



**IBM Internet Security Systems X-Force®  
Research and Development Newsletter**

December 2006

## Part 1: From Botnet to Malnet

### An Evolving Underground Digital Economy

Throughout 2006 X-Force observed an exponential increase in attackers seeking to compromise a victim's desktop through vulnerabilities in Web browsers or Spam-based payloads. Most commonly the attackers sought to install malware armed with 'best-of-breed' rootkit functionality, command-and-control channels, auto-updating and spyware technologies – basically, digital Swiss-army knives.

These distributed malware networks (let's refer to them as 'malnets' instead of 'botnets' because they are much more sophisticated than the dated 'botnet' term implies) have been used for identity theft, conducting coordinated denial-of-service (DoS) attacks and as e-mail relays for Spam distribution. But now attackers have become more conscious of the revenue-generating opportunities available to them via the thousands of computers they control. Looking ahead in 2007, we can expect the owners of these 'malnets' to shift their business operations into less noisy ventures – ones more likely to provide longer-term (perhaps even semi-legitimate) revenue opportunities.

The problems facing the attackers who own an existing malnet is that DoS and Spam are extremely noisy activities and will always draw attention to the infected hosts. Consequently, the probability of discovery and shutdown are high – thereby requiring the attackers to constantly "replenish" their networks by infecting more hosts (which is something that will require more effort in the future as desktop security features continue to advance). The same logic applies to attackers who use their malnet networks to harvest bank account details from the host owners. Transferring money from the victims' accounts will not only quickly result in the loss of control of the infected host, but also carries high criminal prosecution risks.

In the near future, our expectation is that these malnet owners will seek to lower their visible profile and retain their compromised hosts for as long as possible.

#### **The Bot-net Cash Cow**

So, how can the malnet owner cash in on his/her infection success and retain a network of infected hosts? The answer is simple – personal profiling – which legitimate companies have been doing for a long time.

At its most basic level, knowing the name and full postal address of a person is worth cash to the right organization. Combining this information with details such as the person's age and sex is worth a few more dollars to just about every retail organization in

the world. The more information about the person – how much money does he make, how much disposable income does he have each week, what are his favorite shops, etc. – the higher the cash value of the personal profile.

Legitimate organizations do this all the time. Supermarket loyalty cards are a classic example. Knowing who you are, how much you spend and how you spend it are extremely valuable to the supermarket chains. It helps them "tune" offerings to specific customers or groups of customers and increase sales margins. Organizations such as DoubleClick ([www.doubleclick.net](http://www.doubleclick.net)) have made successful Internet businesses out of profiling Internet users (using technologies such as banner advertising, cookie tracking and Web-bugs) and selling that information to corporate clientele.



Now visualize a malnet owner and the potential revenue opportunities available to him. He can monitor

precisely how much money the victim has in his bank accounts, knows which loyalty cards the victim has by parsing incoming e-mail, knows exactly which Web sites the victim visits and how long he spends on each one, knows where the victim posts his holiday photos and what toys he's purchased on Amazon for his daughter's birthday.

How much do you think a car salesman would pay to the malnet owner for name and contact details of a "victim" that has \$80,000 sitting in his savings account and in the last three days has visited 20 Web sites selling cars, spending 50 percent of his viewing time looking up BMW Z4's? A few hundred dollars perhaps? Maybe more if the network owner says he will only charge the car salesman on a completed sale – after all, he'll know when the money leaves the bank account and where it went.

The same potential exists within a compromised corporate network. While the computers may be company assets for conducting work, most people also use them for private activities and it is quite probable that corporate networks could yield similar monetary returns on personal profiling for the malnet owner. Additional opportunities also exist. Surreptitiously copying confidential documents and selling them to the highest bidder – perhaps to one of the applicants in a competitive bid – is certainly possible. Perhaps even selling subsets of information to recruiters – the name and contact details of the person who writes the most lines of C# code per week within the organization.

The advantages to the malnet owner using this revenue generation model are many, but key among them is the fact that the “passively” obtained information can be sold many times, to different organizations, without actually raising attention to the compromised host.

– Günter Ollmann, Director of X-Force

## Part II: From Botnet to Malnet

### Cashing in on Virtual Economies

Moving beyond personal profiling, the malnet owner is also capable of branching out into the new lawless economies such as those associated with online gaming – in particular massively multiplayer online games (MMOG).

