Viral Threats – An Examination of Current and Evolving Technologies

Antonio Martin (SCA Technica, USA, tmemail@gmail.com)

Boston University Conference on Information Assurance and Cyber Security, Dec 2006

Abstract

Virus/Malware/Worms and other such infections are on the increase, technological security advancements are falling behind as zero day exploits become prevalent and system infections become impossible to detect. Security industry dollars are primarily focused on reactive and not proactive solutions; patches and signature definitions are days, if not weeks behind active exploits. Attacks have been confined, limited to individual infected machines tied into "bot nets" numbering into the thousands, utilized primary by individuals for financial gains. This playground is evolving as state sponsored activities are on the rise as seen in the attacks on multiple US government facilities and agencies. Further consideration and awareness must be made for what trends might evolve, not only within the next month or year, but a broader horizon of five plus years, so defensive technology development can begin before problems arise. This paper will attempt to consider the current, near term and future evolution of computational attacks and map these to possible deployment timeframes and developmental complexity and examine possible technologies needed to help combat pending threats. Furthermore, several scenarios will be illustrated, outlining how some of these current and future viral technologies can be leveraged into wide scale attacks. The paper's purpose is to facilitate discussions about future computational infections, the technology they will employ and new ideas for future development.

(Image source: www.ocipep.gc.ca)

The author does not condone any illegal activity and only writes this as a security professional to help raise awareness of potential issues.

I. Introduction

Currently, the internet is facing pressure from viruses that are infecting machines world wide. Their spread can be quick and prolific as we have seen with the Sasser Worm attack that slammed even the most highly protected corporations. Also seen has been a grafting of a network sniffer with a virus. This collaboration of multifunctional abilities into self replicating applications is just a harbinger of infections. The best way to defend against a future attack is to understand what is on the horizon and so as to begin working on solutions before they appear.

II. Current Environment

The current means for fighting virus proliferation is based largely on reactive measures. Once a new virus is released into the wild, it can take days before the anti-virus houses can absorb the information and release an update to the definitions. More computer resources must be used as the virus definitions grow larger, forcing more patterns to be search/compared against. There exists the potential that the number of viral definitions will become prohibitive to the system.

To complicate matters, it is arguably not profitable, at this point in time, for the primary operating system companies to provide a secure and robust product. By allowing multiple vulnerabilities and opening to viruses and spyware, more sales are generated when the average user find their two year old system bogged down and is perceived slow; a new PC is purchased. The sale not only helps the operating system company but the industry as a whole potentially has a vested interest in generating more revenues. Further compounding the issue, recent indications are that pirated versions of operating systems will or are not eligible for security patches. This means to prevent piracy will result in hundred of thousands of known, insecure, target systems that can be slaved in a future attack.

Attacks are getting smarter; the Sobig variants have shown an alarming development; the virus would deactivate itself after a fixed number of days. The author(s) appear to have watched the behaviors and interactions of their systems, industry's reactions and then modified new releases to view the results. At least six variants were released in 2003, each with a time-to-live metric.

> *"It was a set of very well-controlled experiments," says Mikko Hypponen, the director of antivirus research at F-Secure, a computer security company. "The code is high quality. It's been tested well. It really works in the real world."*(1)

It was further suggested by Hypponen that this virus writer was alone, yet the apparent purposeful releases in conjunction with the implemented functionality does not fit behavior patterns found in prior virus writing and authors. Add to this the consideration, the code quality and testing, and this suggests a larger, coordinated operation. It has been suggested by Silicon.com because of the Sobig virus's linkages with spam, identity theft, it might have ties to organized crime.(2)

The UK reported in June 2005, “critical infrastructures” have been the target of ongoing attacks from a series of email based Trojans.

> *"These electronic attacks have been underway for a significant period of time with a recent increase in sophistication. ...the attackers are specifically targeting governmental and commercial organizations. ...IP addresses ... are often linked to the Far-East. Trojan capabilities suggest that the covert gathering and transmitting of otherwise privileged information is a principal goal. Files used by the attackers are often publicly available on the Web or have been sent to distribution lists. ...within 120 minutes of its release, indicating a high level of sophistication."*[3]

The attacks are targeted attempts to gather sensitive data stored on targeted victim’s machines. The recipient of such attacks has been primarily government and commercial entities. To further complicate matters, the attackers continually alter the Trojan/virus, thus rendering current anti-viral detection methods impotent.

