BOTNETS

Have a plan to steal millions from banks and their customers but can’t write a line of code? Want to get rich quick off advertising click fraud but “quick” doesn’t include time to learn how to do it? No problem. Everything you need to start a life of cybercrime is just a few clicks (and many more dollars) away.

Building successful malware is an expensive business. It involves putting together teams of developers, coordinating an army of fraudsters to convert ill-gotten gains to hard currency without pointing a digital arrow right back to you. So the biggest names in financial botnets—Zeus, Carberp, Citadel, and SpyEye, to name a few—have all at one point or another decided to shift gears from fraud rings to crimeware vendors, selling their wares to whoever can afford them.

In the process, these big botnet platforms have created a whole ecosystem of software and services in an underground market catering to criminals without the skills to build it themselves. As a result, the tools and techniques used by last years’ big professional bank fraud operations, such as the “Operation High Roller” botnet that netted over $70 million last summer, are available off-the-shelf on the Internet. They even come with full technical support to help you get up and running.

The customers of these services often plan more for the short term than the long game played by the big cyber-crime rings. They have very different goals. Botnet infrastructures can be applied in lots of ways for different sorts of profit—cash, information, or political gain. There are many ways to make money off botnets beyond outright theft, such as using them to steal advertising clicks, generate spam e-mails for a paying client, or renting out bots for denial-of-service attacks. And the same basic principles used to distribute botnets have been creeping up in more targeted attacks to steal intellectual property or to spread the malware used in the recent “wiper” attack on South Korean banks and broadcasters.

So how easy is it to get into the botnet business? Well, Ars decided to find out. Given the surprising availability of botnet building blocks online, I set out to build a shopping list to understand how everything is bought and sold within this black market. It all started with checking sources through a few Web searches then making trips into Web forums I dared visit only with a virtual machine and Google Translator’s help. All I had to do was paste in “botnet” in Cyrillic, and I was on my way down the rabbit hole.

To assemble your list for some of the simplest get-rich-quick schemes, all you need is about $600, a little spare time, and no compunctions about breaking laws to make a profit. I didn’t deploy an Ars-enal of botnet destruction in the end, but I absolutely could have. That may be the scariest lesson here.
It looks like you’re trying to build a botnet…

There are no personal shoppers to help walk you through the underground marketplaces to identify what fits a particular criminal scheme—though there may be plenty of people willing to give you paid advice on how to get started. With absolutely no budget for bitcoins, I got my start with some help from Max Goncharov, a security researcher for Trend Micro who specializes in following the Russian underground marketplaces for online fraud services. Goncharov came to Washington, DC in late March for a Trend Micro press briefing, and he laid out some of the basic things that go into a beginner fraudster’s software and services shopping cart: botnets, malware-spreading tools, and hacking for hire. (Goncharov detailed some of these services in a paper published late last year and presented during this press road show.) Goncharov’s suggested setup came with a $595 price tag for the first month of operations and a monthly cost of $225 to sustain the operation.

Of course, that price is for a particular type of botnet. It isn’t representative of everything that’s running wild on the Internet today. It also assumes total noob-hood. For those seeking to do something a little less overtly criminal than stealing credit card numbers or committing wire fraud, there are less expensive options. With a little sweat equity, you can pull off a workable botnet for a fraction of that price. If you’re willing to try it without the benefits that come from paying professionals—like software updates, monitoring services, and 24/7 technical support—you can cut the cost back even further.

With my rough estimate in place, it was time to actually start some research of my own. Hello overseas VPN connection, Google Translator, and Google.ru—time for the underground hacker marketplace.

The marketplace of (bad) ideas

The “underground” forums do more than just give would-be criminals access to a level of service that might make some enterprise software companies look bad. They also act as a sort of hiring hall for people with very specific skills (like hacking webmail accounts) or botnets of their own ready to do a paying customer’s bidding. On these barely underground sites, hacker wares are made available to anyone willing to pay. Current versions of Zeus and SpyEye botnet software are for sale, or you can find the last version cracked by someone for cheap or free.

