White Paper

Protect Against Advanced Evasion Techniques

Essential design principles

Olli-Pekka Niemi
Head of the Vulnerability Analysis Group
McAfee

Table of Contents

Understanding Evasion Techniques 3

Weak Points in Current Network Security Devices 4

The McAfee Network Security Advantage:
A Data Stream-Based Approach with Layered Protocol Analysis 5

IP 5

TCP 6

Server Message Block 7

MSRPC 8

SunRPC 8

HTTP 8

Centralized Management and Evasion Protection 9

Evasion R&D and In-House Testing: 24/7 Capabilities 9

Commercial Anti-Evasion Readiness Test Tool 10

Conclusion 10

Supporting Research 10

The network security paradigm is currently shifting toward a new reality as advanced hacking methods become more prevalent and harder to detect. An example of such a method is advanced evasion techniques (AETs). Although evasions have been documented extensively in the last 15 years, security vendors have systematically ignored the significance of evasions. Some vendors have even downplayed the threat posed by evasions as being purely theoretical. Yet this debate misses the bigger issue: the risk of network security systems being compromised by AETs continues to grow as more and more cybercriminals actively exploit this vulnerability.

McAfee® Next Generation Firewall addresses this challenge. Combining stream-based inspection with data normalization on multiple protocol layers, McAfee Next Generation Firewall is highly resistant to AETs and offers a novel approach to design and implementation to prevent these evasion techniques.

This paper explains the technical and design principles behind our breakthrough anti-evasion technology.

Understanding Evasion Techniques

Background

> *"The implementation of a protocol must be robust. Each implementation must expect to interoperate with others created by different individuals. While the goal of this specification is to be explicit about the protocol, there is the possibility of differing interpretations. In general, an implementation should be conservative in its sending behavior, and liberal in its receiving behavior. That is, it should be careful to send well-formed datagrams, but should accept any datagram that it can interpret (e.g., not object to technical errors where the meaning is still clear)."*
>
> *—RFC 760, DoD Standard Internet Protocol, January 1980*

A leading principle in Internet protocol design is the robustness principle, as quoted above. It is a sound engineering principle that is the cornerstone of the Internet.

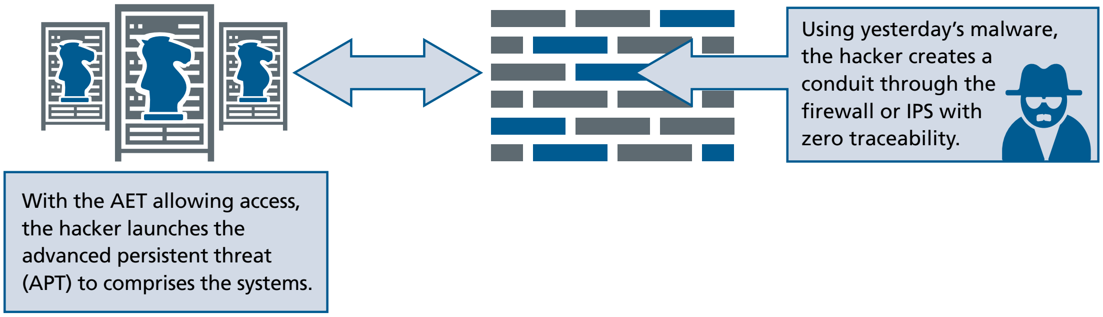
However, Internet protocols are often complicated and allow various interpretations in implementation. By making use of rarely used protocol properties in unusual combinations, an attacker may make it difficult for information security systems to detect an attack. In addition, an attacker may make detection even harder by deliberately crafting network traffic that disregards conventional protocols. If the receiving end of the traffic liberally attempts to interpret the traffic, an attack may reach the destination undetected. Such obfuscation techniques are collectively known as evasion techniques.

Key principles

Advanced evasion techniques can be identified according to certain underlying principles:

- Delivered in a highly liberal way.
- Security devices are designed in a conservative way.
- Employ rarely used protocol properties.
- Use unusual combinations.
- Create network traffic that disregards strict protocol specifications.
- Exploit the technical and inspection limitations of security devices: memory capacity, performance optimization, design flaws.

Evasion techniques are a means to disguise cyberattacks in order to avoid detection and blocking by information security systems. Evasions enable cybercriminals to deliver malicious content to a vulnerable system without detection that would normally stop the threat. Network security systems are ineffective against evasion techniques in the same way a stealth fighter can attack without detection by radar or other similar defensive systems.



