When Worlds Collide:
Head Banging in IT Security.

Martin Overton, IBM Global Services, UK

Email: ***overtonm@uk.ibm.com***
WWW: ***http://www.ibm.com/uk***

Tel: ***+44 (0) 2392 563442***

Abstract:

This paper will investigate the differences in the way security issues are approached in both camps (Security and Anti-Virus). This will be covered in the first part of this paper will, and will also include the thorny issues of:

- *Disclosure.*
- *Employment of miscreants (virus writers/hackers).*
- *Issues of trust and accountability.*
- *Ethics (Moral/Professional conduct).*
- *Co-operation with competitors.*

The second part of this paper will look at the new 'Blended' or 'Automated hacking' worms (such as CodeRed, Nimda, Goner and Gokar) and other malware, which are starting to appear. This will require closer co-operation (or strategic partnerships) with others in different camps (AV or Security) to tackle these new complex threats.

This paper looks at the above scenarios/issues, and attempts to answer the questions below that many companies are starting to ask:

- *What benefits will the end-user (customers) see?*
- *How will this affect the effectiveness and size of the products?*
- *Will this co-operation improve end-user (customer) protection?*
- How will this affect the underground (Hackers, Malware Authors)?

This paper was written for, and presented at, the 2002 Virus Bulletin conference at the Hyatt Regency, New Orleans, USA on September 26th – 27th 2002.
I would welcome any constructive feedback on this paper and its content.
(Martin Overton 1st October 2002)

Introduction:

This paper will investigate the differences in the way security issues are approached in both camps (Security and Anti-Virus).

It will go on to examine some of the possible solutions to the so-called 'Blended-Threats' or 'Cocktail-Malware' issue that many believe are a new phenomena. In reality, this is mainly just a case of the malware authors/hackers/crackers working together and re-discovering old techniques and re-engineering them to best fit their personal agendas and causes.

Because of the new partnership between the virus/malware authors and the hacking/cracking communities as well as the rebirth of complex worms and other malware, the usually insular Anti-Virus and Security industries have started to work far more closely together than ever before. This is also due to the blurring of the 'old and distinct boundaries' that used to exist between both factions:

- Viruses/Trojans were considered to be the property of the Anti-Virus industry
- Exploits and hacking tools were considered to be in the domain of the Security industry.

This is no longer the case as the so-called 'Blended-Threats' have broken the 'old' model, as clearly defined by the likes of Nimda which spread like a worm, infected files like a virus, and also contained known exploits for several widely used web server application. To make matters worse it aggressively scanned both private and public IP based networks for new 'hosts' to infect/affect.

Nimda is just one example of these re-born multi-vector threats; other examples include Gokar, Klez, and CodeRed.

1.1 Part One

Part one of this paper will cover the thorny issues of: *Disclosure, Employment of miscreants (virus writers/hackers), Issues of trust and accountability, Ethics (Mora/Professional conduct), and Co-operation with competitors*. Each of these issues will be examined by first looking at each of the camps independently: 1.Anti-Virus and 2.Security (both product and services vendors), I will then cover the so-called 'Middle-Ground', which is an attempt to identify the best/worst of each of the industries, and what each can learn/take from the other to improve their services and products.

1.2 Part two

Part two of this paper will look at the different technologies and methodologies that vendors are now investigating and planning to use to counter these new complex threats.

Furthermore, this section will try to answer the following questions related to solutions to the so-called 'Blended-Threats' or 'Cocktail-Malware':
What benefits will the end-user (customers) see?
How will this affect the effectiveness and size of the products?
Will this co-operation improve end-user (customer) protection?
How will this affect the underground (Hackers, Malware Authors)?

1.3 Prerequisites

Before you continue reading this paper I would suggest that anyone that is unsure of the 'buzz' words and other nomenclature that will be used in this paper, should read appendix A: *Definitions*, which was included to try and ensure that most people can get the best from the contents of this paper.

Part One:

Sarah Gordon stated the following in her Virus Bulletin 1999 paper[i]: "To an outsider, it may come as a surprise that the traditional computer security discipline and the mainstream anti-virus world are not one and the same thing - after all, in many ways, computer viruses and malicious code are just a subset of the more global system security problem. However, currently there is a distinct gap between these two worldviews in several important ways: skill-sets, philosophy, population… the list is long."

That was a reflection on how things appeared to be in 1999. Now in 2002, some three years later, have things changed? If so has the situation improved or degraded? Let's see….

2 Disclosure:

2.1 Disclosure: Anti-Virus

The AV industry does not like full disclosure, as many in it see it as being irresponsible to publish details and exploit code for new holes found in their own products and malicious code generally. Many vendors and researchers are keen to restrict or even block the flow of malware source code and compiled samples, as they believe that access to this 'knowledge' will make the malware problem worse. In the security industry (outside of AV) this would be generally be derided, and simply thought of as 'security through obscurity'.

Knowledge is a powerful tool, but just like most tools it can be put to both positive and negative uses. Does this mean that we should all be only given access to knowledge on a need to know basis? Some would argue that this is the only way to protect civilization; others argue that information should be free.

My own take on this is somewhere in between, there will always be some information that should not be placed in the public domain, how the right balance can be achieved is well beyond the scope of this paper!

However, there have been a number of flaws identified recently (over the last 12 months) in many of the anti-virus products or their management tools which seems to indicate the following:

- Customers are not getting the levels of support and commitment from the vendors that they expect, and major security holes are being ignored by the vendor due to other commercial, management or resourcing pressures.
- Researchers/Miscreants are now spending more time looking at anti-malware products than the usual set of target applications from certain large software vendors (i.e. 'The usual suspects')

To finish this section I'd like to quote from a couple of well known individuals from the anti-virus side, on why disclosure is different for malware than for security exploits:

David Chess of IBM had this to say:
"Unlike bug exploits, where at least a case may be made that it's a valid last resort if a vendor has been notified of a bug and ignored it, viruses don't go away when you just fix a bug.[ii]"

Graham Cluley of SOPHOS had this to say on the subject:

"When it comes to computer viruses there is a very real danger that disclosing too much information (for instance, the virus's source code) will do far more harm than good. System administrators do not need to know the intricate details of how a virus implements polymorphism to try and hide itself from anti-virus products, for instance, in order to protect themselves against the threat.

Disclosing such detailed information may lead to other viruses using similar techniques and creating a greater burden for the anti-virus companies and system administrators alike.[iii]"

2.2 Disclosure: Security

This one is a bit of a mixed bag; some vendors say 'publish-and-be-damned', while most of the others say 'just-tell-us-and-don't-go-public'.

Elias Levy wrote an interesting article about disclosure of security holes[iv], in which he claimed the following: *"One has to surmise then that Microsoft's advisory is just as likely to have triggered the worm* [CodeRed] *as Eeye's*"

This seems to be suggesting that any open (public) posting regarding a new flaw in a product is dangerous as it may be the catalyst for a new worm, attack or other piece of malware. This ties in quite nicely with the proposed and much maligned 'Microsoft Security Partnership Agreement'[v] in which they strongly encourage those that sign-up to it, from publishing flaws which they identify in Microsoft's products. Many attack this proposal as being "censorship" and are planning to boycott it.

My own stance is that full disclosure should be the final step if the vendor refuses to take notice of a serious (and genuine) security hole, and should not just used as an 'ego-trip' for a number of individuals/groups that seem to delight in 'full disclosure' publication. Sometimes, even without (in some cases) informing the vendor whose product is accused of being flawed.

Let us look at this in more detail with a number of example scenarios:

Scenario 1:

- New flaw found in a major web server, the researcher who discovered it contacts the vendor.
- Vendor replies, and requests time to fix the issue and create a security bulletin for its customers.
- Researcher agrees to timescales from the vendor.
- Vendor creates fix and informs customer base via security bulletin.
- End-users patch systems to remove flaw (after testing it of course).
- Problem solved.