Many of the sites run under the thin veneer of “security” discussion boards. But they’re often paid for by advertisements for the tools sought by a certain class of cyber-criminal: botnet-herders and the service provider ecosystem that has sprung up around them. These are largely the small and medium businesses of cybercrime, following a well-worn approach to making money. If you cast a big enough net, you’re bound to catch some fish.

The botnet herders’ standard business plan is to “use exploit kits, and then run a phishing campaign or some sort of campaign against massive numbers of people with hopes that someone is going to click on a link and get the exploit to drop a botnet or banking trojan onto their machine,” said Nicholas J. Percoco, senior vice-president of Trustwave and head of the company’s SpiderLabs penetration testing and security research team. “Once they’ve done that, it goes down the path of them monitoring them when they do banking transactions, or the botnet may be involved in spam or distributed denial of service attacks. Or maybe it’s a sort of Swiss Army knife botnet that can do many different things depending on what that botnet herder decides, or what he makes it available to do for people who want to utilize his or her botnet.”

No matter what the racket, Percoco told Ars, the equation for botnet herders is the same. “From a criminal’s perspective, they’re looking at massive numbers of attacks to achieve their financial goals.”

They’re also looking at massive turnover. When a piece of malware like a botnet lands on thousands of PCs, “it may hit the radar of an antivirus company pretty quickly,” Percoco noted. That means time and money spent on finding new victims, deploying patches and updates, paying for new exploits, and generally continuing the game of “whack-a-mole” with antivirus companies and other organizations—as the mole.

Building a botnet shopping list

I did some additional research afterward to check Goncharov’s math, and I also looked at some alternative approaches. The underground software market for hacking, fraud, and botnet tools has matured to the point where developers provide most of what you’d expect from legitimate software and online service providers—maybe even more. There’s full support for the paid services, including 24/7 voice support in some cases, in a business where positive word of mouth in forums is the best (and often only) advertising. And there’s no shortage of “consultants” to help you get started.

Botnet software itself is an important part of the whole equation, but it’s only a fraction of first-month startup costs—and one that’s fungible if you’re willing to invest some of your own sweat equity in the setup (or dispense with the “legitimate” route and use a cracked version without software support). Just like any Internet business, launching a financial fraud botnet—or any kind of long-running botnet endeavor—requires a sustainable business plan. You need to know your target market, ensure distribution, keep your installed base a step ahead of the competition, and keep your business processes secure.

Here’s a typical botnet-herder’s startup shopping list:

A “bulletproof” VPN

Before you start building a bot army of incredible magnitude, you need—just as with any other hacking endeavor of questionable legality—to hide yourself from prying eyes. That means using some sort of tool to avoid monitoring by your ISP, law enforcement, and other cybercriminals. Generally speaking, the best way is a virtual private network.

As confessed LulzSec member Cody Kretsinger found out, not all VPN providers are created equal. He used a service called HideMyAss.com, a VPN and proxy service run by UK-based Privax Ltd. Unfortunately, he didn’t read the company’s privacy and legal policies, and they gave up his logs when law enforcement came knocking. “Bulletproof” VPN services are ones that claim to be shielded from law enforcement requests because of their location or logging practices. Many of these services have disclaimers about “abuse” of the services, but the fact is that they take a number of anonymous forms of payment (CryptoVPN, for example, accepts Liberty Reserve, Bitcoin, and a number of other similar anonymous payment services). At worst, these services may just cancel your account if it attracts too much trouble.

A typical “bulletproof” VPN service, such as CryptoVPN runs about $25 a month. If you’re thinking long-term, you can sign-up for $200 a year. However, it’s best not to think long-term if you’re botnet-herding; it may behoove you to change services every now and then to keep your profile low.

Budget Botnet Shopper’s Price: $25 / month.
A “bulletproof” host

Once you’ve got your network secured, you need some place to host your botnet’s command and control network and all of the other assorted badness needed to launch a massive assault on the unsuspecting world. For those without the skills, time, or desire to simply go hack someone else’s server every couple of weeks, that means buying a dedicated or virtual dedicated server from someone who doesn’t care what you’re doing—lest your botnet’s nerve center be wiped during a security sweep or seized by law enforcement.

