



## X-Force<sup>®</sup> Research and Development Newsletter

November 2006

## Trends in Web Exploitation

Over the last few years, attackers have increasingly begun to refocus their attention upon the lowly desktop; in particular exploitation of browser-based vulnerabilities

The frequency of Web browser exploitation is on the rise once again and this class of attack brings new protection challenges, such as defeating JavaScript obfuscation. Browser attackers traditionally have fallen into two categories: opportunists and small syndicates. Today we are observing disturbing trends which demonstrate innovation in Web exploit delivery. In order to best understand the significance of these new threats, we will be exploring two case studies.



### Example One

Starting October 23, 2006, we observed a surge of sites identified through our Whiro Crawler (an X-Force® research initiative focusing on detecting and cataloguing new Web-browser-based exploits in the wild) that redirected to a single malicious host serving up an exploit for CVE-2006-3730/MS06-057, also known as the ActiveX WebViewFolderIcon setSlice vulnerability. This is a known vulnerability and has been resolved in the October 2006 Microsoft super-Tuesday patches.

Whiro identified 356 domain names exhibiting this behavior; sites associated with salacious content and bogus search pages/engines. All domain hosts appeared to be hosted by the same Ukrainian company, Inhoster. With only a quick search-engine query, a lot of negative information is learned about Inhoster, which is nicely summarized in the following quote from a Spam forum:

*"Inhoster is a spam, malware, phishing and bot-friendly Ukranian hosting service. I got hammered last week from bots with IPs in the Inhoster blocks." –Forum Member at <http://www.vbulletin.org/forum/archive/index.php/t-115417.html>.*

With respect to the 356 domains we identified, we were able to obtain domain registration information for 291 of them. Of these 291 results, there were only four unique registrations. Further examination

identified that there were only two major participants. What was curious is that of the two minor participants, their surnames are suspiciously similar despite one registration in London, and the other in the former Soviet Union.

Domain Name: DZTALK.COM

Registrant:  
Pupkindt LTD  
Vsevolod Pupkindt  
33 Hogarth Road  
LONDON  
London, SW5 0QQ  
GB  
Tel. +44.438674593548

Domain Name: WSEXI.COM

Registrant:  
Pizdataya Compania Inc.  
Vasiliy Pupklindtovich  
Grlrznh Drovosekov 15  
Urupinsk  
null,195156  
CC  
Tel. +91.4896785423

Historically when there is a many-to-one relationship of sites to a single malicious site, there is a link inserted into the pages that link to a different site hosting an exploit. In most cases, the sites which are attacked have had their Web hosting login hacked one way or another. This differs from our example in that the 300+ sites we reference did not have any content on their own and forced the browser to switch URLs through redirection—a non-malicious capability on its own.

### Example Two

During the week of November 6th, X-Force researchers identified that a hosting provider had one or more servers compromised to facilitate browser exploitation. In this case, the method of action was novel and interesting. All that was required was for a victim to go to an invalid URL path on a domain hosted by a compromised system.

Normally, a "404 Error" will be presented to the user to explain they have attempted to reach an invalid page. What we observed was that the "404 Error" contains a link to malicious JavaScript which will then be executed by the browser without the user knowing. Tricky, eh? There's more.

First, the JavaScript link is created dynamically, so once it is visited, it is invalidated. Similarly, once you have been served one of these malicious links from one 404 message, subsequent invalid requests produce non-malicious 404 messages. Secondly, the filename for the JavaScript is random so it is clear that the exploit writers did not want the file to be an easy to track static JavaScript page. Third, the actual (malicious) JavaScript page features

obfuscation techniques, though it is not dynamically changed each time the page is generated. The malicious JavaScript contained two exploits:

- DevStudio2005 ActiveX WMI Broker (which contains classids that were vulnerable prior to MS06-014), and
- IE ActiveX DirectAnimation.PathControl Overflow.

Curiously, there is a reference in the exploit JavaScript code to a PHP counter on a different site. It is a realistic assumption that whoever is monitoring the counter information is involved. After visiting the domain from a non-X-Force IP address, it gives the impression that the registrar could be involved as the index page doesn't post any data back, so the site is live but "locked down." This activity would be highly unusual for hacked accounts. Similarly carded accounts—carded accounts being those paid with stolen credit card numbers—are unlikely to go through this trouble. It is expected that at least the registration name is bogus.

