A White Paper by
Paul A. Henry MCP+I, MCSE, CISSP
CyberGuard Corporation

CYBERGUARD CORPORATION

Covert Channels Provided Hackers the Opportunity and the Means for the Current Distributed Denial of Service Attacks

The recent DDoS attacks have been labeled a wake-up call; if that is the case then many have been hitting the snooze button repeatedly, since the warnings started as early as 1983.

Covert channels are not a new methodology; in fact the theoretical dangers of covert channels were first addressed in the National Computer Security Center's (NCSC) - Trusted Computer System Evaluation Criteria (TCSEC) as early as in 1983 and 1985.

- Orange Book Parts I and II: *THE CRITERIA, RATIONALE AND GUIDELINES*
  http://www.stacken.kth.se/pub/linux/libs/security/Orange-Linux/refs/Orange/OrangeI-II-8.html

Later in 1990 as covert channels moved from the realm of theoretical to possible, in France, Germany, the Netherlands and the UK a testing methodology for covert channels was developed and published: Information Technology Evaluation Criteria (ITSEC).

- Information Technology Security Evaluation Criteria ITSEC
  http://www.itsec.gov.uk/docs/pdfs/formal/ITSEC.PDF

In the mid 1990s as covert channels moved from the realm of possible to probable many papers were published outside of government that explicitly detailed covert channel exploits at the application level and in many cases provided working source code to build a fully functional covert channel.

- Project LOKI - ICMP Tunneling
  Phrack Magazine, Volume Seven, Issue Forty-Nine
  http://www.2600.com/phrack/p49-06.html
- LOKI 2 The implementation
  Phrack Magazine, Volume 7, Issue 51
  http://www.2600.com/phrack/p51-06.html
- Covert Channels in the TCP/IP Protocol Suite
  Craig H. Rowland
  http://www.psionic.com/papers/covert/covert.tcp.txt

Most recently, covert channels were yet again addressed in Common Criteria (CC) which was established as an international alignment of TCSEC, ITSEC and the Canadian CTCPEC for carrying out security evaluations.

- COMMON CRITERIA VERSION 2.1(aligned with IS 15408) Part 3 - Assurance Requirements
  http://csrc.ncsl.nist.gov/cc/ccv20/p3-v21.pdf

They were aware of the threat and aware of the technology available to eliminate this threat. This was not a failure on the part of the government to spread the warning, it was a failure of organizations with networks connected to the Internet to exercise due diligence in protecting their networks with available technology.

Covert channels are the principle enablers in a □ □ DDoS attack.

Without covert channels, attackers would not have the ability to command distributed agents used to launch these attacks. If you eliminate the ability to communicate with the agent that launches the attack you effectively eliminate the threat of the attack.

Many vendors in response to the tremendous media attention generated from recent DDoS attacks are claiming to offer "new products" or "new product suites" which can eradicate the threat of a DDoS attack. There is no magic pill to eliminate the threat of a DDoS attack. Some products do provide a methodology for reporting the fact that you are under attack to your ISP, but they simply do not eliminate your chances of being attacked. The only effective way to eliminate the threat of a DDoS attack is to prevent the deployment of the respective distributed agents and /or eliminate the covert channels used to control them.

What is a covert channel?

A "covert channel" can be described as: *"Any communications channel that can be exploited by a process to transfer information in a manner that violates the system's security policy." [1] Essentially it is a method of communication that is not part of an actual computer systems design but can be used to transfer information to users or system processes that normally would not be allowed access to the information.*

Covert channel exploits typically require a malicious client or server program operating on a PC outside the protected network and a malicious server or client program operating on a server inside the protected network.

The malicious PC outside the protected network would encapsulate the desired protocol within a given protocol that is allowed by the security policy of the protected network's firewall. The malicious PC on the outside of the protected network would then transmit this allowed protocol through the firewall, directed to the IP address of the server running the malicious receiving program inside the protected network. The receiving program would strip off the transport protocol thereby leaving the original malicious data in its original protocol form. These packets would either then be used by the server running the receiving program or be automatically sent to a predetermined IP address of another server or PC within the network.

Without covert channels, DDoS Attacks would simply not be possible.