A series of papers posted by Indiana University examining virtual economies estimates the value of game-based assets to lie between \$200 million and \$1 billion, while IGE (an organization that specializes in buying and selling game-based virtual currency and assets) estimates trade of these virtual assets could become a real-world economy of around \$2.7 billion in 2006 and reaching \$7 billion by 2009.

Well-known real-world organizations are now in the process of developing virtual representations of their businesses and are “setting up shop” within the various MMOGs. One recent and notable addition, the international Dutch banking entity ABN AMRO has set up a virtual bank within ‘Second Life’ to provide financial advice and would obviously like to become a future financial bridge between the two economies.

#### Dutch bank ABN sets up branch in Second Life

Fri Dec 1, 2006 7:45am ET

[Email This Article](#) | [Print This Article](#)

##### MARKET VIEW

AAH (ABN Amro Holding)

Last: €22.53  
Change: -0.18 (-0.79%)

AMSTERDAM, Dec 1 (Reuters) - Dutch bank ABN AMRO NV (AAH.AS: [Quote](#), [Profile](#), [Research](#))(ABN.N: [Quote](#), [Profile](#), [Research](#)) became the latest enterprise to tap into the growing potential of Second Life, by opening a branch on Friday inside the Internet-

At the present time ‘Second Life’ virtual currency (called “Linden dollars”) can be exchanged for U.S. dollars, essentially turning it into a real currency, with more than \$600,000 being spent in a single day. Several third-party currency exchanges already exist to convert the plethora of in-game money types into real money, with live exchanges and fluctuating rates.

To understand how these virtual economies become real-world economies, it is perhaps best to take a closer look at two of the largest and most talked about MMOGs – Second Life and World of Warcraft.

#### Second Life:

Since January 2005, Second Life’s population has grown from 100,000 residents to a little over 1.7 million, and is expected to reach 40 million within the



next two years. In this MMOG, these players (or ‘residents’ using the games terminology) can create virtual goods within the game (including the buying and selling of ‘land’) and are allowed to retain the IP rights to their creations – thereby being able to sell them at various in-world venues.

This virtual economy

has already seen its first real-world millionaire. Anshe Chung turned her initial investment of \$9.95 per month into more than \$1 million from profits earned entirely inside a virtual world. Her character recently appeared on the front cover of Business Week magazine.



#### World of Warcraft:

This number-one leading fantasy-based subscription MMOG currently consists of more than 7.5 million players worldwide. World of Warcraft allows them to battle each other online or conduct team-based missions and scenarios in order to advance their characters.

As with many MMOGs that focus on character advancement, high level characters and powerful weapons are frequently traded amongst players. Top ranked players with unique weapons or armor are seen as being valuable and can be purchased at sites like eBay for values of \$1,000 or more.

#### Malbot Revenue from MMOGs

The opportunities for financial gain by the malbot owner, while limited, are interesting because of the way government legal systems currently handle virtual assets. In essence, these virtual assets have no real-world value and typically any value or ‘ownership’ is at the discretion of the MMOG developers and owners. This means that there is no legal discourse for settling disputes.

Consequently, if the malnet owner steals a player’s character and sells it to another player, the victim cannot seek legal recompense; similarly to if the attacker sells the player’s businesses and assets within the game or through real-world brokerages. Malnet owners may see this as a ‘safe’ way of generating revenue. With tens of millions of online players already out there and an anticipated exponential growth in new members, the potential for developing a profitable business is very high.





process will not work on-the-wire. Similarly, the only alternative is to protect at the desktop/browser itself. Let's explore them both.

Duplicating the page rendering process on the wire would require JavaScript and VBScript engines. There are multiple issues present with this approach. First, it is not practical to write these engines from scratch without a significant development overhead. Second, such engines may be available with an open-source-like license, but may not be feasible to integrate into a commercial offering. Third, it would be trivial to determine how to conduct a denial-of-service (DoS) attack against the processing engines or at least obfuscate the content enough so that we give up before "seeing" the malicious activity. Lest we forget that the emulation itself will be computationally expensive. Finally, the engines themselves might be vulnerable to attacks other than DoS.

Protecting at the browser level is an interesting idea. There are commercial offerings which sandbox the browser for instance. This basically means that the product will block system calls based upon whether or not they follow rules. These offerings may or may not work so well depending on various factors such as whether the exploit is in a native or third-party component, and whether the exploit is a buffer overflow or feature or logic bug. Given that there is such variety in terms of technique and quality, only some of these factors will apply to any given product. However, there isn't a product on the market which specifically looks to protect the browser before incoming content is processed. This is no small feat, but protecting at the browser level has a bright future.

