

MyDoom ? Hacktivism or Cyberterrorism

Creative Technology Technoculture Module

Joshua Shindler

On the 26 January 2004 the MyDoom virus was released from an unknown computer based somewhere within Russia. Within 24 hours of the release of the virus, it had infected one out of every 12 emails world wide. Not only did the virus cause havoc with emails on the infected computers, but it also programmed the infected computer to send out information to the SCO Group's website and the Microsoft corporation website on specific dates. The result of this assault caused the SCO group to change their domain name as their web server simply could not deal with the large amount of information that was being sent to them. Microsoft also had problems but these were on a much smaller scale because the information was sent from a different variant of the virus which did not infect as many computers as had the first version.

These two companies were not targeted at random; both companies have legal and financial battles with the open source community. The SCO group are currently trying to sue IBM, Novell and Red Hat for allegedly stealing codes that can be found in the Linux operating system. Although Microsoft has not taken any direct action against the open source community, they still see it as a threat to their monopoly over the software market. As a result, it is no surprise that the virus is believed to have been created by someone linked to the open source Linux community. This essay focuses on the history and understanding of viruses, worms and Trojans, and the impact that they are having on 21st Century society. Although the essay primarily discusses the western world's reliance on the computer and the effect of the virus in the commercial sector, it also delves into the idea of the David and Goliath battle ensuing over the dominance of companies like Microsoft and the power that the simple virus has for the open source communities. The final part of the essay - and the main question posed by it - will deal specifically with the issue of MyDoom and whether it is can be considered an act of Cyberterrorism or an act of Hacktivism.

Viruses, Worm's and Trojans.

To the average computer user the difference between intruders into the various computer systems is insignificant. But for the purpose of this essay it is important to state briefly the differences between the technologies. This essay will focus on the three main intruders, Viruses, Worms and Trojans. All three programmes can serve the same purpose but they act in three very different fashions.

Viruses

A Virus seems to be the word that governs all computer infections whether they are a virus, a worm or a trojan. The basic premise behind a virus is that it should replicate itself. This is no different to the viruses that are present within biology.

For a virus to be successful it obviously needs to be able to replicate. If a virus kills its host and thereby isolates itself - for example by wiping the hard drive - then it can no longer survive as it has effectively committed suicide. The most successful viruses are those that are allowed to spread from computer to computer.

*'A computer virus is an executable file designed to replicate itself while avoiding detection. A virus may disguise itself as a legitimate program. Viruses are often rewritten and adjusted so that they will not be detected. Anti-virus programs must be updated continuously to look for new and modified viruses. Viruses are the number one method of computer vandalism.'*ⁱⁱ

Worms

The major difference between a worm and any other type of computer malware is that a worm is self-sufficient. It does not involve any type of involvement from a user and does not depend on a host program. It can spread across a computer network or just infect one computer. As with both the Trojan and the virus, the worm spreads through emails, Internet, peer 2 peer networking and similar methods.

*'The computer Worm is a program that is designed to copy itself from one computer to another, leveraging some network medium: email, TCP/IP, etc. The Worm is more interested in infecting as many machines as possible on the network, and less interested in spreading many copies of itself on a single computer (like a computer virus). The prototypical worm infects (or causes code to run on) a targeted system only once; after the initial infection the worm attempts to spread to other machines on the network.'*ⁱⁱ

Trojans

*'I distinguish between a prank and a Trojan on the basis of intent to damage. The Trojan horse was the gift with betrayal inside; so a Trojan horse program is an apparently valuable package with a hidden, and negative, agenda.'*ⁱⁱⁱ

A Trojan fulfils exactly the same function as the famous horse at Troy. It enters the computer system as a dummy file, sometimes disguised as an mp3 music file and when opened by the user it becomes destructive. Trojans are mainly distributed through electronic bulletin boards sometimes appearing as warez (illegal software distribution) applications or utilities. In recent years, peer 2 peer file sharing, such as Kazza, has been cause of many of the Trojan infections.

The History of the Computer Virus

The Early Viruses

The computer virus came into existence in a number of different locations during the 1980s. The first recorded virus was produced on an Apple II in 1981, but it was not until the mid to late eighties that viruses came into their own. In 1986 several programmers, mainly in academic locations realised that the floppy disks of the time possessed a built in code them that could be changed. All the creators of viruses all gave them the same ability - to replicate. This is what two programmers 'Basit and Amjad' realised when changing the code of the 360kb floppy disks. 'In 1987, the University of Delaware realised that they has a virus, when they started noticing the label "(c) Brian" on floppy diskettes. That's all it did – copy itself, and put a volume label on diskettes.'^{iv}

At the same time in 1986 another programmer showed this replication technique at the Chaos Computer Club conference. His virus, 'Virdum' was again harmless, but the virus caused an interest in the field.

