Introduction
Malware authoring and distribution has become very profitable over the years. Earlier, malware was written mainly for fame and notoriety. However, it has now become a very profitable enterprise, backed by a strong business model.

The process of propagating and distributing malware has been evolving constantly. A few years back, the main distribution technique was self-propagation. Worms would exploit server-side vulnerabilities that would allow propagation without any user interaction and simply required the computers to be on and connected to the network. Once the worm infected the computer using the vulnerability, it would scan for other vulnerable computers on the network, and the process would start all over again.

Over the years these types of server-side vulnerabilities dried up, and the focus quickly turned to client-side attacks and classic social engineering. Most client-side attacks exploit vulnerabilities in client applications, such as browsers and browser plug-ins. Both client-side vulnerabilities and social engineering require some sort of user initiation. This means that the victim needs to visit an infected Web site, click on a malicious link, or open an email attachment. So the question is how does one propagate malware on a large scale using client-side vulnerabilities?

To solve this problem, malware authors have come up with a distribution model dubbed “pay-per-install”. This is not a new online concept and has roots in the online advertising and pornography industries.
Pay-Per-Install Distribution Model

The pay-per-install distribution model is based on revenue sharing and commission. Malware authors do not have the resources or bandwidth to spread their malware on a large scale. Instead they rely on a network of affiliates, who distribute the malware, and in return get paid a commission for every install.

Figure 1 is a graphical representation of the pay-per-install model.

The pay-per-install model

The “kingpin” sets up a pay-per-install Web site. The kingpin then recruits affiliates to sign up on the Web site where they get access to malware links or binaries. The kingpin may create the malware directly, outsource malware creation to a third-party, or simply distribute malware created by others for a fee. In turn, the affiliates install the malware onto the victims’ computers using a variety of methods, and then get paid for every successful install.

Usually the kingpin is able to pay affiliates because he or she receives money from others who “place orders” to perform activities such as sending out spam emails, distributing scareware products, or stealing credit card numbers and credentials from or through the infected computers. For example stolen credit card numbers or game credentials have a definite dollar value in the underground economy. The profits from these orders are distributed back down the chain.
Figure 2 is an example of this chain. Let’s say a malicious software vendor wants to sell fake antivirus products. In order to distribute their software, they would contact a pay-per-install kingpin. After the kingpin negotiates terms with the malicious software vendor, he provides the fake antivirus installer to his network of affiliates. The affiliates would silently install this product onto the victim’s computer via clientside vulnerabilities or other social engineering methods. Once installed, the fake product would constantly pop up messages indicating the computer is infected, scaring the user into purchasing protection for nonexistent threats.

This is a great social engineering trick, and many unsuspecting victims may end up purchasing this fake product. The money is then distributed back into the channel. The malicious software vendor would pay the kingpin for every successful install, and the kingpin in turn would pay the affiliates.

Figure 3
Fake antivirus product pop-up

You may be vulnerable!

WARNING!
You may have Spyware

TOP 10 threats for last week:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Alert level</th>
</tr>
</thead>
<tbody>
<tr>
<td>N-case.win32</td>
<td>Spyware</td>
<td>Average</td>
</tr>
<tr>
<td>CoolWebSearch(CWS).win32</td>
<td>Spyware</td>
<td>Danger</td>
</tr>
<tr>
<td>T-Worm.50big</td>
<td>Virus</td>
<td>High</td>
</tr>
<tr>
<td>Backdoor:5dBot.gen</td>
<td>Virus</td>
<td>Critical</td>
</tr>
<tr>
<td>Trojan/Comper.2S输卵al</td>
<td>Virus</td>
<td>Critical</td>
</tr>
</tbody>
</table>

Suspect files found: **45**

Recommendation: click the “Protect now” button to download security tool to upgrade your computer.
This model works really well for the malware authors, as they can then concentrate on soliciting orders and authoring or sourcing malware to execute those orders, leaving the distribution of the malware to someone else. In addition, affiliates provide cover for the kingpin, putting distance between the kingpin and the actual act of installing the malicious software. More affiliates mean more distribution channels and that ultimately translates to more profits.