Financial motives are a growing trend in virus proliferation. In a report about the changing nature of virus writer’s motives, the BBC talked with Mr. Hypponen, a chief researcher at F-Secure.

> *"This has changed who is our enemy," said Mr Hypponen. "We used to be fighting kids and teenagers writing viruses just for kicks." … "Now most of the big outbreaks are professional operations," he said. "They are done in an organized manner from start to finish."* [4]

It is clear that the current motives, means and resources for hackers are growing along with financial backing.

(Image source: amstelxp.blogspirit.com)

III. The Evolving Tends

> ***Alan Cox:*** *... at the moment computer security is rather basic and mostly reactive. Systems fail absolutely rather than degrade. We are still in a world where an attack like the slammer worm combined with a PC BIOS eraser or disk locking tool could wipe out half the PCs exposed to the internet in a few hours. In a sense we are fortunate that most attackers want to control and use systems they attack rather than destroy them.* [5]

The future of computer based attacks will not be the hacker breaking into a system, but a group who develops automated attacking systems based on virus like behavior.

There are several enabling technologies available and being enhanced or currently under development that will enhance the potency of future viral attacks.

- Bypassing Deep Packet Inspection
- Rate Based Detection Prevention
- Polymorphism / Mutation
- Undetectable Infections
- Multi-Mode Denial of Service Attacks
- Multi-Payload Attack Capabilities
- Multi-Waved Attack
- Multi-Platform Attacks
- Viral Symbiosis
- Self Modification / Child Modification
- Emergent Behavior
- Natural Language Processing
- AI

These technologies are all in various states of development with most available, some nearing completion and others still three to five or more years away.

• Bypassing Deep Packet Inspection

Deep packet scanning is the ability to scan across multiple data packets for tell-tail signatures of viruses and malware. Thus it is an effective means for examining data as it traverses across a network that might span multiple packets.

Hidden or Unknown Signatures

Deep packet scanning is easily by-passable because of the nature of the checking algorithms. Current virus signature checking mechanisms rely on finding fixed patterns of data that uniquely identify a virus or malware. This can be fool by altering the bit pattern in a sufficient manner while still retaining the functionality desired. Simplistic means of doing this are by using a polymorph engine attached to the virus, altering the code structure and recompiling, or hand editing the machine language/assembler, moving sections around and linking logically the execution path with jump sequences. See: Polymorphism / Mutation

Breaking Signature Code Across Multiple Files or Data Streams

If the signature of a viral system can be distributed across multiple paths, detection can become more difficult if not impossible. The purpose of this code is to reassemble an obscuficated virus that can bypass deep packet inspection systems; the code is part of the initial infection vector. It is small, and its functionality can be rewritten in a multitude of ways. This allows for a new attack to be generated quickly with simplicity of design and functionality. The executable will drop in as a root kit, remaining undetectable. It will then download, via http like means, 5 .jpg files. It will then reassemble a worm whose code image / binary as been spread across the jpg files.

This is a code snippet example for reassembling viral code from multiple file parts. First an agent downloads five ".jpg" files with valid JPG headers; the internal data contains malicious code that will be reassembled. The application then takes the five files and runs the following…

```
    image = malloc(size of  data* 5);  // Buffer to hold image
    for ( i = 0; i < size of  data; i++) {
        image[i] = file1 jpg [i + jpg_header_offset];
        image[i+1] = file2jpg[i + jpg_header_offset];
        image[i+2] = file3 jpg [i + jpg_header_offset];
        image[i+3] = file4 jpg [i + jpg_header_offset];
        image[i+4] = file5 jpg [i + jpg_header_offset];
    }
```

This code snippet can be hand crafted and reworked in so many different variations that the detection of the signature for this Virus Reassembly code is nearly impossible.