In order to fully understand the part covert channels played in the recent DDoS we first need to look at the DDoS attack model:

Distributed DOS attacks are highly complex and intelligent. A malicious user typically gains access to a protected network via a common exploit such as buffer overflow of various RPC utilities for Solaris-based servers, weaknesses in services such as WUFTP in Linux-based servers and through executable programs attached to email messages in NT-based servers. Once access to these systems has occurred, the user places the master and agent programs onto these systems in inconspicuous locations and renames them to appear as localized utilities on that system.

> Prevention of a breach that would allow an attacker to deploy a Trojan on your network is critical. In many cases it is not necessary to attack the firewall to gain entry into the corporate network...

Once installed, the DDOS "network" is established. The malicious user contacts the masters via various mechanisms such as covert channels in ICMP or UDP broadcasts. Typically, the master communicates with the agents using a covert channel derived from modified ICMP echo reply packets that contain various instructions to control the behavior of the agents. The list of IP addresses associated with the agents is usually encrypted so that if the master were discovered, the agent systems will remain unknown. Some masters are so intelligent as to incorporate remote file copying in order to deploy new agents onto compromised systems or to permit the automatic upgrading of established agents.

Masters and agents are also intelligent in so far that they are capable of deploying "decoy" packets to confuse intrusion detection systems and other DOS attack tracking programs from locating them.

The DDoS Attack model consists of:

· Client, which can initiate commands to hundreds of masters.

· Masters, who are typically hidden on compromised systems with moderate bandwidth availability that processes client commands for up to 1000 agents.

· Agents (Daemons), which are typically hidden on compromised systems with high bandwidth availability, which carry out these commands.

In this model the attacker can distribute the "work" of the denial of service attack effectively across potentially thousands of compromised computers. The client issues a single command to the masters, and they in turn contact their respective agents and the attack commences against the defined target.

In a DDoS, it is the communications between the client, master and agent that takes advantage of the covert channel flaws in most protective mechanisms such as firewalls. Specifically in the recent DDoS attacks indicated, the ICMP protocol was used as the covert channel to issue the commands to the distributed agents. Additional stealth was gained by using encryption to further hide the DDoS commands within the covert channel.

A comprehensive acceptable use policy as a part of your security policy and a strong firewall on a secured operating system to guard your network connection to the Internet are your best defenses.

Employees must be trained to recognize the risks they are taking when they download software from the Internet, open executable files attached to email and load software from any source on a PC in the organization's network. Education of your employees should be an ongoing effort to keep pace with the ever-changing threat.

Prevention of a breach that would allow an attacker to deploy a Trojan on your network is critical. In many cases it is not necessary to attack the firewall to gain entry into the corporate network;

· Why attack a strong firewall if the operating system it runs on has known weaknesses? Think of it as you would your own home; operating a supposedly strong firewall on an unsecured operating system is equivalent to locking the front door but leaving the back door and all the windows of your home open.

· The attacker can attack weak services i.e.; WUFTP, IIS4, or Send Mail to find a known weakness that provides entry.

With respect to weakness in services, using strong proxy technology to verify the length of protocol headers to reduce the possibility of protocol header-based buffer overruns is also an often-overlooked defense.

Once a Trojan has been installed there is little any firewall can do to prevent data from being transmitted over a covert channel. Simply put the technology does not exist to inspect the payload of a packet to determine if in fact the data that is contained within the packet belongs to the protocol being utilized.

Prevention of the deployment of the Trojan is crucial as numerous protocols in the TCP/IP protocol suite have weaknesses that allow an attacker to construct a covert channel i.e.; TCP, UDP, ICMP, HTTP and FTP. If you allow an attacker the opportunity to deploy a Trojan on your network that enables a covert channel, the attacker can use this covert channel in a wide variety of ways:

· Bypass Firewalls

- Run services that were not permitted by the firewall over covert channels in protocols that are permitted, i.e., even with a restrictive firewall, if HTTP access is allowed through a common HTTP proxy, it is possible to establish a covert channel and telnet or PPP connect to a computer outside the firewall.