## Results

What we've observed in the first example is a mass redirection of junk Web sites owned by only a few people to a single malicious host. In the second example we've explored a compromised Web host that is surreptitiously facilitating Web browser exploitation. Both methods of attack are significant because they highlight the increasing complexity by which Web browser exploitation is being architected. While the techniques discussed might be infrequently seen moving forward, we can unfortunately expect consistent innovations from attackers moving forward in the realm of Web-browser attacks.

— Robert Freeman, X-Force Adv. Researcher

---

## Switch Security

### Insertion of Inappropriate Technologies

Ethernet switches are a very old technology and many computer security professionals assume that there is nothing new to learn about them and not much to know in general. Unfortunately, X-Force believes that this ambivalence creates a false sense of security that leads network engineers to rely on switches to perform certain security tasks without putting a lot of effort into ensuring that their switches are secure. It's important to understand that switches are not designed to be security devices, and many general operational properties of switches that engineers rely upon may not work correctly when under pressure from an attacker.

The most important assumption that many network engineers make about Ethernet switches is that you

cannot sniff traffic on a switched network. Nothing could be further from the truth. In general, unlike Ethernet Hubs, switches do not broadcast each packet to all of the hosts on the LAN. However, under pressure from an attacker, the situation changes.

Switches contain a MAC address table that maps Ethernet MAC addresses to switch ports. Every time a packet arrives at a switch, the switch checks the destination MAC address against this list to determine which port to forward the packet out of. By spoofing a large number of randomly-chosen source MAC addresses to a switch, an attacker can fill up this table. Switches are designed for performance, and the switch allows a fixed, limited amount of time to check this MAC address table prior to forwarding a packet to its destination. If the switch is not able to search the entire table in time, it will begin to act just like a hub, forwarding each packet out of every interface.

A tool, called 'macof', which performs this attack is openly distributed on the Internet as part of the 'dsniff' toolkit. Some new Ethernet switches offer features which can help mitigate this threat. For example, the Port Security feature in Cisco Catalyst switches limits the number of MAC addresses that can be associated with a single Ethernet interface.

ARP cache poisoning is another way to sniff traffic on a switched network. By spoofing ARP responses, an attacker can get in between any two other systems on a LAN, including a host and the router. From there, all traffic can be viewed and manipulated, and man-in-the-middle attacks can be performed against cryptographic key exchanges. Tools which perform this sort of attack, such as dsniff and Cain & Abel, are widely available on the Internet. The attack vector is difficult to mitigate. One tool called ArpWatch, a miniature IDS system for ARP cache poisoning, is freely available. Cisco switches have a similar feature called ARP Inspection. A Proventia<sup>®</sup> IDS system attached to the LAN will also detect these attacks and fire the IP\_Duplicate protection decode.

In addition to relying on switches to prevent network users from viewing each other's traffic, network engineers often also rely on VLAN technology in switches to isolate one network from another. Figure 1 is a network diagram for a typical "three legged stool" network architecture found in offices everywhere. The Internet and internal network are separated by a firewall, which also connects a "demilitarized zone" LAN containing Internet-facing services such as mail and Web servers. The firewall acts as a traffic cop between these three networks, preventing Internet systems from connecting deep into the internal network, even if public hosts on the DMZ are compromised.

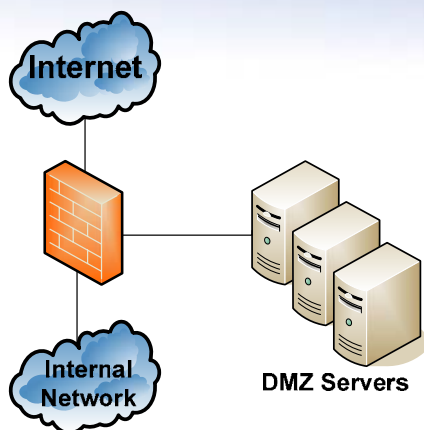


Figure 1

Unfortunately, this network requires three different switches and a lot of wiring to construct. Many network engineers are fond of replacing this architecture with a central VLAN switch as shown in figure 2. The Internet, DMZ, and internal network are all connected to a single Ethernet switch on different VLANs. These VLANs are 'trunked' across to a firewall which serves as a Layer 3 traffic cop between them. What's important to observe about Figure 2 is that the Ethernet switch has now become the keystone upon which the security of the entire network rests. This can be a dangerous configuration, as unlike the firewall, the switch is not designed as a security device.