There are many kinds of “bulletproof” hosts catering to various kinds of customers. Most of them buy space in data centers around the world in places with either weak data privacy laws or plain disregard for what other countries’ laws say. This provides a sort of insurance policy for their customers, Goncharov said. At a minimum, the data on the servers won’t be given up to law enforcement.

Some are smaller hosting companies such as Hostim VSE, a Romanian hosting company with a Russian language website more targeted at protecting pornographers, pirates, and other targets of DMCA takedown requests. Hostim VSE publicly denounces botnetters and financial fraudsters to prevent attention from local law enforcement. It describes “bulletproof hosting” as “hosting resistant to complaints and other types of attacks on competitors. When placed on a standard website hosting, your site can receive complaints from competitors under the guise of copyright holders. In consequence of this, most other hosting providers disable your site until the circumstances [change]. We also review all such complaints, check its validity, conduct a site audit, demand [the accuser] to produce documents confirming the rights, and otherwise deal with all to settle the conflict, and only then disable the client's site."

All of this, the company says with a wink, takes a lot of time and human resources, and as a small company there may be some delays before it gets around to it. In other words, "don't worry—we're inefficient." Hostim VSE's dedicated servers start at $39/month with additional charges for more bandwidth. The company also, ironically, provides DDoS protection and other support services. But prices for its services will rise dramatically if you're attracting too much attention or using too much bandwidth.

For really hard-core criminal undertakings, there are the more specialized underground "bulletproof" hosting services that are run specifically for malware owners. These offer hosting at a significant markup in exchange for looking the other way. These operations generally don't maintain webpages. They advertise strictly in underground forums and do business over ICQ, Jabber, and other instant messaging.

Mihai Ionut Paunescu, the 28-year old Romanian behind underground host powerhost.ro, was caught in December by Romanian authorities. His servers were home to the Gozi financial malware command and control network. Paunescu kept tabs on exactly what sort of business his users were up to and charged accordingly. In some cases, the rates reached thousands per month, averaging better than a 100-percent margin on the servers he managed.

Of course, many of these hosting companies provide support (in some cases, 24-hour voice support via phone or Skype) and help with configuring Apache and MySQL on dedicated hosts for customers who are generally clueless about such things.

Budget Botnet Shopper's Price: $50/month, plus spot "consulting."
Bulletproof domains and "fast flux"

In order for your bots to reach your host reliably, you need some domain names—fully qualified domain names that allow you to have full control over the domain name service (DNS). You'll want a bunch so you can avoid making yourself obvious in the DNS logs of networks that get infected.

You'll also want to register those domains with a registrar that's not going to roll on you and shut you down on the first complaint of abuse. You need someone who will shield your identity from the prying eyes of security firms and law enforcement. In other words, you want a bulletproof registrar. Preferably, it's one that accepts payments via Western Union or some other anonymous service.

Of course, it's never a bad idea to have some additional protection to make sure that you cover your trail completely by using a "fast flux" scheme. This hides your servers' true location by assigning the DNS addresses to a rapidly changing set of proxies. Fast flux providers will take your domains —or even register them for you—and then assign host names to a collection of their own bots. These in turn pass traffic between your bots and your server. By using a short "time to live" for the host "A" name records in the DNS server, fast flux systems create hundreds of potential communication paths for the bots.

Fast flux service is costly. An advertisement on one forum recently offered to support five DNS name servers for customers starting at $800. So for most starting botnet operations getting their feet wet, just registering a few domain names may be enough to begin with.

Budget Botnet Shopper's Price: $50 for five domains.
Your choice of botnet / C&C platform

The current editions of botnet-building frameworks are sometimes sold by their developers for premium prices. Carberp was sold by its developers prior to their recent arrest for a whopping $40,000 as a kit, while the current Zeus toolkit sold for about $400 when it first hit the market. But the market pays what the market can bear, and most first-timers can find less expensive options that are easier to sustain.

