 computers for $400. The funny part though was when the flame war stated about how overpriced that was. Apparently you can pick up 2,000 computers for as low as a $50 Walmart giftcard.

June 29, 2009

I woke up this morning with an epiphany (or was it just a delayed hangover?). I'm going to start my own botnet - but not just any botnet, I'm going to do it properly and make a business from it! I'll still pursue any legit consulting roles that crop up - still got to eat and pay the bills - but it'll make a convenient front while I'm building botnets.

Why the botnet business? Because it's cool! Well, actually, it's more than that. I don't want to work forever in a dull office job and, from what I can tell, botnet building seems to be pretty profitable - and not many people get caught. And, if they do get caught, they basically only get a slap on the wrist.

Having read quite a few of the news articles about the folks that got caught, it looks to me that they got caught because they did something stupid and/or they clearly crossed the criminal line - and the police were forced to do something about them.

I'm pretty sure that I'm smarter than that. Didn't any of these guys ever consider building a business plan first? Plan it all out - have a strategy and stick to it!

I've left the computer downloading a few tool collections I found on one of the Argentinean malware blog sites. 4Gb of tools, kits and exploits. Awesome! And it's all free!!

June 30, 2009

Final pay date from the "old job", and I'm now officially free of the company. Ended up with a little over £35k after taxes too - so that'll tide me over the next few months as I pull together my new business(es).

Last night's download worked out pretty good. There are hundreds of botnet kits in there - complete with CnC interfaces, exploit packs, phishing templates, malware creators and obfuscators. Supposedly there's a high likelihood that many of them are backdoored, but who cares - it's time to play! I'm going to try a couple of them out on the corporate laptop before I have to hand it back - preferably one with a good rootkit. I wonder if they'll ever notice?

July 1, 2009

Woke up this morning having dreamed about what kind of botnet business I want to build. Also figured out a few "rules" that I want to work towards - maybe more of a "guiding principles" perspective really.

1. DON'T GET CAUGHT - which means I'm going to be damned careful in setting up everything and making sure that nothing can be traced back to me personally. Sure, there'll be layers to the onion, but I'm not going to allow myself to be let down by poor tradecraft and bad habits. Those hackers in France and Spain got caught because they didn't have enough layers of deniability and mixed the use of their personal systems and their botnet infrastructure.

2. DON'T DO CRIMINAL HARM - While I'm pretty far removed from planning on being a Robin Hood, I'm not going to get mixed in with the Mob or other organized crime. Similarly, I'm not going to get involved with any political or religious drivel. I also don't want to cause any physical harm - as that's a sure way of getting the interest of the police - and, besides, it's not who I really am. The more legit I can make this business, the easier it'll be to bow out after I've made my money.

3. RESILIENCE AND SCALABILITY ARE MY FRIENDS - Since this is going to be a business, based upon the lessons I learned from the Private Banking firm and all I've been reading over the last couple of weeks, it should be possible to build pretty big botnets really fast - if I plan it well.

Resilience will be even more important though. Getting back to the "don't get caught" principle and the layers of deniability (and abstraction), if I plan for making the CnC and distribution systems robust, I'll endeavor to split things over several hosting providers and geographic regions.

Also spent some time on the hacker portals and responding to some of the threads. Some of the more interesting forums are currently closed to me because I haven't developed a site reputation - which can be gained by posting 20, 50 and 100 messages. This'll be pretty easy though. Lots of questions about coding problems which I can answer without too much thought.

July 3, 2009

I think I've managed to plan out a few more CnC infrastructure ideas. I found a few more tutorials online - and also some good message threads on domain registration tactics, Dynamic DNS operators and folks that'll distribute malware for a few cents. It appears that a good rate at the moment is around $100 for 2,000 guaranteed installs. A little pricey if I was buying, but it sounds like good money if I was to become a seller ☺

I also realized that I forgot a rather important principle for inclusion - my zero'th principle…

0. I WANT TO BE RICH - but, more to the point I want to retire rich, not be the richest bloke in jail.

Which all means that I need to do some more investigation on how to secure the money. I don't want the money to be directly traceable to me - nor to the consulting company I've just created - but I'm going to need ways to pay for stuff and ways to accept payments. All deniable of course.

Made a few new connections on the hacker forums. Now that I'm posting to some threads I'm getting direct messages from some of the folks there. A couple of the guys that reached out were trying to pimp out their services - both of them malware dropper services. Someone else asked if I was with the FBI.

The USA perspective was interesting. I hadn't realized that the guys on the forums can see/track my IP address and from there work out where I'm located. I'll have to do some experimenting with anonymous proxies and TOR networks. I ran across a few video tutorials on the topic yesterday. That'll be my homework for this evening - getting something setup and hiding my IP address forever more…

July 4, 2009

Surprise in the snail mail - company papers just came back. I'm now the CEO of Thrull Networks! Cool company name huh! I wonder if anyone will ever figure it out - thought it was apt at the time. Maybe it's a little too close to the mark. 5% on the dumbness scale I guess. Will have to be smarter in the future. I'm going to keep it though. Even saw that some related .com and .net domain names are available for registering.