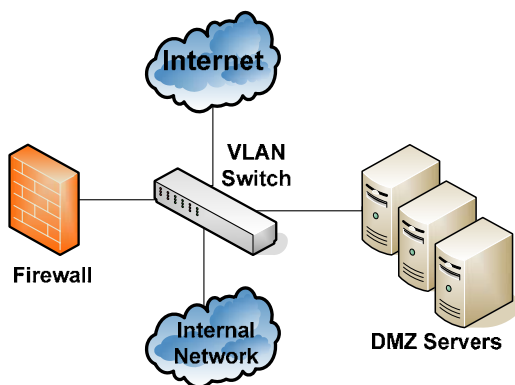


Figure 2

There are a number of techniques that can be employed by an attacker to hop between VLAN'd networks. The most obvious is to attack the switch directly. Advanced switches often run a plethora of network services, many of which continue to have remote code execution vulnerabilities. Furthermore, older switch firmware may contain known weaknesses that enable attackers to leak packets between VLANs. Have you shut down unused management services, Ethernet features, and protocols on your switches? Have you used access lists to limit the networks that can connect to these services? Are you running the latest version of your switch's firmware? Often the need to avoid network downtime makes it challenging for network

administrators to upgrade switch firmware when vulnerabilities are disclosed, in particular for switches that sit in the core of the network where exposure is greatest. This can create a "Catch-22" situation for networks that rely too heavily on switch technology to protect them from attack. These devices become the keystone of a network's security, and yet they cannot be easily upgraded to mitigate vulnerabilities!

Ethernet switches, and associated technologies like VLANs, are powerful tools that have enabled great scalability for corporate networks, as well as new technologies like Voice over IP. However, it is critical that network engineers who employ these tools to solve security problems do so with a good understanding of the risks, as well as solid deployment configuration guides and emergency firmware maintenance plans. Finally, the relative costs associated with the maintenance of switches that perform VLAN-based security isolation versus the deployment of networks with physical air gaps should be seriously considered before new infrastructure is constructed.

– Tom Cross, X-Force Adv. Researcher

## Shattering Records

### It's Beginning to Look a Lot like Christmas

You may think it's too early to start thinking about the holidays, but hidden amid all the holiday planning – who to buy gifts for, what gifts to buy, who to send Christmas cards to, what to have for Christmas dinner, is the bar stocked? – we think you should add one more thing to your list – vulnerabilities!

Vulnerabilities? That's right. Santa isn't the only one gearing up to bring gifts. Attackers around the world are wrapping up all kinds of vulnerabilities in pretty packages and hoping to make an early delivery to a computer near you! The X-Force Vulnerability Database analysts have been busy studying data and have found that the busiest week of the year for the release of new vulnerabilities is actually the week before Christmas.