Using yesterday’s malware, the hacker creates a conduit through the firewall or IPS with zero traceability.

With the AET allowing access, the hacker launches the advanced persistent threat (APT) to comprises the systems.

Figure 1. Advanced evasion techniques: “the method for access.”

Relying exclusively on protocol anomalies or violations to block evasion techniques is not sufficient. While some protocol anomalies and violations occur only when evasion techniques are being used, most protocol irregularities emerge due to a slightly flawed implementation in commonly used Internet applications. For more accurate detection, it is necessary to analyze and decode the data layer by layer. Since the attack may be obfuscated by evasions at many different layers, normalization and careful analysis must be carried out on the appropriate layer.

Weak Points in Current Network Security Devices

For end-user organizations, there are two critical questions:

- Why have many security vendors been unable to offer effective protection against evasions?
- Why is the problem impossible to fix in the same way as exploits?

The answer lies in traffic handling, inspection, and detection. Each of these capabilities is instrumental in building proper evasion protection in network security products.

Throughput-oriented network security devices cannot perform full normalization

Proper security devices should normalize data traffic 100% on every protocol layer before executing payload inspection. The majority of current security devices are designed to optimize the inline throughput performance in a clean (simulated) network that is never the target of a complex, hard-to-detect attack. As a result, security devices use shortcuts and execute only partial normalization and inspection. For instance, TCP segmentation handling is very limited and done only for selected protocols or ports (if not disabled by default). Evasions can exploit these shortcuts and weaknesses in normalization and inspection processes.

Segment or pseudo-packet-based inspection

Proper security devices should be able to inspect constant data stream instead of segment or pseudo-packets. This is a fundamental design issue that is extremely difficult to change. Especially in the case of hardware-based products, the redesign of security devices would require a significant R&D outlay. Data stream-based inspection requires more memory and CPU capacity to continue to perform effectively in throughput. For many vendors, this is a ”mission impossible” and inspection scope is sacrificed. Evasions exploit this liability by spreading attacks over segments or pseudo-packet boundaries.

100% pattern match approach in detection and blocking

An effective protocol reassembly and normalization enables proper evasion handling and ensures that a vulnerability-based approach can detect and prevent attacks successfully. An exploit-based approach relying on packet-oriented pattern matching is significantly more vulnerable to evasions and poses a concrete risk and long-term security liability. In fact, this approach is a ”mission impossible.” It will not detect or block attacks with advanced evasions because the number of the available evasion combinations is astronomical. This means that it is impossible to create signatures for every evasion combination as required by the exploit-based packet-oriented approach.

The McAfee Network Security Advantage: A Data Stream-Based Approach with Layered Protocol Analysis

The McAfee approach differs from other network security solutions in an essential way. McAfee Next Generation Firewall analyzes data as a normalized stream rather than as single or combined packets. The data stream is then fed through multiple parallel and sequential state machines. This analysis is done for all data traffic by default.

In the lower protocol layers, the McAfee Next Generation Firewall makes sure that there is a unique way to reconstruct the data stream. The McAfee Next Generation Firewall passes well-formed Internet protocol (IP) fragments and TCP segments with minimum or no modification. However, fragments or segments with conflicting and overlapping data are dropped. This normalization determines that there is a unique way to interpret the network traffic. The actual data stream can now be reassembled for inspection in the upper layers.

Unlike other firewall products that essentially inspect the TCP layer segment by segment, McAfee Next Generation Firewall inspects the TCP layer as a reassembled data stream. For example, the data transmitted in a TCP connection is assembled into a data stream for inspection when incoming TCP segments enter the intrusion prevention system (IPS) appliance. This is a fundamentally superior design for detecting attacks in the data stream, as approaches that inspect individual segments struggle with attacks that span over TCP segment boundaries.

In the higher layers, McAfee Next Generation Firewall can identify certain protocol elements in the data stream and, when appropriate, inspect them as separate data streams that can be normalized depending on the protocol. For example, compressed HTTP is decompressed for inspection, and Microsoft remote procedure call (MSRPC) pipes using the same server message block (SMB) connection are de-multiplexed for separate inspection.

This data stream-based approach combined with layered protocol analysis and protocol specific data normalization at different levels is an extremely powerful paradigm that allows McAfee Next Generation Firewall to inspect data traffic with unprecedented depth and accuracy.