In 1987 Fred Cohen completed his doctoral dissertation on the computer virus. During his dissertation he experimented with releasing viruses into computer networks to see how they would spread. Cohen understood that like any other virus, for it to be successful, it had to be able to survive. When a virus wipes a hard drive clean or severs a network connection it destroys itself as the process and its ability to infect any future hosts

"a program that can 'infect' other programs by modifying them to include a ... version of itself"
Cohen is seen as the grandfather of virus research and so his definition above has become a standard amongst the computer world.

The first relatively successful virus was said to have originated in Tel Aviv, Israel, although some believe it may have come from Italy. This virus named Suriv-01 (virus spelt backwards) had the

ability to infect any COM file which put it a step above the rest. Suriv-02 went further in being able to infect EXE files and Suriv-03 was able to infect both COM and EXE files.

But it was the fourth Virus from this source that had the greatest impact. It managed to escape, but was eventually located in the computer networks of the Hebrew University in Jerusalem. Thus it was named the Jerusalem virus. The virus acted on specifically Friday the 13th and deleted all files that were meant to run on that day.

The real future direction of the computer virus was not apparent until 1988 when anti-virus companies started to appear. At the time the virus was still only a potential problem and therefore the companies operated only on a very small scale. They began to sell software for as little as \$5 or \$10. Due to the lack of concern it accorded viruses such as Jerusalem, Stoned (when infected the PC notified the user 'Your PC is now Stoned') and Cascade (a virus that was encrypted which made it more difficult to repair any infected files) this provided a real opportunity to spread without detection.

It was also in this year that the first total collapse of a computer system occurred as a result of a computer virus. The virus, Morris, infected more than 6000 computer systems in the USA. This computer virus completely paralysed a number of networks which was said to result in the estimated loss of 96 million dollars.^v

During the next few years, there was an outbreak of damaging computer viruses. These viruses caused the first stir amongst the media in the UK.

'New viruses "Data crime", "FuManchu" appear, as do the whole families like "Vacsina" and "Yankee". The first one acted extremely dangerously – from October 13th to December 31st 1989 it formatted hard disks. This virus "broke free" and caused total hysteria in the mass media in Holland and Great Britain.'^{vi}

The early nineties saw the rise of the larger computer firms making an attempt to control the threat of viruses. This was highlighted by IBM releasing their own anti-virus software in 1989 and the first release Norton Anti-Virus in 1991.

Early to Mid Nineties

The spread of viruses during the early 1990s was caused through viruses breaking free and ending up in bizarre locations such as the PC Today magazine – this was sold with a floppy disk that actually contained the "DiskKiller" virus. Over 50,000 copies were sold. The proliferation of viruses became a bigger problem during the growth of the compact disk. During 1994 CDs became the main method of spreading a virus. Thousands of CDs were infected from a master CD and they could not be altered and as a result had to be destroyed.

The viruses produced on the CDs combined with the development of email and the use of the internet to produce another round of mass media hysteria about the rise of the computer virus. 1995 was labelled the Year of the Hacker.^{vii} This year saw the first rise of Hackers using the internet to attack military and government organisations.

'Hackers attacked Griffith Air Force Base, the Korean Atomic Research Institute NASA, Goddard Space Flight Center, and the Jet Propulsion Laboratory. GE, IBM, Pipeline and other companies were all hit by the "internet Liberation Front" on Thanksgiving.'^{viii}

1995 also produced the first Microsoft targeted virus, a pivotal point in the history of the computer virus. This virus named "alive" targeted MS Word users all over the internet.

1996 fashioned the first virus for Microsoft Excel called "Laroux". It worked by the presence of macros that appear in Microsoft Excel. This cause a snowball effect which created many more viruses that year that attacked the Microsoft Windows 32 operating system and the Microsoft Office Software.

The Age of the Internet Virus

As people started to take up internet connections it gave the opportunity for viruses to spread on a mass scale. In 1997 Microsoft Office 97 was released with a number of faults which gave the virus creators yet another opportunity to attack. In 1997 the world also saw a new type of virus 'the mIRC Worm'. As internet chat became more popular, the 'mIRC' worm was able to travel along a hole in the program. The bombardment of the Microsoft Software suites continued well into 1998. Numerous viruses were produced through out the year.