End result, a win-win situation, the researcher gets the credit, the vendor gets the time to write and QA the fix, and the customer gets a well tested fix to close the hole and protect their systems.

Scenario 2:

- New flaw found in a major web server, the researcher who discovered it contacts the vendor.
- Vendor replies, and requests time to fix the issue and create a security bulletin for its customers.
- Researcher rejects timescales offered by the vendor and publishes the details on various security newsletters and speaks to the media to get the publicity.
- Miscreants use the information to attack numerous systems.
- Media has a field day, and hypes it as the new "CodeRed".
- Vendor rushes to create a fix and informs customer base via security bulletin (and probably introduces other flaws in the rush).
- End-users patch systems to remove flaw (after testing it of course).
- Problem solved.

End result, a partial-win situation, the researcher gets the credit, the vendor does not get the time to write and QA the fix, and the customer gets a badly tested (if at all) fix to close the hole and protect their systems. Finally, the media panics everyone.

Scenario 3:

- New flaw found in a major web server, the researcher who discovered it contacts the vendor.
- Vendor does not reply, or replies that it does not consider it a security risk.
- Researcher creates proof-of-concept attack code and publishes the details on various security newsletters and/or speaks to the media to get the publicity.
- Miscreants use the information to try and attack numerous systems, most fail.
- Researcher/Media have a field day, and hype it as the new 'major' risk when it is a simple trade-off of security against usability.
- Vendor forced to create a fix and informs customer base via security bulletin.
- End-users patch systems to remove flaw (after testing it of course).
- Problem solved.

End result, a no-win situation, the researcher gets the credit, but effectively discredits them self, the vendor does not get the time to write and QA the fix, and the customer gets a badly tested (if at all) fix to close the hole (which was unlikely to be widely exploited) and protect their systems. Finally, the media starts an unnecessary panic.

One thing to bear in mind with all these scenarios is that some system administrators will in some cases be forced (by their management) to take down services that are suspected of being vulnerable until patches are made available.

In some cases this could be seen as a prudent step, but in cases such as in scenario 3, it would (probably) be unnecessary and may cause disruption for no real benefit. In all cases this type of 'protection' is used in some industry sectors as the 'safe' option, rather than be hacked or infected by a new threat. The bottom line is that such events, whether real or perceived threats cost money, both in lost business/productivity and 'security' staff costs.

2.3 Disclosure: The Middle Ground

Right, now we have investigated the differing ways that disclosure of new flaws in products are handled by both Anti-Virus and the rest of the Security industry, let us see if we can find some middle ground:

- *Security Best Practices!*
  Many of the vendors (from both sides discussed in this paper) have 'best practice[1]' documents, if not for their staff, most do for their customers.

  If they have not yet done so, they should create a set of best practice documents and get their staff trained on them and ensure that they are followed.

  If required (and legally able to do so) staff contracts should refer to these 'best practice' documents and make it clear that they can (and will) be disciplined if they flout them. It could even cost them their job.

- *Tighter control of marketing departments.*
  My feelings on this issue are quite strong, especially with regard to the anti-virus vendors, whose marketing departments used to excel in not only bashing their competitors, but also in hyping many viruses so much that they appeared to have

[1] These are policy and procedure type documents, such as Acceptable Use Policies, Security Policies, Business Conduct Policies, etc.

almost 'mythical' or 'super-powers', or even to be almost 'alive'.

This did not help anyone, especially their customers, who were generally forced to run round doing the 'headless-chicken-two-step' trying to firefight the hype, placate/educate their managers and ensure that the systems they are responsible for are protected from the latest over-hyped '*Uber-threat*[2]'.

Lesser levels of hype outside the anti-virus industry have (in my experience) been more the norm. Yes, there have been some examples (such as Code Red) that contradict the overall 'less-hype' model from the wider Security Industry.

"*… warnings from the US and British governments, the FBI and Microsoft that the internet could grind to a halt when Code Red reactiviated after four days of dormancy…*"[vi]

I wonder where they got the information from[vii]?

The only "serious" connectivity problem seen over that period, was indeed due to a meltdown…..of a cable, in a tunnel, where a train had crashed and caught fire. This melted the cable, which was one of the major Internet feeds between parts of the US[viii]. No code or malware was involved in this accident.

CodeRed was a problem, just not on the scale that was suggested, in other words it was over-hyped by the media.[ix]

- *Common sense approach to 'sensitive' or 'dangerous' data*
  I am not suggesting that certain types of 'security industry' information be made illegal outside that industry, as this would be both dangerous and unworkable. What I am suggesting is that those that put sensitive or potentially dangerous security/exploit/malware data into the public domain do so only after examining their reasons for doing so. And then, only the minimum data should be made public; exploit and other code that can be easily misused should not be put in the wider public domain.

- *Self regulation*
  If the security and anti-virus industries do not regulate themselves and police their own 'back-yard', then some governments, will sooner or later introduce legislation and/or governing bodies in much the same way as they have for other sectors.

- *Closer co-operation*
  As with the anti-virus community of researchers, but this should also be extended to include information about security flaws in a competitor's product[3] (or portfolio of products). We are aware that some security firms have at least one person that 'evaluates' and 'tests' their competitors product set.

  After all, anything that is used to 'tar' one vendor can easily be seen as a potential industry-wide issue, the 'tar' sticks to all in the industry, not just the original culprit.

  This closer co-operation will also help to keep security issues and flaws under the radar of the media, and therefore help to minimize the risk of the 'script-kiddies' and other 'wannabes' exercising their right to 'free-speech' with the latest hole in a particular product.

[2] German for 'Super' and a number of other English words: See here for a good list: http://dict.leo.org/?search=Uber&searchLoc=0&relink=on&deStem=standard&lang=en
[3] This is mainly on the security/anti-virus products themselves, not management tools.

3 Employment of miscreants (virus writers/hackers):

Would the Police employ known or convicted criminals?
Would the fire service employ pyromaniacs?
Would….

Of course not (well, not by design) as although it might well be useful to think like a pyromaniac (if you are in the employ of the fire service) or criminal (in you are in crime prevention/detection) so that you better understand what drives these people (know-your-enemy[4]), and in many cases such understanding can help these professionals catch/stop them or profile them, and to finally apprehend them. But you don't need to be one yourself to be good at that specific job.

So why is it that when it comes to computer security that some companies take the risk of employing those that are known virus authors, black-hat hackers or even those convicted for those types of crimes?

Let us have a look at the relevant industries below, and see if some members still believe that employing such miscreants makes 'good' business sense:

3.1 Employment of miscreants: Anti-Virus

To be a good anti-virus researcher, you require many skills that are sometimes shared by the more talented malware writer; the ability to write and read code (both low and high level code), understand security mechanisms, and how to bypass, break or misuse them.

The AV researcher will need the above and the following: the ability to read disassemblies of executables, including the ability to understand polymorphic and other obfuscated code, encryption (both trivial 'xor' and more complex symmetric/asymmetric[5] systems).

The main difference is the social and moral (ethical) stance differs quite significantly between those wearing the white-hats and those from the dark side! No that doesn't mean that everyone in the AV industry is an angel and haven't occasionally done some questionable things (especially the marketing departments), but they are human (even those in marketing), and humans are flawed.

