

Subeil Shahryar, VeriSign

Introduction

2005 is the year when Internet crime came of age, the distinction between the attack types began to blur and hackers' targets became more focussed.

2005 saw the most computer security breaches ever, subjecting millions of online users to potential identity fraud. According to a report published by USA Today on 29 December 2005, over 130 major intrusions exposed more than 55 million Americans to the growing variety of fraud as personal data like Social Security and credit card numbers were left unprotected. The US Treasury Department said that cyber crime has now outgrown illegal drug sales in annual proceeds, netting an estimated \$105 billion in 2004.

In this chapter, we take a close look at the top threats and trends of 2005 and establish a forward look at 2006, including:

- the evolution of Internet crime;
- key security threats of 2005;
- key security vulnerabilities of 2005;
- the business of Internet criminals;
- security concerns for 2006.

The information presented below was gathered from VeriSign's iDefense Weekly Threat Reports, VeriSign's Internet Security Intelligence Briefing® reports, and security news feeds from the Forum of Incident Response and Security Teams (FIRST) issued during 2005.

VeriSign's reports provide comprehensive and actionable intelligence related to cyber security threats and vulnerabilities. Originating from a multi-lingual network of hundreds of research contributors in over 30 countries, the reports offer an early and unique insight into the cyber underground and previously unknown software vulnerabilities. This insight allows key decision makers in the largest financial services firms, government agencies, retailers and other large enterprises to take action in response to threats on a real-time basis.

The evolution of Internet crime

In the 1970's, the word "hacker" applied mainly to benign or ethical computer scientists conducting intrusion experiments to protect sensitive information held in US military computer systems. In the intervening three decades, the evolution of computer crime can be mapped as follows:

- **1980's Hacker Culture:** Mostly harmless, rarely malicious hacking;

- **1990's Internet Vandals:** Mostly attention seeking juvenile delinquents, often malicious, rarely for monetary gain;
- **2000's Professional Internet Crime:** The juvenile delinquents have grown up.

Looking more closely at the progression of means, motives, and associated attacks over the past few years, we observe a change from notoriety to criminal gain; from uncomplicated to refined; and from single to multi-component attacks. We can profile the evolution of Internet crime from 2003 to 2005 and beyond in terms of the most notable characteristics and events for (and predicted for) each year:

- **2003 – Year of the Worm:** Notoriety is fashionable amongst hackers; the dawn of code for cash emerges; and Microsoft's Bounty programme is established;
- **2004 – Worm War and Criminal Code:** Bounty programme curbs notoriety hackers but hardens criminal gain attackers; hundreds of malware variants are released and equally abundant source code releases issued as a legal defence;
- **2005 – Year of the Bot and Ad/Spyware:** Criminalisation and commoditisation become well developed; attacks become more targeted, with espionage and hacker for hire markets escalating rapidly;
- **2006 – Threat of the Unknown: Stealth for Survival and Legal Battles:** Windows rootkits will see increasing use by hackers; and guerrilla warfare tactics will be employed for criminal gain.

Key Security Threats of 2005

The Top 10 Attacks

Table 1 lists the top attacks seen by VeriSign between July and September 2005. Once again, SQL Slammer traffic dominates the list of attacks seen against VeriSign's Managed Security Service customers. Attacks against network and security products through protocols such as IMAP, SMTP, SSL and IPsec also made the Top 10 list each month. Attempts to access the SQL Administrator account without a password were seen on many monitored networks. Finally, worm traffic and email viruses rounded out the list.

Table 1: Top 10 Attacks Seen by VeriSign from July through September 2005

Rank	July 2005	August 2005	September 2005
1	MS-SQL version overflow attempt	MS-SQL version overflow attempt	MS-SQL version overflow attempt
2	SSLv3 invalid Client_Hello attempt	SSLv3 invalid Client_Hello attempt	SSLv3 invalid Client_Hello attempt
3	PCT Client_Hello Overflow attempt	PCT Client_Hello overflow attempt	PCT Client_Hello overflow attempt
4	Client_Hello with pad Challenge Length overflow attempt	Client_Hello with pad Challenge Length overflow attempt	Client_Hello with pad Challenge Length overflow attempt
5	Default sa account access	Default sa account access	Default sa account access
6	ISAKMP first payload certificate request length overflow attempt	IMAP PCT Client_Hello overflow attempt	IMAP PCT Client_Hello overflow attempt