In 1999 "Melissa" was the first of a breed of new super email viruses. It used Microsoft's popular email programs, Outlook and Outlook Express to send itself from the users' computer to all those in their address book. Later in that year there were constant virus attacks on many of the Microsoft product suites.

In 2000 the most famous and then the fast spreading virus of all time was the "Love Letter" or "Love Bug" as it was later coined. This virus spread so quickly that it started shutting down email systems all around the world. 2000 also became the year that saw the first worm attacks against national telephone systems. These took place against the Spanish Internet phone system and the Japanese Emergency Phone system.^{ix}

Over the next three to four years, virus writers made use of the new applications that were associated with the Internet. Although email was the most commonly used method of spreading a virus, some such as "Benjamin" were allowed to spread through Kazza, the peer 2 peer file sharing network.

The use of the Internet and the invention of new technologies have therefore resulted in a vast increase in the number and type of viruses. It has also spawned an alliance between spammers and virus writers^x that may produce new and more deadly viruses in the near future.

Technopolitics

Technology today is one of the key factors that advance the global economy. As the developed nations of the world become more dependant and reliant on technology, it impacts on everyday activities. Cyberspace, the Internet and the home computer are the most vulnerable examples of society's reliance on new technology.

'Globalisation and the rise of the of a new computer and information technology-based economy and society is interpreted in both popular and academic literature as a revolution in which new technologies are transforming every mode of life from how individuals do research to how people communicate and interact socially.'^{xi}

As a result of this continuing relationship with technology, there have been an attempts to develop a alternative use of the technology with the aim of gaining political control. Some commentators argue that technology has in the past hundred years been used to increase political influence in our everyday lives, using television, radio or the printed press, but the essential question for today is how are attempts at control being manifested?

The Internet and cyberspace are the clear forerunners in the new political medium that is being used by today's political activists. Cyberspace is the undiscovered country. There are very few limitations for debate or argument and there are no restrictions on time or place. This has allowed small - and often insignificant – organisations the ability to project their agenda to a much larger audience.

Helen Steel and Dave Morris were two activists who were being sued by McDonalds for making claims about their advertising methods, low pay, unhealthy diet and involvement in the cruel treatment of animals. The two activists counterattacked McDonald with the McLibel campaign. The group that helped organise the campaign created the www.mcspotlight.org website which had over 15 million hits during the three year libel case.

'McDonald's spends over \$2 billion a year broadcasting their glossy image to the world. This is a small space for alternatives to be heard.'^{xii}

The site is said to be the most comprehensive massing of information about any multinational corporation in the world.

A far more direct use of technology has been used by different political groups. Within the Middle East there are repeated attacks on the website of Hezbollah and other organisations who commit acts of terror against civilians by Israeli hackers and the same has allegedly been carried out by pro-Palestine groups on the Israeli army and government sites. The same types of attacks have been taking place between Pakistani and Indian hackers.

Dr Howard Dean, one of the candidates for the Democratic Party nomination for President used the cyberspace in a completely unique way. Dean used the World Wide Web as his main medium in which to communicate with his supporters. Although Dean did lose the race to become the Democrats' candidate, he did manage to raise \$450 million from his website alone and used blogging as a new method of interacting with his followers.

The open playing field of cyberspace allows both the political powers of the world and the political underdogs the same opportunity. The information super highway remains a free throughfare as opposed to a toll paying road.

Hactivism

The difference between the purveyors of Technopolitics and Hactivism are very subtle. Technopolitics uses current technology for political gains where as Hactivism and Hactivist use the technology as an alternative to get their political point across.

'Hactivism is activism gone electronic'^{xiii}

'Despite its connotations of illicit computer break-ins, within hacking circles the hack is more widely defined as an attempt to make use of technology in an original, unorthodox and inventive way.'^{xiv}

The mass media has painted a bleak picture of the hacker being the dark and shady underground computer user who breaks into people's computers to steal their personal information. This is a somewhat distorted view of hacking circles where the method and use of technology defines the hacking process rather than the end result of it. An Hactivist is someone that takes this concept one step further.