Do-it-yourselfers who don't care about things like patches and full support can find “cracked” versions of some of these toolkits (or ways to disable their licensing code) for free. There’s also an option to pick up older but still supported versions on the aftermarket. Zeus’ source code was released to the world last year, sort of turning it into “open source,” so you can now purchase supported versions of it for $125, plus $15 per month for updates to the code and $25 for monthly 24/7 new customer support. That could include everything from helping a noob fix a misconfigured server to doing a whole walkthrough of configuring the PHP scripts and MySQL backends for the system over Skype. You could always just use one of those YouTube guides, though, and save some money.

Budget Botnet Shopper’s Price: $125, plus $40/month for support.
Web attack “injector” kits

The Zeus botnet’s market dominance has created a whole additional ecosystem of software add-ons to make its bots do various things. A big part of that market is “injectors”—the add-on modules that tell the bot what to watch for in browser activity and what code to inject into the browser when it visits targeted websites.

There are financial botnet injectors that insert Web code into banking sites. These injectors try to grab your personal information to hijack your account, make wire transfer withdrawals, or even change the values presented in your online statement to conceal all of it.

Other types of injectors could be used for things like click-fraud—changing the links that users click on to direct them to different websites, while sending a referral code to a Web advertising provider to collect the pay-per-click. Some new botnets have been configured to simply generate clicks in the background on webpages without the computer user seeing them, creating ad revenue without the user scratching his head about why he ended up on a Russian porn site instead of the car insurance site he was trying to visit.

Beginners can buy injector packs for a set of banks through marketplaces and pay for direct support to help install, tune and customize them. In some cases, these require some server setup as well to properly harvest the data collected. It sounds complicated, but there are people happy to help you figure it all out for a small fee.

Budget Botnet Shopper’s Price: $80, plus $8/month for support.
An exploit tool or service

In order to take command of victims’ PCs, a bot herder needs a reliable way of defeating the basic security provided by operating systems, browsers, and e-mail anti-virus scanners. That usually means relying on an “exploit pack” or some other crafted application exploit.

The modus operandi of most bot herders is to use Web links as the delivery method for their malware, sending out streams of spam to potential victims in the hope that someone will fall for their social engineering. One click leads to a webpage set up to drop a package of nastiness on them. There are ready-made exploit packs, loaded with code written specifically for the purpose of planting malware on victim’s PCs that can be purchased and installed on a Web server or “rented” as a service.

Botnet builders can rent capacity on these services or outright buy them. A Phoenix exploit kit (like the one used to seed the recent Bamital botnet), can be purchased for $120, plus another $38 per month for patches and technical support, according to Goncharov. BlackHole, another market leader in exploits, offers its latest and greatest as a leased service for $50 a day, with extra fees for traffic overages. BlackHole also comes with an Oracle-like annual license for those who want to deploy on their own server. That costs $1,500 per year, with various add-on functionality fees.

Budget Botnet Shopper’s Price: $120 for the kit, plus $38/month for support.
Crypters and dropper builders

The problem with just pushing a Zeus bot in its raw form out to targets through an exploit is that the Zeus bot is bound to be detected by antivirus software because of its signature. To prevent that, botnet-herders turn to “dropper” malware that disguises the bot trojan, delivering it in encrypted form to disguise the file signature of the trojan and its associated files.

Creating a “dropper” requires the services of a malware “crypter.” Some are sold as straight software, with added services to see if the signatures of built droppers have been picked up by antivirus companies’ databases.

Others are sold purely as a service, with timer-based licenses, and may include the antivirus signature check as a built-in service.

There are even crypter services now available on the Web, delivered as a service. One such service offers dropper-building at the rate of $7 per "sample."

Another key to not getting caught is "antisandbox" code that detects if the malware has been dropped onto a sandboxed system or virtual machine—such as those used by digital forensics experts and security analysts. If the code detects that it's been deposited inside such a system, it can prevent the botnet trojan from being deployed and giving up the nature of the code it carries. Antisandbox code is a feature of some crypters.