**Recruiting Affiliates**

Most affiliates are recruited through underground circles, such as underground forums and word-of-mouth. However, many are also initially introduced to pay-per-install schemes from pitches such as “join to earn extra cash” or “make easy money from home”. These pitches are sent through SPAM email, online advertising, online classified ads, and even more traditional methods, such as flyers posted to lampposts and newspaper classified ads. The pay-per-install Web sites entice prospective affiliates by marketing this as an extra income program. Figure 4 shows a screenshot of one such Web site.

Joining these Web sites is absolutely free of cost for the affiliate. Most Web sites require very little information and usually anyone can sign up as an affiliate.

Communication between the affiliates and the pay-per-install author is mostly conducted using instant messaging software. Although signing up is free, some Web sites will only approve the account after the affiliate establishes communication with the author. This is to assure the author that the affiliate is genuine.

Furthermore, affiliates are not bound to a single pay-per-install kingpin. In order to maximize profits, affiliates often sign up with multiple pay-per-install kingpins. They then acquire multiple malware executables from different pay-per-install Web sites, and bind them into a single executable. Every time this master installer is executed, it will install different pay-per-install executables on to the system.
The Payload

Once signed up, the affiliate gets access to the payload. The payload in most cases is a malicious executable file or URL links to browser exploits, which then download one or more malicious executables. The affiliate needs to acquire these files and install them onto the victims' computers in order to earn a commission or lead them to one of the malicious links. Figures 6 shows a snapshot of a pay-per-install Web site distributing malicious executable files and figure 7 shows another distributing malicious URL links.

A variety of threats are distributed by pay-per-install Web sites through affiliates including many high profile threats like Trojan.Vundo and W32.Virut. Figure 8 shows the distribution of malware families that use the pay-per-install model in 2009. One can concur that this distribution model is what makes these threat families so prevalent.
While security vendors attempt to keep up with detecting these threats, the malware creators are also constantly changing their threats to avoid detection. The graph in figure 9 illustrates the frequency of new executables available on pay-per-install Web sites. From the data we can see that many pay-per-install Web sites update their payloads almost every hour.

As soon as a pay-per-install executable is detected by a few antivirus vendors the author creates a brand new executable and makes it available for distribution.

**Pay Rates**

Pay-per-install Web sites pay their affiliates for every successful install. The pay rate per install is determined by the country in which the victim resides. Figure 10 shows the rates offered by five different pay-per-install Web sites.

These rates are for one thousand successful installs. From the data we can conclude that North American computers are prime targets, since they command the highest payout rate, followed by computers in Western Europe, with the next highest rate. On an average, an affiliate can get $0.13 USD per install from a North American victim. (One Web site offered as much as $30 per install.) If you multiply this per-install average by an average of 1,000 installs per day, the average profit would be $130 per day.

Most pay-per-install Web sites pay their affiliates on a weekly basis. The affiliates usually get paid using online payment services such as PayPal, WebMoney, Fethard, and others.

Figure 11 gives us a peek at how much money the top affiliates can potentially earn using pay-per install.

The top affiliate on this Web site achieved 2084 installs, and earned $555 in one day! While not typical, if he or she could maintain that level of install rates, they could net over $200,000 USD a year.
There are invite-only, pay-per-install Web sites where the payment-per-install is significantly higher. Last year an invite-only Russian Web site called "Bakasoftware", distributing fake antivirus software, was infiltrated. The statistics page in Figure 12 shows one affiliate was able to install 154,825 copies of a misleading application within a short time period and earned a net commission of $146,524 USD. (Sourced from SecureWorks Research.)

With such high stakes, invitations to these closed pay-per-install networks are invaluable for affiliates. However affiliates need to establish credibility before they are invited to such networks. Often this is done via online networking or proving their distribution abilities by providing their install statistics.

Most pay-per-install Web sites have a statistic page where the affiliate can track their daily progress, providing statistics such as the number of successful installs they have completed and the amount of commission they have earned.