'I think of Hacktivism as a philosophy: taking the hacker ethic of understanding things by reverse engineering and applying that same concept to traditional activism.'^{xv}

Nart Villeneuve, a 28 year old computer science student at the University of Toronto, described what he understood by the term Hacktivism. He is interested in freedom of technology and in particular the world wide web and the restrictions placed on some countries around the world. For example Villeneuve opposed China creation of a Firewall that stopped access to the Google website. Villeneuve produced a look-a-like site that allowed user to access Google in China.

Villeneuve belongs to Hacktivismo, a small group of Hacktivists across the globe. This group and other like it have created techniques for networking anonymously with users in authoritarian countries where the Internet is very closely monitored.

Hacktivism has also been used to attack corporate websites. In June 2000 a group of hackers attacked Nike's website and substituted a global justice message in place of Nike's corporate sign. This is just one of the few examples of campaigns against global corporations.^{xvi}

The Hacker has a two sided approach to the purpose of Hacktivism. The first is the cause and the second is the Hack.

"There is a lot of apathy among my generation with political processes," said Ian Clarke, the 25 year old founder of the Freenet Project. "The nice things about writing code to address the political issues is that we are playing the game on our own turf."^{xvii}

Within cyberspace everything happens with immediate effect. We write an email and it is sent without any delay. The Hacktivists therefore feel at home in this environment, They can see the change they are making right before their eyes. Their actions have had a direct impact on the preferred cause. It is instantaneous.

Cyberterrorism

Just like in the real world there is a thin line between a terrorist and a freedom fighter, so too in cyberspace, there is a very fine line between the Hacktivist and the Cyberterrorist. When the MyDoom virus was released into the world there were those within the open source community who were angry with the creator of the virus for the bad name that it gave the community. But at

the same time, embedded within the code was a line apologising for any disruption caused by the virus and that it was only meant to cause damage to the Microsoft and SCO websites.

Jordan and Taylor express this confusion between Hactivist and Cyber terrorist.^{xviii} They quote the case of the Israeli hacker Ehud Tenebaum, who attempted to hack into the Pentagon's computer system. The US authorities wanted to use Tenebaum as an example of the consequences for engaging hacking and to have him arrested. As Israeli Lawyer representing Tenebaum argued that the Pentagon should actually pay his client for revealing the weaknesses within their system.

In May 2000 Dorothy Denning of Georgetown University gave testimony to the U.S House of Representatives on the immediate and future dangers of Cyberterrorism. She commented that cyberterrorism is usually understood as

'unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.'^{xix}

She cited various cases of Cyberterrorism including the "ILOVEYOU" virus that caused millions of dollars worth of damage. The "ILOVEYOU" virus is the most closely associated virus with "MyDoom" that she quotes in her testimony. The "ILOVEYOU" virus had a similar spread infection as the MyDoom virus and also attacked the websites of Yahoo, CNN, and eBay causing a denial of service.

Denning argued in her testimony that it was essentially a question of judgement as to whether any of the attacks can really be described as Cyberterrorism. She added that the threat of Cyberterrorism is not something to be taken lightly. As the world moves to more and more automated systems that are controlled by computers the threat of Cyberterrorism will become greater and greater.

In a recent episode of ABC's programme Alias, cyberterrorism was used as a storyline. Alias is a fictional television show about a spy, Sidney Bristow who works for the CIA. In the three series that have been broadcast so far, Sidney has battled against nuclear terror, bioterrorism and nanoterrorism just to name a few. But the most recent episode certainly reflects the mood of the current times even though it may be fiction.

'This past March, Japans Metropolitan Police Department reported that a software system they had procured to track 150 police vehicles, including unmarked cars, had been developed by the Aum Shinryko cult, the same group that gassed the Tokyo subway in 1995, killing 12 people and injuring 6,000 more. At the time of discovery, the cult has received classified tracking data on 115 vehicles.'^{xx}

Although Denning's point of view may be one step away from what could be considered science fiction, she stressed that if the systems were vulnerable enough then it could cause major damage in real space as opposed to cyberspace.