7	MS-SQL version overflow attempt	MS-SQL version overflow attempt	MS-SQL version overflow attempt
8	NETBIOS DCERPC LSASS buffer over flow exploit attempt	ISAKMP first payload certificate request length overflow attempt	WORM-NETSKY-P-001
	WORM-NETSKY-P-001	WORM-NETSKY-P-001	Outbound W32.Novarg.A worm
	Outbound W32.Novarg.A worm	SPYWARE:SITE-2NDTHOUGHT	Outbound W32.Novarg.A worm
9	IMAP PCT Client_Hello overflow attempt	WORM-BOBAX-P-001	NETBIOS SMB-DS DCERPC LSASS DsRolerUpgradeDownlevelServer exploit attempt
10	NETBIOS DCERPC LSASS buffer over flow exploit attempt	EXPLOIT ISAKMP first payload certificate request length overflow attempt	WORM-NETSKY-P-001

Figure 1 shows the number and type of attacks over the past twelve months. The average number of new alerts sent by VeriSign each day has increased from approximately 21 alerts to 59 alerts. Most of this increase is due to more new alerts about malicious code such as viruses, worms, bots, and spyware.

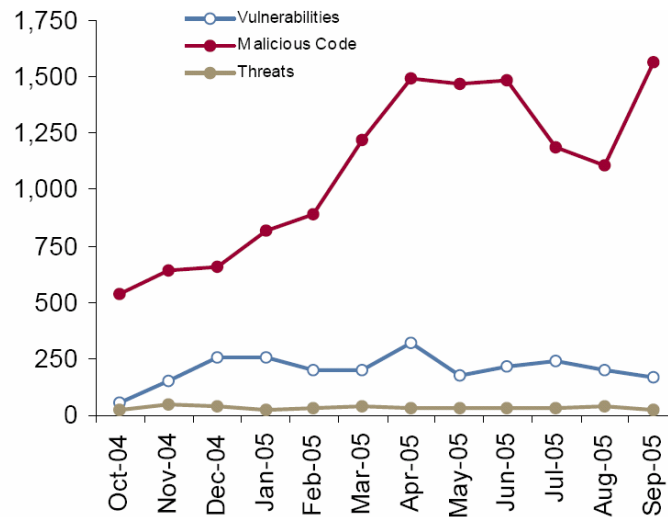


Figure 1: Threats and Trends: October 2004 to September 2005

Figure 2 ranks alerts by priority, giving more weight to vulnerabilities, threats, and malicious software that are likely to cause more damage.

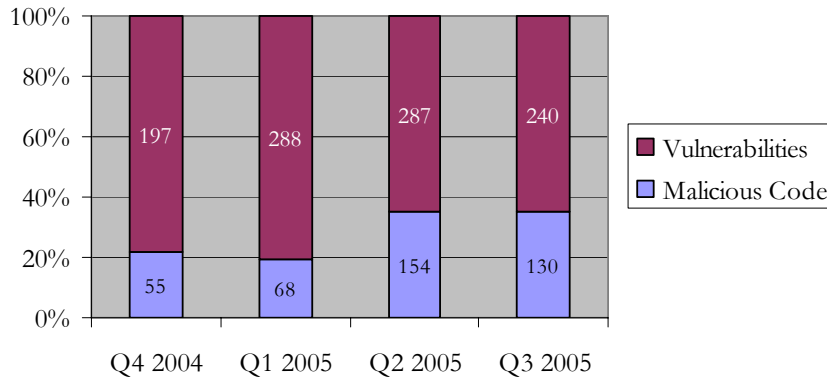


Figure 2: Types of medium and high priority security events per quarter

High Volume of Malicious Code

A huge volume of malicious code emerged in 2005, increasing by nearly 50% from 2004. Most of these, however, were low-level minor variant codes. Figure 3 identifies total number of malicious code reports by VeriSign from January to October 2005:

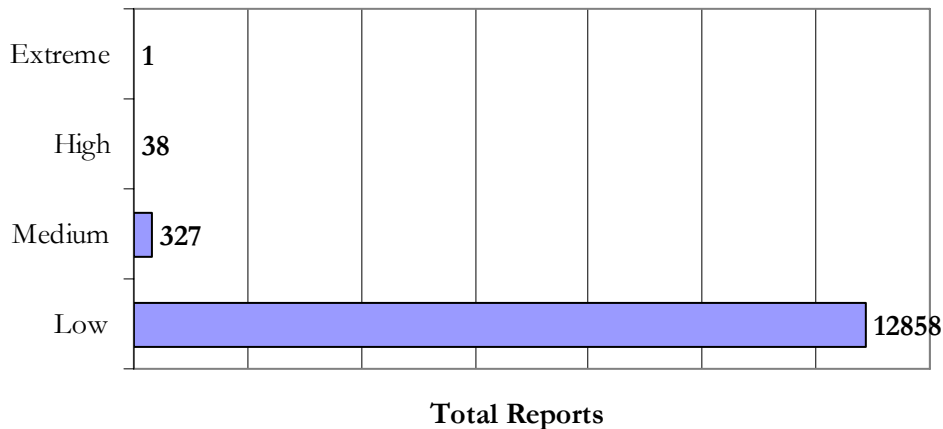


Figure 3: Malicious code reports from VeriSign: January to October 2005

The high volume was partly predicted due to the boom in 2004 in the growth of Internet bots. 2005 was the year of the bots.

Bots are malicious software agents that unknowingly install themselves on people's computers so that they can be remotely used in an attack, such as a Distributed Denial of Service. The advent of cheap broadband connections has made the UK one of the top countries in the world with hundreds of thousands of computers controlled by bots. A recent report by anti-virus company Symantec suggested that 27% of UK computers were already compromised by bots.

Trojans and sophisticated multi-stage attacks – that take advantage of multiple vulnerabilities – were also launched throughout the year.

Although only one VeriSign report, for the rapid Universal Plug-and-Play (UPnP) bot exploitation of MS05-039, was rated as extreme, the regular stream of malicious code events required immediate triage, investigation and risk management effort to keep our networks from being affected.

Our analyses of these attacks show that:

- The source codes for many malicious codes are now available, making it trivial for attackers to quickly create new minor variants of code that are highly functional;
- Bots are increasingly automated and prevalent, resulting in thousands of new variants in 2005;
- Multi-variant wave attacks has proven effective and a popular method of attack with authors of common worms like that of Beagle/Bagle and Sober, e.g. a Beagle multi-wave virus attack which had nine fast-distribution variants spread over 72 hours before the Christmas weekend and were not detected in time by the leading anti-virus vendors, leaving 85% of global users unprotected;
- Trojan authors have continued to create many new minor variants to avoid detection for various attacks, e.g. new Trojans outnumbered Window worms by 2:1
- The advent of adware and spyware has also resulted in the use of many downloader Trojans and minor variants to best launch such attacks without anti-virus detection of the new minor variant.

The Year of Adware and Spyware

Adware and spyware grew into significant problems in 2005. Illegitimate installations of such software exacerbated the situation, creating undesirable performance degradation and breaches of confidentiality for thousands. The increased use of exploits against vulnerable browsers also helped hackers install thousands of illegal adware and spyware applications. For example, in reviewing the top 10 threats, as detected by McAfee signatures over a 30 day period in 2005, adware, spyware and several exploits were all identified in the top 10.

VeriSign examined common adware and spyware applications to discover how they installed themselves on end users' computers. We found that many of these programmes take advantage of the same operating system vulnerabilities. Specifically, we found that the following four exploits are regularly used to install adware and spyware:

- Exploit-ByteVerify
- JS/Exploit-HelpXSite
- Exploit-ANIfile
- JS/Exploit-MHTTRedirect.gen

Somewhat surprisingly, patches for these vulnerabilities have been available for quite some time. The fact that malicious software continues to exploit these vulnerabilities indicates that many end users do not regularly install security patches for their operating system and application software. However, we believe that promptly installing security patches can help prevent infections from spyware and adware.

To address this problem, anti-virus and other vendors are also beginning to offer software that provides some protection against spyware.

From Spams and Phishing to Pharming

Thanks to spam filtering, the number of computers affected by spam attacks during 2005 was less than the previous year. The United States remains the worst offender in the top ten list of source

countries for spam. Together with South Korea and China, they accounted for more than half of all spam. Our analyses show that bot infected computers were the source of over 50% of the spam. This means that the culprits are most likely manipulating these computers from another country to send their spam.

