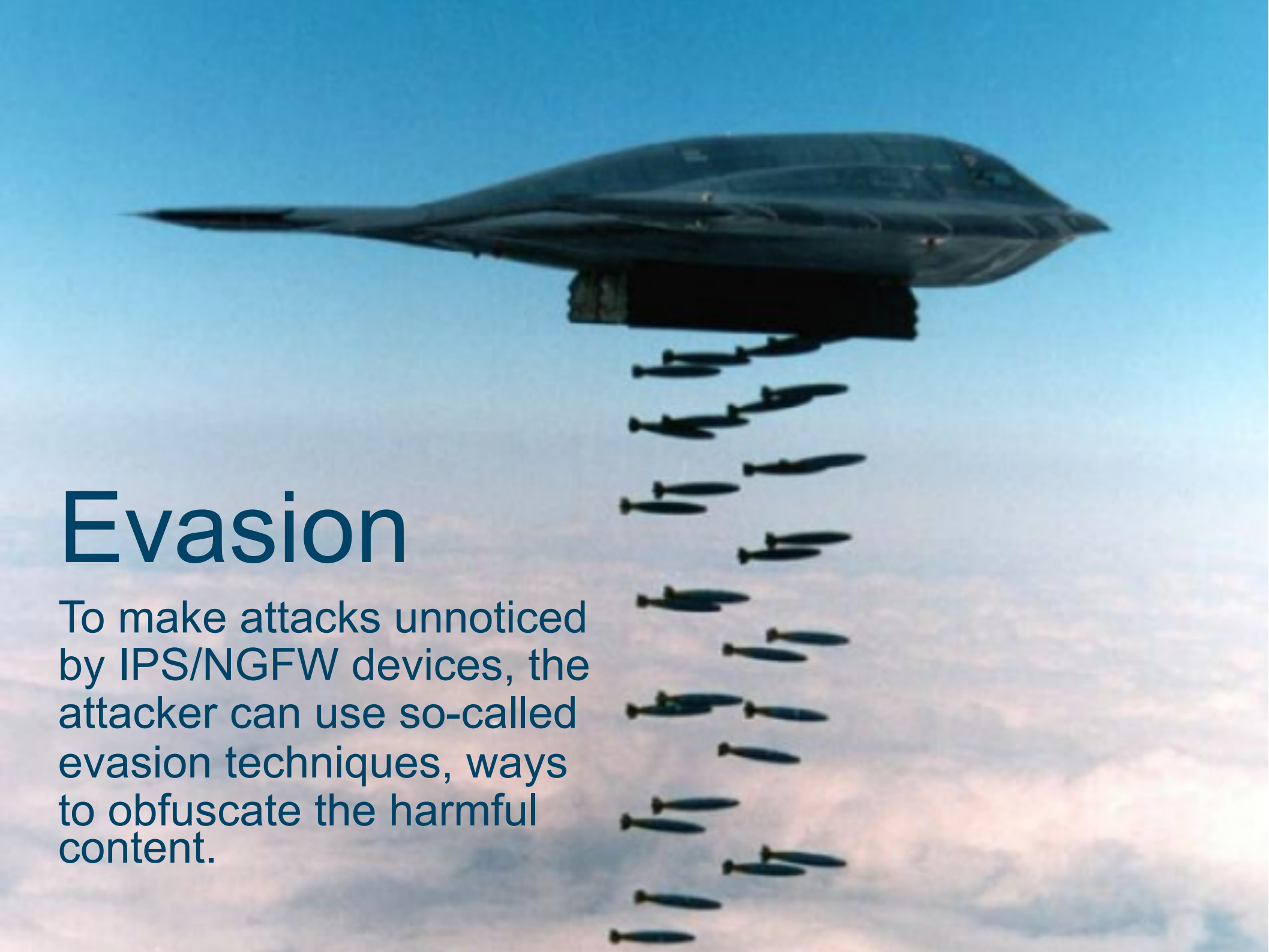
OLLI-PEKKA NIEMI & ANTTI LEVOMÄKI

# Bypassing Intrusion Prevention Systems

STONESOFT

# Who?

- ANTTI LEVOMÄKI
  - Stonesoft R&D
  - Evasion Research & TCP/IP Black Arts
  - Postgraduate student at Aalto University
- OLLI-PEKKA NIEMI
  - Stonesoft R&D
  - Head of Vulnerability Analysis Group
  - Evasion Research & Network Based Threat Analysis