Technological Autonomy

'The next generation of terrorists will grow up in a digital world, with ever more powerful and easy-to-use hacking tools at their disposal. They might see greater potential for cyberterrorism than the terrorists of today, and their level of knowledge and skill relating to hacking will be greater. Hackers and insiders might be recruited by terrorists or become self-recruiting cyberterrorists, the Timothy McVeigh's of cyberspace. Some might be moved to action by cyber policy issues, making cyberspace an attractive venue for carrying out an attack. Cyberterrorism could also become more attractive as the real and virtual worlds become more closely coupled, with a greater number of physical devices attached to the Internet. Some of these may be remotely controlled. Terrorists, for example, might target robots used in telesurgery. Unless these systems are carefully secured, conducting an operation that physically harms someone may be easy as penetrating a Web site is today.'^{xxi}

Denning described the possible future of cyberterrorism. She speculates that the 'next generation of terrorists are growing up in the digital world and will use a technology driven society as an instrument to aid them with terrorism. Although Denning states that seem this to be far fetched and even scare mongering, it is still a powerful comment on the direction that of society is heading in and the push towards a fully technologically automated society.

During the 1950s, television programmes suggested that the housewife of the future could sit back and let robots clean, iron, vacuum clean, wash up etc. In Chandler's essay Technological or Media Determinism, he uses Asimov to describe this 1950s vision.

'The whole trend in technology has been to devise machines that are less and less under direct control and more and more seem to have the beginning of a will of their own. A chipped pebble is

almost part of the hand it never leaves. A thrown spear declares a sort of independence the moment it is released.

The clear progression away from direct and immediate control made it possible for human beings, even in primitive times, to slide forward into extrapolation, and to picture devices still less controllable, still more independent than anything of which they had direct experience.^{xxii}

Chandler continues in his essay by quoting Ellul and his idea of technology determining the direction of technology rather than society defining the direction of society. This is the basic premise that seems to govern all commentators who suggest that society has lost control over technology. Chandler's quoting Postman seems to suggest something closer to the likes of the Matrix and the Terminator perspective on technology.

'Postman argues that 'Technique, like any other technology, tends to function independently of the system it serves. It becomes autonomous, in the manner of a robot that no longer obeys its master' (Postman 1993, p. 142).

Elsewhere he defines 'The Frankenstein Syndrome: One creates a machine for a particular and limited purpose. But once the machine is built, we discover, always to our surprise - that it has ideas of its own; that it is quite capable not only of changing our habits but... of changing our habits of mind' (Postman 1983, p. 23). Although Postman denies that that 'the effects of technology' are always inevitable, he insists that they are 'always unpredictable' (Postman 1983, p. 24).^{xxiii}

It is this theory of technology that raises the fears those cyber crime and cyber terrorism will dominate. As newer and newer technologies are adopted and the rate of change exceeds the ability of society to cope with the change, then the less control society will have over the technology. Hence, the more unpredictable the technology will become. This is not to say that machines are going to take over the world, but as Microsoft has shown time again, when technology is released without due care and attention, numerous problems appear which were never predicted.

The Open Source Battle

There are two types of different computer software in today's society, closed propriety software and open source software. The open source software allows programmers to view all the coding that is involved in the development of computer software. This software is also usually free as

long as it is not used for commercial purposes. The most popular and most famous open source programme is the Linux Operating System.

Closed propriety software only discloses the programming code only to those who either wrote the code or who own the code. These applications are usually only used by large corporations that do not want to reveal their code for fear of competition or through the threat of their programmes being hacked. The most renowned company to do this is the Microsoft Corporation, who like The SCO Group was also attacked by the MyDoom virus.

'Open source software goes one step beyond freeware. Not only does it provide the software for free, it provides the original source code used to create the software. Thus, curious users can poke around with it to see how it works, and advanced users can modify it to make it work better for them. By its nature, open souce software is pretty well immune to all types of computer virus.'^{xxiv}

The result of a recent uptake of the Linux operating system has produced avigorous debate between the more popular Microsoft Windows operating system and Linux. One result of this debate is a White Paper entitled "Opening the Open Source Debate" by the Alexis de Tocqueville Institution (AdTI). This paper did not seem produce any solutions and it could be argued that it simply made the situation worse. The paper's aim was to assess the value that open source programming has to the computing world. The validity of this paper has been questioned by many within the Open Source community and ridiculed as no more than a Microsoft whitewash.

'The AdTI never quite gets around to saying why the open-source community is a "myth". Apparently, the hundreds of collaborators who gave the world the Linux kernel are mythical. How about the countless programmer-hours that went into the GNU system? Perhaps the outstanding KDE desktop environment was written by unicorns. And one supposes that GNOME, another outstanding desktop environment, was produced by, well, gnomes. Apache---it's a myth. PHP---doesn't exist. Mozilla---pshaw.'^{xxv}

The "MyDoom" virus was released around the 26 January 2004. Written within its code was a dDOS attack on the SCO website that would take place on Sunday 12 February 2004, Superbowl Sunday. The "MyDoom" virus was said to have infected hundreds of thousands of computers, if not millions. On the 12 February 2004 hundreds of thousands of computers simultaneously tried to contact the SCO website. As a result the SCO Group changed their domain name and withdrew their current web address from the domain name directory. This calculated attack seems to be the result of SCO Group civil lawsuit against IBM, Novell and Red Hat.