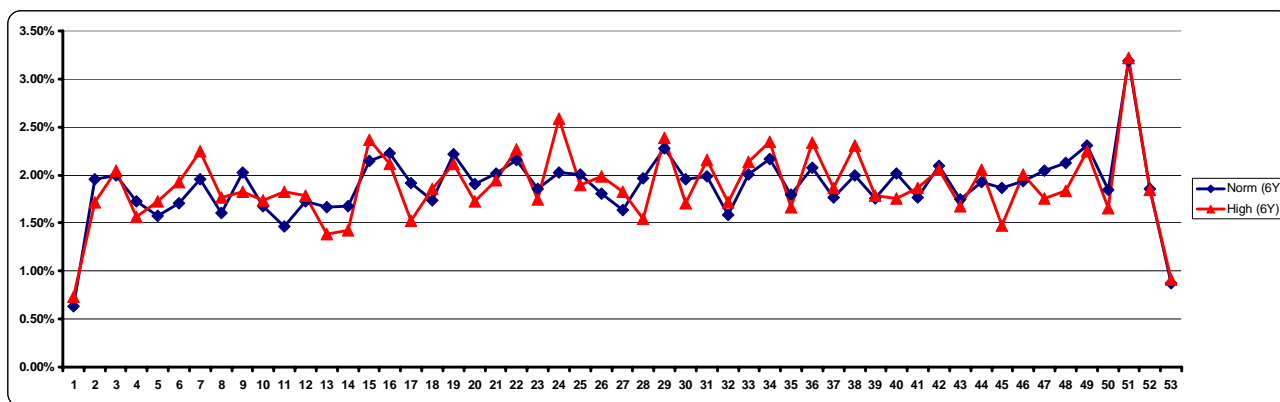
### Trends Analyzed

With the X-Force Vulnerability Database dating back to 1997 and covering more than 30,000 vulnerabilities, it is possible for us to examine vulnerability trends over the past nine years. X-Force vulnerability analysts queried our database to find the number of vulnerabilities released during each calendar week since the beginning of 1997. Once the number of vulnerabilities was determined for each week per year, the weekly number was divided by the total number of vulnerabilities for that year, giving the team a percentage to study. A trend was

soon discovered. Since the year 2000, the number of vulnerabilities has significantly increased during Week 51, which is the week before Christmas.

### Results of data

The following chart illustrates that the number of vulnerabilities disclosed is of a greater percentage during the week before Christmas than any other week of the year (based upon a normalization of the previous six years of data [Blue], and compared with similarly normalized high impact vulnerabilities [Red]).



With a closer examination of the data, this trend starts to develop in 2000, with the percentage showing a slight up tick; 2.7% of the annual vulnerabilities were disclosed during Week 51, the week before the holiday, compared to 2.5% in Week 49 and 2.5% in Week 50. By 2003, the percentage of vulnerability disclosure rises to 2.3% of the year, compared to 1.4%, 1.7% and 1.8% in the three weeks prior. The trend is very prevalent in 2004, with 187 vulnerabilities being disclosed in Week 51, 5.4% of the total number for the year. Over the weeks preceding Week 51, the team logged in only 56 (1.6%), 65 (1.9%), and 45 (1.3%) vulnerabilities in Weeks 48, 49, and 50 respectively. In 2005, the rise in disclosed number of vulnerabilities continues, with 4.0% (191) of the vulnerabilities for the year being disclosed. Weeks prior to Week 51 are 135 (2.8%), 128 (2.7%) and 105 (2.2%) in Weeks 48, 49, and 50. Week 51 of each year is highlighted in both the Actual Number of Vulnerabilities table and the Percentage of Annual Vulnerabilities table below:

Week	1997	1998	1999	2000	2001	2002	2003	2004	2005	Total
47	3	15	12	35	32	46	44	69	110	366
48	1	4	20	38	39	44	38	56	135	375
49	4	10	34	34	38	69	48	65	128	430
50	1	18	13	34	21	49	51	45	105	337
51	5	8	13	36	39	60	65	187	191	604
52	2	13	26	31	23	19	31	89	143	377

Actual Number of Vulnerabilities

Week	1997	1998	1999	2000	2001	2002	2003	2004	2005	Total
47	1.3%	4.5%	1.5%	2.6%	2.0%	1.7%	1.6%	2.0%	2.3%	2.2%
48	0.4%	1.2%	2.5%	2.8%	2.5%	1.7%	1.4%	1.6%	2.8%	1.9%
49	1.8%	3.0%	4.3%	2.5%	2.4%	2.6%	1.7%	1.9%	2.7%	2.5%
50	0.4%	5.4%	1.6%	2.5%	1.3%	1.9%	1.8%	1.3%	2.2%	2.1%
51	2.2%	2.4%	1.6%	2.7%	2.5%	2.3%	2.3%	5.4%	4.0%	2.8%
52	0.9%	3.9%	3.3%	2.3%	1.5%	0.7%	1.1%	2.6%	3.0%	2.1%

Percentage of Annual Vulnerabilities

Averaging the percentages of Week 51 over the nine-year history of the X-Force Database shows that in Week 51, there is an overall increase in new vulnerability disclosures of 2.8%. That may not seem like a lot, but consider that 2.8% is the average over nine years. In the first three years, 1997, 1998 and 1999, the trend does not exist. More recently, the trend has really become apparent. In 2004, there was an increase of 5.4% while in 2005, the percentage reached 4.0%. In both 2004 and 2005, these percentages were the biggest increases in new vulnerabilities for the entire year!