- **Rate Based Detection Prevention**

One of the principle means of intrusion detection is watching for out-of-pattern traffic on a network. These "finger prints" of viral activity are key indicators and should be understood so as to avoid such patterns.

Traffic Mimicking:

If it is possible to monitor the traffic on a network, then it would be possible for an attacking agent to mirror its data flow to look like normal traffic patterns. This would allow the flow to fall beneath the threshold of detection. This would require an attacking agent to be equipped with a pack sniffer and monitoring not just data rates, but also port and destination routing, building a map and then conforming to said maps patterns.

Time and Rate Based Propagation:

If an attacking agent is incapable of monitoring the network traffic for mimicking, because of complexity added to the executable or the network type (switched) does not allow, time and rate of propagation must be considered. With basic network pattern knowledge, a few rules can be devices to help a system fall within the normal traffic patterns for a network.

Intelligent/Controlled Infection Paths

Most infections do not contain cognation to identify machines already infected or have had attempts run against them. As a result, each new infection creates massive traffic as it wastefully attempts to attack machines already hit multiple times. This generates traffic and can be a quick indication of an infection and can be minimized by utilizing a parent child relation where the parent assigns to the child, a range of address to attack

- **Polymorphism / Mutation**

Self alteration of structure so that normal pattern matching detection systems fail; using polymorphism for chameleon capabilities. Current polymorphism focuses on encrypting the viral body with a small and difficult decryption sequence at the executables front. In this way, the body of the virus can be altered and difficult to detect and is a currently utilized technique.

A truly polymorphic virus could make a new copy of itself with a random name in a random location. The copy would be modified at the assembler level with various jump statements and other rearrangement of assembler code to allow the executable bit patterns to be altered, set the new viral image to boot next time and delete the parent virus. This would render the virus undetectable to today’s virus scanners as known executable image patterns would be changed.

A million, byte-different but functionally the same, worms flooded on the internet would require the collection and examination of each/most to build pattern matching, detection templates.

- **Multi-Mode Distributed Denial of Service Attacks**

Any infection vector will have a limited life span since patches to the exploit will be made available and virus signature files will be updated. An infection, as it spreads that attacks update points can prevent both infected and uninfected systems from applying the proper updates, allowing the infection system to propagate further.

Further attacking ISP networks, corporations (operating system companies, virus update locations), core internet infrastructure, DNS servers, cell phone towers, land line switching stations. It takes two to three days for a patch to be developed as a new virus is discovered; it takes weeks for an operating system to be updated to patch known security issues. By using timing mechanisms, a virus can spread rapidly and then leverage an added attack on operating system and virus definition update sites. Such a DDOS system can prevent any updates and solutions for not just infected systems but also uncompromised ones. This will help it to spread and remain embedded.

- **Undetectable Infections**

The ability to insert code into a system that tools cannot detect, common term “rootkit.” Infections can operate at the kernel level of Windows, Linux and Unix based operating systems or modify the OS to intercept the kernel/system calls and override the return, misinforming detection tools. This can render the operating system and any programs running in it, impotent; it also allows such programs to bypass or disable software firewalls and remain hidden from spyware and virus detection / removal tools and other protection systems running.

As rootkit technology evolves, it is becoming more difficult for tools existing within the compromised system to detect. Virtual Machine Based Rootkits (VMBR) install a virtual machine on the target system and then host the target OS, undetectable from within the hosted OS.

> *“When you are dealing with rootkits and some advanced spyware programs, the only solution is to rebuild from scratch. In some cases, there really is no way to recover without nuking the systems from orbit.”* . Danseglio, PM, Security Solutions Group, Microsoft (InfoSec World conference, April 2006)