On the 7 March 2003, Cladera Systems Inc and The SCO Group initiated a law suit that is now resulting in Cladera/SCO now seeking \$3 Billion Dollars in damages.

'claiming that IBM, through its support and development of Linux, has breached contracts IBM entered into with Cladera/SCO 's predecessors in Unix ownership regarding the non-disclosure of Unix code.'^{xxvi}

Although The SCO Group and Microsoft are not the most favoured organisations within the Open Source Community, there was a clear sense of disgust by the community following the aftermath of the MyDoom virus.

"Whoever wrote MyDoom is definitely a Linux fan," says Jack Clark, technology consultant at McAfee Associates, an anti-virus company. Most Linux users, however, condemn the virus author. "Well, you stupid, ignorant bastard, if you're reading this - no one admires you," reads one post on tech community site Slashdot.org.'^{xxvii}

There of course is no absolute certainty that the main purpose of the "MyDoom" virus was to cause damage to the Microsoft and SCO website as it may have been a screen for another action, spamming. The result of the MyDoom virus has been a reward of \$250,000 by both Microsoft and SCO and the Linux community is still blaming Microsoft for a lack of security within their systems.

MyDoom and Spam

For the average computer user, whether the MyDoom is a trojan, worm or virus is not relevant. What is important is the fact that it has caused an estimated \$100 billion dollars of damage. But the immediate effects of the virus itself are not what really concern many of the computer experts around the world, but the future consequences arising out of its action.

These consequences register on a number of different levels. Firstly MyDoom has sparked a fire that can grow and grow. It has shown the world the frailties of the Internet and the lack of knowledge and security therein to both single users and companies.

"The MyDoom attack should never have propagated so far into the Internet," he said "It is obvious that we need another layer of software to protect during the first hours of attack."^{xxviii}

'Initially, the number of copies of the new virus - christened MyDoom after a misspelling of "my domain" in its code - were small, just a few hundred. Three other, more dangerous looking viruses were swirling around the world's email networks at the time.

"We were concentrating on those," says Alex Shipp, a senior anti-virus technologist. "MyDoom wasn't that interesting."^{xxix}

The impact that MyDoom has had on the computing world is extreme. MyDoom has been a wake - up call for many of those involved in computer security, e-crime and the open source debate. Some believe that the Virus has another purpose and that this was its original intention. The MyDoom virus opens a backdoor into the user's computer in order to turn it into spam relay robots. The creator of the virus may have wanted to kill two birds with one stone. The attack on the websites and the spam may have just been a cover for the other. Some computer experts have even suggested that viruses are being commissioned by spammers.

'Virus outbreaks may be dramatic, maintain experts, but they are just occasional annoyances compared to spam. A massive 62% of all email in the world is now spam. On a visit to the UK last week, Bill Gates signalled Microsoft's focus on developing email technology to allow recipients to verify the sender of emails. "This is critical for security," he said, "and for getting rid of spam." While welcoming the comments, some security experts are more pessimistic, even fatalistic. "Email is dying," says Hypponen. "It's coming to its end." Any day now, he says, a MyDoom-style virus could quickly overload and break the entire email system without a chance of recovery - simply by sending out millions of generic, unfilterable messages in a loop, round the clock, forever. Then we would have to drop email as we know it. Every email server, every email client in the world."^{xxx}

The MyDoom computer virus now reigns supreme, at number one as the most potent virus to have been released and to have cause the greatest degree of infection. The immediate effects of the virus are still being calculated, but it is the long term implications that concern people. Whether any preventative action will take place in the future is still yet to be seen, it might take a super virus to wipe out the whole of the email system before people sit up and take notice.

Conclusion

As has been mentioned previously in this essay, there is a very fine line between hacktivism and cyberterrorism. It is usually a personal opinion and stance that decides into which category the virus should be placed. What the MyDoom virus has indicated is that the situation is not a simple

black and white scenario. There are too many different facets which characterise the virus such that it becomes extremely difficult to have a definite conclusion.