### Why?

The reasons why we see a spike in vulnerability activity during the week before Christmas is not easy to pin down. It could be that "bedroom security warriors" and script-kiddies armed with their favorite 'Fuzzers' are out of school for the holiday and have more time to finish and publish vulnerability research. Corporations may also wish to release disclosures for vulnerabilities they have just patched prior to the end of the calendar year, essentially clearing out their pipelines before the Christmas festivities begin. It may also be that hackers wish to get a few last vulnerabilities published before the end of year to establish annual bragging rights. It could even be that these wannabe security researchers are given new systems and tools as early Christmas presents, and they are eager to try them out!

Whatever the reason, the X-Force Database analysts expect the trend to continue. Already in 2006, we have witnessed the biggest year in vulnerability disclosure. At the end of October, the team had analyzed and recorded 5,967 vulnerabilities, a 43% increase over the same time period in 2005. And there is no evidence that the number of vulnerabilities to be released in Week 51 will decrease. If the average spike in vulnerability disclosure from the year 2000 (3.3% of the annual total) is applied to the number of vulnerabilities through the end of October for 2006 (5,967), we're looking at approximately 197 vulnerability disclosures during the week before Christmas!!

## Have a 'Safe' Holiday

This alarming progression of new vulnerability disclosure brings new meaning to the phrase "Have a Safe and Happy Holiday Season." You might want to ask Santa for an early Christmas present – perhaps some elves to help you with your patching? With such an influx of new vulnerabilities, it is imperative that companies staff adequately during this holiday period. Traditionally, this is a week of long overdue vacations and time off. Our customers should be aware that the week before Christmas is the highest concentration of newly released vulnerabilities, and should try to plan their resources accordingly. It's one more thing to add to a long list of holiday activities, but a vital one. Stay staffed and stay safe!

– Luann Johnson, X-Force Manager

## 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 October.

### Vulnerabilities:

Compared to October 2005, X-Force researchers identified, catalogued and analyzed 54 percent more vulnerabilities.

Overall, thus far in 2006, X-Force has covered 43 percent more vulnerabilities over the same period in 2005.

	Reported					YTD
	Crit.	High	Med.	Low	Total	
<b>OCT</b>	0	109	408	150	<b>667</b>	<b>5967</b>

Of these vulnerabilities, 551 were remotely exploitable, 122 could only be exploited locally and six could potentially be exploited both remotely or locally.

Vulnerability Breakdown	
<b>Bypass Security</b>	<b>12</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>62</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>50</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.

**Gain Access** **379**

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.

**Gain Privilege** **19**

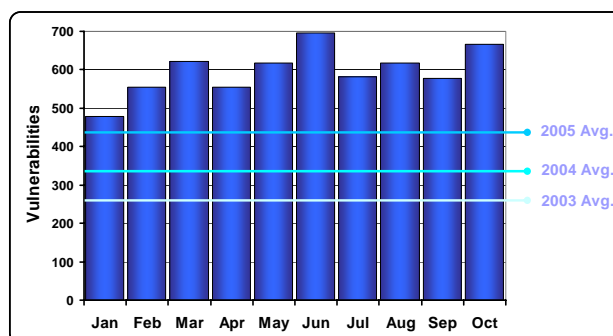
An attacker can gain privileges on the local system only.

**Obtain Information** **48**

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

Oracle	<b>101</b>
Microsoft	<b>27</b>
PhpBB	<b>13</b>
Apple	<b>9</b>
HP	<b>8</b>

\* Right-hand column represents unique vulnerability count

### Malcode:

October was an interesting period for Malcode, with particular threats such as Stration and Haxdor taking the limelight. In this month's newsletter, we take a closer look at these two threats and how X-Force's "Catfish" research project identified and tracked them.