In North America, factors such as jail sentences for spammers, tighter legislation and better system security were also having an effect. On 29 December 2005, the Associated Press (US) reported “Man Pleads Guilty To Worm Attacks Against eBay, Others.

”Anthony Scott Clark, of Beaverton, Oregon, faces 10 years in prison, a \$250,000 fine, three years probation and other penalties for the 2003 denial-of-service attacks against 20,000 computers... According to court documents, Clark and unidentified accomplices used a worm that exploited a vulnerability in the Windows operating system to gain control of the computers. The bots were then directed to an Internet Relay Chat server, where they were given further orders. They were used to launch denial of service attacks against eBay and other businesses in July and August 2003.”

While phishing was the scam of the day in 2004, another more sophisticated method for extracting data called pharming became popular in 2005. Whereas, in a phishing scam, e-mail messages that look like they come from a legitimate web site, such as a bank, are sent to users to lure them into entering sensitive information, a pharming scam redirects users to spoof URLs and is potentially more sinister than phishing because it avoids the need to coax users into responding to junk email alerts.

Pharming is a new name for the well known DNS spoofing attack method, which is based on “poisoning” the DNS cache (or manipulating the hosts file) to redirect users to an attacker’s site. This means even a user who does not follow any link in a phishing e-mail and instead enters the URL by hand can land on the counterfeit webpage hosted on the attacker’s server. While DNS spoofing is rarely a threat to securely configured DNS servers of large ISPs, smaller, privately controlled DNS servers within company networks are especially vulnerable.

Creating Coding for Cash

A new and innovative technique for phishing, suggested at BlackHat 2005, resulted in actual exploitation a few weeks later. It involved Google Adwords exploitation. The attack idea was simple: sign up for Google Adwords as if you are from a known and trusted company, configure the Adwords account and start directing online users to phishing sites. Figure 4 shows how this attack worked, when a consumer queried “digital camera”:

The screenshot shows a Google search for "digital camera". The search bar contains "digital camera" and the search button is labeled "Search". The results page shows "Results 1 - 10 of about 106,000,000 for digital camera. (0.15 seconds)". The first result is a sponsored link titled "Buy Digital Camera" with a URL that has been redacted. The text below the link says "Bargain Prices. Limited offer. Take advantage while in stock!". A red box highlights this text. To the right of the link, the text "Sponsored Link" is circled in red. Below the sponsored link are several organic search results, including news articles and reviews. On the right side of the page, there is a sidebar with more search results, including "Digital camera" from Polaroid, "Cameras at Circuit City", "Digital Cameras" from PriceGrabber, "10% Off Digital Cameras" from BestBuy, and "Compare Digital Cameras" from BuyersEdge.

Figure 4: Phishing attacks using Google's Adwords

This technique causes the consumer to trust both Google and the company represented in the Adwords results, called a "Sponsored Link." However, the actual link is not to the domain listed but to a redirector site that points consumers to one of several possible phishing sites. The phishing sites are designed to look like the targeted company to fool victims into placing an order through the phishing site. Once the phishing has occurred, the consumer is silently redirected to the legitimate commercial website in the category for digital cameras.

Attacks Getting More Sophisticated

In January and February 2005, hackers managed to gain remote access control over multiple servers in various global locations. Servers were compromised through opportunistic vectors, including an AWStats.pl vulnerability. Once the hackers got into the computers, they then leveraged them for a highly sophisticated adware, spyware and malicious code attack. More than 2,000 DNS servers were poisoned and likely millions of consumers silently redirected to hostile websites.

Hostile websites were managed by the attackers who rotated IP addresses at the domain registrar level every few hours and days to avoid shutdown to their operations. The hostile websites attempted to exploit vulnerable versions of Internet Explorer to then silently install up to 20 MB or more of code, 45 or more individual malicious files and up to 17 different malicious code families for just a single silent attack.

The primary motive of these attacks was financial. Unfortunately, this was a highly sophisticated attack that was persistent in the wild for at least three consecutive months before it became largely mitigated.

Keyloggers on the Rise

Keystroke logging (or keylogging) is a software method for capturing the user's keystrokes. Writing keylogging programmes is trivial, and like any computer programme can be distributed as a Trojan or as a part of a virus or worm. The programmes often evade detection by anti-virus tools and can be difficult to detect once installed.