If the MyDoom virus possessed just one function and that this was the attack on the SCO and Microsoft website, then a conclusion would be simpler. It could be viewed benevolently as Hacktivism or it could be condemned by viewing it as an act of Cyberterrorism. But even this is not concrete totally clear since there are those who would agree with the act but still consider it cyberterrorism. Owing to the extra back door spamming component there is no way of making an assessment or a conclusion either way.

Although there can be no conclusion as to whether the virus is an act of hacktivism or cyberterrorism, the massive impact of MyDoom has been able to teach the computing world a lot about the future direction of Internet security and viruses. Over the past five years - from "Melissa" in 1999 to "MyDoom" in 2004 - the world has seen the creation of the super virus. This has resulted in all sorts of predictions by commentators but two of which are more pertinent than the others.

The first of prediction about the future is that the more technology becomes automated the greater the threat from cyberterrorists. One of the reasons for not reaching a conclusion as to whether MyDoom is an act of Hacktivism or Cyberterrorism is because it happens in cyberspace. Although it occurs in cyberspace, the ramifications are felt in real space and therefore this will be called an act of Cyberterrorism. There is no doubt that the more society becomes enveloped in technology the greater the risk that a computer virus will cause real world damage.

The second prediction states that at some point in the future, users and antivirus software are going to have to take more control of their electronic environment or there will be no email or Internet since it will be swamped with viruses.

Both these predictions are of course not certainties. The computer virus has only had a very short history of twenty years and just as computer power seems to be growing exponentially so to do the quantity and the potency of the viruses. The only certainty for the future is that there will be more viruses of greater potency. Whether or not the world will be prepared for them is yet to be seen.

References

ⁱ <http://www.microsoft.com/technet/prodtechnol/sbs/reskit/sbrk2000/sbrkglo.asp> - Microsoft

ⁱⁱ An Environment for Controlled Worm Replication and Analysis.

ⁱⁱⁱ <http://www.cknow.com/vtutor/vtslademacmag.htm> - Slade

-
- ^{iv} Solomon, Alan - *A brief History of PC Viruses*
^v <http://www.virus-scan-software.com> – *The History of Computer Viruses*
^{vi} Ibid
^{vii} <http://www.cknow.com/vtutor/vhistory.htm>
^{viii} Ibid
^{ix} Ibid
^x <http://www.wired.com> Dello, Michelle *Virus Era Hits 5-Year Mile Stone*
^{xi} Kellner Douglas *Globalisation, Technopolitics and Revolution*
^{xii} <http://www.mcspotlight.org/>
^{xiii} Jordan, Taylor *Hacktivism & Cyber Wars Rebels with a Cause?*
^{xiv} Ibid
^{xv} Lee, Jennifer *Guerrilla Warfare, Waged with Code*
^{xvi} Kellner Douglas *Globalisation, Technopolitics and Revolution*
^{xvii} Lee, Jennifer *Guerrilla Warfare, Waged with Code*
^{xviii} Jordan, Taylor *Hacktivism & Cyber Wars Rebels with a Cause?*
^{xix} Denning, Dorothy *Cyberterrorism*
^{xx} Ibid
^{xxi} Ibid
^{xxii} Chandler, Daniel *Technological or Media Determinism*
^{xxiii} Ibid
^{xxiv} <http://www.saugus.net/Computer/Terms/> Glossary of Computer Terms
^{xxv} <http://www.roaringpenguin.com/adt2.php3> *Opening the Open-Source Debate*
^{xxvi} SCO vs IBM Executive Summary Page.
^{xxvii} McCandless, David *Anatomy of a Virus* Guardian 5.2.2004
^{xxviii} Lemos, Robert *MyDoom Spread Sparks Antivirus Critique* Cnet News.com
^{xxix} McCandless, David *Anatomy of a Virus* Guardian 5.2.2004
^{xxx} Ibid

Bibliography

Books

- Jordan, Tim and Taylor, Paul A (2003) *Hacktivism & CyberWars: Rebels with a Cause?*