#### The Strations

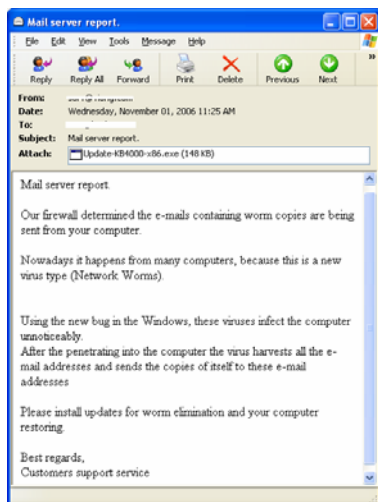
On October 1, Catfish had seen another major serial variant attack of W32.Worm.Stration. This attack lasted for 24 hours and totalled 61 variants, averaging around two-to-three variants per hour. Each variant differs just slightly from the other. Some of the differences we uncovered include:

- The download URL which points to additional malcode changes.

- The name of the dropped file changes.
- Most of the time, the decryption code for internal strings changes.

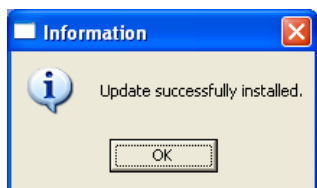
We can speculate that (1) the malcode author is very diligent and has time to manually generate multiple variants or (2) the malcode author has several code generating techniques (via C macros, scripts, etc.) to quickly generate new variants.

Additionally, these newer Stration variants also send themselves in an e-mail spoofing a software patch, enticing innocent users to execute the attachment:



(E-mail spammed by Stration spoofing a software patch)

Once the user executes the attachment, the malcode will then show the following message box, saying the update (worm) was successfully installed.



Update successfully installed.  
(Meaning... "Worm successfully installed")

October 18 was another milestone for the Stration family of worms. This time, Catfish received six new variants of Stration. However, these new variants did not have a mass-mailing engine. So, how do these variants spread? They spread by spamming a downloader; this downloader is the one responsible for downloading and executing the main worm on the affected system and then the cycle continues.

This technique is used by some variants of notable worms such as the Bagle family of worms. There are several reasons why the author has done this:

- The Stration downloader differs greatly in terms of code appearance against Stration worms, hence, pattern/heuristic-based AV scanners will initially fail to notice them.
- The downloaded worm can be updated anytime by the malcode author.

An article in *InfoWorld* magazine describes these Stration attacks and how they are causing headaches to AV vendors. Below is a snippet from the article:

*"In the past, malware has been known to create variations of itself, but the code to create those variations was contained inside the malware. So when a sample was obtained, security analysts could study it and identify potential new versions, he said.*

*Now, the hacker's program is compiling the code and rapidly churning out new versions, but analysts don't know how the new code is generated.*

*That characteristic is a headache for security software firms that issue special updates to their software to detect the malware. F-Secure alone has issued at least 150 signatures for the malware.*

*It gets very complex to detect an attack like that because the code keeps changing Hypponen said."*

[http://www.infoworld.com/article/06/10/30/HNtrickynewmalware\\_1.html](http://www.infoworld.com/article/06/10/30/HNtrickynewmalware_1.html)

Certainly, the answer to this headache is behavioral detection which operates on a simple premise: as long as it does "bad things", then, it is bad.

### Haxdoor

While searching the string "37679041.zip" in Google, it returned a forum with someone posting this (on October 10, 2006 at 18:49):

Got this in my email today:

"Dear Customer,

Thank you for ordering from our internet shop. If you paid with a credit card, the charge on your statement will be from name of our shop.

This email is to confirm the receipt of your order. Please do not reply as this email was sent from our automated confirmation system.

Date : 08 Oct 2006 - 12:40

Order ID : 37679041

Your Order Summary located in the attachment file ( self-extracting archive with "37679041.pdf" file ).  
<snip>

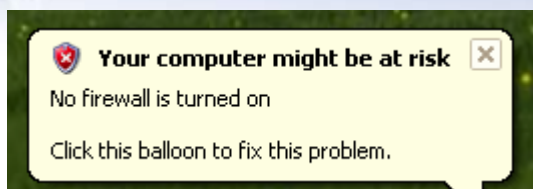
We hope you enjoy your order! Thank you for shopping with us! "

The attached file wasn't a .pdf file but a file marked "37679041.zip" (and no, I didn't open it).