Keyloggers have been around for years and are also sold as legitimate applications, often as monitoring tools for concerned parents or suspicious spouses. However, new keylogging programmes soared higher this year, as part of a wave of multi-function malware with integrated keylogging features. Malicious keyloggers use these programmes to obtain the user's password, credit card details and other sensitive data by stealth.

According to VeriSign's iDefense intelligent network, the number of keyloggers released by hackers has increased by 65% in 2005. The following figure shows the growth of keylogging from 2000 to 2005. In 2005, hackers deployed 6,191 different keyloggers. This is up from 3,753 in 2004 and 300 in 2000, an increase of 2000% over the last five years.

Anti-virus companies have developed signatures that will stop many of those programmes before they can be installed, but new programmes with unique signatures are readily available from malicious code download sites.

Hackers Changing Focus to Applications

As vendors such as Microsoft are beginning to introduce secure development methodologies in their practices, some hackers are turning away from operating systems and focussing their attentions on finding vulnerabilities in applications that run on top of Windows and interact directly with the user.

According to the SANS Institute, where the most critical vulnerabilities of 2004 were associated with Windows and UNIX/Linux operating systems, more than a third of the vulnerabilities in 2005 are in applications.

IBM's survey shows financial applications and online shopping accounts to be the most popular targets for Internet-based hacking. They estimate approximately 90% of hacking is targeted towards web-based applications.

Research firm Gartner estimates that approximately 70 percent of all attacks happen at the application layer and that it is vastly less expensive for all concerned to fix the vulnerabilities during development rather than after deployment.

According to OWASP, the top web application vulnerabilities are invalidated input (including cross-site scripting flaws, injection flaws, and improper error handling); broken access control, broken authentication and session management; and insecure configuration management.

The Problem of Social Engineering

According to Gartner, the greatest IT security threat for businesses is posed by employees. Over 70% of unauthorized access to IT systems is committed by employees. 95% of these attacks result in a considerable financial loss for the company. Gartner identified social engineering as a growing threat to companies.

Social engineering is the manipulation of people using a combination of spying, theft and deceit to successfully breach an enterprise's security. It exploits the helpfulness, gullibility, or insecurity of employees, for example, by attempting to gain access to usernames and passwords of employees of a company by pretending to be a system administrator or security officer on the telephone. By claiming an urgent computer problems and feigning knowledge of the user's department (e.g. names of supervisors, work procedures, etc.), the victim is fooled into revealing the desired information.

The problem of social engineering should not be neglected or left to the IT department. It is important to train and inform staff members regularly in the field of information security.

Key Security Vulnerabilities of 2005

Vulnerability disclosures continued at a high pace for 2005. According to US-CERT, a record 5,198 vulnerabilities in software products were reported this year, nearly 38 percent more than the number of flaws reported in 2004.

About 3,000 malicious codes were discovered in 2005 that exploited vulnerabilities disclosed in 2005. Table 2 identifies the number of malicious codes known to be exploiting specific vulnerabilities, originally reported by VeriSign from January to October 2005:

Table 2: Number of Codes Exploiting Vulnerabilities

<u>Number of Exploit Codes</u>	<u>Vulnerability</u>
1,010	LSASS
447	WebDAV
272	Cumulative Update for Microsoft RPC/DCOM
239	Workstation vulnerability
207	Microsoft ASN.1 BERDecBitString() Buffer Overflow
194	Microsoft Plug-and-Play Buffer Overflow
156	Microsoft Windows DCERPC DCOM Heap Overflow
150	SQL Server
148	UPnP

From January to October 2005, VeriSign published 2,461 new vulnerability reports and re-versioned 11,292 reports. This shows an increased depth of sophistication and analysis required for new vulnerabilities. Improvements in secure coding and vulnerability management has resulted in more difficult vulnerabilities being reported, resulting in more ongoing expert analysis of such threats to an enterprise network.

LSASS ranked as the top exploited vulnerability, largely due to widespread exploitation that occurred rapidly from late May 2004 onwards. This was kicked into high gear when HOD published exploit code to BugTraq. That quickly resulted in Sven Jaschan using the exploit for his Sasser.A creation. More than a dozen new LSASS exploiting families emerged within the following two weeks. Once hackers found this to be highly successful, the code was popularized and shared heavily on the underground, leading to LSASS being the most heavily exploited vulnerability today.