Eventually it is possible that the encryption techniques used for malicious Web content will become significantly different than that of non-malicious content. Thus we will be in a good position to revisit heuristic detection of malicious encrypted Web pages. In the meantime, X-Force will continue to research next-generation technologies that will allow us to provide preemptive protection.

– Robert Freeman, X-Force Adv. Research

## A Month in Review

In this section of the newsletter, X-Force briefly covers some of the security content developed or processed in the month of November.

### Vulnerabilities:

Compared to November 2005, X-Force researchers identified, catalogued and analyzed 53 percent more vulnerabilities.

Overall, thus far in 2006, X-Force has covered 44 percent more vulnerabilities over the same period in 2005.

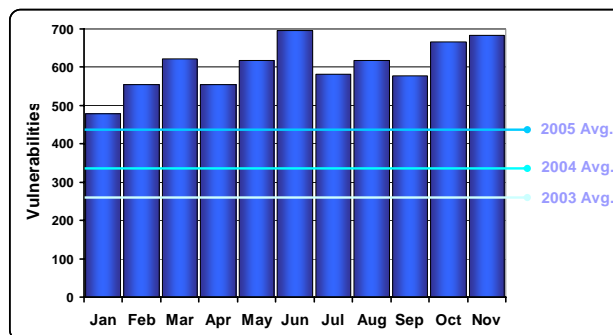
	Reported					YTD
	Crit.	High	Med.	Low	Total	
Nov	0	108	462	113	683	6650

Of these vulnerabilities, 606 were remotely exploitable, 86 could only be exploited locally and nine could potentially be exploited both remotely or locally.

Vulnerability Breakdown	
<b>Bypass Security</b>	<b>38</b>
An attacker can bypass security restrictions such as a firewall or proxy, an IDS system or a virus scanner.	
<b>Data Manipulation</b>	<b>154</b>
An attacker is able to manipulate data stored or used by the host associated with the service or application.	
<b>Denial of Service</b>	<b>71</b>
An attacker can crash or hang a service or system, or take down a network.	
<b>File Manipulation</b>	<b>10</b>
An attacker can create, delete, read, modify or overwrite files.	
<b>Gain Access</b>	<b>300</b>
An attacker can obtain local and remote access. This also includes vulnerabilities in which an attacker can execute code or execute commands, because this usually allows the attacker to gain access to the system.	
<b>Gain Privilege</b>	<b>29</b>
An attacker can gain privileges on the local system only.	
<b>Obtain Information</b>	<b>67</b>
An attacker can obtain information such as file and path names, source code, passwords or server configuration details.	

\* Right-hand column represents unique vulnerability count

### Vulnerabilities per Month vs. Annual Average



Top 5 Vulnerable Vendors	
Apple	18
Linux Kernel	18
Microsoft	17
Novel	8
Cisco/GNU/Mozilla/Sun/ContentNow	6

\* Right-hand column represents unique vulnerability count

### **Malcode:**

On November 15, X-Force's malcode discovery and protection engine testing platform (Catfish) was able to identify yet another interesting password-stealing trojan named W32.PWS.Small.BS. This sample had rootkit capabilities which allow it to hide its process, dropped files and registry entries. Furthermore, once installed in the system, it will act as a SOCKS proxy enabling a remote attacker to utilize the affected system to relay spam or other attacks. It seems like password-stealing, proxying plus rootkit capabilities make a nice combination for malcode authors seeking financial gain.

Catfish also witnessed yet another serial variant attack of W32.Worm.Stration. The first serial variant attack started on November 6 around 9 pm, this attack is another major attack in which 43 variants were received in a span of 22 hours averaging two samples per hour.

Additionally, on November 26, a second W32.Worm.Stration serial attack occurred, this second attack is just minor in which six new variants were received in a span of eight hours.

Nobody knows when the author of Stration will stop creating new variants and stop causing headaches to signature-based AV companies and customers – probably when he/she has something more interesting to do or gets caught by the authorities. Until then, being ready and being ahead of this threat is our best weapon.

### **Sample Harvesting:**

It is worth noting that as part of X-Force's continued strengthening of IBM Internet Security Systems antivirus, anti-spyware and anti-malware protection, we investigated and added another 44,685 new samples to our malcode zoo this month.

**Copyright© 2006 IBM Internet Security Systems, Inc. All rights reserved worldwide.**

Internet Security Systems, the Internet Security Systems logo, Proventia, the Proventia logo, SiteProtector and Ahead of the Threat are trademarks or registered trademarks of IBM Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owner and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.