STONESOFT

Protection against Advanced Evasion Techniques in Stonesoft IPS

Whitepaper

Multilayer Traffic Normalization and Data Stream Based Inspection: Essential Design Principles of the Stonesoft IPS

Contents

1 Introduction

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 fifteen 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.

The recent string of successful yet unexplained attacks against high profile organizations suggests that evasion techniques are being used effectively. This claim is supported by forensic cybercrime investigation. Stonesoft – for its own part – discovered the immense power of evasions in 2010, when leading security products were tested against advanced evasion techniques by Stonesoft's research laboratory. The incredible result was that all the tested devices failed to detect exploits that applied evasion techniques. This raises the following questions: Is there a network security solution that protects against advanced evasion techniques? How would this solution differ – in both approach and design – from existing security devices?

The Stonesoft IPS (Intrusion Prevention System) answers this challenge. Combining stream-based inspection with data normalization on multiple protocol layers, the Stonesoft IPS is highly resistant to advanced evasion techniques and offers a novel approach to IPS design and implementation. Other Stonesoft products such as Stonesoft Security Platform incorporate design elements from the Stonesoft IPS and also provide effective protection against AETs.

This paper explains the technical and design principles behind Stonesoft's breakthrough anti-evasion technology.

2 Understanding Evasions Techniques

2.1 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.

2.2 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
- Use of rarely used protocol properties
- Use of unusual combinations
- Craft network traffic that disregards strict protocol specifications
- Exploit the technical and inspection limitations of security devices: memory capacity, performance optimization, design flaws, etc.

Evasion techniques are a means to disguise cyber attacks in order to avoid detection and blocking by information security systems. Evasions enable cyber criminals 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.

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.

3. 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 an IPS or next-generation firewall NGFW product.

Many IPS devices are throughput oriented and cannot perform full normalization.
Proper security devices should normalize data traffic 100% on every protocol layer before executing payload inspection. The majority of existing 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.

These weak points explain why many of the leading IPS devices are vulnerable to evasion-disguised attacks. When running 124 randomly selected advanced evasion techniques through the leading security devices, the results were indisputable: the devices were unable to detect advanced evasion techniques. In this study, the advanced evasion techniques were reported through the CERT-FI vulnerability coordination process flow.

4. The Stonesoft Edge: a Data Stream Based Approach with Layered Protocol Analysis

The Stonesoft approach differs from most IPS solutions in an essential way. The Stonesoft IPS 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 Stonesoft IPS makes sure that there is a unique way to reconstruct the data stream. The Stonesoft IPS passes well-formed 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 passing through the IPS. The actual data stream can now be reassembled for inspection in the upper layers.

Unlike other IPS products that essentially inspect the TCP layer segment by segment, the Stonesoft IPS 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 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, Stonesoft 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 MSRPC named pipes using the same SMB connection are demultiplexed for separate inspection.

This data stream based approach together with layered protocol analysis and protocol specific data normalization at different levels is a extremely powerful paradigm that allows Stonesoft to inspect data traffic with unprecedented depth and accuracy.

Evasion Protection: Comparision of Stonesoft IPS and other IPS Products

Stonesoft IPS	Other IPS Products
Full-stack visibility Stonesoft decodes and normalizes traffic on all protocol layers	Single layer analysis
Minimum traffic modifications	Traffic modifications and interpretations
Normalization based evasion removal Normalization process 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
Inhouse research and tools Evasion-proof product quality assured with automated evasion fuzzing tests	Publicly available information and third party tools
Updates and upgrades Antievasion technology automatically updated in Next Generation IPS and Firewall engines	Limited evasion coverage and delayed updates

5 IP

In the TCP/IP protocol suite, the Internet Protocol (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.

An IDS that does not properly handle out-of-order fragments is vulnerable; an attacker can intentionally scramble her fragment streams to elude the IDS. (Newsham & Ptacek, 1998)

Furthermore, IDS systems are challenged by the fact “that received fragments must be stored until the stream of fragments can be reassembled into an entire IP datagram. (Newsham & Ptacek, 1998)

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 Stonesoft Approach

The Stonesoft IPS 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, Stonesoft IPS passes the datagram to the next protocol layer for normalization and further inspection. No fragments are passed through without successful IP datagram reassembly.

6 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 select not obey flow control.

6.1 TCP Stream Reassembly

Unlike most of the other IPS solutions, the Stonesoft IPS inspects the actual data stream transmitted within a TCP connection instead of the TCP packets or segments. This is why Stonesoft 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 Stonesoft IPS appliances have sufficient memory and processing power to meet this challenge.

6.2 TCP Resource Handling

All IPS devices have limited resources and capabilities. Nevertheless, every TCP connection requires maintaining a connection state and possibly storing a number of TCP segments. To manage IPS resource use, we have to make compromises between perceived “virtual wire” behavior and robustness against evasions. The Stonesoft IPS 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.