The bullet points below cover a few well known instances of malware writers approaches to anti-virus companies, I'm sure there are others, but whether they are true or the malware fraternity 'blowing-smoke' to 'obfuscate' and 'muddy-the-waters' is currently unknown:

- Priest/Little Loc (employed by an AV vendor for a while, while his virus NATAS was infecting systems around the world and causing havoc.)[x]
- Onel de Guzman and Michael Buen (Love Bug), two principal suspects accused of making the destructive Love Bug (almost, but not quite, employed by an anti-virus company)[xi].
- Mike Ellison (StormBringer) appealed to the anti-virus community at the Virus Bulletin conference in 1997[xii], where he presented his paper, that he and his cohorts should not be excluded from working in anti-virus just because they wrote computer viruses. His case was listened to, but no one offered him a job.

Certainly the usual line that is trotted out, which is: "Surely the anti-virus companies write

[4] "Hence the saying: If you know the enemy and know yourself, you need not fear for the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." – The Art of Ware (Stanza 18) - Sun Tzu

[5] See here for a reasonable, but non-techie explanation of the difference: http://www.pcworld.com/howto/article/0,aid,15230,00.asp

viruses to keep themselves in a job" is not backed up with any genuine evidence, and is, even if it were true, unnecessary due to the insistence of the malware authors, script-kiddies and other mal-contents in creating and releasing new code/malware into the public domain.

3.2 Employment of miscreants: Security

It seems that outside of the anti-virus industry that it is quite common for firms (especially small or niche players in the market) to be willing (where no other skilled individuals are available) to employ ex-black hat hackers and occasionally even convicted ex-hackers to enable them to offer a security service. The following cartoon appears to be worryingly on the right track as to the current reality of the hiring policy of some security firms.

There are even security firms set up by convicted hackers[xiii].

The larger firms mainly appear to have a strict ethical policy to not employ such individuals, which, when taking into account the size and sensitivity of some of the accounts they perform services for, is both advisable and from a customers point of view, extremely desirable.

Just imagine that an active black-hat hacker (although claiming to be reformed) was to test a large military or financial organizations networks for holes and vulnerabilities and he found a 'major' security hole, where would his allegiance lie? He'd be dying to inform his fellow hackers (on the dark-side) of the flaw, so that he could claim the kudos, and increase his level of respect. But, on the other hand he ought to inform the company that employs him so that they can inform the client…..Decisions, decisions!

3.3 Employment of miscreants: The Middle Ground

Personally, I don't believe there is any middle ground here. If you have been very active in creating and/or spreading malware, or accessing and/or defacing systems you have no authorization to, then you are at least ethically suspect or at worst, ethically bankrupt.

Yes, all of us make mistakes, but if you continue to make the same mistake over and over again (for the kudos, because you know its wrong, etc.) then your ethical 'Armour' is full of holes and rusty. You will also have a hard time convincing potential employers that you have changed your ways, and have now grown-up.

Simply put, if you knew you were doing wrong, and still did it, and did it again, and again

then you must have understood and accepted there are consequences to be paid for your actions?

However, if you make an 'honest' mistake and have learnt from it, rather than keep repeating it, there is a world of opportunity out there, outside the Security or Anti-virus industries.

All intelligent people experiment with technologies, but only a small subset appears to be drawn to being anti-social with regard to their use of computers. This is akin to 'Graffiti Artists' adorning any surface they can, allegedly in the name of Art!

4 Issues of trust and accountability:

4.1 Trust and accountability: Anti-Virus

The levels of trust in the AV industry, at developer/researcher level are not generally hindered by not working for the same vendor. Computer Antivirus Research Organisation (CARO) has a great deal to do with this lack of constraints, and active sharing of both samples and information is common-place, almost certainly to the annoyance of the marketing departments of those AV companies that have CARO members.

CARO - Computer Anti-Virus Researchers Organisation:
This is an invitation-only group of predominantly virus researchers, mainly representing anti-virus vendors. One of the purposes for creating CARO was to try and agree naming standards for viruses, which works to a greater or lesser degree. Another purpose of CARO membership was the need share virus samples in a secure manner. CARO membership was mainly used as a sort-of yardstick by which other members can judge whether an individual can be trusted with samples, very few researchers not affiliated with and anti-virus company were invited to join.

REVS – Rapid Exchange of Virus Samples:[6]
Here's part of the press release announcing the launch of REVS:
"*Sophos Anti-Virus, Europe's leading developer of corporate anti-virus solutions, and The WildList Organization International, the world's premier source of virus information, have today launched REVS (Rapid Exchange of Virus Samples), a ground-breaking new system which will enable members of the entire anti-virus industry to quickly and securely exchange 'urgent' virus samples such as Melissa. This service enables all anti-virus developers worldwide to pool their resources and expertise in the fight to protect end-users from the threat of rapidly spreading viruses.*

Any company that produces an anti-virus product can participate in the REVS messaging service free of charge. The WildList Organization's mission is to provide accurate, timely and comprehensive information about "In the Wild" computer viruses to both users and product developers. The WildList, a list of computer viruses found in the wild and reported by a diverse group of over 55 qualified volunteers, is made available free of charge by the organization. For more information about The WildList Organization, visit http://www.wildlist.org."

The Wildlist Organisation:
Here a quick description of what the wild list organization is and what it does (quoted from the FAQ)[xiv]:
Over the years, antivirus expert Joe Wells has collected reports of which viruses have been found spreading in the real world. He decided to create a list of these viruses and make that list available to the public, free of charge, to offset some of the 'numbers games' played by some antivirus product developers.

[6] http://www.sophos.com/pressoffice/pressrel/uk/20000427revs.html

The list was 'The WildList'. From its humble beginnings in Joe's garage, The WildList has grown into the world's authority on which viruses users should really be concerned with. Used as a basis for testing antivirus software by proficient and competent testing authorities, The Wildlist remains available free to computer users worldwide.

The list is created each month by a team of volunteers, using reports from over 55 antivirus researchers and corporations world-wide.

On the 15th day of each month, the formal WildList is extracted from all verified reports, and published at http://www.wildlist.org. Archives of past WildLists are available in the archive.

Outside the Anti-Virus vendors own closed lists and societies/organizations, there are other excellent groups and mailing lists, such as:

- **AVIEN**[7]**-** This organization is firmly focused on the end-user community, especially those that are responsible for security and/or anti-virus in many of the Worlds largest organizations. They have a number of focused mailing lists, as well as the Early Waning System (EWS) list, which has tipped off its subscribers to a number of new threats before they were identified by the anti-virus vendors. This allowed the to take preventative steps to minimize the impact of these fledgling attacks.

- **focus-virus**[8] – This list discusses the how-to's and why's of the various products, tools and techniques available to help secure the common user from virus threats. This list is meant as an aid to network and systems administrators and security professionals as well as casual users who are interested in the latest developments in virus and anti-virus technologies.

The final issue, which I'd like to cover under this heading, is 'product certification' and 'Awards'. The current certifications and respected award schemes that many anti-virus products can attempt to obtain include:

- **VB 100%**[9]
- **ICSA Labs**[10]
- **West Coast Labs**[11] CheckMark (3 distinct certificates, Level 1 (Malware detection), Level 2 (Malware removal) and Trojan.

This does not include the usual array of magazine awards from the non-specialist trade journals/magazines as to put it bluntly most of them really only scratch the surface and do not usually test the core functions of anti-virus products, which is to detect viruses and other malware.

Most mainstream computer magazines tend to focus on; usability, features and how it looks [look-and-feel]. Those that do test the virus detection capabilities of products tend to use 'simulated or crippled viruses', very few use real verified samples. Those that do test with a suitable test set [both in size of the test set and validated 'real' samples] tend to work with a vendors virus lab, which can lead to 'skewed' or 'biased' test results.

Good, quality functional testing of anti-virus products is not easy to achieve or to maintain. There are a few well-respected companies and educational organizations that have repeatably demonstrated their capabilities of 'doing-it-right'.