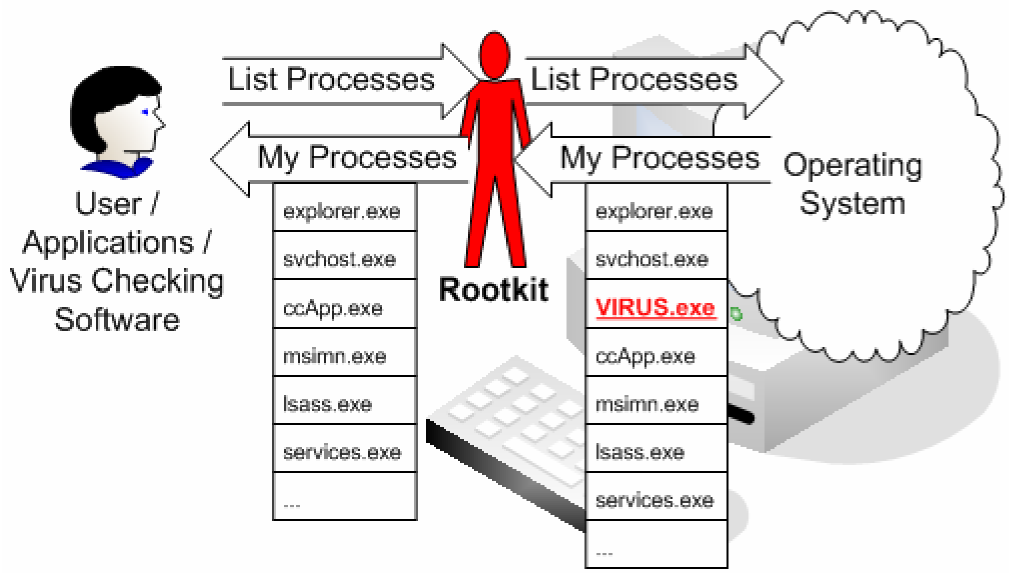

Figure 2. A rootkit overrides operating system calls, scrubbing data requested to hide itself and other viruses. This example illustrates how a user, running applications, including all current virus checking programs can be circumvented. The operating system cannot be trusted as its functionality is bypassed and all means of self checking.

This issue can be further extended since a majority of computers share a common set of hardware and drivers for video cards. With a limited number of players in the video card market, producing unified drivers and firmware, provides a target where base viral signatures can be embedded and will remain undetected. A virus can overwrite a portion of a video card's or other peripheral's firmware. This would cause the device to reactive the infection and no current virus protection programs have the capability to scan, detect and remove problems in a secondary device's memory.

Other attack vectors for systems are printers, file systems and other networked devices with increasingly more powerful memory and process capabilities but no protection or detection mechanisms.[6]

- **Multi-Waved Attack**

The ability to embed code into a BIOS, a video card or other boot strap program/processes so as to create a future weakness in a system that can be exploited by another viral wave/attack. On entry into a home network and disable a certain port in the home networks firewall since forty percent of home routers are default configuration with no password change. After the weaknesses have been inserted, the virus deletes all tracks of itself. This approach would require a well planned order of execution but would allow a second wave of attacks to spread in a devastatingly rapid manner. A series of different infections, over a period of time, can serve to create weaknesses exploitable for a later coordinated attack.

- **Multi-Payload Attack Capabilities**

The facility to attack via multiple means; the true blended attack. Not only the ability to spread via Email and worm like via the internet, a further capacity to jump from home wireless node to a neighboring wireless node and a means to attack multiple security vulnerabilities. Attack password systems by including a simple dictionary brute force attack sequence on operating system, WEP, WPA and Bluetooth wireless networks. In dense residential areas, with about 65% of all networks unencrypted, a virus capable of jumping locally, infecting network after network, bypassing router firewalls and then leverage the newly infected system to spread out via email and worm.

Different modules could also contain the ability to sniff a network, like a cable modem's, identify and infect machines before they update. By spoofing return packets for updates on the network, machines can be tricked into accepting a small download that actually contains the virus.

- **Multi-Platform Attacks**

Targeting not just PCs of different operating systems, but PDAs, cell phones, vehicles, etc… This is a variant of the Multi-Payload attack. The ability to recognize a target OS and request a payload capable of infecting the target or carry and select a payload targeted for a different operating system. Infect first one component in a home system and then spreading out, working on new systems. When a new target is found, the viral system attempts to identify the operating system and platform, broadcasts this information and seeks a new payload used to break and infect the target.