· Bypass HTTP Content Filtering

- Most content filtering applications restrict an internal user's access to websites who's URL is contained in a database of websites that are not permitted. The malicious user can establish a covert channel over HTTP to a PC outside the protected network. To the content filter it appears that the user is connected to a website that is not in the database of websites that have been restricted. The user is able to freely surf the dark side if the Internet unimpeded by the organization's content filtering application.

· Bypass Anti Virus Filtering

- With a covert channel over a protocol that is not serviced by the organization's anti virus application, the user is free to move a Trojan over the covert channel to a server behind the protected network.

Once a Trojan has been installed, there is little any firewall can do to prevent data from being transmitted over a covert channel.

· Move data secretly out of a protected network

- Using a covert channel in a protocol that is not commonly logged the attacker user can steal your organization's intellectual property and move it out of your network without a trace.

· Move data secretly into a protected network

- Using a covert channel in a protocol that is not commonly logged the malicious user can "park" files stolen from other compromised networks to othe r compromised networks for storage and future retrieval. By storing these files on other compromised systems the attacker eliminates the risk of being caught with these materials on the attackers own PC.

· Move hacking tools secretly to servers within a protected network

- Using a covert channel that is typically not logged the attacker can move remotely controlled hacking tools to the protected network

· Launch discovery operations into other networks while hiding within a compromised network

- The attacker can use a covert channel to secretly operate remote hacking tools to search for vulnerabilities to be exploited in other networks. Should the activities be discovered by the protection mechanisms in the other network, it would appear that the probe originated from the compromised network not from the IP address of the attacker.

Most protective mechanisms simply do not address the issue of covert channels.

Recent quotes from Rich Pethia, director of a federally funded computer emergency response operation at Carnegie Mellon University in Pittsburgh:

"There is little evidence of improvement in the security features of most products. Developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities."

"Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on security features"

In the days of slower microprocessors many firewall vendors chose to sacrifice security for overall firewall performance. In minimizing the security-related work they perform to increase performance, they do not provide the capability to inspect the packets passing through the firewall in enough detail to determine if a covert channel is being utilized.

These type of firewalls are only typically concerned with source - destination address, source - destination ports, communications state and to a limited degree the filtering of specific application level commands contained within the payload of the packet. Often the inspection is limited to known protocol header fields specific to a given protocol. Malicious data can be passed through in a multitude of areas that are not used for normal transmission or are optional fields to be set as needed by the sender of the packet.

In many cases the packet can carry all of the necessary correct information for an allowed protocol while in fact the data portion of the packet contains the malicious data specific for a protocol that would otherwise not be permitted. Typically these packets would be sent to a Trojan program running on a server behind the firewall that would have the ability to properly decode these packets in to a usable form for the attacker.

As network security has advanced, so has malicious covert channel technology. When stateful technologies were initially deployed, unless explicitly permitted, they effectively blocked external users from opening a connection to a server behind a firewall without the internal server first requesting this communication. Attackers quickly modified their malicious programs to cause the internal program, either at a specific time or desired interval, to open a connection from behind the firewall to the external malicious program facilitating the connection required for the covert channel. Since the internal malicious program was using a permitted protocol it simply looked like just another internal user accessing what was permitted within the firewall security policy.

Unfortunately, as processor speeds increased, many vendors chose to add additional bells and whistles rather then increasing the overall level of security their products could attain.

If you do not break the client - server model, you cannot break the covert channel.

Many firewall vendors irrationally claim that not breaking the client-server model offers some form of security advantage. With older slow microprocessors this did effectively increase performance as less work is physically done, but it reduces the level of security that can be attained and in fact subverts the purpose of a firewall: securing the Internet connection. This misguided approach in failing to break the client-server model provides a direct path for the attacker to implement a covert channel.

With today's faster microprocessors and the incorporation of Symmetrical Multiprocessing capability in firewall software, performance is simply no longer an issue. Stronger security methodologies can be exercised without an unacceptable negative impact on performance.

Strong proxy technology breaks the client-server model and solves in part the covert channel dilemma.

In a strong application proxy the client-server model is broken:

· Acting on behalf of the user, the proxy terminates the connection at the proxy within the firewall.