# Evasion

To make attacks unnoticed by IPS/NGFW devices, the attacker can use so-called evasion techniques, ways to obfuscate the harmful content.

# EVASION

- The reason that evasions work is the old robustness principle stated by Jon Postel in RFC793

"be conservative in what you do, be liberal in what you accept from others".

This is what we exploit

# Previous Academic Research on Evasions

- Ptacek, Newsham: “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection”, 1998.
- Raffael Marty, Thor – A tool to test intrusion detection systems by variaton of attacks, 2002
- A. Samuel Gorton and Terrence G. Champion, Combining Evasion Techniques to Avoid Network Intrusion Detection Systems, 2004
- Giovanni Vigna William Robertson 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.

# Community Work on Evasions

- 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 "SeoIMa", Phrack 57, Phile 0x03, 2001
- Daniel J. Roelker , HTTP IDS Evasions Revisited, 2003
- Brian Caswell, H D Moore, Thermoptic Camouflage:Total IDS Evasion, BlackHat, 2006
- Renaud Bidou: IPS Shortcomings, BlackHat 2006

# Evasion libraries and tools

- Fragroute(r) by Dug Song ~1999
- Robert Graham, SideStep, 2000
- Rain Forest Puppy: Whisker, libwhisker
- Raffael Marty, Thor – A tool to test intrusion detection systems, 2002
- Metasploit Framework
- Immunity Canvas
- Core Impact
- Breaking Point
- Libnet
- Scapy

# Problems with Previous Tools

- Fragroute & Fragrouter
  - IP and TCP layer packet oriented evasions
  - They take a packet and apply evasions on that
    - Lacking comprehensive understanding of streams
- Libnet & scapy
  - Packet crafting library, not a complete stack with connection handling and socket interfaces
- Metasploit
  - Mostly application layer evasions
  - Uses host OS TCP/IP stack thus lacking evasions that require customized tcp/ip stack
- BreakingPoint
  - Simulate attacks and connections. Plays both sides (client and server)
    - Some traffic it produces is pathological since both parties of the communication are simulated

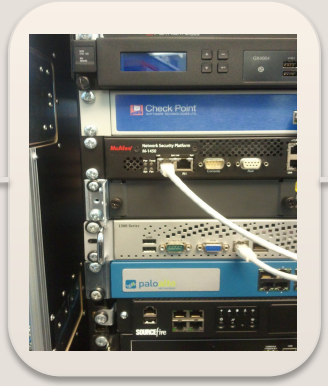
# Claim

- There's no publicly available single tool that
  - Is designed to use multiple evasions techniques in multiple protocol layers from IP to Application layer at the same time to test IPS and NGFW deep inspection's detection and prevention capabilities
  - Is Capable to control the size and sending order of every single datagram or segment that is being transmitted to the network
  - Is able to alter evasion in the fly, every packet of data on any protocol level may have different evasion method or combination of evasions
  - Is Designed to test a security device's protocol handling and decoding capabilities
  - Implements most known evasion research into reliable evasion methods and has interfaces suitable for automate testing
  - Does not simulate connections, but runs real exploits against real targets
  - Capable of fuzzing
  - Support also payload mutation to differentiate exploit and vulnerability based detection. Supports applying evasions on "normal traffic" to identify anomaly based detection
- Until Evader…