- **Viral Symbiosis**

The capability to hunt out new viruses, and merge or leverage their functionality, viral symbiosis. A smart virus (leach) scans and finds that a new virus (host) is infecting machines and leaves an opening on port X. The smart virus then scans for infected machines that have an opening on said port and moves into the infected machine. If the host virus propagates via email, the smart virus attaches itself along side the new. If the host virus propagates as a worm, the leach scans the machines IP activity to identify the new host viruses activity, jumping over / following.

A smart virus infects a mobile device and is brought inside of a trusted network (a home network). The smart virus scans the local machines to see what is available and can be targeted. If it is unable to break into any of the machines, it will then seek out a symbiotic infected machine outside of the trusted network. The smart virus on the mobile infected machine will act as a proxy for another virus; by accepting the attack request and redirecting it at a designated target machine. This will infect the target machine and the smart virus will then leverage the opening, infecting the target. Such a smart virus is able to leverage emerging threats, and thus, a once contained smart virus could surface weeks, if not months later.

- **Self Modification / Child Modification**

The capability of self modification or child spawning, once a better mode is discovered. This allows a parent virus to spawn a better version or variant, releasing it into the wild and having said variant report back to the parent any success. A parent virus can attempt different means of defeating virus pattern scanning system by spawning new copies with an altered image but the same attack means. It could further try randomizing attack functionality.

- **Emergent Behavior**

A means of communicating with children and sibling processes across the net for coordination, broadcasts of new discoveries and an evolving, complex pattern/process of highly distributed, coordinated, malicious system. Current virus models have a construct where each instance runs independent of each other, spending considerable energy and resources attempting to re-infect already targeted computers. If a machine is already infected or there was a prior failure to infect, further attacks on said system, with no change in the attack vector, will only result in wasted resources, resulting in a slower spreading infection.

Most virus writers do not have the knowledge or understanding of multiple systems/instances working in conjunction and the intercommunication that would allow for the evolvement of emergent behavior. The result is a mass coordination of a vast host of different attack, infection and destruction processes across LANs and WANs, all working in conjunction, growing stronger and more capable with each new infection.

> *"Emergent phenomena are often unexpected, nontrivial results of relatively simple interactions of relatively simple components. What distinguishes a complex system from a merely complicated one is that in a complex system, some behaviors and patterns emerge as a result of the patterns of relationship between the elements."* [7]

Emergent behavior would arise from such a wide network of infected systems that were designed and able to intercommunicate with each other, not acting as stand alone, slaves. This would result in a distributed system much more capable then any single infection point.

- **Natural Language Processing**

The capacity to parse natural languages from vulnerability assessment sites, gaining understanding and knowledge of current openings and exploits from search engines and security web sites. As a problem is found and described, the virus can parse the information and use it to further an arsenal of attacks. Furthermore, future viruses could leverage freely available “proof of concept” exploits.

- **AI / Cognitive Systems / Situational Awareness**

This is an enabling technology that will allow a virus to improve its attack vectors. An example of which could include a virus, with a small AI/Cognitive functionality, that has the ability to alter and change attacks, hunting for better means of penetration. Limited in scope applications could augment functionality and behavior, not necessarily acting as a system controller. Example: Utilizing an artificial intelligence to probe and monitor an intrusion detection and prevention system and then to devise means to dynamically defeat the pattern and protocol matching. Monitoring, learning and mapping a networks behavior so that attack patterns can blend in, avoiding intrusion detection systems.