Evasion Protection: Comparison of McAfee Next Generation Firewall and Other Vendors

McAfee Next Generation Firewall	Products from Other Vendors
Full-stack visibility McAfee decodes and normalizes traffic on all protocol layers.	Single layer analysis.
Minimum traffic modifications.	Traffic modifications and interpretations.
Normalization-based evasion removal Normalization processes remove the evasions before the data stream inspection.	Inspection of individual segments or pseudo–packets.
Application data stream-based detection Vulnerability-based fingerprints detect exploits in the normalized application-level data streams.	Vulnerability-based, exploit-based, shell code detection, banner matching.
In-house research and tools Evasion-proof product quality assured with automated evasion fuzzing tests.	Publicly available information and third-party tools.

IP

In the TCP/IP protocol suite, the IP is used to transmit datagrams from source to the destination. IP does not attempt to guarantee that the datagram reaches the destination; any required reliability features must be implemented in the upper layers of the protocol stack.

When IP datagrams are transmitted over a link where the maximum transfer unit is smaller than the datagram, the datagram must be split into several IP fragments. IP fragment handling is critical to successful data traffic normalization.

IP-level evasions

A well-known evasion method used in the IP layer is to fragment the IP datagram and send fragments out of order. Each individual fragment bears a marker that denotes where it belongs in the context of the original packet. IP implementations must be able to accept a stream of packet fragments and, using their offsets, reassemble them into the original packet. Insertion attacks disrupt stream reassembly by adding packets to the stream that would cause it to be reassembled differently on the host. The inserted packets could change the sequencing of the stream, preventing the network security device from dealing properly with the valid packets that follow it.

IP defragmentation—fragments collection, reordering and validation—is handled effectively by most IPS systems nowadays. Yet overlapping or malformed data handling can cause problems or potential blind spots for IPS systems in some cases.

The McAfee approach

McAfee Next Generation Firewall collects incoming IP fragments and carries out a number of checks that can detect malformed IP fragments. Overlapping IP fragments with conflicting data are detected and dropped. When all fragments are received and reassembled to form a complete IP datagram, McAfee Next Generation Firewall passes the datagram to the next protocol layer for normalization and further inspection. No fragments are passed through without successful IP datagram reassembly.

TCP

The transmission control protocol (TCP) provides applications a connection-oriented, reliable data stream functionality. Once a connection is established, each endpoint may write data to the stream, and the other endpoint will receive it. TCP wraps the stream data into TCP segments, which are transmitted as IP datagrams; upon receiving data, the receiver will acknowledge it, and if the sender does not receive an acknowledgement, it will resend the data after a timeout.

TCP-level evasions

TCP segments may arrive at the endpoint out of order, and duplicates are also possible.

The sender may also send several segments without waiting for acknowledgements. TCP provides a method of flow control by adjusting the window size, which indicates the amount of data the receiver is willing to accept. The attacker may exploit this vulnerability and send segments in his chosen order and sizes and purposefully elect to not obey flow control.

TCP stream reassembly

Unlike most of the other solutions, the McAfee Next Generation Firewall inspects the actual data stream transmitted within a TCP connection instead of the TCP packets or segments. This is why McAfee Next Generation Firewall assembles the TCP segments into a data stream before inspecting data content. TCP segments are buffered until the destination endpoint has acknowledged them. This protects the network against evasions that are based on sending TCP segments out of order or overlapping TCP segments with conflicting content.

This approach is memory intensive, as the amount of data that needs to be stored for each connection is roughly equal to the TCP window size. The 64-bit McAfee Next Generation Firewall has sufficient memory and processing power to meet this challenge.

TCP resource handling

Every TCP connection requires maintaining a connection state and possibly storing a number of TCP segments. To manage next-generation firewall resource use, we have to make compromises between perceived “virtual wire” behavior and robustness against evasions. McAfee Next Generation Firewall enables users to balance resource usage, inspection, quality, and data traffic integrity without compromising overall system performance.

The core issue is that high-speed TCP connections require large transmission windows. The IPS must store the TCP segments in a separate memory until they have been acknowledged. This is the only way to detect maliciously ordered or overlapping TCP segments with conflicting data. However, the amount of data that needs to be stored is roughly equal to the window size. To inspect a large number of connections with finite memory in an IPS would require limiting memory use.

McAfee Next Generation Firewall handles TCP traffic in the TCP strict mode and the TCP normal mode (see below).

TCP strict mode

In TCP strict mode, McAfee Next Generation Firewall forces the TCP segments to pass through the device in the correct order. If segments arrive in the wrong order, the later segments are kept waiting until the previous segments have arrived and the stream has been inspected up to that point.

