Fearsome Beasties and What They Target

Matthew McGlashan
SANS Security Essentials
GSEC Practical Assignment
Version 1.2b

Introduction

The increasing sophistication and complexity of virus development is a matter of great concern for the IT industry and government/business as a whole.

Fighting virus infections used to involve an endless and persistent cycle of scanning all of an organisations' information system assets, all while still monitoring incoming emails and internet downloads. If (or when) an outbreak did occur, it was necessary to co-ordinate a complete power-down and clean process for the desktop environment. Destroyed or infected files were recovered from backups after an attack, and the cycle of scanning started again - business as usual.

Developments in the complexity of virus-generation techniques have made the task of virus defence a far greater challenge than ever before. Previously, virii were catalogued according to payload, propagation, and any stealth techniques. It has now become increasingly difficult to categorise virii under this simple scheme, as the difference between virus, worm, trojan horse program and backdoor has blurred [I-1].

This paper is an overview of the genre of malicious agents. It examines those that require human interaction to be triggered (virii and trojan horse programs) - and those that do not (worms). Thus there are two broad categories that also identify the actual vulnerabilities targeted:

- for virii and trojan horse programs, the true risk stems from exploitation of people - ie those that execute anything - gullibility is essential for these attacks to succeed;
- for worms, the true risk stems not from people (more likely the lack thereof!), but exploitation of vulnerabilities in operating systems and applications.

Following are the *types* of attacks that are executed by malicious agents.

Virii

The Availability Attack: Love Bug (V-1)

The Love Bug is a VBScript-based email virus that spreads via email. It propagates by using Microsoft Outlook and mIRC clients.

Impacts	Vulnerability class
Confidentiality	People
Downloads a password stealing trojan horse program from a particular internet site	Social engineering aspect - people cannot resist the "hook"
Availability	Practices
Effect of propagation technique - affected systems may cause a Denial of Service to other systems or networks and may delete files from the infected system	Default scripting configurations - applications and operating systems automatically running scripts

Overall the Love Bug will be remembered mostly for its massive availability impact. It's effectiveness can partly be attributed to the social engineering aspect and partly attributed to the vulnerability of the default scripting settings of the time. Better examples of confidentiality attack follow.

The Confidentiality Attack: W97M/Caligula (V-2)

W97M/Caligula is a Word macro virus with an attack directed against the popular PGP (Pretty Good Privacy) encryption program. The virus spreads by keeping it's code in a file called c:\io.vxd and possibly the files picture.exe and note.exe

Impacts	Vulnerability class
Confidentiality	People
PGP secret key compromise - the virus locates the secret keyring file of PGP and tries to FTP it to a site in the codebreakers.org domain (was ftp.codebreakers.org and the incoming directory). If the attacker can break the passphrase, they can then open PGP encrypted files sent to this user.	
Availability	Practices
	Weak passphrase for PGP key - passphrases are a weak link in public key cryptography

The Confidentiality Attack: W97M/Marker (V-3)

W97M/Marker (also known as HSFX) is a polymorphic Word macro virus.

Impacts	Vulnerability class
Confidentiality	People
Some variants of it collects the user information from Word and use FTP to send it over the internet. Variants add a log at the end of the virus body for every infected user. This log contains information for system time, date, users name and address. Variant 'C' - tries to upload the logfile to ftp.codebreakers.org. This virus opens up the possibility to create large lists of vulnerable sites - great for a future target-specific attacks. This virus 'recons' for others.	
Availability	Practices

The 'Mutating' Attack: Hybris (V-4)

This virus has the ability to intercept data (including email) that is sent and received and scan it for email addresses. The virus then propagates by modifying the WSOCK32.DLL file to allow it to attach itself to the intercepted email addresses.

The interesting aspect of Hybris is the ability it has to mutate/evolve as the behaviour and function of Hybris depends on plug-ins that are encrypted in the body of the worm. Hybris attempts to connect to the newsgroup alt.comp.virus to post its own plug-ins and download newer versions. These uploadable and downloadable plug-in posts are intended for the running worms to update their behaviour.

Examples of the behaviour of some of the plug-ins are:

- Infecting all EXE files in ZIP and RAR archives; and
- Propagating itself to remote machines compromised with SubSeven

Numerous mutations of this virus have been seen and are continuing to be found.