The UPnP exploitation of MS05-039 has that same potential leading into 2006, having been popularized by ZoTob and related bots in the summer of 2005 and striking major networks. LSASS and UPnP auditing should rank as top priorities on any network performing regular audits of network resources for compliance.

525 exploit codes emerged in 2005 from January to October 2005. They ranged from proof-of-concept codes to Metasploit modules and fully functional free standing exploits. Exploits are becoming increasingly automated, when feasible, and therefore more available to hackers. This is similar to the same trend seen with worm generation kits several years ago, until such kits became more private for criminal gain. It is likely that exploitation frameworks and kits will evolve in a similar manner and be leveraged for criminal gain in 2006.

Almost all of the exploits are for Windows. Windows continues to be the most widely exploited platform by malicious code. Attacks are migrating from server-based attacks to workstation attacks. This will force enterprise administrators to make endpoint security a top priority in 2006.

Linux and Macintosh operating systems have not faced significant malicious code threats in 2005. There are basically no existing Macintosh threats in the wild for all of 2005. The few threats for Linux are not significant. F-Secure also makes an interesting observation of this fact by identifying that Macintosh computers used to be one of the primary operating systems infected with viruses in the 1980s, and now is virtually virus-free.

The Business of Internet Criminals

Hackers Marketing Their Wares

Hackers are making use of a wide range of options to make money out of Internet crime. They no longer simply do one thing, but now attempt to leverage any stolen data or resources for cash. They join forces to produce campaigns that coordinate virus, spam, phishing, and spyware attacks, blurring the distinction between them. Hackers are even stealing shipping account numbers for popular shipping companies in an attempt to sell them for cash. This was the case with Diabl0, author of several MyTob worms and ZoTob.

Diabl0 was the brains behind the bot for both MyTob and ZoTob creations. He is a member of the 0x90-team and has been very active in the bot scene for months. His real name is Farid Essebar, an 18-year-old from Morocco. He reportedly sold code to C0der, a 16-year-old Turkish youth. Both are now being investigated for their alleged involvement in a fraud ring. A reporter also disclosed an interview with Diabl0 indicating that he had formerly created MyTob creations as a way to help lower security settings on browsers of infected computers to then make money via adware and spyware. It is clear that Diabl0 and others are making money through multiple venues and are working with others to help move stolen goods and leverage stolen information.

“Hacker-for-hire” is the role Diabl0 was performing when he allegedly sold code to C0der. It is now common to find hacker for hire announcements on the underground. Figure 5 shows a screen shot of a Russian hacker website offering an undetected UnPN bot for sale for \$500.

Продам ТКCFBot, ddos, worm

Подписка на тему | Сообщить другу | Версия для печати

Сафсервис	Дата	Цитировать
<p>Дата: Sep 9 2005, 01:51 AM</p> <p>Бит</p> <p>Профиль: Группа: Members Сообщений: 1 Зарегился: 9-September 05 Проживает: Матрица</p> <p>Рейтинг: < -5 () 5 ></p>	<p>Вообщем судя по всем здешним толикам эти боты становятся интересными.</p> <p>Вот есть приватный бот ТКCF. Продам за 500\$. ТОЛЬКО ЧЕРЕЗ ГАРАНТА!!!! Максимум двум людям!!! Не будем делать из привата паблик</p> <p>Вообщем что он делает -</p> <p>1) ддос - син, удп, ицмп, пинг</p> <p>2) нагон траффа - спец. функция - нагоняет трафик путем захода на дан-ую страницу и гульни по ней - не попадает на другие сайты - тоесть заходит только на страницы в зоне дан-ного домена</p> <p>web-hack.ru - forum.web-hack.ru - web-hack.ru/bleh1 - web-hack.ru/test.html и т.д.</p> <p>(!) Внимание - для слабых сайтов где проблемы с MySQL или с траффом - лучше не испытывать так как сайт может упасть минут на 10 - особенно если большой ботнет</p> <p>3) червь - расплзается через</p> <p>- 1) PnP - очень быстро</p> <p>- 2) Veritas - попадает на много серверов</p> <p>- 3) LSASS/DCOM и остальная классика</p> <p>- 4) Так же брутит пассы для netBios</p>	<p>Цитировать</p>

Figure 5: Posting on Russian Web-hack.ru forum offering bot for sale, \$500 US (9 Sep 2005)

Hackers aren't the only ones seeking to profit from Trojans and stealing of sensitive information. Operation Horse Race in the spring of 2005 revealed a group of individuals targeting 80 specific companies over a period of 18 months. A private investigation firm paid a programmer to develop custom Trojans undetected by anti-virus companies. Michael Hephreti, a 41-year-old programmer, was arrested for creating codes for about \$3,600 each. To date, over 20 people have been arrested.