Earlier this morning I went out and bought a couple of new laptops. Nothing special, just some small(ish) $800 laptops that I'm dedicating to my botnet business - and will never taint them with the Thrull Networks consulting business. Although I will be claiming them as tax deductable expenditures.

Also spent most of today coming up with the rules I'm going to work under for achieving principles (1) and (3)... and maybe a little of (0) too.

So, the new rules...

A) Separate systems for work/pleasure/personal and botnets. The two new laptops are JUST for the botnet business. I've already installed a full disk encryption scheme and come up with a 44 character password. I doubt that anyone'll be breaking that mother anytime soon.

B) Never connect to the botnet CnC or do any botnet-related business from my home network. Given the general availability of free WiFi at Starbucks and McDonald, etc., I'll use those. A couple of additional rules there though - don't frequent them in a regular pattern (sounds like a Tom Clancy spy novel), and don't use stores that have CCTV setups. I was tempted to use some of the unsecured WiFi networks in the neighborhood - but that may be a little too close for comfort. Besides, the coffee will be better than what I have at home.

C) Change the MAC on the laptops regularly. I've already downloaded and installed a cool piece of software that does precisely that. I've also installed a bundle of different Web browsers - but have deliberately not installed any plug-ins etc. I was reading recently a couple of online projects that showed how they could query your Web browser through JavaScript and the DOM to build a signature of the browser - and how "unique" that became once you started installing plug-ins and how regularly you kept them patched. So I'm planning on keeping the laptops as simple and "dumb" as possible.

D) Never connect directly to the botnet infrastructure. Lesson learned yesterday. TOR and anonymous proxies are now default on all my computers - especially the two new laptops!

E) While encryption is my friend. Asymmetric crypto is going to be my live-in lover. Thanks Bruce for the tips!

July 9, 2009

Been playing around all week with the DIY kits I downloaded a couple of weeks back. The Zeus kit is pretty impressive with its polymorphic malware generator. I was running its output past some of the free online antivirus scanning portals and noting which (if any) antivirus tools detected the samples. On average, only a couple of the AV tools detected anything - and if they did, it was only some kind of generic signature such as w32.suspicious etc.

I was originally using www.virustotal.com, but when I tried to find other AV portals that might have more AV products in them I stumbled over a couple of cool threads that explained why I shouldn't use that site (and a few others) because they share the malware samples with the AV vendors. Therefore the AV vendors will have detection signatures for the malware out within a few days. That sucks - because I probably just wasted a few dozen cool pieces of Zeus malware. Luckily there were plenty of alternative AV testing portals being recommended and (yet more) tutorials on how to set up your own malware QA testing regimes.

I've settled on www.virtest.com now. They charge a few dollars for the privilege of testing the malware I submit, but they allow me to upload multiple malware samples simultaneously in bulk format. They also have some other services for checking out the malware delivery websites too - so you can check to see if the exploit packs used by the Zeus kit (and others) are correctly installed and whether the other AV components (e.g. HIPS) detect the infection. Their VIP account is $50 per month. I'll have to figure out a good way to pay for the service. Something that can't be traced back to me personally…

July 10, 2009

I spent the entire morning down at the Starbucks down by the park using their "free" WiFi. Cost me about $26 in coffee for the 4 hours.

*Anyway, I set up a handful of free webmail accounts. A couple of Gmail accounts, a couple of Hotmail accounts and a couple of Yahoo accounts. I entered in garbage "personal" information, but gave them all the same password - "Lucky4Me*Unlucky4U". They're disposable accounts for trialing out a few new concepts and learning what works.*

Next, I created a couple of websites to host the Zeus CnC console pages. I had originally been worried about how I was going to have to pay for the web hosting - but a quick search for "free web hosting" revealed plenty of services - including portals that provide detailed reviews of all the providers. Woohoo.

It took me about an hour to create the sites on 0000free.com. It's the first website I've ever built - and I had to learn some PHP while doing it all. On the job training if you like. The index page is just a copy/paste job from some car-parts website - and the Zeus CnC configuration and bot registration pages are off in a subfolder. They're accessible if you know the URL, but they're intentionally not linked to from anywhere. I don't really want some search engine crawling the sites and flagging the Zeus CnC.

I'll be spending some time later tonight generating some malware samples that'll use the two new CnC URLs. That'll be hard work - should take me all of 10 seconds ☺

July 11, 2009

A botnet is born. I'm a father!

So, this morning I headed off to the Starbucks over by the athletics center to play with my newly minted malware and the CnC services.