[7] Web site for AVIEN (**A**nti-**V**irus **I**nformation **E**xchange **N**etwork): http://www.avien.org
[8] From Securityfocus.com: http://securityfocus.com
[9] Web site for Virus Bulletin: http://virusbtn.com
[10] Web site for ICSA Labs: http://www.icsalabs.com/html/certification/index.shtml
[11] Web site for West Coast Labs: http://www.check-mark.com/cgi-bin/redirect.pl

These include: Those award/certification providers listed above, and the following educational establishments: Universities of Hamburg, Madgeburg (Both in Germany) and Tampere (Finland).

4.2 Trust and accountability: Security

Mainly it appears that the largest and most respected security product/service vendors are concerned about the issues of trust and accountability (of staff, and the quality and service levels for their offerings, both services and products) which is rather worrying as this was the situation with the anti-virus industry during the late 1980s up until around 1995, when things started to improve.

ICSA Labs and West Coast Labs have extended their testing and certification programs to include other technologies other than anti-virus, these include:

ISCA Labs:

- Anti-Virus Software
- Network Firewalls
- IPSec Products
- Cryptography Products

West Coast Labs:

- Firewall
- VPN
- Application Gateway

Outside of the security industry there have been some testing, certification and compliance programs available for some time (mainly from government or standards organizations). These include:

- CLEF (which uses the Common Criteria (CC[12]) which has become ISO 15408).[13]
- ISO17799/BS7799[14]

Security mailing lists are a wonderful resource for those of us that 'do security' for a living. However, the information offered on these lists should be seen as a 'double-edged sword' (that is, the information is not only used by the 'good' guys/gals, but also by those we are trying to keep out of our systems, the 'bad' guys/gals). This 'data-leakage' can even happen on so-called 'closed mailing lists' either accidentally, or by design via a misguided member of the list.

I am not suggesting that 'all information is censored' all I am suggesting that knowledge comes at a price, that price is responsibility.

Some of these mailing lists details appear below, many are offered at no cost:

NTBugTraq
This is the Microsoft NT Operating System specific equivalent of BugTraq.

SecurityFocus.com Mailing Lists:

Below is a list of a number of the mailing lists offered by SecurityFocus, the best known of

[12] See here for details on CC: http://csrc.nist.gov/cc/
[13] See here for more details: http://www-3.ibm.com/security/services/consult-vendor.shtml and here for certified products: http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/index.asp
[14] See here for more details: http://www.bsi-global.com/Business+Solutions/Infosec/index.xalter

these is BugTraq. The list includes a number of 'Focus' mailing lists, which deal with a specific security topic or technology area. Many of these are 'goldmines' of information for the security professional, and of course their nemeses.

BugTraq - BugTraq is a full disclosure moderated mailing list for the ***detailed*** discussion and announcement of computer security vulnerabilities: what they are, how to exploit them, and how to fix them. This list is now available in Spanish and Japanese languages.

focus-ids – Information about vulnerabilities and discussions on both how to exploit them and how to defend against them are widespread. This list takes a different point of view, namely: How can we detect intrusions, both intrusion attempts as well as systems that have already been compromised?

focus-ih - Focus-IH is a forum geared towards the discussion of the handling of computer security related incidents. It is not to be confused with the 'Incidents' mailing list which deals with the reporting of real-time incidents, technical discussion of trojans, backdoors, worms, etc. The **Incidents** mailing list is for the timely discussion of security events. FOCUS-IH concentrates on secondary analysis of these and the assessment of how they should be better handled and responded to. This also includes how to protect against them in future, the "Best security practices" of active security.

There are a number of other mailing lists offered[15], including ones covering penetration testing, vulnerability development, security papers and jobs, etc.

4.2.1 The Middle Ground

The anti-virus industry, although not perfect, has shown that there is a requirement for vendors to accountable and to encourage and promote trust of not only products but also processes and procedures.

Furthermore the levels of certification for anti-virus products has tended to be more exhaustive than for the rest of the security industry, even though the latter is starting to catch up, and may well overtake them if they rest on their laurels.

5 Ethics (Moral/Professional conduct):

I've already touched on this subject in several earlier sections, so this will be a summation of the points raised. I will cover some areas in more detail, as they are the key ones.

Let us have a look at the differences in real and perceived ethics in the relevant camps:

5.1 Moral/Professional conduct: Anti-Virus

- Good moral and professional conduct overall:
  Still rather poor (in some cases) at acknowledging and fixing some security issues in their products.
- General policy of not hiring virus/malware authors:
  Part of this is due to the ethical stance that the AV vendors adopted from very early on, and secondly their competitors would have a field day with them. They would be excluded from access to other vendor's collections of samples (zoos), access to the likes of REVS, CARO, etc. would probably also be revoked.
- Some vendors have been guilty of stirring up or hyping threats to help bolster sales:
  This has improved over the last few years; there have been less hype from the majority of vendors. The situation will continue to improve due to pressure from the other anti-virus vendors policing their own industry, and from offending vendors

[15] See http://online.securityfocus.com/archive for a full list.

own customer base, as they want the facts and not hype. If vendors fail to take heed then their customers will vote with their feet, taking their corporate budgets with them.

5.2 Moral/Professional conduct: Security

- Good professional and moral standards overall in the larger more respected security firms, but this is not always the case in some of the smaller, or niche security vendors/service suppliers.
- General policy of not hiring virus/malware authors, known 'black-hat' or convicted hackers:
  Part of this is due to the ethical standards that the larger, and more respected security vendors/service suppliers require from their staff in general, and secondly if their customers or competitors found out they would loose not only 'face', but also many of their customers.
- Some vendors have been employing 'FUD[16]' to help meet their sales targets.

5.3 Moral/Professional conduct: The Middle Ground

- No more FUD or hyping to bolster sales.
  There are companies out there that tell is as it really is, rather than 'milking' it. Those that do not will find that before long their customers will get wise, and vote with their feet taking their corporate budgets with them.
- Don't hire those from the dark side!
  You can never be sure they have really changed. They may well be wearing the black hat under that nice new shiny white one.
- Self-regulation and policing, including the above issues:
  This will help to bolster the levels of trust from not only their competitors and partners, but also more importantly, their customer base.

6 Co-operation with competitors:

6.1 Co-operation: Anti-Virus

As mentioned earlier the level of co-operation (at virus researcher level) in the anti-virus industry is high. They share samples and information freely on malware code.

What we are beginning to see now is cross-industry-co-operation, which is what has been needed for some time, and is certainly needed now to try and counter the changes in the threats that many companies are now seeing on an increasingly frequent basis.

It is not just the speed of change and of distribution of these new threats, but also the complexity and overlapping techniques they use which has changed the old model of: "It's a virus/worm/trojan, anti-virus companies will deal with it." to "It's a mass-mailing worm that also spreads by network shares and exploits an number of known security flaws in xyz products. So the anti-virus and IDS/Firewall/Sniffer vendor also needs to deal with it".

6.2 Co-operation: Security

The levels of co-operation between security companies seems to be very hit-and-miss, as there have been few (if any) formal mechanisms or a suitable environment for this type of co-operation/discussion to take place. It often seems that is left to a 'full-disclosure' posting on BugTraq or from CERT before they all sit up and take notice.

[16] **F**ear, **U**ncertainty and **D**oubt.

It requires a more pro-active and open communication model, at least at the vendor researchers/developer level to ensure that their customers get the level of support that they are paying for.

6.3 Co-operation: The Middle Ground

The model seen in the anti-virus industry could be adopted by the wider security industry. If the security industry does not take action then both they (the vendors) and their customers will end up as the losers in a game which is getting increasing more complex as it requires very fast reactions to stop further Nimda and CodeRed fiascos.