Impacts	Vulnerability class
Confidentiality	People
Ability to intercept data including emails - plug-ins give potential for increased risk in this area	Social engineering aspect - pornographic-related message and attachments. Plug-ins have increased the effectiveness of this impact
Availability	Practices
Mail servers may suffer increased load as the worm propagates making those servers unstable or unusable - plug-ins give potential for increased risk in this area	Plug-ins give potential for increased risk in this area

Trojan Horse Programs

The Remote Control Attack: NetBus (T-1), Back Orifice 2000 (T-2) and SubSeven (T-3)

NetBus is not really a virus , but a trojan horse program. Some features include open/close the CD-ROM tray once or in intervals, swap mouse buttons, start optional applications, shutdown Windows, reboot, logoff or power off, cause default web - browser to load a URL, key logging, screenshots, update with plug-ins, record sounds that the microphone catch, and full files system access.

Back Orifice 2000 is the new version of the famous Back Orifice backdoor trojan horse program. It was created by the Cult of the Dead Cow group in July 1999. Some features include rebooting, locking up system, listing of passwords, key logging, TCP file sending, adding and removing network shares, process control, full access to Registry, complete file access, and server control (plug-ins).

The SubSeven Windows backdoor was first discovered in May 1999 and is usually distributed under different names via newsgroups and emails. Recent versions of SubSeven come with a server configuration utility allowing it to customise the server. Some features include open web browser to specific address, restart windows, control and configure mouse and keyboard behaviour, record sound from remote microphone and video from camera, operate CD-ROM Drive, alter display resolution, get detailed windows information (version, directx version, etc), server control (password, update, close, start ftp server), ICQ, IRC, e-mail connection, screen capture, flip screen, edit registry, and practically full file system control.

SubSeven is recognised as being the most advanced trojan horse program available.

Impacts	Vulnerability class
Confidentiality	People
Once trojaned - nothing is sacred	Social engineering aspect - usually comes via an infected attachment or newsgroup posting
Availability	Practices
Once trojaned - you are not in charge anymore until you disconnect	Trojan horse servers generally attempt to listen on a non-privileged port - inadequate (or non-existent) firewalls or intrusion detection systems are the threat

Worms

The Fully-Automated Attack: Netlog / Network. vbs(W-1)

Netlog / Network.vbs -Visual Basic worm - When executed, the worm enters in an infinite loop. The worm begins the loop with the generation of random IP class C subnet addresses, scanning for windows file -shares named "C" from each address. If a share is found, the worm maps the remote drive to local machine and copies itself to various areas including the startup directory. This is obviously the infection routine as when the remote machine is restarted, the worm will be executed. Finally the worm takes the next address in the subnet, or chooses the next random IP address and starts again.

Impacts	Vulnerability class
Confidentiality	People
The worm has full access to any documents on the shared directory – potential impact here is high. Also the noise this worm generates soon attracts a lot of attention, all heading your way as everyone will know you have been infected	Functionality over security – users enabling file sharing of their entire hard drive
Availability	Practices
The worm generates a lot of netbios noise when scanning for shares. If enough infected PCs are scanning your subnet then this could cost you a fair amount of bandwidth (and money if charged for traffic by the megabyte)	Procedures (or lack of) allowing inadequately secured Windows installations

The Fully-Automated Attack: Ramen (W-2)

Ramen is a worm which propagates via Redhat 6.2 and 7.0 default installs (although has potential to cross to other linux). It attempts to infect the system by exploiting three known securit y vulnerabilities - found from wu-ftpd, rpc.statd and lpd services. Ramen replaces all "index.html" pages on the system including the web server's, if one is running, with its own (W-1).

It also adds itself to the "/etc/rc.d/rc.sysinit" file causing the worm to be active after the system is restarted. Ramen also makes changes to the system to effectively disable vulnerable services, so Ramen will not infect the system again. Finally the worm will scan random class B subnets for vulnerable hosts and, if such hosts are found, infect them. Variants exist which install a backdoor and a distributed denial of service agent into the compromised system (W-1).

Impacts Confidentiality	**Vulnerability class** People
Key privileged information is available to this worm – eg the password file, ifconfig information. Also consider impact of defacement and scanning on public image	Users often are running services that they do not want or need
Availability	Practices
Obviously when Ramen shuts down the vulnerable servi ce on the RH install those services are unavailable. Also the website, being defaced, is unusable	Procedures (or lack of) allowing inadequately secured OS installations – particularly unpatched and old versions of particular services are a risk

The Fully-Automated Attack: Lion (W-3)

Lion – a worm which propagates via Linux on x86 platforms with unpatched BIND services but could be expanded to other UNIX platforms. Affected versions of BIND include 8.2, 8.2-P1, 8.2.1, 8.2.2-Px and 8.2.3-beta.

The original version of the worm installs a rootkit to hide itself, replacing many system utilities. Newer versions of the Lion Internet worm have the potential for causing much more damage than originally expected. In addition to automatically propagating itself, the worm installs multiple backdoors and the Tribe Flood Network (tfn2k) distributed denial of service (DDOS) tool. The original version of the worm simply propagates and installs a single backdoor. Should the tfn2k tool be activated, all infected machines could be used to perform a large scale distributed denial of service attack.