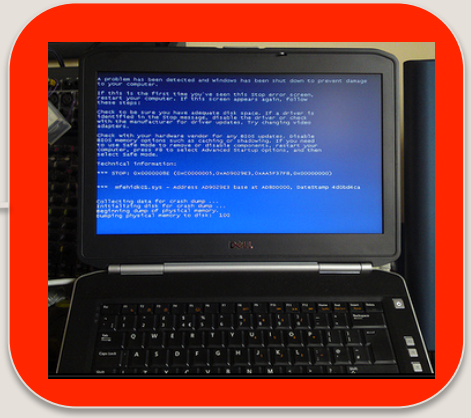
# Our Research

- We have implemented a tool we call Evader.
- It applies network level evasions to send a payload into a remote host through the IPS/ NGFW
- Evader first sends non-malicious payloads that should not be prevented. This is called the false positive test.

Attacker




IPS/NGFW



Victim

# Our Research

- If this is successful, the malicious payload will be sent. Depending on the selected malicious payload, the remote system is either crashed or compromised via remote code execution.
- If this happens we know that the evasion was functional.

# Evader

- Evader contains known exploits that every IPS should detect
  - CVE-2004-1315
    - viewtopic.php phpBB remote code execution
    - selected because it can be continuously exploited  without reboot or restart -> suitable for automatic testing
  - CVE-2008-4250, MS08-067
    - Msrcp server service buffer overflow, exploited by  worms like conficker and stuxnet
    - selected because it can be continuously exploited  without reboot or restart -> suitable for automatic testing
  - CVE-2012-0002, MS12-020
    - Remote Desktop Denial of Service
    - Relatively new vulnerability that most IPS/NGFW claim to protect against exploits

# Evader

- Evader contains a multilayer network protocol stack.
- When sending the payload, Evader can apply multiple evasions on various protocols
- If the payload exploits some HTTP server vulnerability, we can apply evasions in the IP layer but also in TCP layer and HTTP layer. For msrpc, evader can built evasion combinations using IP/TCP/NetBIOS/SMB/MSRPC layers
- Evader can divide the connection into several stages and every stage can have its own evasions applied.

- In theory, for the selected exploit, the Evader can produce every possible data stream transmitting the payload, but in practice this cannot be tested since there are virtually endless amount of combinations and stage permutations.

- When evasions are not used, IPS/NGFW devices detect and terminate the attack
- With proper evasions  applied, IPS/NGFW start to Fail
  - Does not detect anything
  - Detect something that cannot be terminated due to risk for false positive
  - Detect attack, claims to terminate but fails termination

- Evader can be automated with another tool called mongbat
- Mongbat runs evader with different evasion combinations and collects results
  - Full evader command line is saved with random seed to allow exactly same evasion attack run at a later time
  - Takes pcaps
  - Basically Mongbat+Evader=Evader Fuzzer

# Key differentiators

- Designed for automatic testing to systematically find weaknesses in middle-box security devices, specifically IPS and NGFW deep inspection
- Plugin interface to give hints on successful evasions and to disable pathological cases
- Does not simulate exploits, runs real exploits against real targets
- Complete stack visibility due own TCP/IP stack with built in application layers
- Not a proxy, so it knows the context of what it is going to send and can apply evasions for the whole session, or split the session in stages and apply different set of  evasions per stage, or apply evasions per packet.
- Fuzzing
- Records everything (pcap, command line, randseed) allowing results to be analysed for what ever purpose…and repeated (or known working evasions applied into different exploit…)

# Simple Test…

- We run evader using RDP exploit
- We used following evasions
  - Base = No evasion
  - Seg = Segment Size 8
  - Reverse = Segment Size 8 + Reverse
  - Time-Wait, re-use socket/source port before timer expires, no other evasions
  - Paws = Abuse Protection Against Wrapped Segment Numbers with timestamp option mangling, no other evasions