With the formation of SAINT this issue should be at least partially addressed, as it will be an enabler, allowing closer co-operation between security vendors.

Part Two:

In this section we will discuss the impact of the so-called 'blended-threats' and the expected impact on the security and anti-virus industry, and finally what that will mean to us, the customers.

7 Possibly Solutions to the ever-changing threat:

It is clear from speaking to anti-virus researchers, security researchers and those individuals that are responsible for security in many large organizations that the so-called 'blended-threat' or 'malware-cocktail' is real, and a trend that appears to be accelerating as malware writers and hackers/crackers are increasingly working together and sharing their skills and knowledge.

This, cooperation (between hackers/crackers and malware authors) is a marked transition in behavior for both groups, as previously they tended to shun each other and be very insular, focused on their own divergent aims.

This has been verified by data from the ISCA Labs Virus Prevalence Survey 2001[17]. This shows that the e-mail vector[18] has begun to fall for the first time since the survey started in 1996. However, this fall is balanced by the resurgence of 'internet/non-email' borne malware, such as CodeRed and Nimda.

Complex worms, which use multiple exploits to gain entry to systems, are not new; the Morris worm[19] of 1988 is the first real example. Many would argue that the Morris worm was far more successful; it certainly had far more effect on the then 'fledgling' Internet. As with most things in life: fashion, fads, etc. all things repeat themselves, or get re-discovered, in fairly predictable and regular cycles. To follow this example through, you could think of Nimda as the grandson of the Morris worm, a 'real chip off the old block'.

More recent examples of 'blended-threats' include the very widespread Klez family of malware which is causing misery to many organizational security teams due to both the large numbers of samples appearing daily at the mail gateway, along with its ability to forge mail headers, which is causing lots of extra work trying to convince customers, third parties, partners, etc. (many of whom are quite irate) that they did not send them the malware, and finally its ability to use Windows file shares.

Furthermore, the waters are further muddied when SMTP (or groupware) gateway anti-virus products are configured to send the 'claimed originator' (taken from the e-mail headers) a notification when a virus is found. This can (and does) lead to a bounce-war between companies that have enabled this feature on their mail server anti-virus protection.

7.1 Technology:

Most of the largest security/anti-virus vendors are planning or already developing products, which merge the current disparate technologies of personal firewalls, anti-malware and personal IDS systems.

Whatever tools are developed or blended together to counter the so-called blended-threat[20] they will need to include the ability to detect threats at packet level as otherwise threats that are created which borrow features from CodeRed will not be detected as it [CodeRed] only exists as a string of data packets and is never written to physical data storage (hard drive/floppy/flash, etc.)

Furthermore I expect to see more research into generic and heuristic technologies, including

[17] Page 26 of the 2001 ICSA Labs Virus Prevalence Survey.
[18] A method of carrying/transmitting a virus/Trojan/worm to a new host.
[19] See here for a good overview of the worm: http://rr.sans.org/malicious/morris.php
[20] Blended threats are malware which use multiple methods (vectors) and techniques (methodologies/exploits/payloads) to propagate and attack systems and networks. Examples include: CodeRed and Nimda. You could say they are automated hacking worms/malware.

behaviour blocking, integrity management, 'kernel' or 'OS' wrappers, honey-pot and similar decoy/trap systems.

The resistance of some of these 'kernel/OS' wrappers to new attacks, buffer overflows, stack smashing, etc. is quite amazing. The best-known product for Windows NT is Entercept from ClickNet[21] and for various flavours of UNIX it is the PitBull product from Argus Systems[22].

There have been some interesting developments in the 'trap/decoy' type systems. The best known of these is known as LaBrea Tarpit[23], also worthy of mention is Roger Thompson's excellent WormCatcher[24]. LaBrea is of specific interest as it bogs-down any trapped systems, tying up resources, which effectively hobbles the worm, slowing it down to a exceedingly slow crawl.

Over the next eight to twelve months I expect to see commercial products that are a direct response to the 'blended threats' as a result of joint partnerships between the anti-virus and security industries. This may even generate new 'hybrid' companies that merge the technologies in new and exciting ways to deal a hard blow against the malware writers, which will give the poor overworked system administrators and security staff the breathing space they need before they recover and the next round starts.

7.2 Human:

This is the hardest element to address, due to the lack of interest in security, which most end-users display, even to the extremes of openly flouting the rules and ignoring the security policies and procedures in place, much to the chagrin and disgust of the security staff that created them to protect their companies systems and networks.

In a recent article[xv] for Virus Bulletin I commented about this 'human problem', not just those that are identified above but the overall view of most end-users that security is an IT issue, and therefore not their problem. This goes for not only those above, but also those that think they are helping by sending on 'Electronic Ephemera' (Hoaxes and their kin), virus warnings, jokes, electronic greeting cards, using Instant Messaging clients, etc. They seem to think that the technology will save them, what they really need to understand is that they are part of the problem, and are currently exacerbating it.

7.3 Services:

I believe that the increasing need of multiple security/anti-malware technologies will speed up the already burgeoning outsourced security trend, as the skills required to collate and cross reference the vast array of data sources (firewall, IDS, anti-malware, sniffer, system and router logs, vulnerability assessment, etc.) is beyond all but the largest and most security conscious companies[25].

8 What benefits will the end-user (customers) see?

The following, and probably others as part of the trend of merging security products, outsourced security or competitors working more closely (partnerships):

- Increased security due to integration of previously disparate security and anti-virus products.
- Improved levels of cross-compatibility.
- Improved manageability of diverse security products.
- Improved choice of managed security/anti-virus services.
- More integrated security/anti-virus product suites or diverse products managed through a single central console.

[21] See here for more details: http://www.clicknet.com/
[22] See here for more details: http://www.argus-systems.com/product/overview/lx/
[23] See here for more details: http://www.hackbusters.net/LaBrea/
[24] See here for more details: http://www.wormwatch.org
[25] See here for a good debate about the issues of outsourcing security:
http://www.infoworld.com/articles/tc/xml/01/02/12/010212tcpcp.xml

- Cost savings when using integrated products (both in support and product costs).
- Increased co-operation between the anti-virus and the wider security industry.

8.1 How will this affect the effectiveness and size of the products?

Well, guess!

Yes, some of the products will get even larger, more complex and require even more resources than before. However, as several of the individual parts of the 'integrated-security-suite' perform similar functions, it is expected that the footprint (in memory) will be smaller than the 'do-it-yourself-piecemeal-security-solution'.

Furthermore on the plus side, there is a very good chance that such a 'integrated-security-suite' would be able to be managed via a single management product, rather than: one for the AV, one for the IDS, one for the Firewall, etc. (ad nauseum) you get the idea?

Looking at the downside of such an 'integrated-security-suite', my main concern would be the ease of a targeted attack, as you will almost certainly have lost some of the protection benefits of having diverse security products from several (or more) vendors. Of course, in a worst case scenario an attacker would target the OS (and most probably the end-user too, as social engineering should not be overlooked as a very successful attack methodology, as commented on by Bruce Schneier, he stated that it was "very effective" and "went straight to the weakest link in any security system: the poor human being trying to get his [or her] job done…"[xvi]) and just sidestep both the 'integrated-security-suite' as well as the 'do-it-yourself-piecemeal-security-solution'.

As with all security it is a case of accepting how much risk your company is prepared to accept and sign-off.

As mentioned elsewhere in this paper a number of vendors have mentioned that they plan to deal with the 'blended-threats' and 'cocktail-malware' issues by working with other security companies and effectively offering a 'best-of-breed' solution with an integrated management tool.