Threat Availability and Complexity Chart

Technology Type	Availability	Project Complexity
Bypassing Deep Packet Inspection	Now	Low
Rate Based Detection Prevention	Now	Low
Polymorphism / Mutation	Now	Low
Multi-Mode DDoS	Now	Low
Undetectable Infections	Now	Moderate
Multi Waved	Now	Moderate
Multi Payload	Now	Variable – Moderate to High
Multi-Platform	Now	Variable – Moderate to High
Viral Symbiosis	Now to Near Future	Moderate
Self and Child Modification	3 to 5 Years	High
Emergent Behavior	3 to 5 Years	High
Natural Language Processing	5+ years	High
Ai / Cogitative Systems / Situational Awareness	5+ years	High

By utilizing a combination of these methods, the entirety of the net could be overwhelmed with an infection. There would be no way to update or patch systems as networks and the needed update sites would be clogged. As soon as you could patch a system, a new attack is discovered or another portion of the virus has gone undetected, embedded deep and broadcasts the new patch attempt allowing others to stop further patches. ISPs as a whole would need to cut off their services, whole countries would need to be block/quarantined. (Pentagon already is blocking access from certain country ISP's to .gov and .mil sites) A reassessment of the current connectivity would take place and be a reactive consideration with possible grave, long term ramifications.

IV. Solutions Must be Developed Now

A large problem is today's means of security is reactive and not proactive. To stop future infections, once proliferated, will be next to impossible if counter technologies are not already in place.

The following technologies must be enhanced or developed and built into existing firewall and network infrastructures prior to any major outbreaks.

- Combining network intrusion, virus detection and firewall protection systems into a single, cohesive and well behaved fusion of information gathered from across a network for a higher overall situational awareness.
- Utilizing "Angel" systems or processes capable of scanning for infected or insecure machines and can also identify infected machine behavior, penetrate and inoculate or terminate said target's connection. This would probably be best controlled by ISPs and be a requirement by their terms of service.
- Allowing for highly distributed protection systems to be able to intercommunicate securely with high authentication, allowing for information sharing about current situational awareness.
- The addition of AI, or cognitive systems, at multiple levels, into systems that can observe and learn normal patterns, looking for out-of-patterns states and more importantly, behaviors. Firewall and Viral protection systems must continue to evolve from current static blocking means to a cognitive, pattern and behavior recognition systems, has the ability to react by proactively increasing defensive states shring information in standardized reporting methods. ISPs must employ network traffic analysis tools with pattern recognition systems that can detect and stop emerging viral communication patterns/finger prints. Localized virus protection programs that can recognize the patterns or behaviors of a virus inside of a system by monitoring the activities of executing processes and the ability to warn or broadcast this information to increase network cognition.
- Development of out of band defensive technologies utilizing high assurance, EAL 6+ environments to secure less robust user interface programs.
- The placement of such protection system through out the internet, not just on corporate network, but also ISPs, home networks, data centers, routers, DNS systems, satellites, etc… A total infrastructure network of loosely conglomerated protection systems and processes.

V. Possible Scenarios

Save for the last, the following scenarios all leverage technologies available today. They are presented to future understanding of the potential harm that can be wrought.

Scenario 1: Rouge Country Cyber Attack.

Scores of embedded agents are placed throughout North America and Europe; some are on student visas, others fly into various countries, request asylum only never to report for their hearing, others just cross through unprotected borders. These agents embed themselves into various metropolitan areas with limited idea of their mission. Over a year passes and then one day, they are sent encrypted emails containing a payload of a bootable CD image and instructions of operations.

Day One: Christmas Eve

On Christmas Eve morning, by instruction, the agents boot the payload on 802.11 enabled laptops and drive all day in dense, suburban, affluent neighborhoods. The laptops scan for unencrypted networks, bypassing the wireless system's firewall and directly infect the network's computers. The agents continue to drive into the late evening, finishing by going to the airport and boarding a plane to home for Christmas.

Once a home network is infected, the system spends the rest of the evening attempting to break into neighboring wireless network. This is the first attack vector that is leveraged by the virus. With an included dictionary and brute force attack, it is able to spread, wirelessly, jumping across home networks. It also attempts a buffer overflow exploit with malformed packets, able to bypass encryption. The virus reconfigures the system to attack to the victim's network and is able to worm its way into the target machines utilizing a recently discovered and unpatched operating system opening.