TCP strict mode is also an exception to the principle that TCP segments should be passed through unaltered. In TCP strict mode, McAfee Next Generation Firewall may clear dubious TCP option bits and change the window size in the

TCP header, which may limit throughput. As this mode is more rigorous and may modify the frames passing through the device, performance is usually lower than in TCP normal mode (see below).

TCP normal mode

In TCP normal mode, McAfee Next Generation Firewall allows the TCP segments to pass through regardless of order.

If segments arrive out of order, the later segments are passed through, but also stored in the device memory. When the next TCP segment in the connection is visible, McAfee Next Generation Firewall reconstructs the stream as far as it can and passes the data to inspection; if inspection detects a problem, the TCP segment may be dropped and the connection terminated. This blocks evasions related to the reordering of TCP segments.

Storing the TCP segments is memory intensive. If enough memory to store the segments in the TCP window cannot be reserved, there are two options.

To maintain performance, packets can be allowed to pass through uninspected. On the other hand, to ensure inspection quality, the IPS may be configured to drop packets that are too far ahead of the current point in the data stream. This does not violate the TCP protocol since TCP segments are transmitted as IP datagrams and there is no guarantee that an IP datagram will reach its destination. This approach relies on the TCP implementation to resend segments after a timeout. The frame dropping also indirectly controls the congestion window of the sending TCP stack.

Urgent data

TCP has a mechanism that indicates whether urgent data has been placed in the data stream. In this case, the TCP headers contain information about the end position of the urgent data in the stream. According to the Internet Engineering Task Force (IETF) specifications, the TCP urgent data mechanism marks an interesting point in the data stream that applications may want to skip to even before processing any other data. However, "urgent data" must still be delivered "in band" to the application.

Unfortunately, nearly all TCP implementations process TCP urgent data differently. Applications may decide to receive urgent data in line or out of band. If the urgent data is delivered out of band, the data is excluded from the normal data stream.

As a result, different implementations of TCP may encounter a different data stream, which, in turn, provides a backdoor for evasions. Fortunately, urgent mode is rarely used; McAfee Next Generation Firewall provides several options for terminating connections if it observes the urgent mode being used.

Server Message Block

> *"Server Message Block (SMB), also known as common Internet file system (CIFS) operates as an application-layer network protocol mainly used to provide shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network. It also provides an authenticated inter-process communication mechanism. Most usage of SMB involves computers running Microsoft Windows, where it was known as "Microsoft Windows Network" before the subsequent introduction of Active Directory."*
>
> *—Wikipedia*

TCP-level evasions

SMB write data (for example, MSRPC) can be segmented into arbitrarily sized segments. It is also possible to generate multiplex SMB writes to different named pipes or files within a single TCP connection. This requires that IPS/next-generation firewall systems support SMB protocol validation and normalization capabilities.

The McAfee approach

For example, McAfee Next Generation Firewall has matching contexts for reading and writing files over SMB. However, the Windows "named pipes" with SMB are a more interesting application from the inspection standpoint. The Windows "named pipes" can be used with SMB to transmit MSRPC requests. McAfee Next Generation Firewall analyzes the traffic in depth. For example, small writes (and reads) are defragmented for the MSRPC analysis and each named pipe using the same SMB connection is analyzed separately (de-multiplexing).

MSRPC

The RPC mechanism allows an application to seamlessly invoke remote procedures, as if these procedures were executed locally. MSRPC is the Microsoft implementation of the distributed computing environment (DCE) RPC mechanism. In particular, Microsoft added new transport protocols for DCE RPC. This includes the ncacn_np transport that uses named pipes carried into the SMB protocol. For a more in-depth discussion, visit http://www.hsc.fr/ressources/ articles/win_net_srv/msrpc_intro.html.

There are numerous vulnerabilities that exploit MSRPC and the Windows services that use MSRPC.

MSRPC can be transported over TCP, UDP, SMB, or HTTP.

Evasions on MSRPC

MSRPC support both little and big endian encoding of data. Little endian is normally used, but implementations accept also big endian. The latter can be used as an evasion in some cases.

The McAfee approach

Fragmented RPC messages can be used as an obfuscation method to hide attacks. For example, McAfee Next Generation Firewall defragments fragmented MSRPC requests. To apply the right fingerprints, McAfee Next Generation Firewall follows the protocol execution and provides the fingerprinting system the necessary service information (for example, object UUID, opnum field, endianness) in addition to the request payload data. It also explicitly follows some evasion techniques, like changing the endianness in the middle of a connection.