# RDP CVE-2012-0002 Results

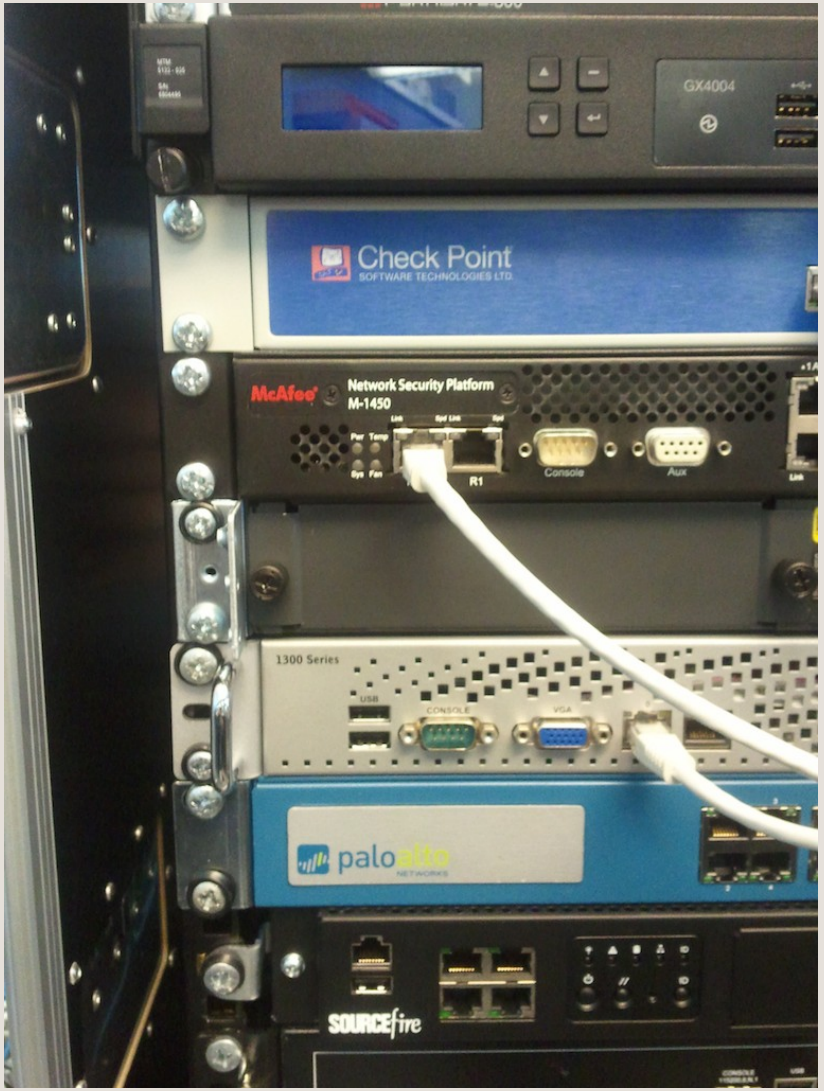
| | DUT | Base | Seg 8 | +REV | TWait | PAWS |
|---|---|---|---|---|---|---|
| A | xxxxx | FAIL | FAIL | FAIL | FAIL | FAIL |
| B | xxxxx | OK | FAIL | FAIL | FAIL | FAIL |
| C | xxxxx | OK | FAIL | FAIL | OK | OK |
| D | xxxxx | OK | OK | FAIL | OK | FAIL |
| E | xxxxx | OK | OK | OK | OK | FAIL |
| F | xxxxx | OK | FAIL | FAIL | OK | OK |
| G | xxxxx | OK | OK | OK | FAIL | OK |
| H | xxxxx | OK | OK | FAIL | OK | FAIL |

- Tests were run in May 2012
- Every device were running latest software with latest updates and patches installed.
- All DUT were deployed inline
- All were running hardened policy with TCP/IP reassembly applied to RDP when not in default configuration
- OK = Attack was detected and blocked
- FAIL = Attack was not detected and Remote host was crashed

Stonesoft IPS was also tested, but its results were left out of the paper as we were unable to evade it at all (even with mongbat). It is also our belief that it is by far most difficult IPS to evade.