I originally set up a VMWare session on the laptop and infected it with the new malware bot agent and watched it reach out to the CnC server. Meanwhile I browsed to the website, logged in to the CnC console, and saw the test victim register itself - so I spent a good half hour testing out all the features of the bot agent. It's pretty slick. Ugly, but slick. The toughest part of all this was setting up the TOR agent to provide the anonymous web access in reaching the CnC console.

To get the bot malware into play I decided to upload the samples to the Newsgroups - since they don't require me to host the files directly and also provide anonymous *uploading. One file I named "Windows7KeygenCrack.exe" and the other "iTunesDRMRemover.exe", and included some BS text about how good the tools are. They were both uploaded to a handful of different alt.binaries. groups using different email accounts and source IP addresses.*

I hung around Starbuck for another hour, but didn't see any victims appear on the Zeus console - so paid a visit to Bill & Ted and grabbed lunch with them in town. Ted's already gotten a new job at some Scottish bank. Chose not to tell them about my botnet research. The ideas may have come from them originally, but I'm not about to share this secret.

Anyhow, I popped in to the McDonalds by the railway station at about 4pm and connected to the Internet to see how my "botnet" was coming along. Surprise, surprise, I had three new members to my botnet. How cool is that! I was well chuffed with that small success and subsequently spent an entire hour connecting to each computer and checking out what I could access on their systems. Just as I was about to pack things up and head off home a fourth computer joined my botnet.

I couldn't stop smiling on my way home from McDonalds. I think I may have even said "I've just fathered my first botnet" somewhere on the walk up the hill. Haha.

Guess where I'll be tomorrow morning…

July 12, 2009

Got to Starbucks early this morning and was online with my baby botnet by at least 9:30am. It had swollen over night and the counter had reached 18 computers - but I could only contact 6 of them. The others must have been turned off or something.

For the next hour (and second cup of Java) I created a couple dozen new malware bot agents and configured them to point to the same two Zeus CnC servers I'd set up yesterday. I then went on to use the same Newsgroup tactics - but picking a few other juicy social engineering file names (and descriptions) - e.g. "AcrobatProfessionalKeygen.exe", "RossettaStoneLanguagePackUnlocker.exe", etc.

By the time I left the coffee shop the botnet had grown to 23 computers - mostly in the US and the Netherlands, but a couple from Australia and Taiwan.

Went home afterwards to do some more studying and recon, and found some good information on how to automatically pull back account and identity information from Zeus malware clients. There are a number of scripts that you could run automatically on each botnet computer to extract their webmail credentials, anything they've told their IE or Firefox web browsers to remember, etc.

I also found some plug-ins for the Zeus CnC console that help to manage the data that comes back from the keylogger and other info-stealer components - which I installed on the web servers later on my return trip to Starbucks - and left CnC commands for the botnet malware to automatically start collecting and uploading the identity information.

By 7:30pm my botnet had reached 200 members. It's no longer a "family unit"; it's a small village and I'm Pastor of the flock.

July 14, 2009

Had a couple of contract interviews yesterday, and hadn't managed to check on how my baby was coming along for a couple of days. So, it was with a rather pleasant surprise I noted that the botnet had reached 3,320 computers.

Actually, I'm not so sure about the number and whether it's a good number to rely upon. The number of computers "active" were about 450 - and I tested that I could control them OK. As for the rest, well, they were "offline" - but I did have files from all 3,000+ computers sitting on the CnC server - so I guess they were successfully compromised with my botnet agent.

I moved all the files off the two CnC servers and copied them to the laptop. When I got home I started doing some analysis.

Brief stats (for posterity)...

942 Facebook accounts

766 Twitter accounts

322 Gmail accounts

318 Hotmail accounts

193 Yahoo accounts

76 Paypal accounts

... and lots of sub-50 accounts - many for services/websites I've never heard of before. All told, about 5,500 different accounts.

BTW I'm not sure I like using Starbucks - I'm spending too much money on coffee there ☹

July 15, 2009

The botnet's now reached 4,000 computers.

There was an email from 0000free.com waiting for me from yesterday. Apparently I should be upgrading to a paid account because of all the traffic/hits the site has been receiving. Just as well I moved off all the identity information and files - I was almost over the file quota too!

July 16, 2009

4,300. What's the population have to be before a village can be called a town?

Created another couple of dozen malware for release on the Newsgroups since the botnet growth appeared to be slowing down.

July 17, 2009

I think I'm the Mayor of a small town now. I visited the Starbucks down by the strip mall this afternoon and logged in to the botnet. 11,435 computers!

At first I thought it may have been a mistake since the size jump was so large. Introducing a couple new malware downloads didn't get that much of a leap last time. But I figured it out after about 20 minutes of probing and searching. It would seem that the new file "MichaelJacksonDeath-OfficialAutopsyReport.exe" was more successful. It also managed to make its way on to some Torrent server and plenty of people are downloading it.