Day Two: Christmas Day

Christmas morning, a second attack vector is added and starts to propagate via a worm and as an Email attachment; only at this time do the first signs of the infection appear. The Email attachment sends itself claiming to be Christmas morning pictures taken by the user. The infection attacks different security holes and exploits, by email attachment and continues to attack wirelessly. Furthermore, it hijacks the DNS/Hosts entries for Window's update and several anti- virus vendors, redirecting their queries to shadow sites that download more infected code. As a final blow, the virus installs itself as a series of drivers known as "root kits" with one remaining hidden at the kernel level. Removal of the infection triggers the hidden driver to examine the program attempting the deletion, stop it, reinstall and then prevent the removal tool from further execution.

Day Three

The day after Christmas, all infected machines add a third phase and start a Distributed Denial of Service against Microsoft's update and major virus protection update sites. The infection continues to spread, preventing possible fixes.

Day Five

All infected systems start attacking DNS machines, major online shopping sites, search engines, banks, and other critical infrastructure sites. This is the main target of the infection, a massive denial of services against the infrastructure of the internet.

Christmas time frame is chosen so that key personal will be out of offices, in many cases difficult to reach as they are on vacations for a week or more. While most corporate networks will not be heavily infected, the home networking systems will, and the reaction to find a solution will be days in coming because of the holidays.

Scenario 2: Industrial espionage/attacks.

A rival company creates a malicious worm that will infect just inside a target company's network. Using a modified satellite dish and an over powered 802.11g network card, they link into a rouge, unsecured wifi access point from half a mile away. The virus is directed to infect certain machines in the network and gather up key files, zip them and sends them back out. The virus continues to spread in the system for two hours and then uses a multiple pass overwrite on all .zip, .c, .cpp, .h, .doc, .ppt, .pdf, .exel, databases, emails, all files in recent lists both on local hard drives and then on networked drives. It then multiple-pass overwrites its own file signature, the hard drive swap space and then formats the local hard drives.

Scenario 3: Anti Business Group Attack.

A small group develops a virus and one of their members is able to gain employment inside the target company. The group member works for just over a month and then one evening, slips into a nearby cubicle, inserts a CDRom into the drive and boots the machine from the CD. The program executes a simple worm that waits a couple of hours before it spreads across the network, infecting machines, attempting to find files of interest and uploading to one of a multitude of ftp sites; these sites then Bittorrent the information. Targets for upload are consumer database files, accounting records including employee salaries, any file with two or more possible SSNs, personal data files, financial records, outlook and outlook express email databases. The purpose of the attack is to expose, embarrass and cause financial hard to the company.

Scenario 4: 2021

Breakthroughs in computational power, wireless and wired networking and communication protocols have allowed for the complete integration of the home network. All computers, phones, cars, answering machines, home monitoring and security systems have blended into a shared computing home resource, a highly interlinked system with basic self awareness provided by a distributed artificial intelligence. These systems are then linked into higher level, adaptive geo-location based clusters linked by regional nodes and global section nets. Global wireless communication based routing protocols and efficient MANET algorithms have pushed wired communication into a pure backbone support mechanism. Personal / Home systems are now capable of high distribution where the user on another continent can cheaply and easily access owned resources.

At first, the infection spreads quietly, from device to device, leap frogging networks and devices, pulling resources as needed and replacing AI functionalities. It is not a single infection but a system of viruses and worms, capable of coordinated symbiotic and multiplatform attacks with basic AI for finding, testing, monitoring and avoiding / bypassing detection systems.

A few days later, once a certain penetration threshold is achieved, the machines all stop. A majority of the transportation systems are gone, compromised communication systems stop functioning, power distribution's communication is interrupted and a cascading shutdown takes place. Huge chucks of systems halt and uninfected systems, reliant on the now shutdown systems cannot function properly. Without communication or their systems, stores cannot update inventories, warehouses cannot distribute to stores, and electricity distribution grids face wide scale brownouts as a critical percentage of the suppliers go offline.