8.2 Will this co-operation improve end-user (customer) protection?

If the disparate vendors from both the AV and 'other' Security vendors decide to co-operate then it will be a win-win scenario for both the vendors and their customers, the only ones that have something to fear are those vendors whose products are not really up to scratch when compared to their competitors.

Below are some suggestions of ways this might work:

- Partnerships.
  As we have seen already between Internet Security Systems and Network Associates Inc.
- Cross licensing.
- Spin off companies.
- Buy-outs.
  Such as the acquisition of Axent by Symantec.
- Mergers.

8.3 How will this affect the underground (Hackers, Malware Authors)?

Well, the 'integrated security suite' will not really change the malware/hacking scene very much. Those that download tools, scripts, malware (script kiddies or malware writer wannabes) will continue to be a nuisance, although I do expect that this will become less of an issue, for a while, until new complex 'blended-threat' point-and-click generation tools are released.

As to the 'core' malware writer/hacker, those that 'roll-their-own', and those few exceptional individuals that are driven by the intellectual challenge, will just see this as all part of the on-going game, and will only momentarily lose their stride.

Finally I expect to see those security companies that create a single integrated security suite to be targeted by the malware creators first, as it is significantly easier to target a single integrated product than a diverse collection of security protection products.

9 Conclusions

Vendors are already working much more closely with each other, both within the AV industry and the wider IT Security industry, than in 1999. In the last few weeks there have been a number of announcements indicating that both camps are either now, or soon will be, working in partnership or via technology licensing with the opposite camp.

A small number of vendors are trying to create (or have by now created) anti-malware products that combine functions from other security areas, such as IDS and Firewall with anti-virus.

Other vendors seem to be following a different path; they are instead forming strategic and technological partnerships with other security vendors whom they consider the best match for their products and ethical stance.

What we are seeing here are vendors who are not trying to be good at many things (Jack of all trades, and master of none), but remaining true to themselves by being the best at what they do (experts in their own field).

They are gravitating to other vendors in other security sectors that have the same outlook and commercial savvy. Working in partnership with them, working on integrating their diverse product offerings. They are looking at the problem from a management point of view, and believe they will address the problem by creating a single management tool to manage their combined (but disparate) security products.

This will allow them to leverage the 'best-of-breed' technologies for both their own, and their customers benefit which can lead to a 'win-win' situation where both the vendor and their customer base get what they both want.

Another 'option' rather than the twin-poled solutions discussed above, is for many organisations which do not have any, or a sufficient number of trained security staff, is to outsource the management of the security services to a third party. This will allow the organisation to deal with the 'human' issues of security, which is in many ways the bigger and more complex challenge.

So, for you the customer, you will have three major choices:

1. Use a fully integrated product that has IDS, Firewall, and AV in one 'package' that can be managed via a central management console.
2. Use a 'best-of-breed' product suite, that uses separate IDS, Firewall and AV from different but strategically allied vendors, which can be managed via a central management console (or more than one, depending on the levels of integration).
3. Outsource security services (AV, Firewall, IDS, etc.) to a company specialising in outsourced security services.

Technology is not the complete answer, it never has been; Security is a cyclical process that encompasses not only technologies, but also people, policies, processes and procedures. As soon as one revolution of the security cycle is completed, you start again with the information garnered and lessons learnt from the previous cycle, ad infinitum.

STOP PRESS: Just as I was finishing off this paper, one Anti-Virus vendor and one vendor from the wider Security industry went back to their old ways of hyping (Anti-Virus) and ill-timed full disclosure (Security).

The former was concerning a new so-called graphic file infector (Perrun[xvii]), and the latter was the Apache flaw posted to BugTraq early on June 17th. A mere ***eight*** hours later a security vendor posted a full disclosure of the flaw, causing panic and confusion[xviii].

It seems from these two recent examples that old habits die very, very slowly. It will be interesting to

take another snapshot of the anti-virus and security industries again in another three years to see if these less than desirable habits have finally been put to the sword…..

Appendix A: Definitions

Blended Threat[xix]
Blended threats combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By utilizing multiple methods and techniques, blended threats can spread rapidly and cause widespread damage. Characteristics of blended threats include the following:

- Causes harm: Launches a denial of service attack at a target IP address, defaces Web servers, or plants Trojan horse programs for later execution.
- Propagates by multiple methods: Scans for vulnerabilities to compromise a system such as embedding code in html files on a server, infecting visitors to a compromised Web site, or sending unauthorized email from compromised servers with a worm attachment.
- Attacks from multiple points: Injects malicious code into .exe files on a system, raises the privilege level of the guest account, creates world read and writable network shares, makes numerous registry changes, and adds script code into html files.
- Spreads without human intervention: Continuously scans the Internet for vulnerable servers to attack.
- Exploits vulnerabilities: Takes advantage of known vulnerabilities such as buffer overflows, http input validation vulnerabilities, and known default passwords to gain unauthorized administrative access.

Effective protection from blended threats requires a comprehensive security solution that contains multiple layers of defense and response mechanisms.

Cocktail-Malware
See 'Blended-Threats'

Electronic-Ephemera[xx]
The group (Genus) name for the all the distinct classes of EE, such as Hoax, Urban Legend, Scam, Spoof, Chain Mail, etc. All of these are only considered species of EE if they are sent/received electronically.

Exploit *(Symantec)*
A program or technique that takes advantage of a vulnerability in software that can be used for breaking security or otherwise attacking a host over the network.

Malware[26]
Short for **mal**icious soft**ware**. Software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.

I created a definition for this in my 1999 Virus Bulletin Paper, as at that time there was no published definition:

"Code that causes unwanted effects: such as Viruses, Trojans, Worms and the side-effects thereof[xxi]*."*

Hacker
A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s). Among professional programmers, depending on how it used, the term can be either complimentary or derogatory, although it is developing an increasingly derogatory

[26] Unless otherwise stated all definitions are from the following source: http://www.webopedia.com

connotation. The pejorative sense of hacker is becoming more prominent largely because the popular press has co-opted the term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is cracker.

Sniffer
A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal.

On TCP/IP networks, where they sniff packets, they're often called packet sniffers.

Trojan Horse (Symantec)
A program that neither replicates or copies itself, but does damage or compromises the security of the computer. Typically it relies on someone emailing it to you, it does not email itself, it may arrive in the form of a joke program or software of some sort.

Virus (Symantec)
A program or code that replicates, that is infects another program, boot sector, partition sector or document that supports macros by inserting itself or attaching itself to that medium. Most viruses just replicate, a lot also do damage.

Vulnerability (Symantec)
Any characteristic of a computer system that will allow someone to keep it from operating correctly, or that will let unauthorized users take control of the system.

Worm
A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

IDS
An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

There are several ways to categorize an IDS:

- misuse detection vs. anomaly detection: in misuse detection, the IDS analyzes the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network’s traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.
- network-based vs. host-based systems: in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall’s simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.
- passive system vs. reactive system: in a passive system, the IDS detects a potential security breach, logs the information and signals an alert. In a reactive system, the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

Though they both relate to network security, an IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system

Firewall
A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert.

A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

Appendix B: CodeRed (Source: Symantec)

The CodeRed Worm affects Microsoft Index Server 2.0 and the Windows 2000 Indexing service on computers running Microsoft Windows NT 4.0 and Windows 2000 that run IIS 4.0 and 5.0 Web servers. The worm uses a known buffer overflow vulnerability contained in the file Idq.dll. Information about this vulnerability and a Microsoft patch is located at:

http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

A Cumulative Patch for IIS that includes the four patches released to date is available at:

http://www.microsoft.com/technet/security/bulletin/MS01-044.asp

System administrators are encouraged to apply the Microsoft patch to prevent infection from this worm and other unauthorized access.