SunRPC

> *"Open Network Computing Remote Procedure Call (ONC RPC) is a widely deployed remote procedure call system. ONC was originally developed by Sun Microsystems as part of their Network File System project, and is sometimes referred to as Sun ONC or Sun RPC."*
>
> *—Wikipedia*

> *"When RPC messages are passed on top of a byte stream transport protocol (like TCP), it is necessary to delimit one message from another in order to detect and possibly recover from protocol errors. This is called record marking (RM). Sun uses this RM/TCP/IP transport for passing RPC messages on TCP streams. One RPC message fits into one RM record. A record is composed of one or more record fragments."*
>
> *—RFC 1057*

The McAfee approach

Fragmented RPC messages can be used as an obfuscation method to hide attacks. McAfee follows the record marking protocol and internally defragments fragmented RPC messages before fingerprinting.

HTTP

The hypertext transfer protocol (HTTP) is the foundation of the web, where it is used for transferring hypertext and other types of data.

In most cases, a web browser (the client) opens a TCP connection to a website (the server), requests a resource, such as a hypertext document or an image file, and receives it from the server. HTTP can also be used by the client to submit data for the server to process (for example, online forms and surveys).

HTTP is currently one of the most important avenues of attack against computer systems. If a client can be tricked into requesting a file with malicious content, a bug on the client computer may be exploited to gain access to the system.

The McAfee approach

The McAfee Next Generation Firewall HTTP module follows the execution of the protocol. Protocol parsing and validation are used to detect attacks and evasions. The HTTP module can also extract certain parts, such as headers and URLs requested, for inspection in a separate matching context. Before actual inspection, these parts are normalized: URLs are decoded and re-encoded in a normalized format. This includes, for example, percent hex encoding, Unicode characters, IIS codepage translations, and directory traversal.

Transfer and content encodings are decoded before fingerprinting. For instance, URL parameters on the request line and in the POST body are combined to cope with these types of fragmentation tricks.

Centralized Management and Evasion Protection

The average enterprise deploys dozens of firewalls, IPS, SSL VPN, and other physical and virtual network devices. Centralized management in network security has become a required line of defense in the fight against increasingly sophisticated network security threats. Without centralized management, a task as simple as updating a rule across the network is time- consuming and susceptible to human error.

The McAfee Security Management Center is a powerful centralized management tool that allows the administrator to easily monitor the status of the security devices in the entire network. Secondly, when a network attack occurs, McAfee Security Management Center can be used to quickly and decisively enact new security policies throughout the entire network. Furthermore, McAfee Security Management Center can be used to efficiently distribute new dynamic update packages also, in case of evasion protection and fingerprints, to counter recently discovered network threats. Without centralized management of network devices, it's practically impossible to monitor and update disparate network devices with the immediacy that is required.

For many threats, centralized management is the most important—and critical—line of defense. In the case of AETs, where advanced evasion techniques deliver payloads without being detected by network security devices, there is no bulletproof solution. For a dynamic threat like AETs, network security protection must be continuously updated to keep up with the threats. Situational awareness, detailed analysis of attack methods, and understanding how the exploits were conducted play a key role. It is not enough to just know which attacks were created; it's equally important to know how they were created.

The difference in the level of evasion detection and protection provided by different network security vendors is enormous. Since network administrators may not be able to proactively protect against AETs, their only option is to be prepared for immediate and effective reaction.

That means being able to centrally monitor all network devices—regardless of vendor or types—for suspicious activity. They must be able to pinpoint the attack, remediate, and quickly update and configure network devices to minimize damage. A single, centralized management console enables administrators to not just monitor from a single location, but also to create configurations only once before deploying to all devices on the network.

Contrary to what some independent lab tests suggest, there is no 100%-guaranteed protection against AETs. In fact, current tests show that devices can detect and block only predefined and well-known evasion techniques. If the evasions are changed slightly or combined together in a more complex way, the devices fail the test. The dynamic and constantly evolving nature of evasions means that centralized management is a must-have defense for networks and critical digital assets.

Evasion R&D and In-House Testing: 24/7 Capabilities

In 2010, McAfee discovered that current network security devices are highly vulnerable to advanced evasion techniques. This discovery is now a widely discussed topic in academic research, independent testing labs, and security auditing/consultancy companies. But no matter where the conversation is taking place, R&D work must be redirected toward prevention of novel attack methods. Yet many security vendors focus on exploits exclusively and downplay the impact of these methods.

