WIKIPEDIA

TCP reset attack

TCP reset attack, also known as "forged TCP resets", "spoofed TCP reset packets" or "TCP reset attacks", is a way to tamper and terminate the Internet connection by sending forged TCP reset packet. This tampering technique can be used by a firewall in goodwill, or abused by a malicious attacker to interrupt Internet connections.

The Great Firewall of China is known to use TCP reset attack to interfere with and block connections, as a major method to carry out Internet censorship.

Contents

Technical Background

The Internet is, in essence, a system for individual computers to exchange electronic messages, or packets of IP data. This system includes hardware to carry the messages (such as copper and fiber optics cables) and a formalized system for formatting the messages, called "protocols". The basic protocol used on the Internet is the IP (Internet Protocol), which is usually coupled with additional protocols such as TCP (Transmission Control Protocol[1]) or UDP (User Datagram Protocol). TCP/IP is the protocol set used for email and web browsing. Each protocol has a block of information, called a header, included near the front of each packet. Headers contain information about which computer sent the packet, which computer should receive it, the packet size, etc.

TCP is used with IP when a two-way virtual connection is required between two computers. (UDP on the other hand is a connectionless IP protocol.) TCP software on the two machines which will communicate (for example a workstation with a browser and a web server) by exchanging a stream of packets. Using a TCP connection gives the computers an easy way to exchange data items too big for a single packet, such as video clips, email attachments, or music files. Although some web pages are small enough for a single packet, they are sent over TCP connections for convenience.

TCP resets

In a stream of packets of a TCP connection, each packet contains a TCP header. Each of these headers contains a bit known as the "reset" (RST) flag. In most packets this bit is set to 0 and has no effect; however, if this bit is set to 1, it indicates to the receiving computer that the computer should immediately stop using the TCP connection; it should not send any more packets using the connection's identifying numbers, called ports, and discard any further packets it receives with headers indicating they belong to that connection. A TCP reset basically kills a TCP connection instantly.

When used as designed, this can be a useful tool. One common application is the scenario where a computer (computer A) crashes while a TCP connection is in progress. The computer on the other end (computer B) will continue to send TCP packets since it does not know that computer A has crashed. When computer A reboots, it will then receive packets from the old pre-crash connection. Computer A has no context for these packets and no way of knowing what to do with them, so it might send a TCP reset to computer B. This reset lets computer B know that the connection is no longer working. The user on computer B can now try another connection or take other action.

Forging TCP resets

In the scenario above, the TCP reset bit was sent by a computer that was one of the connection endpoints. It is possible for a 3rd computer to monitor the TCP packets on the connection and then send a "forged" packet containing a TCP reset to one or both endpoints. The headers in the forged packet must indicate, falsely, that it came from an endpoint, not the forger. This information includes the endpoint IP addresses and port numbers. Every field in the IP and TCP headers must be set to a convincing forged value for the fake reset to trick the endpoint into closing the TCP connection. Properly formatted forged TCP resets can be a very effective way to disrupt any TCP connection that the forger can monitor.

Legitimate use of TCP reset injection

One obvious application of a forged TCP reset is to maliciously disrupt TCP connections without the consent of the two parties which own the endpoints. However, network security systems using forged TCP resets have been designed as well. A prototype "Buster" software package was demonstrated in 1995 that would send forged resets to any TCP connection which used port numbers in a short list. Linux volunteers proposed doing something similar with Linux firewalls in 2000,[2] and the open source Snort used TCP resets to disrupt suspicious connections as early as 2003.[3]

The IETF considered TCP resets by firewalls, load-balancers and web-servers harmful in RFC3360.[4]

Comcast Controversy

By late 2007, Comcast began using forged TCP resets to cripple peer-to-peer and certain groupware applications on their customers' computers.[5][6] This started a controversy, which was followed by the creation of the Network Neutrality Squad (NNSquad) by Lauren Weinstein, Vint Cerf, David Farber, Craig Newmark and other well-known founders of and champions of openness on the Internet.[7] In 2008, the NNSquad released the NNSquad Network Measurement Agent, a Windows software program written by John Bartas, which could

detect Comcast's forged TCP resets and distinguish them from real endpoint-generated resets. The technology to detect the resets was developed from the earlier open-source "Buster" software which used forged resets to block malware and ads in web pages.

In January 2008, the FCC announced it would investigate Comcast's use of forged resets, and, on August 21, 2008, it ordered Comcast to terminate the practice. [8]

Prevention

IPsec

Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

See also

- DNS hijacking

References

1. TCP specification (http://www.ietf.org/rfc/rfc0793.txt)
2. May 2000 Linux discussion archives (http://lists.netfilter.org/pipermail/netfilter/2000-May/003971.html)
3. SNORT discussion archive: TCP resets (http://marc.info/?l=snort-users&m=107792974908563&w=2)
4. Inappropriate TCP Resets Considered Harmful (https://tools.ietf.org/html/rfc3360)
5. Section of Wikipedia Comcast article
6. Associated Press, Comcast Blocks Some Internet Traffic (http://www.msnbc.msn.com/id/21376597/)
7. NNSquad home page (http://www.nnsquad.org/)
8. Commission Orders Comcast To End Discriminatory Network Management Practices (https://apps.fcc.gov/edocs_public/attachmatch/DOC-284286A1.pdf)

External links

- SNORT Official website (http://www.snort.org/)
- EFF report on Comcast use of resets (https://www.eff.org/wp/packet-forgery-isps-report-comcast-affair)
- ICMP Attacks against TCP. Similar attacks using ICMP (https://tools.ietf.org/html/rfc5927)
- Improving TCP's Robustness to Blind In-Window Attacks (https://tools.ietf.org/html/rfc5961)