For the various ways to check for this threat and the underlying vulnerability, or if you are using Symantec Enterprise Firewall, please see the Additional Information section near the end of this document.

Also Known As: W32/Bady, I-Worm.Bady, Code Red, CodeRed, W32/Bady.worm
Type: Worm
Infection Length: 3569

Damage:

Payload:
Degrades performance: Will spawn multiple threads and utilize bandwidth.
Causes system instability: Will spawn multiple threads.

Target of infection: Unpatched systems running Microsoft Index 2.0 or Windows 2000 Indexing Service

The worm sends its code as an HTTP request. The HTTP request exploits a known buffer-overflow vulnerability, which allows the worm to run on your computer. The malicious code is not saved as a file, but is inserted into and then run directly from memory.

Once run, the worm checks for the file C:\Notworm. If this file exists, the worm does not run and the thread goes into an infinite sleep state.

If the file C:\Notworm does not exist, then new threads are created. If the date is before the 20th of the month, the next 99 threads attempt to exploit more computers by targeting random IP addresses. To avoid looping back to infect the source computer, the worm will not make HTTP requests to the IP addresses 127.*.*.* .

If the default language of the computer is U.S. English, further threads cause Web pages to appear defaced. First, the thread sleeps two hours and then hooks a function, which responds to HTTP requests. Instead of returning the correct Web page, the worm returns its own HTML code.

The HTML displays:

Welcome to http:// www.worm.com !
Hacked By Chinese!

This hook lasts for 10 hours and is then removed. However, reinfection or other threads can rehook the function.

Two versions of this worm have been seen in the wild. The second version does not cause the webpages to be defaced.

Also, if the date is between the 20th and 28th of the month, the active threads then attempt a Denial of Service attack on a particular IP address by sending large amounts of junk data to port 80 (Web service) of 198.137.240.91, which was www.whitehouse.gov. This IP address has been changed and is no longer active.

Finally, if the date is later than the 28th of the month, the worm's threads are not run, but are directed into an infinite sleep state. This multiple-thread creation can cause computer instability.

NOTES:

If you are running Microsoft FrontPage or a similar program that is used to design Web pages, IIS may be installed on your computer.
For additional information, including the string that is added to the IIS log files, go to the CERT Coordination Center page at:

http://www.cert.org/incident_notes/IN-2001-08.html
According to Qwest, some DSL subscribers who are using Cisco modems series 675 and 678 may have had their modems affected by this worm. For additional information, go to:

http://www.qwest.com/dsl/customerservice/coderedvirus.html

Additional information on problems related to the worm and Cisco hardware or software is available at:

http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml
Hewlett-Packard Jet Direct cards listening on port 80 may also suffer a denial of service.

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

Turn off and remove unneeded services. By default, many operating systems install auxiliary services that are not critical, such as an FTP server, a telnet server, and a Web server. These services are avenues of attack. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.

If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.

Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.

Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.

Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.

Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

Appendix C: Nimda (Source: Symantec)

W32.Nimda.A@mm is a mass-mailing worm that utilizes multiple methods to spread itself. The name of the virus came from the reversed spelling of "admin". The worm sends itself out by email, searches for open network shares, attempts to copy itself to unpatched or already vulnerable Microsoft IIS web servers, and is a virus infecting both local files and files on remote network shares.

The worm uses the Unicode Web Traversal exploit. A patch for computers running Windows NT 4.0 Service Packs 5 and 6a or Windows 2000 Gold or Service Pack 1 and information regarding this exploit can be found at http://www.microsoft.com/technet/security/bulletin/ms00-078.asp.

When the worm arrives by email, the worm uses a MIME exploit allowing the virus to be executed just by reading or previewing the file. Information and a patch for this exploit can be found at http://www.microsoft.com/technet/security/bulletin/MS01-020.asp
If you visit a compromised Web server, you will be prompted to download an .eml (Outlook Express) email file, which contains the worm as an attachment. You can disable "File Download" in your Internet Explorer internet security zones to prevent this compromise.

Also, the worm will create open network shares on the infected computer, allowing access to the system. During this process the worm creates the guest account with Administrator privileges.

Information for Macintosh users:
Although Macintosh computers cannot be infected by this worm, it can be passed through Macintosh email to Windows computers. Also, if you share a network with Windows computers, files could be placed on your hard drive. For additional information, read the document Are Macintoshes affected by the Nimda virus?

Information for Novell users
Novell servers are not directly vulnerable, but a Novell client running under Windows can access the Novell server and execute the file from there (using a login script or other means), which can spread the virus further.

NOTE: Microsoft has released a cumulative roll up for IIS 4.0 on NT 4.0 SP5 and later as well as all security patches released to date for IIS 5.0. This can be found at http://www.microsoft.com/technet/security/bulletin/MS01-044.asp.

Microsoft has provided information regarding this virus at the following website:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/nimda.asp

Also Known As: W32/Nimda@mm, PE_NIMDA.A, I-Worm.Nimda, W32/Nimda-A, Win32.Nimda.A
Type: Virus, Worm
Infection Length: 57344

Payload:
Large scale e-mailing: Uses MAPI to send itself out as Readme.exe (Readme.exe may NOT be visible as an attachment in the email received)
Modifies files: Replaces multiple legitimate files with itself.
Degrades performance: May cause system slowdown
Compromises security settings: Opens the C drive as a network share

Name of attachment: README.EXE (This file may NOT be visible as an attachment in the email received)
Size of attachment: 57344
Ports: 69
Shared drives: Opens network shares
Target of infection: Attempts to infect unpatched IIS servers

Infection by way of a Web Server

W32.Nimda.A@mm attempts to infect unpatched Microsoft IIS web servers. On Microsoft IIS 4.0 and 5.0, it is possible to construct a URL that would cause IIS to navigate to any desired folder on the logical drive that contains the web folder structure, and access files in it. A patch and information regarding this exploit can be found at http://www.microsoft.com/technet/security/bulletin/ms00-078.asp.

Successful exploitation of the Directory Traversal Vulnerability gives the attacker the ability to install and run code, as well as add, change or delete files or web pages on the compromised server. The limitations of the original vulnerability include:

1. The server configuration. The vulnerability only allows files to be accessed if they reside on the same logical drive as the web folders. For example, if a Web administrator had configured the server so that the operating system files were installed on the C drive and the Web folders were installed on the D drive, the attacker would be unable to use the vulnerability to access the operating system files.
2. The attacker must be logged onto the server interactively.
3. The privileges gained would be only those of a locally-logged-on user. The vulnerability only would allow the malicious user to take actions in the context of the IUSR_machinename account.

However, by using the W32.Nimda.A@mm worm as a delivery mechanism, the attacker is able to compromise a vulnerable IIS server remotely and once compromised, create a local account on the targeted server with administrator privileges regardless of which drive the IIS server is installed on. The worm uses directory traversal techniques to access cmd.exe on unpatched IIS servers. The worm also attempts to use IIS servers that had previously been compromised by CodeRed II to propagate and to access root.exe from the inetpub/scripts directory.

NOTE: If Norton AntiVirus RealTime protection is detecting files such as "TFTP34%4.txt" as infected with W32.Nimda.A@mm in your inetpub/scripts folder, you may have been previously exposed to CodeRed II. It is recommended that you download and execute the CodeRed removal tool to make sure that your system has been cleaned of the CodeRed II threat. The tool can be found here.

The worm searches for Web servers using randomly generated IP addresses. Using the Unicode Web Traversal exploit, the worm copies itself to the Web server as admin.dll via TFTP. Infected machines create a listening TFTP server (port 69/UDP) to transfer copy of the worm.

This file is then executed on the Web server and copied to multiple locations. In addition to this exploit, the worm attempts to exploit already compromised web servers using the files root.exe or cmd.exe that are located in remotely executable web directories.