If you want to save some money—and aren't particularly concerned about whether your bot gets picked up after a while by antivirus scans—there are sites offering "cracked" crypter kits for free.

Special delivery: Spam and social engineering services

But wait! You still have to deliver the exploit link to drop your botnet package on your unsuspecting (or possibly suspecting) victims. How do you get them to click on that link? The traditional route is by blasting semi-convincing spam messages and hoping people are dumb enough to click on a link in them to see a video, download a document, or reconfirm their PayPal information.

That typically means buying a spam blast, often from another botnet operator. Some spam-masters have moved their focus to social networks and charge not per message but per hit. You can spam out to social networks and over SMS with clickjack links using "borrowed" credentials or leave it to the professionals to do it for you for around a buck per thousand targets.

But that's the old-fashioned way. The new-fashioned way is to use "spear-phish" attacks that use social information about the target in some way that convinces them to click the link, either through a social network message in a compromised account or an e-mail that appears to be from a friend. If you want to make it even more convincing, you can always pay someone to hack a victim’s e-mail address to get access their account and contacts. Then it’s a simple as posing as the victim to fool all their friends.

For beginners, spam remains the best bet. It can be used to hit a variety of potential targets and it’s relatively cheap: cheap spamming services can run as little as $10 per 1 million e-mail addresses, with better services based on stolen customer databases running five to ten times as much.

Budget Botnet Shopper’s Price: $50 for an initial blast to qualified addresses.
Economies of scale

Using our budget shopper prices, that adds up to about $576 for the first month of operation.

None of these purchases guarantee success, obviously, and it could take multiple spam attempts and help from other specialists to finally establish that botnet you’ve dreamed of. Even then, the payoffs are not necessarily that big. There’s a glut of botnets already out there and botnet herders may be up against a short window before detection.

On the upside, it’s an easy game to buy into—unlike the bigger, more enterprise-scale cyber-crime rings behind big corporate data breaches. While the whales of the cybercrime game may share some of the basic technology approaches with their smaller cousins, they have more in common with the intellectual property stealing “Advanced Persistent Threat” (APT) hackers alleged to be associated with the Chinese military (though they may surpass them in skill). Trend Micro Chief Technology Officer Raimund Genes said during the DC briefing that he thought the recent alleged Chinese APT attacks had been uncovered largely because they lacked the finesse of Eastern European cybercrime rings.

The bigger financial hacking organizations—which are a small number of organizations of hundreds or perhaps even thousands of people—operate in their own closed forums, sometimes on “darknets,” where you can only gain access by being invited. While there’s some use of botnets by the major cyber-crime rings, they tend to want to protect their investments in the more specialized, targeted attack tools they use. Botnet use is sparse in that space. “Once they get access to the environment,” Percoco said, “they then deploy custom pieces of malware that are sometimes written from scratch, brand new, never been utilized before—and they plant them on specific systems within the environment.”

As a result, the data breaches caused by these targeted hacks can go on for months, even years before being detected. A study released by Percoco’s team at Trustwave in February found that the average targeted attack went more than 210 days before it was detected. And this detection was usually because of a customer complaint or notification by law enforcement or a payment processor, not because antivirus software detected the hack. At some companies, the hacks lasted more than three years without being detected, all while millions of credit card transactions and other data were being pumped back to the hackers.

Botnet operators generally go big or go home in their attacks. But the tools they use can just as easily be applied to the long game if they’re used in a targeted fashion and they apply some of the lessons learned by the big-time hacking organizations. “Swiss Army knife” botnets and remote administration tools can be used as part of a poor man’s APT by those who are willing to take the time to do the research and social engineering to get their malware in the right place. And just because Zeus and other botnets are a known threat doesn’t mean they can’t be used in stealth. According to the siteZeusTracker, the average detection rate for Zeus binaries by antivirus software is only 38 percent. And that’s for known Zeus botnets.