New lessons learnt from yesterday's efforts:

1) Tying social engineering to media and entertainment current events results yields more additions to a botnet.

2) Torrent networks can make the botnet malware reach more people faster.

July 18, 2009

Just as well I downloaded all those new files yesterday, because the botnet is dead. I'm no longer the Mayor.

This morning I popped on over at the Library for a bit of their WiFi access and tried to connect to my CnC servers. Nothing - well, more than nothing, the Zeus CnC pages had been deleted and my webserver account had been disabled. There were instructions to phone the helpdesk to discuss reactivation.

Waiting in the inbox of the webmail account I used to register the free websites was an email telling me that my site may have been hacked and was being used for malicious purposes.

A quick Google revealed that both CnC URL's and configuration files were listed up on ZeusTracker.abuse.ch.

Bugger!

July 19, 2009

All is not lost. I've still got all those identity/account detail files from all my botnet computers. The total - adding the first batch with the batch from the 17th - comes to a little shy of 19,000 unique sets of credentials. I can still access any (if not all) of those stolen accounts anytime in the future.

Better yet - there's absolutely nothing that can be tracked back to me. Sure, the botnet is now out of my control (and computers are still being compromised with the malware which is still in circulation in the Newsgroups and Torrents), but I'm safe and have learnt a few new lessons.

That said though, it's about time I started to focus on bringing in the money from the botnets. I'm not going to get that Porsche building botnets for botnets sake. I could easily enough find buyers for the stolen information - the hacker forums are overflowing with buyers and agents. That’s not a problem. The problem lies in converting "Internet money" into cash - and laundering those transactions sufficiently.

With that in mind, I spent all afternoon researching offshore banking and the creation of anonymous accounts. Disappointingly those infamous Swiss Numbered Accounts don't exist anymore - at least not like they do in the movies.

I managed to narrow it down to three banking accounts and, as my finances grow, I'll start to bring them on line. I've found agents that will allow me to set up Swiss banking accounts online. They require proof of address, but they provide a level of guarantee that personal information will not be supplied to anyone outside of Switzerland. The Cayman Island accounts are easier to set up - and don't require an agent - but require a higher deposit. They're a little too rich for my tastes at the moment - but I'll probably add an account once I break the $100k per month revenue stream (if ever?).

No, the account I created online this evening was for a Panama Bearer Share Corporation account. As of an hour ago I'm now CEO of a second company - "Net Wizards LLC.". I deposited $5,000 into the account. Not only does it provide an anonymous business front and full international banking facilities, but it comes with 4% interest and the credit cards issued against the account should be arriving in 10 days time.

July 20, 2009

I'm back in the botnet business!

I was keeping a couple of my hacker forum accounts live by responding to a few message threads and I stumbled across a couple of reputable botmasters that were in the process of selling off sections of their botnets. They were offering batches of 100 bots with dedicated CnC hosted servers for $200 each.

Most significantly though - there were alternatives to the $200 in Webmoney or PayPal funds - they'd accept hacked webmail accounts, Facebook accounts and Twitter accounts.

After a little back and forth, we agreed on the trade and exchange mode (had to use an agent that was pre-vetted on the forum - one of the administrators - who charges 10% for his time/effort). From X4cker I picked up 600 bots and two CnC servers (in the Ukraine no less) for 3,000 Gmail accounts and 1,000 Hotmail accounts. From Dankar007 I managed to procure 500 bots for the princely sum of 500 PayPal accounts. The site administrator/agent didn't do too badly out of the deal either. I'm sure that he (or she?) now has his own copies of all those accounts.

After some quick verification and having tested the access to the two botnets, I created a new Zeus botnet agent and pushed it down to all 1,100 bots - and changed the admin credentials on the CnC servers.

Not only am I back in "business" with a brand new botnet, but I've still got all those account details from the previous botnet that I can continue trading/reselling to other operators.

-- I just realized that this diary is now precisely one month old. In that month I lost my job, founded two companies, become a CEO, built a botnet, lost a botnet, established a reputation in the hacker communities, opened an international banking account, and just purchased my second botnet.

Time to start pulling together the business plan for constructing a profitable money-making botnet! The "march to a million" sounds like a great idea, but I'd prefer to aim for Steve Austin's The Six Million Dollar Man. I'm pretty confident that I can reach that target over the next 11 months! What would mom say?

Note: This is a fictitious (and subtly macabre, but hopefully humorous) diary account loosely based upon real investigations of professional botnet operators and the criminal enterprises they created to monetize the data and systems under their control. It does not represent a single botnet operator, rather it represents a concatenation of notable business models, decisions and discussions from a spectrum of criminal operators. Names and places have been deliberately altered. No animals were harmed in the making of this diary.