The worm then attempts to modify files named default, index, main or readme, or files with the extensions .htm, .html, or .asp, by adding JavaScript. The JavaScript causes visitors who open infected pages to be presented with Readme.eml, which was created by the worm. Readme.eml is an Outlook Express email file with the worm as an attachment. The email messages utilizes the MIME exploit. Thus, a computer may be infected simply by browsing the infected Web page.

System Modifications

When executed the worm determines from where it is being executed. The worm then overwrites Mmc.exe in the \Windows folder, or creates a copy of itself in the Windows Temporary folder.

The worm then infects executables, creates itself as .eml and .nws files, and copies itself as Riched20.dll in folders that contain .doc files on the local drive. The worm searches for files in the paths listed in the registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\App Paths

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Explorer\Shell Folders

The worm hooks the system by modifying the System.ini file as follows:

Shell = explorer.exe load.exe -dontrunold

It also replaces the file Riched20.dll. Riched20.dll is a legitimate Windows .dll file that is used by programs such as Microsoft Word. By replacing this file, the worm is executed each time programs such as Microsoft Word are executed.

The worm also registers itself as a service process or adds itself as a remote thread to the Explorer process. This allows the worm to continue to execute even when a user is not actively logged on.

The worm copies itself as the file:

%Windows\System%\load.exe

NOTE: %Windows\System% is a variable. The worm locates the \Windows\System folder (by default this is C:\Windows\System) and copies itself to that location

Next, the worm creates open network shares for all drives on the computer by modifying the registry key:

HKLM\Software\Microsoft\Windows\
CurrentVersion\Network\LanMan\[C$ -> Z$]

A reboot of the computer is required for these settings to take effect.

The worm searches for all open shares on the network by iterating through Network Neighborhood and by utilizing randomly generated IP addresses. All files on any open network shares are examined for possible infection. All .exe files are infected by the worm except Winzip32.exe.

Next, .eml and .nws files are copied to the open network shares and the worm copies itself over as Riched20.dll to any folder that contains .doc files.

The worm changes Explorer settings to not show hidden files and known file extensions.

The worm adds the user Guest under the groups Guests and Administrators. This gives the guest account Administrative privileges. In addition, the worm actively shares C$ = C:\ No reboot is required.

Mass-Mailer

Nimda contains a mass-mailing routine which is executed every 10 days. The worm begins this routine by first searching for email addresses. The worm searches for email addresses in .htm and .html files on the local system. The worm also uses MAPI to iterate through all messages that are contained in any MAPI-compliant email clients. Any MAPI supporting email clients may be affected including Microsoft Outlook and Outlook Express. The worm uses these email address for the To: and the From: addresses. Thus, mail sent from the infected computer will appear to have been sent by the people whose addresses have been found by Nimda, not by the person whose computer is infected.

The worm uses its own SMTP server to send out emails using the configured DNS entry to obtain a mail server record (MX record).

When the worm is received by email, the worm uses a old known MIME exploit to auto-execute itself. The worm will be unable to execute using Microsoft Outlook or Outlook Express if the system has been patched against this exploit. Information regarding this exploit can be found at http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

Infecting Executables

The worm also attempts to infect .EXE files. First, the worm checks to see if the file is already infected. If the file is not infected the worm makes a copy of itself in the Temporary directory. The victim file is embedded inside the copy. This new file is then copied over the victim file replacing the originally clean file with an infected version. Infected executables will be approximately 57344 bytes larger. When an infected file is executed, the worm will extract the original clean file to a temporary file and execute it along with itself. Thus, one may not notice their executable has become infected.

During execution, the worm may attempt to delete copies of itself. If the file is in use or locked, the worm will create the file Wininit.ini with an entry to delete itself upon reboot.

When infecting files, the worm may create two temporary files in the Windows Temporary folder as:

mep[nr][nr][letter][nr].TMP.exe
mep[nr][nr][letter][nr].TMP

Both files will be hidden and have the system attribute set.

Ports used by this worm are listed below. It should be noted that these are all standard ports.
TCP 25 (SMTP) - used to send email to targets with addresses taken from the compromised client.
TCP 69 (TFTP) - opens port 69/udp for the TFTP transfer of admin.dll for the IIS infection. As part of this protocol it makes outgoing connections to transfer the files.
TCP 80 (HTTP) - uses this port to target vulnerable IIS servers.
TCP 137-139, 445 (NETBIOS) - used in the transmission of the worm.

Additionally, the worm watches for connections carrying a particular sequence of bytes and then opens a port specified in the incoming connection request. This port is not restricted to any particular range.

The worm contains bugs and can be resource intensive. Thus, not all actions may occur and system instability may be noticeable.

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

Turn off and remove unneeded services. By default, many operating systems install auxiliary services that are not critical, such as an FTP server, a telnet server, and a Web server. These services are avenues of attack. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.

If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.

Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.

Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised. Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.

Isolate infected computers quickly to prevent further compromising your organization. Perform a

forensic analysis and restore the computers using trusted media.

Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

References:

[i] When Worlds Collide: Information Sharing for the Security and Anti-virus Communities – Sarah Gordon and Dr. Richard Ford - Proceedings of the ninth Virus Bulletin conference pp 27- 40
[ii] David M. Chess, 1999 – Private electronic communication. Used with permission.
[iii] Graham Cluley, 2002 – Private electronic communication. Used with permission.
[iv] Full Disclosure is a necessary evil – Elias Levy - SecurityFocus.com (http://online.securityfocus.com/news/238)
[v] MS to force IT-security censorship – Thomas C. Greene, The Register – SecurityFocus.com (http://online.securityfocus.com/news/277)
[vi] http://www.guardian.co.uk/internetnews/story/0,7369,530701,00.html
[vii] See here for one example: http://www.onbusiness.ie/2001/0731/codered.html
[viii] http://news.bbc.co.uk/hi/english/sci/tech/newsid_1470000/1470246.stm
[ix] See here for a good analysis of the impact: http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml
[x] The Virus Creation Labs: A Journey Into the Underground – Published by American Eagle; ISBN 0-929408-09-8. An extract covering Priest/Little Loc can be found here: http://www.soci.niu.edu/~crypt/other/vcl.htm
[xi] http://www.computeruser.com/news/01/01/05/news10.html
[xii] Defecting from the underground – Are ex-virus writers of use to the anti-virus industry – Mike Ellison – Proceedings of the seventh international Virus Bulletin conference pp 215-218
[xiii] "From convicted hacker to dotcom backer" 28th January 2001 http://www.telegraph.co.uk/money/main.jhtml?xml=/money/2001/01/28/ccprof28.xml
[xiv] http://www.wildlist.org/faq.htm
[xv] You are the Weakest Link, Goodbye! – Malware Social Engineering Comes of Age – Martin Overton - Virus Bulletin March 2002 pp 14-17
[xvi] Secrets and Lies: Digital Security in a Networked World, Bruce Schneier - Published by John Wiley & Sons; ISBN: 0471253111
[xvii] http://securityresponse.symantec.com/avcenter/venc/data/w32.perrun.html
[xviii] Irresponsible Disclosure – Jon Lasser (SecurityFocus.com) - http://online.securityfocus.com/columnists/91
[xix] http://securityresponse.symantec.com/avcenter/refa.html#blended_threat
[xx] Hoaxes and other Electronic Ephemera:- Taming the beast (or at least managing it) – Martin Overton - Proceedings of the eleventh Virus Bulletin conference pp 211-234
[xxi] Viruses and Lotus Notes: Have virus writers finally met their match? – Martin Overton - Proceedings of the ninth international Virus Bulletin conference pp 149-174