The infection system was able to spread quickly, not raising any red flags, till the prescribed time. Unlike other attacks, it avoided already mapped out detection points, exploited vulnerabilities in software defined systems, leveraged openings in one trusted device to exploit others in a quiet and efficient manner. After a prescribed time and monitoring for effective penetration, a signal was sent out, cascaded by the infected systems and within ten minutes, shutdown their systems, overwriting boot strap, the BIOS, critical files, hardware and storage, rendering the devices useless. Vehicles, phones, computers, security systems, distribution systems, all compromised and then in an unparallel coordinated means, millions of systems rendered useless.

VI. The Aftermath, At What Cost

In the aftermath of a large scale attack, one capable of rendering useless machines either from DDoS on update sites with no cure to the infection (Scenario 1) or the destruction of BIOS and/or boot straps (Scenario 4), the cost to the national economy would be considerable. The ability to obtain a fix or protection would have to rely on receiving physical media with said protection software. This would require finding a solution to the virus system and the distribution of patches and signature detection applications media to the public with a simple means of installation that the average user would be capable of installing. Needless to say, this would require some time to coordinate and distribute.

The psychological impacts from large scale devastations create ripple effects that reverberate into the day to day patterns of even those who are not directly affected. The depths of the impacts of a nation wide crippling of the Internet, directly or indirectly hitting every user, would have profound and massive repercussions whose. A simple assertion, current Internet growth would be halted. New usage/expansion would stop as people would withdraw to a "comfort zone". A withdrawing to a "comfort zone" for the average user base might further result in shrinkage of Internet usage. The more obvious correlation would be a drop of commercial online usage patterns impacting online purchases, banking and nearly halt IT spending as user confidence in networked systems would degrade. A small, but significant percentage of the user base would outright reject the "Internet" out of a fear and mistrust. Second and third order effects would send profound reverberation throughout our national and world economy and possibly drive our country into a depression. Consumer confidence would plunge and spending would dry up.

Sources:

(1) Thompson, Clive "The Virus Underground" accessed February 24, 2004
http://www.collisiondetection.net/mt/archives/000704.html

(2) Silicon.com, "Top 50 Agenda Setters 2003", accessed March 22, 2004
http://www.siliconagendasetters.com/list42.html

(3) NISCC Briefing 08/2005, "Targeted Trojan Email Attacks", accessed June 19, 2005
http://www.niscc.gov.uk/niscc/docs/ttea.pdf

(4) Ward, Mark "Money motive drove virus suspects" BBC News, accessed September 6, 2005
http://news.bbc.co.uk/1/hi/technology/4205220.stm

(5) Dumbill, Edd, "The Next 50 Years of Computer Security: An Interview with Alan Cox" O'Reilly Network, accessed September 20, 2005 http://www.oreillynet.com/pub/a/network/2005/09/12/alan-cox.html

(6) Schuman, Evan "When Safe Devices Become Smart and Dangerous" Ziff Davis Internet, accessed October 6, 2005 http://www.eweek.com/article2/0,1895,1863742,00.asp

(7) Wikipedia, "Emergence", accessed June 19, 2005 http://en.wikipedia.org/wiki/Emergent
Minasi, Mark "Follow-Up: Why Microsoft Can't Stop Root Kits" accessed February 29, 2005
http://www.windowsitpro.com/Article/ArticleID/45518/45518.html?Ad=1

Naraine, Ryan "'Shadow Walker' Pushes Envelope for Stealth Rootkits" eWeek.com, accessed October 6, 2005 http://www.eweek.com/article2/0,1895,1841266,00.asp

Oleg Kolesnikov, and Wenke Lee "Advanced Polymorphic Worms: Evading IDS by Blending in with Normal Traffic" Georgia Institute of Technology http://www.cc.gatech.edu/~ok/w/ok_pw.pdf

President's Information Technology Advisory Committee, "Cyber Security: A Crisis of Prioritization" accessed February 29, 2005 http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

Princeton Survey Research Associates International, "Leap of Faith: Using the Internet Despite the Dangers" October 26, 2005 http://www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm

Raja, Sanjay "Network Intrusion Prevention Systems - Why "Always On" Stateful Inspection and Deep Packet Analysis are Essential to Deliver Non-Stop Protection" Top Layer Networks, Inc. January 16, 2005