At McAfee, we believe that elimination of different attack (delivery) methods is a more effective way to improve network security. This proactive attitude to network security is also essential to evasion protection. For security device vendors, the most effective course of action is to ensure continuous in-house R&D work and product testing. Without appropriate test tools and R&D competence, vendors cannot offer preventative and proactive protection against advanced evasion techniques.

McAfee Next Generation Firewall products are constantly tested and updated against AETs. Our proven R&D track record and automated in-house testing framework ensure that McAfee Next Generation Firewall provides optimal protection against AETs.

Commercial Anti-Evasion Readiness Test Tool

As a public service to the security industry, McAfee released a free tool for testing a controlled set of evasive techniques that have proven successful against all IPS and next-generation firewall solutions. The tool, called Evader, allows companies to test in their own environments to see if a known exploit can be delivered—using advanced evasion techniques—through their current security devices to a target host. Evader launches AETs against the tester's own network defenses—firewall, IDS/IPS, or UTM. The tool runs on virtual environments, as well as on physical PCs, and includes two fixed exploits and a controlled set of dynamic AETs.

The first version of Evader includes stackable and dynamic AETs that have been through the computer emergency response team (CERT) vulnerability coordination process. In a recent survey, 63% of those who downloaded Evader were able to successfully evade their network security, and 93% would recommend it to a colleague.

The tool is free to download and use, and can be downloaded at evader.stonesoft.com. It was first introduced during Black Hat 2012 in Las Vegas on July 23, 2012.

For more information on the Anti-Evasion Readiness Test, visit www.stonesoft.com, aet.stonesoft.com, or www.mcafee.com/evader.

Conclusion

The recent increase in serious network security breaches is proof that cybercriminals are developing new and effective ways to execute targeted and advanced attacks. The bad guys show no mercy as they attack and infiltrate organizations that are supposed to be protected with the best–of-breed security systems. How is this possible? First, organized cybercrime has the money, motivation, and talent to change the security game. Second, the risk-reward ratio is too good to believe, as the chance of being caught remains low. For C-level managers, network security has become a major risk management challenge.

Customers expect to get the best protection money can buy, but the latest security trends tell another story. Because security devices protect mission-critical computer networks, sensitive data assets, and critical systems, such as CRM and ERP and SCADA networks, cybercriminals make these devices their first call of business. Here AETs offer an effective way to execute successful attacks without being detected. Advanced evasion techniques work like a "master key" and allow criminals to use exploits that would otherwise be detected and blocked. In reality, there are countless evasion techniques that make malicious content more difficult to detect in network traffic.

McAfee provides effective protection against evasion techniques by focusing on the actual data content in the data stream. McAfee can see through commonly used obfuscation methods and analyze and inspect the transmitted content. The innovative McAfee approach to data inspection also detects evasion techniques even when they are applied on multiple protocol levels.

Supporting Research

- Ptacek, Newsham: Insertion, *Evasion, and Denial of Service: Eluding Network Intrusion Detection,* 1998
- Raffael Marty, *Thor–A Tool to Test Intrusion Detection Systems by Variation of Attacks,* 2002
- A. Samuel Gorton and Terrence G. Champion, *Combining Evasion Techniques to Avoid Network Intrusion Detection Systems,* 2004
- Giovanni Vigna, William Robertson, and Davide Balzarotti, *Testing Network-Based Intrusion Detection Signatures Using Mutant Exploits,* 2004
- Shai Rubin, Somesh Jha, and Barton P. Miller, *Automatic Generation and Analysis of NIDS Attacks,* 2004
- Varghese, et al, "Detecting Evasion Attacks at High Speeds without Reassembly," *Sigcomm,* 2006
- Horizon, "Defeating Sniffers and Intrusion Detection Systems," *Phrack Magazine,* Issue 54, 1998, article 10 of 12
- Rain Forest Puppy, *A Look at Whisker's Anti-IDS Tactics,*1999
- "NIDS Evasion Method Named 'SeolMa'," *Phrack 57,* Phile 0x03, 2001
- Daniel J. Roelker, *HTTP IDS Evasions Revisited,* 2003
- Brian Caswell, H D Moore, "Thermoptic Camouflage:Total IDS Evasion," Black Hat Conference, 2006
- Renaud Bidou, "IPS Shortcomings," Black Hat Conference, 2006
- Michael Dyrmose, "Beating the IPS," SANS Institute, 2013
- William McGlasson, "Testing Application Identification Features of Firewalls," SANS Institute 2013

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com