Impacts	**Vulnerability class**
Confidentiality	People

As for Ramen – key privileged information is available to this worm – eg the password file, ifconfig information. Also consider impact of defacement and scanning on public image	Users often are running services that they do not want or need
Availability	Practices
Lion trojans programs and this means a reinstall and thus some downtime. Being a platform for DDOS means likely network congestion	Unpatched and old versions of particular services are a risk. Lack of IDS or firewall watching for or blocking incoming connections to unusual ports

The Fully-Automated Attack: Adore(W-4)

The Adore worm propagates via Linux on x86 platforms exploiting vulnerable versions of the services LPRng, rpc -statd, wu-ftpd and BIND. As for both Ramen and Lion before it, Adore could quite possibly be altered to infect UNIX platforms as well. Like the other worms, Adore scans Linux hosts to determine their vulnerability (W-4).

The original version of the Adore worm trojaned only one system binary (ps), and moves the original to /usr/bin/adore. It then attempts to mail the following information: /etc/ftpusers; ifconfig; ps -aux (using the untrojaned binary); /root/.bash_history; /etc/hosts; /etc/shadow to external addresses: adore9000@21cn.com, adore9000@sina.com, adore9001@21cn.com, adore9001@sina.com. The worm then runs a binary called icmp which listens for a specific connection, port and packet length before dropping a rootshell to allow connections. The specifics can be configured in the icmp tarball which is part of the worm(W-4).

Adore also sets up a cronjob in cron daily to run and hide itself and reboot - but without removing the backdoor.

Impacts	Vulnerability class
Confidentiality	People
As for Lion and Ramen – key privileged information is available to this worm – eg the password file, ifconfig information. Also consider impact of defacement and scanning on public image	Users often are running services that they do not want or need
Availability	Practices
Trojans programs thus a possible reinstall and necessary downtime. Being a platform for DDOS means likely network congestion	Unpatched and old versions of particular services are a risk. Lack of IDS or firewall watching for or blocking incoming connections to unusual ports

How to Cope

Be wary of hype and irrational fear about virii. If you take a controlled approach to virus protection and control, the risk of damage can be managed (C-1).

Understanding your enemy is vital. Anti -Virus FAQs are a good start for background information, for example - newsgroups such as 'alt.comp.virus' and 'Virus - L/comp.virus' (C-2,C-3). The main anti-virus software vendors also publish wh ite papers and technical tips on virus defence that are worth checking

Common-sense must prevail:
From the FAQs mentioned above (C-2, C-3) key steps are to:

- Stay calm – five minutes of rational thinking will not cause too much more damage but a hasty decision may;
- Try to get expert help before anything else;
- If you are an 'expert', then get the latest information on the specific virus;
- Do not attempt to continue to work with an infected system. Disconnect from the network, consider powering down un til expert help arrives;
- Check other machines/systems connected to the infected computer;
- Do not exchange files between infected and non -infected machines; and
- Get all data devices connected to infected machines and check them all. You may need to consider all data on the infected systems corrupt or untrustworthy.

Prevention is better than cure [C-4]:

Implement a Data Screening Policy:

- Email and document checking - never trust email attachments;
- Foreign Disks - enforce a strict code of practice regarding foreign disks; and
- Downloads / Quarantine - quarantine files downloaded from the Internet.

Anti-virus software vendors offer solutions that have automated: server-side scanning and monitoring of workstations on a network; definition updates; and automated uploads and quarantines of infected files. However, remember that this software is only as good as its current database on new virii. Updates should be done daily or at least weekly.

Also keep your operational systems up-to-date. Anti-Virus vendors expect to release their software for the latest version of operating systems. Be aware of what new trends have been observed of late, for example - virii exploiting new vulnerabilities or insecure application / operating system releases.

Plan for a breach:

Part of any virus-defence strategy should be the Disaster Recovery Plan on restoring data and systems in event of a critical failure from a clean backup [C-1]. Have a virus attack protocol for users to follow, even if that procedure is to simply call a technician / security administrator responsible for dealing with such problems. This does not even have to be specific to virii but can cover any form of security incident.

Damage Control:

Assume all computing resources connected in any way to the infected system may themselves be infected, and then work from the outside-in, eliminating machines from the list as you go. It may seem too obvious to mention, but an effective backup strategy must include some aspect of periodic virus scans [C-2].

Conclusion

Virii, trojan horse programs and worms can damage information systems if left unchecked. These nasties may also impact business with a substantial resources drain if they spread within the organisation. Even if a virus payload is not malicious an organisation must expend effort checking for signs of damage and this in itself is a form of denial of service attack [I-1].