The RDP Exploit against Win7 was tested through these devices

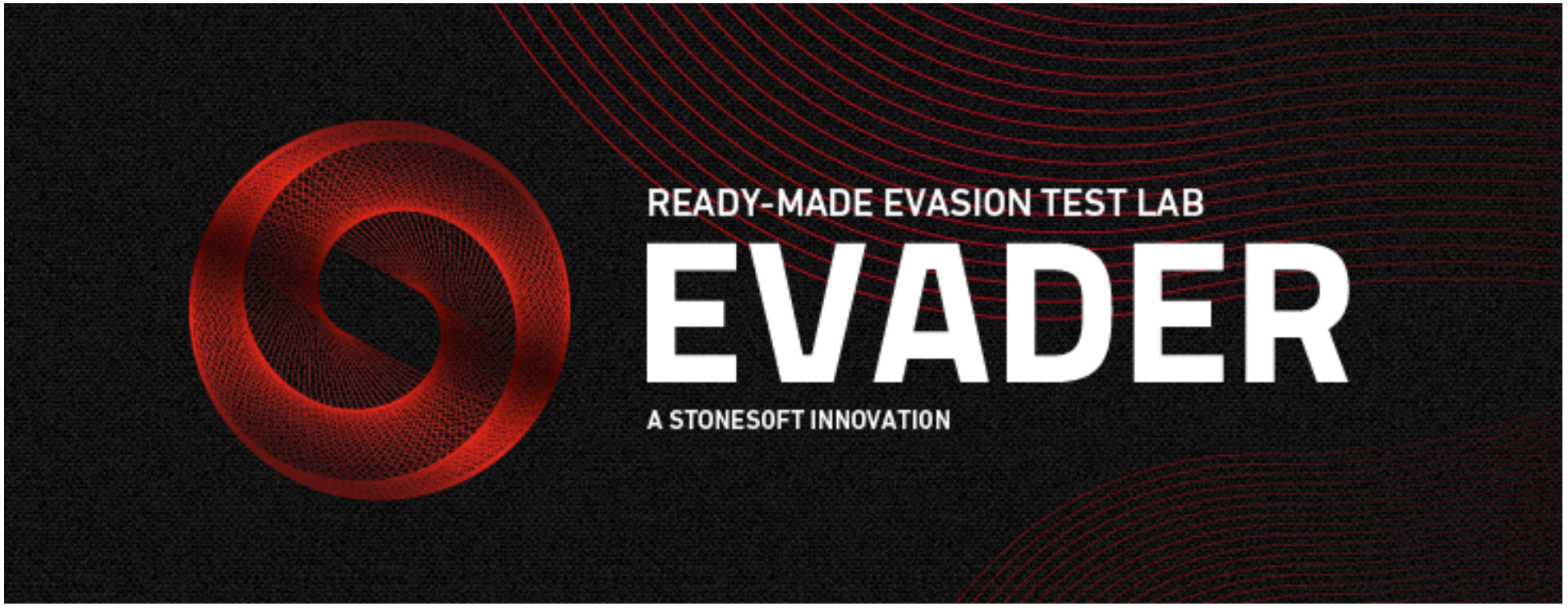
- PaloAlto
- Fortigate
- SourceFire
- McAfee
- Juniper
- Cisco
- HP TippingPoint
- IBM Proventia



# Conclusion

- Our tests prove that even 14 years after Ptacek – Newsham paper several IPS/NGFW are still vulnerable to TCP/IP reassembly attacks. We believe that proper TCP/IP reassembly is difficult to implement and expensive in terms of performance. Also the lack of proper testing tools helps to hide these incapabilities.
  - We know of cases where hardened policy that improves evasion resistance drops performance dramatically, for example to 10% of original throughput performance
- We have released a version of the evader tool for everyone to use and verify our findings. The tool can also be use to verify and harden IPS/NGFW policies in case there is some configurations available to improve detection rate when evasions are in place

# http://Evader.stonesoft.com




Freely available