**Statistics**

Pay-per-install Web sites keep track of statistics like the number of successful installs per affiliate and the country of the victim. This information is used to calculate payment amounts for the affiliates. In order to correlate installations to the correct affiliate, each malware file is customized for each affiliate by embedding a unique number or name called an affiliate ID inside the malware binary. This ID uniquely identifies each affiliate and is assigned to the affiliate upon sign up. On install, the malware installer transmits this affiliate id back to the pay-per-install home server, recording a successful install for that particular affiliate.

Figure 13 is a snapshot of a communication channel between the pay-per-install home server and the pay-per-install malware. The pay-per-install malware is transmitting the affiliate ID as one of the HTTP parameters in an HTTP request. In this case, the affiliate ID is a six-digit number.

The affiliate ID used in the communication above is embedded within the malware installer file itself. Sometimes the ID is located in an obvious place in the binary; other times it is encrypted under multiple layers in a configuration file.

Another technique is to modify an inconsequential part of the malware binary, such as the default message string in the MS-DOS stub. Figure 14 shows one such file where the message string, “This Program cannot be run in DOS mode”, in the executable is overwritten with the affiliate id.
Payload Distribution Techniques

Once the payload is acquired, it has to be installed on a large number of computers in order to earn a high commission. The affiliate uses various mechanisms to infect victims, such as distributing files through file-sharing networks, injecting code into legitimate Web sites, poisoning search results, buying online ads, and sending spam. Each method is discussed in more detail below.

File-Sharing Networks

Using file-sharing networks (typically using the BitTorrent protocol) is by far the most popular method of distribution for affiliate. An affiliate obtains the malicious payload from the pay-per-install Web site and then binds it to some legitimate program or application. The resulting executable is given an enticing name such as “Paris Hilton Videos.exe”. A torrent pointing to the executable is made and seeded on torrent trackers and search sites. Various tutorials are available online that provide step-by-step instructions on how to create and distribute malicious torrents.

Social engineering tricks like using enticing file names or changing an executable icon to a data file icon are often employed to entice the victim to download the torrent. For example, figure 15 shows an affiliate discussing social engineering tricks like renaming the file name to “Rihanna – Umbrella.mp3 powered by mp3leech.com”. To an unsuspecting victim, the file would be perceived as a regular .mp3 file, when in reality the .com file extension would cause the file to be treated as an executable.

Figure 15
Affiliate social engineering tricks

Malware served up through file-sharing network

Figure 16 is an example of one such torrent on a popular file-sharing network. If a victim were to download this torrent and execute the file, he or she would be infected with Trojan.Vundo, which originated from a pay-per-install Web site and was distributed in this manner by an affiliate.

Naming of the torrent files is not restricted to names referencing adult content. Affiliates also commonly use file names of popular commercial software or “cracks” or “serial key generators” for popular software applications.

Infected Web Sites

Instead of attempting to lure unsuspecting users to a malicious Web site, affiliates will often hack into legitimate Web sites and add code to the Web site that exploit client-side vulnerabilities, such as vulnerabilities in Internet browsers or their plug-ins, secretly installing the pay-per-install malware. Also, instead of injecting the malicious code directly into the Web site, an iframe tag is injected, which causes the Web site to load the malicious content from another site that is under the control of the affiliate.
Affiliates inject their malicious code into legitimate Web sites using various techniques. One of the most popular methods is to buy hacked account credentials for Web servers. (This method is covered more in-depth in the Tools and After-Market Services section.) Using this method, the affiliate has full access to all the files on the Web server and can easily modify and inject malicious code into the source files of the hacked Web site.

Some affiliates also take advantage of specific vulnerabilities in Web applications built on technologies like PHP or SQL (often referred to as “SQL injection”) to get access to the Web server content. Once the affiliate can modify the Web server content, they often inject obfuscated JavaScript code, as shown in figure 17.