Of the types of attack listed above, the most successful virii and trojan horse programs rely on an extremely enticing "hook" to be executed. What occurs after being executed defines the impact they will have. Hybris demonstrates this by the fact that, while it does not necessarily spread as rapidly as Melissa, but it does have the ability to change the "hook" it uses (by altering the language of its message and the executable name). This allows Hybris to exist for longer in the wild.

For worms, the most successful attacks listed above rely upon exploiting the latest application and operating system vulnerabilities (predominately those in linux).

However, being aware of the latest vulnerabilities and the latest viral outbreaks is only part of a defense against malicious agenst.

Overall protection from fearsome beasties is a matter of:

- implementing safeguard procedures and softw are solutions to help fight infection;
- applying some common -sense risk management including disaster recovery plans;
- a disciplined approach to foreign file screening, and a clearly defined procedure for user to follow if they suspect a virus infection; a nd
- vigilant pursuit of AV-software, OS and other application updates and recent news of vulnerability trends and all forms of malicious agents.

References

Introduction

I-1. McPherson, Mark. "Evolution of the Computer Virus" AusCERT Newsletter Volume 4, Number 1 - March 2000

I-2. Trend Micro's "Virus Primer".
URL: http://www.antivirus.com/pc-cillin/vinfo/vprimer.htm

Virii

V-1 Love Bug
http://www.f-secure.com/v-descs/love.shtml
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=VBS_LOVELETTER
http://www.ca.com/virusinfo/encyclopedia/descriptions/vbsiloveyoua.htm

V-2 W97M/Caligula
http://www.europe.f-secure.com/v-descs/calig.shtml
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=W97M_CALIGULA
http://ca.com/virusinfo/encyclopedia/descriptions/caligulaa.htm

V-3 W97M/Marker
http://www.europe.f-secure.com/v-descs/marker.shtml
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=W97M_MARKER
http://www.ca.com/virusinfo/encyclopedia/descriptions/markera.htm

V-4 Hybris
http://www.europe.f-secure.com/v-descs/hybris.shtml
http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_HYBRIS.B
http://ca.com/virusinfo/encyclopedia/descriptions/hybris.htm

Trojan Horse Programs

T-1 NetBus
http://www.europe.f-secure.com/v-descs/netbus.shtml
http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_NETBUS
http://ca.com/virusinfo/encyclopedia/descriptions/netbus.htm

T-2 Back Orifice 2000
http://www.europe.f-secure.com/v-descs/backori.shtml
http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_BO2K.28672
http://ca.com/virusinfo/encyclopedia/descriptions/backorifice2000.htm

T-3 SubSeven
http://www.europe.f-secure.com/v-descs/subseven.shtml
http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_SUB7.20
http://ca.com/virusinfo/encyclopedia/descriptions/subseven.htm

Worms

W-1. Netlog / Network.vbs
http://www.europe.f-secure.com/v-descs/netlog.shtml
http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_NETLOG.B
http://www.ca.com/virusinfo/encyclopedia/descriptions/vbsnetwork.htm

W-2. Ramen:
http://www.europe.f-secure.com/v-descs/ramen.shtml
http://ca.com/virusinfo/encyclopedia/descriptions/ramen.htm
http://www.sans.org/y2k/ramen.htm
http://xforce.iss.net/alerts/advise71.php
http://www.whitehats.com/library/worms/ramen/index.html

W-3. Lion (1i0n):
http://www.europe.f-secure.com/v-descs/lion.shtml
http://ca.com/virusinfo/encyclopedia/descriptions/lion.htm
http://www.sans.org/y2k/lion.htm
http://www.whitehats.com/library/worms/lion/index.html

W-4. Adore:
http://www.europe.f-secure.com/v-descs/adore.shtml
http://ca.com/virusinfo/encyclopedia/descriptions/adore.htm
http://www.sans.org/y2k/adore.htm

Conclusion

C-1 McPherson, Mark. “Computer Virus Prevention HOW-TO”, AusCERT Newsletter, Vol4, No3 Nov 2000

C-2 Harley, David and Burrell, Bruce. “alt.comp.virus (Frequently Asked Questions)” 23 April 2000. URL: http://www.sherpasoft.org.uk/acvFAQ/

C-3 FitzGerald, Nick. “VIRUS-L/comp.virus Frequently Asked Questions (FAQ) v2.00” 9 October 1995. URL: http://www.faqs.org/faqs/computer-virus/faq/index.html

C-4 Computer Associates. “Virus FAQ - Frequently Asked Questions About Computer Viruses”. URL: http://www.ca.com/virusinfo/faq.htm