· The proxy creates a new "blank" empty packet.

· The proxy is "application aware" and fully inspects the original packet; if a permitted command is found in a protocol header, then that command alone is entered into the new packet. Any data that may have been encoded in unused headers in the original packet is dropped, as it is simply not included in the new packet.

· All protocol headers are inspected to verify header length is RFC compliant.

· The proxy creates a new connection between the proxy and the protected server.

· The proxy sends the newly created packet to the protected server.

In a strong application proxy there is no direct connection between the malicious user and the protected server. Any malicious data that is hidden in unused protocol header fields is simply dropped and is not passed to the protected server. Strong proxy technology is not new and can be found in existing firewall offerings.

Unfortunately, as processor speeds increased, many vendors chose to add additional bells and whistles rather then increasing the overall level of security their products could attain...

Covert Channels in Operating Systems

While operating system covert channels are not currently commonly exploited, due diligence dictates that the threat be recognized and dealt with accordingly. A firewall can only be as strong as the operating system upon which it operates. The technology exists which effectively eliminates the issue of covert channels in the operating system. Vendors basing their firewall design on the published guidelines of the NCST Orange Book "B" Level of Trust are quickly becoming more popular as organizations recognize the inherent value of operating their firewall application integrated with a Secure Operating System.

Recommendations for effectively dealing with the threat of DDoS attacks

· If you do not have a firewall, apply anti-IP spoofing rules at your boundary routers (Network Ingress Filtering).

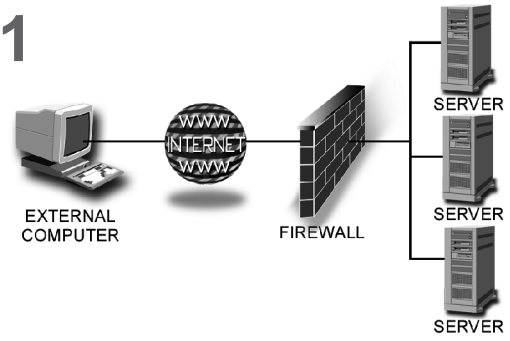
· If you have a firewall apply anti-IP spoofing rules on the external interface to block incoming spoofing attempts and just as importantly apply anti-IP spoofing rules to your firewall's internal interfaces to prevent your internal users from IP spoofing packets that are leaving your network destined to external servers.

· Secure your network connection to the Internet with a firewall operating on a secured operating system, which has been independently certified to offer a Level of Trust that meets with the requirements of your organization's security policy. In today's litigious

-- continued on page 6

HOW IT'S DONE...

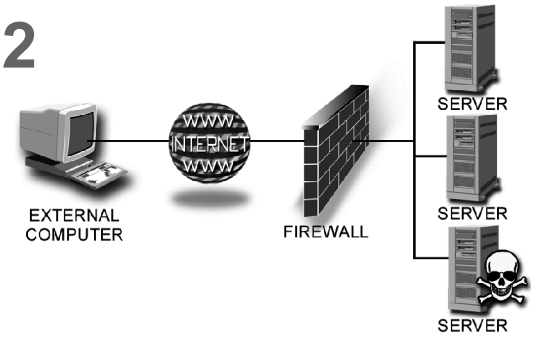
1



Typical corporate configuration.

Firewall blocks all connections originating from outside but allows internal users to surf the web, telnet to outside computers and use FTP to download files from the Internet.

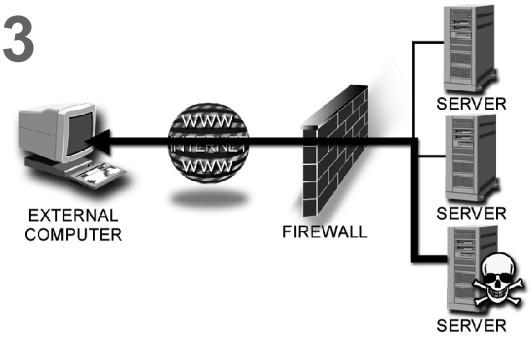
2



A tunnel Trojan program is loaded on a server behind the firewall.