Once this JavaScript is decoded, as in figure 18, it is actually an iframe tag that loads a malicious Russian page, which contains more obfuscated JavaScript. This code, once obfuscated, attempts to exploit vulnerabilities in Acrobat Reader and Flash Player by silently requesting malicious .pdf and .swf files. Figures 19 and 20 show the code before and after deobfuscation.

Once the vulnerability was successfully exploited, the exploit code would download and execute many malicious executables on to the victim’s computer. Figure 21 is the HTTP request for one such malicious executable that was obtained from one of the pay-per-install Web sites.

Once this executable was executed, it installed fake antivirus software called Antivirus Pro 2010 onto the victim’s computer. This fake product then started falsely alerting the victim that his or her computer is infected with malware and offered to clean up the computer, if the victim were to purchase the product.

If the victim fell for this grand social engineering ploy, they would end up purchasing this fake antivirus software for $49.95 or $69.95. Misleading applications, often attempt to cross sell additional fake products, as well multi-year subscriptions.
The victim's credit card would be charged and these funds would then pay a part of the profit to the pay-per-install kingpin who helped facilitate the distribution. The kingpin would in turn pay the affiliates. From this example, one can infer how profitable this business model is.

**Search Result Poisoning**

Search engine optimization (SEO) is defined as methods and tricks employed to influence the search ranking of a Web page. Although many Web sites use SEO techniques legitimately, affiliates often employ them for malicious purposes.

The affiliate's main goal is to have a lot of victims visit a malicious Web site via search engines results. In order to do so, the affiliate's malicious Web site should be listed and ranked higher than other Web sites in the search engine results. Keywords related to recent trends and events are used as bait for these short-lived Web sites. Using these keywords and other SEO tricks, the affiliate's Web site would end up getting listed very high in popular search queries. This would then drive a lot of traffic to the malicious Web site. For example, during the US tax season, if someone made a typographical error searching for the term “Federal Income Tax form”, they would get back a healthy mix of malicious Web sites in their search results, as shown in figure 23.
If the user were to click on these links, they would be directed to a malicious Web site owned by the pay-per-install affiliate. The Web site would then use social engineering tricks to fool the victim into downloading pay-per-install malware or exploit client side vulnerabilities in order to silently install the malware. Figure 24 is the fake security alert the victim would encounter, if he or she chose to click on the search engine results above.

In another example, if someone recently searched for the term “Serena Williams outburst”, they would have gotten the search result link in figure 25. If the victim clicked on this link, they would be taken to a malicious Web page that mimicked the Windows Explorer interface. This malicious Web page (also called a “fake scan” page), would then trick the user into downloading a fake antivirus application.

Figure 25
Search result for “Serena Williams Outburst”

Figure 26
A fake scan
Malicious Sponsored Links

Malicious code distributors have also started using search engine and sponsored link advertisements to direct users to fake product download Web sites for brand name or technicall-sounding applications. For example, if we perform a Web search for the keyword “directx”, one of the sponsored links points to a page cleverly pretending to be the download page for the official version of DirectX.

If the victim were to click on this advertisement, he or she would be directed to a fake product Web site owned by a pay-per-install affiliate. The application that the victim would download from this page is in fact a pay-per-install malware executable.

“Malvertisements”

These are malicious ads—usually in the form of Flash, JavaScript, or DHTML—that redirect the user to fake scan Web pages or exploit a client side vulnerability. Affiliates buy advertisement space in an online advertisement network. Often the initially displayed advertisement looks legitimate, or is even a legitimate advertisement from a mainstream company, used without its consent. Once their advertisement is placed in the network rotation and begins appearing on legitimate Web sites, the advertisement is modified to deliver malicious content. This allows the affiliate to easily distribute their code to hundreds of thousands of users.

Mainstream Web sites are susceptible to such malvertisements, since the administrator of the Web site normally does not have fine-grain control over what advertisements are shown on his or her Web site. In addition, advertising networks provide varying degrees of advertisement screening. The New York Times Web site recently had malvertisements on their Web page. Any unsuspecting user who visited nytimes.com and clicked on a particular article was hit with a malicious Flash advertisement that came through a legitimate advertisement network being used by The New York Times. This advertisement redirected the victim’s browser to a fake security scan page previously shown in figure 26.