Stonesoft handles TCP traffic in the TCP strict mode and the TCP normal mode (see below).

6.2.1 TCP Strict Mode

In TCP strict mode, Stonesoft forces the TCP segments to pass through the IPS 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, Stonesoft 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).

6.2.2 TCP Normal Mode

In TCP normal mode, Stonesoft 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, Stonesoft 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 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.

6.3 Urgent Data

TCP has a mechanism that indicates if 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 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; Stonesoft IPS provides several options for terminating connections if it observes the urgent mode being used.

7 SMB

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 (e.g. MSRPC) can be segmented into arbitrary 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/NGFW systems support SMB protocol validation and normalization capabilities.

The Stonesoft Approach

For example, Stonesoft 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. Stonesoft analyzes the traffic in-depth. This includes, for example, small writes (and reads) are defragmented for the MSRPC analysis and each named pipe using the same SMB connection is analyzed separately (demultiplexing).

8 MSRPC

The RPC (Remote Procedure Call) mechanism allows an application to seamlessly invoke remote procedures, as if these procedures were executed locally. MSRPC is the Microsoft implementation of the 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 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 Stonesoft Approach

Fragmented RPC messages can be used as an obfuscation method to hide attacks. For example, Stonesoft IPS defragments fragmented MSRPC requests. To apply the right fingerprints, Stonesoft IPS follows the protocol execution and provides the fingerprinting system the necessary service information (e.g. 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.

9 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 Stonesoft Approach

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

10 HTTP

The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide 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 web site (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 (e.g. 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 Stonesoft Approach

The HTTP module in Stonesoft IPS 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 this kind of fragmentation tricks.

11 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. In fact, Gartner, Inc. estimates that more than 99 percent of all security breaches are caused by misconfigurations*.

The Stonesoft Management Center (SMC) 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, SMC can be used to quickly and decisively enact new security policies throughout the entire network. Furthermore, SMC 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 – if not crucial – line of defense. In the case of AETs, where advanced evasion techniques deliver payloads without being detected by firewall and IPS devices, there is no bullet proof solution. For a dynamic threat like AETs, network security protection must be continuously updated to keep up with the threats. Situation awareness, detailed analysis of attack methods and understanding about how the exploits were conducted play a key role. It is not enough to know which attacks were made, but how.

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 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% 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.

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

In 2010, Stonesoft 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 towards prevention of novel attack methods. Yet many security vendors focus on exploits exclusively and downplay the impact of these methods.

At Stonesoft, we believe that elimination of different attacking (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 competences, vendors cannot offer preventative and proactive protection against advanced evasion techniques.

Stonesoft IPS and NGFW products are constantly tested and updated against AETs. Our proven R&D track record and automated in-house testing framework ensure that Stonesoft IPS and NGFW provide optimal protection against AETs.

13 Commercial Anti-Evasion Readiness Test–Service

In June 2011, Stonesoft launched the Anti-Evasion Readiness Test as a way to increase evasion awareness in the security community and improve network security in companies and organizations. The innovative service is provided by independent IT testing professionals around the world.

The Anti-Evasion Readiness Test service leverages Stonesoft Evasion Readines Test Suite developed by Stonesoft Labs to test, assess and report security devices' capabilities to protect against AETs. The test is developed to meet the needs of organizations that use network security devices like Next Generation Firewalls, Intrusion Detection and Intrusion Prevention and Unified Threat Management systems. To meet compliance and audit requirements and protect critical digital assets, organizations must tackle these security issues effectively.

The Anti-Evasion Readiness Test provides customers with an extensive test report on evasion detection and block rates for existing or planned security devices. The test report also includes practical recommendations and risk mitigation advice from people with the most in-depth evasion protection knowledge. The test is easy and cost efficient to take and requires no in-house expertise or investments in testing tools.

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

14 Executive Summary

The recent increase in serious network security breaches is proof that cyber criminals 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.

Today more than USD 3 billion is spent annually on network security devices. 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, cyber criminals 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.

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

Stonesoft intrusion prevention systems (IPS) and next-generation firewalls (NGFW) detect well-known and documented evasion techniques and provide the most effective line of defense against evasion techniques in the wild. Stonesoft's dedicated R&D team is continuously testing and discovering new evasion techniques and building immediate protection against them.

The Stonesoft Edge in Evasion Protection

- Evasionproof IPS and NGFW technology with Multilayered protocol analysis and data stream based inspection capabilities
- In-house evasion research and testing framework. Thought leader in evasion research.
- Powerful and intelligent management system to deliver immediate evasion protection updates and upgrades
- Dynamic (software) based security products that can be adapted any customerenvironment. Physical, virtual or hybrid.

STONESOFT

Stonesoft Corporate

Itälahdenkatu 22 A
FI-00210 Helsinki
Finland
tel. +358 9 476 711
fax. +358 9 476 713 49

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338, USA
tel. +1 866 869 4075
fax. +1 770 6681 131