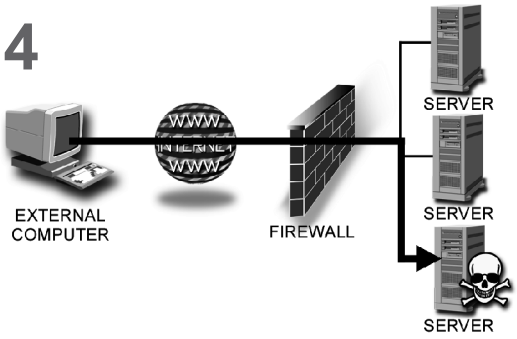
Deployment can be a buffer overrun, weakness in FTP service, an attachment in an e-mail, social engineering, a disgruntled employee or simply an employee trying to outsmart the administrator who blocked access to his computer from his home.

3



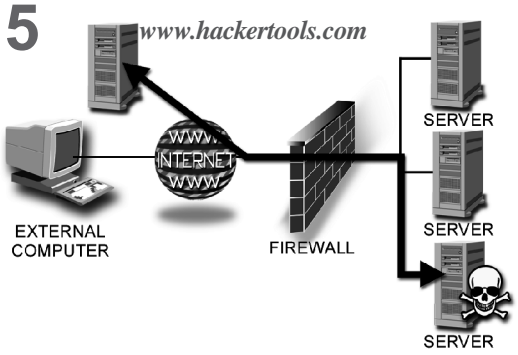
Trojan program at a specific time, opens a www connection to the remote computer. This simply looks like an internal user connecting to an external web page to the firewall. The connection uses the allowed http protocol and simply instructs the remote computer that the server is now ready for remote commands. This effectively opens a connection through NAT as well.

4



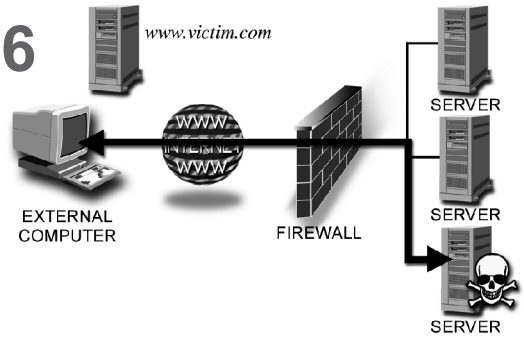
Now that a connection is open, the remote computer using the http protocol can send his reply with embedded commands to the server.

5



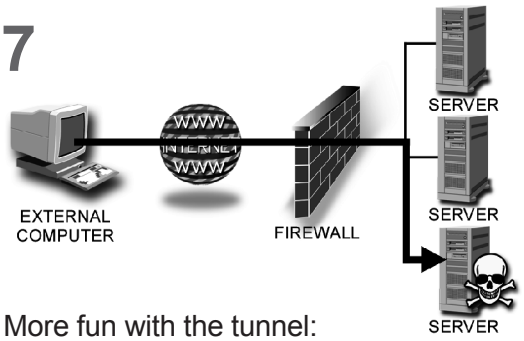
Remember, internal users are allowed to use FTP that originates internally ... The server looks like an internal user to the firewall. The external computer can tell the server to FTP an external server that contains hacking tools and to download discovery and DoS exploit tools ...The Trojan on the server FTPs the hacker tools from the remote FTP server and stores them on the server. Again, this FTP connection is originated from the internal network and looks like a normal internal user to the firewall.

6



Trojan program uses the http tunnel to tell the remote computer that the download is complete. The hacker can now control these new tools over his covert channel to attack other networks while hiding behind the address of the compromised network.

7



More fun with the tunnel:

*Send me all *.xls files from accounting*
*Send me all *.ccp files from development*
*Send me all *.doc files from legal*

society, if you ignore due diligence and attach a weak system to the public Internet, you may find yourself financially liable for putting your neighbors at risk

· Scan your internal network for detection of DDOS master and daemon programs on compromised systems.

· Block any and all protocols to your internal network that cannot be examined with strong application proxies.

· Do not allow remote users access to internal servers without strong authentication and encrypted communications (VPN).

· Move all public access servers to an isolated DMZ.

· Block all access from internal users to servers located on the DMZ.