Spam

Affiliates often send spam emails or post spam links on blogs and message forums with enticing content that actually links to a malicious Web site or executable. In the example shown in figure 29, a fake YouTube message
is sent with a link to a video of Michael Jackson’s last moments. Fake videos and messages appear that state the user needs to download a video codec, which is really a malicious binary, to watch the video.

Spam links are also sent in instant messages. The post shown in figure 30 is an IM received by an unsuspecting victim, falsely warning him or her of malware on the computer. The message asks the user to download the patches from a link, but the patch file is actually a malicious executable originating from a pay-per-install Web site.

Social networks are another common method of communication today and spam links are also commonly posted to places such as Twitter, Facebook, and MySpace.

While these methods of distribution are the most prominent, affiliates have harnessed almost every commonly used service to distribute their files.

**Tools And After-Market Services**

The pay-per-install distribution model has created a huge underground economy for tools and after-market services. These services and tools are targeted at affiliates and mainly help them to scale their operations. Part of the profits that an affiliate makes is often reinvested to purchase these tools and services. Many of these tools are also packaged into a single application and sold on online forums.

**Binders**

Binders are software applications that allow an affiliate to bind two or more files together to create one single executable, such that both the files will be run when the main file is executed. These tools are often used by the affiliate to bind a malicious executable to legitimate software. If the victim were to execute the main executable, the legitimate software application in this bundle would provide cover for the malicious executable, running silently in the background. Usually the prices for binders in the underground marketplace are between $50 - $100 USD.

**Packers**

Packers are tools that morph a malicious executable into a stealthy form, such that it is harder for security vendors to detect the malware, and others from being able to determine the behavior of the executable code. Packers use various tricks and techniques in order to achieve this.

Many packers will change internal structures of the malicious file, introducing anti-debugging, anti-
emulation, anti-sandboxing tricks, and adding encryption and obfuscation in order to evade analysis and detection. Packers usually sell for anything from $20 to $100 on average in the underground market and services are also provided where a file can be packed for an attacker.

Resource And Icon Cloners

Resource and icon cloners clone visual resources of a legitimate file or application into the malicious executable, such that to the victim the malicious executable looks visually similar to legitimate software. The goal is to entice the victim to trust and execute this malicious executable.

Downloaders

Downloaders are tools to generate executables that, when installed, silently download and execute other secondary executables. An affiliate would first attempt to install a downloader onto the victim’s computer. Once the downloader is executed, it would contact the affiliate’s server to download and install additional executables. This allows the affiliate to push more than one pay-per-install threat onto the victim’s computer, and more easily change what files are being sent to the victim. Downloaders usually sell for $25-$100 in the underground market. The more stealthy the downloader is, the more costly the price. In order to be stealthy, downloaders will often inject code and run from system processes.

Seed Boxes

Affiliates often use torrents to spread their malicious pay-per-install payloads. In order to do so, the affiliate must create an account on popular torrent trackers, upload their malicious torrents, and also seed those malicious files. Affiliates cannot scale their operations using home computers and thus, rent a seed box to seed their torrents. Seed boxes are shared or dedicated servers, solely for the purpose of hosting files shared on peer-to-peer networks. They are like Web servers, but host only torrent files instead of Web pages. Most seed boxes come with preinstalled, torrent management software, and have a cap on the number of active torrents you can have at any point in time. Affiliates with larger operations end up purchasing a virtual dedicated server in order to seed their torrents files.
Seed box services are provided by many companies and usually there are many pricing options and plans that an affiliate can pick from. On average, an affiliate could end up spending anything from $20 - $100 dollars a month for renting a seed box.