The user makes an excellent decision not to open this message, because if he did, he would have been 'rooted' by Haxdoor.

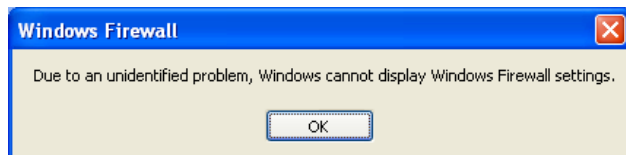
Catfish caught a sample of W32.Backdoor.Haxdoor.AU on October 10, the same day the person posting the message did. The Haxdoor family of Trojans is known for its rootkit capability in addition to its backdoor and password-stealing capabilities.

Now let's change the scenario. This time, the person who received the spam did execute the attachment (Haxdoor) on his system. What would happen? Well, the first thing he would notice is that Windows will show a notification stating that no firewall is turned on.



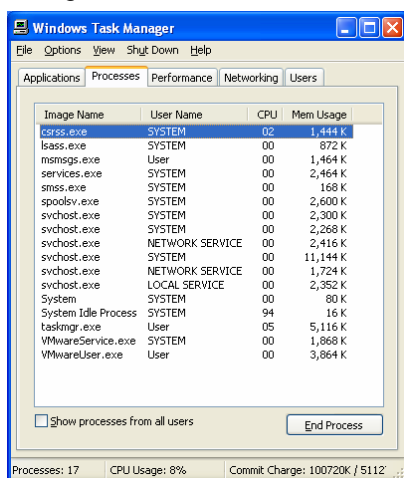
(No firewall turned on. This is bad...)

But unfortunately, it cannot be easily turned on, because the malware deleted some registry entries used by the Windows Firewall and Security Center service which causes these services to fail to start.



(Can't configure firewall. This is really bad...)

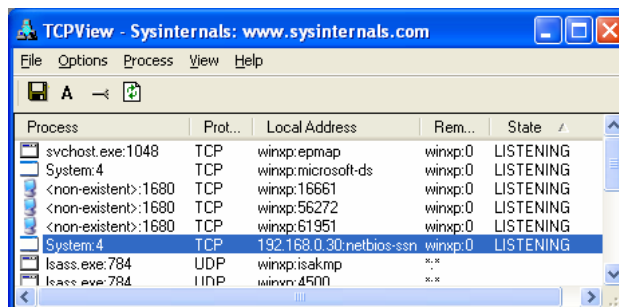
Another less obvious problem that he would notice is that Explorer.exe and Winlogon.exe are not listed in the task manager!



(Where did my Explorer go?)

Hiding Winlogon and Explorer was part of the malware's rootkit capability. The said processes have been injected with malware. What a nice way to hide the malware by hiding the processes hosting it? Additionally, its rootkit capability allows it to hide the malware dropped files. The malware achieves this by modifying the SSDT (System Service Descriptor Table), which allows it to hook system calls and then return tainted results.

Now that the malware is installed, it can perform its mission such as harvesting passwords, turning the system into a proxy (which in turn can be used to relay spam and other attacks), and running a backdoor (which allows complete control of the affected system, allowing downloading/executing of files, etc.).



(Locked and loaded. Hidden explorer.exe listening on three TCP ports)

Above is the screenshot of a hidden explorer.exe listening on three TCP ports. TCP Port 16661 is for the backdoor port. The next two TCP ports are randomly selected and they are for HTTP proxy and SOCKS connections. These ports and other information are reported to the attacker by sending the information to a remote server via Web request to a PHP script.

October 11, 2006 (ZDNet.co.uk)

*"The Metropolitan Police have revealed that cybercriminals used a particularly malicious piece of malware called the Haxdoor Trojan to steal data from thousands of UK users."*  
<http://news.zdnet.co.uk/security/0,100000189,39284024,00.htm>

### 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 49,462 new samples to our malware 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.