· Separate all offered public services on independent servers within the DMZ.

· Remove all unused services on all public access servers on the DMZ.

· Remove all unnecessary services on client computers within the protected network.

· Profile network traffic flows for changes that may be an indicator of malicious use.

· Keep regular Audit Trails - Do not allow log files to roll over thereby overwriting potential evidence.

· An organization's security policy is not a static policy to be occasionally reviewed and locked away. Adjust your organization's security policy continuously to match the ever changing current security threats

- Review and update your organization's security policy to establish, monitor and enforce acceptable use policies to prevent introduction (downloading) of malicious applications.

- The response to a DDoS attack goes well beyond the target organization capabilities to defend itself and requires a coordinated effort between the target and the target's ISP. As your Internet access may be effectively eliminated during a DDoS attack you must plan for out - of -band communications to your ISP to support a coordinated effort in blocking hostile connections well before they reach your Internet gateway.

- Pre-determine (1) whom to contact to elicit the assistance of local, state and federal authorities and (2) how to contact them on an out-of-band channel.

An organization's security policy is not a static policy to be occasionally reviewed and locked away. Adjust your organization's security policy continuously to match the ever changing current security threats.

- Have the necessary tools and training for rapid log file analysis to define offending source network IP addresses.

- Make intrusion scanning and vulnerability assessments with current signature files on your gateway and internal network a regular practice and not an occasional event

- Monitor the status of critical programs on your gateway, public access servers and important internal servers with a program like TripWire for changes that may be an indicator of malicious activity.

- Regularly educate employees on the ever-changing threats to network security and their respective individual responsibilities to uphold the organization's network security policy. Use every possible opportunity to reinforce the need for adherence to the organization's acceptable use policy. ■

References:

· The Criteria, Rationale And Guidelines Orange Book I & II

· "Information Technology Security Evaluation Criteria ITSEC"
http://www.itsec.gov.uk/docs/pdfs/formal/ITSEC.PDF

· "Project LOKI - ICMP Tunneling"
Phrack Magazine, Volume 7, Issue 49
http://www.2600.com/phrack/p49-06.html

· "LOKI 2 The implementation"
Phrack Magazine, Volume 7, Issue 51
http://www.2600.com/phrack/p51-06.html

· "Covert Channels in the TCP/IP Protocol Suite" Craig H. Rowland
http://www.psionic.com/papers/covert/covert.tcp.txt

· "COMMON CRITERIA VERSION 2.1(aligned with IS 15408)"
Part 3 - Assurance Requirements
http://csrc.ncsl.nist.gov/cc/ccv20/p3-v21.pdf

Additional Information:

· CyberGuard Corporation *http://www.cyberguard.com*

· "CERT Analysis of DDoS" *http://www.cert.org/advisories/CA-2000-01.html*

· "Trinoo Analysis" *http://staff.washington.edu/dittrich/misc/trinoo.analysis*

· "Tribe Flood Network (TFN) Analysis" *http://staff.washington.edu/dittrich/misc/tfn.analysis*

· "Stacheldraht Analysis" *http://staff.washington.edu/dittrich/misc/stacheldraht.analysis*

· "TFN2K Analysis" *http://packetstorm.securify.com/distributed/TFN2k_Analysis.htm*

· "Strategies for Defeating Distributed Denial of Service Attacks"
http://razor.bindview.com/publish/papers/strategies.html

· "Network Ingress Filtering RFC 2267 (January 1998)" *http://www.ietf.org/rfc/rfc2267.txt*

· "Reverse WWW Tunnel" *http: //www.infowar.co.uk/thc/files/thc/fw-backd.htm*

· "Leap Frog 1.0 - Telnet over Covert Channel" *http://www.cotse.com*

· Agent Discovery Tools

http://dr.watson.ibm.com/nsa

http://www.fbi.gov/nipc/trinoo.htm

http://staff.washington.edu/dittrich/misc/sickenscan.tar

http://staff.washington.edu/dittrich/misc/ddos_scan.tar

2000 West Commercial Boulevard, Suite 200
Fort Lauderdale, FL 33309
954-958-3900
fax: 945-958-3901