The Criminal Value Chain

From the Internet activities of the hackers over 2005, the following criminal value chain emerges:

- 1. Botnet/Zombie Acquisition:** Individual or small groups of hackers after infecting computers with bots (collectively known as botnets or zombies) are selling them on to phishing gangs for cash
- 2. Arm Supplies:** Successful phishing gangs are building caches of sophisticated technology, including phishing tools with full Windows GUI interfaces to improve their productivity over decreasing time windows. Some of these tools have been recovered by police. In some cases, phishing gangs are making use of the hacker for hire schemes.
- 3. Phishing Spammers:** Phishers are also specializing in evading spam filters, e.g. by reducing the number of computers targeted by each spam attack so that the threat would sneak under the radar of anti-spam techniques that measure email volume.
- 4. Carding Gangs:** The phished information is then sold on to specialists in exploitation, including existing organised crime rings

Comprehensive Approach to Internet Crime

To deal with the increasing rise and sophistication of Internet crime, co-ordinated action is required from all the stakeholders, where:

- Organisations need to make their employees aware of the problem and teach them how to prevent, detect, and react appropriately when a security incident takes place;
- Internet/infrastructure service providers and product vendors need to improve the detection of virus, spyware, spam and other malware filters as well as to improve the security of systems software and the applications that run over them;
- Governments, police, lawyers, and regulators need to go after the Internet crime gangs and hackers in a co-ordinated and urgent manner, regionally and globally, and with better resources.

The following is a simple public health guide for Internet users:

- **avoid or reduce** infection by ensuring your personal computer and mobile devices are adequately protected with tools, such as anti-virus, anti-spyware and personal firewalls and keep them daily updated;
- **cure or mitigate** infection without delay and as thoroughly as possible, as soon as you suspect or realise you are infected and, if necessary, take advice from a specialist – a little money spent now may save you a big headache and even bigger expenses in the future;
- **prevent or reduce** the transmission of malware by ensuring all electronic messages are received and sent via approved e-mail/IM gateways with effective anti-spam and other filtering.

Security Concerns for 2006

We expect the types of threats and vulnerabilities described above to continue into 2006. Multi-variant attacks and multi-staged attacks will be a major factor in 2006. With so many opportunistic bots using many different possible exploits, the no single malicious code presents a major threat to a network, but any single code among the masses could prove to be successful in attacking an enterprise network. Concurrently, targeted attacks will become increasingly likely. All of this will drive the growth of the underground market for malicious software and stolen information.

Hackers are expected to go after new types of devices. On the infrastructure side, these may include routers, switches, back-up systems as well as instant-messaging systems and web-based applications. At the user end, cell phones and mobile devices will become more of a target for hacking with the spread of Internet technologies into telecommunications and as financial data climbs onto their hard drives and networks.

The dual drives, on the one hand, for greater interconnectivity and uniformity of networks enabled by the spread of IP-based technologies – everything is getting more and more connected and will be part of a huge web – and on the other hand, for exploiting the growing richness of software and mobility, will provide more exploitable opportunities for threat groups and, at the same time, more vulnerabilities of the complex software to exploit.

We end with an optimistic note. Although terrorist groups have shown themselves to be adaptable and capable learners, physical attacks will continue to be their favoured option and it is unlikely that they will develop the expertise in 2006 to carry out electronic attacks against our financial systems and critical national infrastructures or to affect the Internet in any major way.

Suheil Shahryar is Director, EMEA of Global Security Consulting at VeriSign in the UK.

VeriSign operates intelligent infrastructure services that enable and protect billions of interactions every day across the world's voice and data networks. Every day, we process over 14 billion Internet interactions and 3 billion telephony interactions. We also provide the services that help over 3,000 enterprises and 450,000 Web sites to operate securely, reliably, and efficiently.