Articles and Papers

- Lee, Jennifer (2002) *Guerrilla Warfare, Waged With Code* The New York Times: 10.10.2002
- McCandless, David (2004) *Anatomy of a Virus* The Guardian Online: 05.02.2004
- <http://www.aber.ac.uk/media/Documents/tecdet/tecdet.html>
Chandler, Daniel (1995) *Technological or Media Determinism*
- Left, Sarah and Perrone, Jane (2004) *Viruses and Worms* The Guardian Online: 20.01.2004
- Whalley, Ian, Arnold, Bill, Chess, David, Morar, John, Segal, Alla and Swimmer, Morton (2000) *An Environment for the Controlled Worm Replication and Analysis*, IBM TJ Watson Research Center
- <http://www.gseis.ucla.edu/faculty/kellenr/kellner.html>
Kellner, Douglas *Globalisation, Technopolitics and Revolution*

-
- Denning, Dorothy (2000) *Cyberterrorism – Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services - U.S. House of Representatives* Georgetown University 23.05.2000

Websites

- <http://www.guardian.co.uk/online/businesssolutions/story/0,12581,1155714,00.html>
Users Can Cure Virus The Guardian, 26.02.2004
- <http://news.zdnet.co.uk/internet/security/0,39020375,39147959,00.htm>
Kotadia, Munir (2004) *Viruses and DDoS Attacks Flood UK Firms* ZDNet UK: 02.03.2004
- <http://news.zdnet.co.uk/internet/security/0,39020375,39147317,00.htm>
Wearden, Graeme (2004) *Firms Keeping Quiet About E-Crime* ZDNet UK: 24.02.2004
- <http://news.zdnet.co.uk/internet/security/0,39020375,39145515,00.htm>
Kotadia, Munir (2004) *Phishers Improve Bait as they Target ISPs* ZDNet UK: 05.02.2004
- <http://www.roaringpenguin.com/adti2.php3>
Skoll, David (2002) *Opening the Open Source Debate*
- http://www.eweek.com/print_article/0,1761,a=118051,00.asp
Vaughan-Nichols, Steven (2004) *SCO's My Doom DDoS Hammering Begins* Eweek: 01.02.2004
- <http://www.wired.com/news/infostructure/0,1377,62401,00.html>
Delio, Michelle (2004) *New MyDoom Virus Packs a Wallop* Wired News: 24.02.2004
- <http://asia.cnet.com/newstech/systems/0,39001153,39171259,00.htm>
Kotadia, Munir (2004) *SCO.com Emerges from Virus Battle* CNET Asia: 09.03.2004
- <http://www.eweek.com/article2/0,1759,1514997,00.asp>
Vaughan-Nichols, Steven (2004) *MyDoom, Windows Linux* Eweek: 03.02.2004
- <http://sco.iwethey.org/>
Executive Summary – SCO vs IBM
- <http://news.zdnet.co.uk/software/developer/0,39020387,39145278,00.htm>
Lemos, Robert (2004) *MyDoom Trail Traces back to Single Author* CNET News: 03.02.2004
- <http://news.zdnet.co.uk/internet/security/0,39020375,39145276,00.htm>
Lemos, Robert (2004) *MyDoom's Spread Sparks Antivirus Critique* CNET News: 03.02.2004
- <http://news.zdnet.co.uk/internet/security/0,39020375,39145072,00.htm>
Lemos, Robert (2004) *Microsoft Offers Bounty for Creator of MyDoom Variant* CNET News: 30.01.2004
- <http://www.washingtonpost.com>
Krebs, Brian (2004) *Windows Leak Could Affect Home Users* Washington Post: 13.02.2004

-
- <http://www.ladlass.com/archives/001635.html>
Thompson, Clive (2004) *The Stealth Worm Era* TheStar.com:15.02.2004
 - <http://www.wired.com/news/linux/0,1411,62058,00.html>
Delio, Michelle (2004) *MyDoom Targets Linux Antagonist* Wired News: 27.01.2004
 - http://www.windowsecurity.com/articles/Protecting_Email_Viruses_Malware.html
Shindler, Deb (2003) *Protecting your Email from Viruses and Other MalWare* Windows Security: 05.06.2003
 - http://www.windowsecurity.com/articles/Trojan_Horse_Primer.html
Shimonski, Robert (2003) *Trojan Horse Primer* Windows Security: 03.09.2003
 - <http://www.wired.com/news/infostructure/0,1377,62809,00.html>
Delio, Michelle (2004) *Virus Era Hits 5-Year Milestone* Wired News: 26.03.2004
 - <http://www.cknow.com/vtutor/vhistory.htm>
Virus History
 - <http://www.virus-scan-software.com/virus-scan-help/answers/the-history-of-computer-viruses.shtml>
The History of Computer Viruses