**Proxies**

Many torrent tracking sites disallow malicious torrents and ban users who seed such torrents. Tracker sites are often tracking the user’s IP addresses and on abuse disable the user’s accounts. Affiliates are constantly struggling to overcome this challenge and use various ways to avoid getting their accounts banned. Some affiliates use proxies to mask their IP address. By employing a proxy server, the affiliate attempts to anonymize him- or herself to minimize the risk of having the account banned. This has created an underground market for proxy servers that affiliates can use on a daily basis. Proxies are also commonly used for other activities as well whenever the affiliate needs to mask their IP address. There are Web sites that act as marketplaces for proxy servers where someone can get a daily list of proxy servers for less than $5 a month.

**Mass Torrent Submitters**

Affiliates often need to submit their malicious torrents to many torrent trackers, in order to achieve better download rates. Tools that automate this process are widely for sale.

**Web Exploit Kits**

Exploit kits are a collection of browser-based exploits that an affiliate can buy from the underground market. The affiliate can serve browser exploits to victims with ease by installing these exploit kits onto their Web server (or a hacked Web server). Most toolkits are highly configurable and come with a management console, where the affiliate can track statistics like how many victims have been infected, the country of the victim, and which exploits were successful. They can also choose which executables need to be installed on the victim’s computer.

Many exploit kits are available in the underground. Some popular ones are NeoSploit, Nuke Packs, and Unique pack. Most of the exploit kits sell for from $50 to $1000. Toolkits with newer exploits cost much more. Affiliates also trade zero-day exploits through private channels and underground forums.

**Instant Messaging Spammers**

Instant messaging spammers are programs that can hijack popular IM applications on a victim’s computer and send malicious links to all the friends the victim has on his or her IM contact list. This is a great social engineering technique, since the friend of the victim would often trust the link, assuming it came from the victim. These tools, averaging about $80 USD, work across a broad range of IM clients such as Yahoo!, MSN, ICQ, and Skype.
Web Site Credentials

One way an affiliate can spread their malware is by injecting malicious code into legitimate Web sites. Whenever a victim visits this legitimate Web site, the malicious code will direct the user to the malicious Web page owned by the affiliate. The affiliate can then use social engineering tricks, or serve browser exploits in order to install the pay-per-install malware onto the victim’s computer.

FTP, SSH, and cPanel are common means by which Web site owners update their Web site content. Stolen cPanel credentials often give the hacker access to all the domains hosted by that Web server. Using these credentials an attacker or affiliate can inject their code on all the Web pages on all the domains hosted on a Web site.

The average cost for buying full access to one legitimate domain is extremely low. For example, a hacker was selling access to cPanel credentials for 700,000 servers for as low as $120. However the cost increases if the domain or Web site already attracts large amounts of traffic.

Social Networking Accounts

Social networking sites like Twitter, Facebook, and MySpace all provide a rich playground for affiliates to spread pay-per-install malware.

For example, affiliates can take advantage of the viral nature of Twitter, to reach thousands of victims, with an enticing message and a URL link to a malicious site. Even worse, most URL links on Twitter are reduced using URL-shortening services, such that the victim has no good way to be sure of what domain he is going to visit, when he clicks on the shortened URL.

In figure 36, a black-hat user is selling eight Twitter accounts, with 2000 followers for as little as $7.

Figure 37 shows an affiliate trading Facebook, MySpace and Hyves credentials. For these social networking sites, an affiliate usually is able to command higher click-through rates for each malicious post he sends out, since many victims would click on a link coming from a “trusted” friend.
Web-Based Email Accounts

Affiliates also trade account credentials for hacked email accounts. Affiliates can then use these credentials to send out emails with malicious links to the users the victim has on his or her contact list. Many users tend to reuse the same passwords for multiple Web sites, like social networking sites and online banking. Therefore compromising an account on one Web site can often lead to account compromises on other Web sites.

Conclusion

Using pay-per install, malware distribution has become extremely streamlined, where anyone can acquire and distribute malware and make a handsome profit. This model has also fueled a huge underground economy for malicious tools and services. Malware distribution is no longer restricted to an elite few, but now is open to the average person looking to earn some extra cash. In this economy, we really wonder how many people intend to do just that.