Effectiveness of blocking evasions in Intrusion Prevention Systems

White Paper

April, 2013

Konstantinos Xynos, Iain Sutherland, Andrew Blyth

University of South Wales, Pontypridd, Wales.

Effectiveness of blocking evasions in Intrusion Prevention Systems

Konstantinos Xynos[1], Iain Sutherland[1,2,3], Andrew Blyth[1]
{k.xynos, iain.sutherland, andrew.blyth}@southwales.ac.uk
[1]University of South Wales, Pontypridd, Wales.
[2]Noroff University College, Kristiansand, Norway.
[3]SRI -Security Research Institute, Edith Cowan University, Perth, Australia.

Introduction

Attacks on networked systems are becoming increasingly complex and targeted. Evasion techniques make use of protocol design flaws, or use the current protocol design, to their advantage such that an attack may go undetected. By combining evasion techniques it is possible for attackers to evolve a more stealthy approach, one that is even harder to detect and often resulting in a successful attack. These are known as Advanced Evasion Techniques (AET) and are likely to become increasingly significant as detection engines become more efficient and organisations more complacent by the protection provided at the perimeter.

Recent trends[1,2] concerning techniques used to evade detection by Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) have proved troubling to the security community. This report presents the findings of an experiment that tested a number of evasion techniques against a set of well-known and commercially available Intrusion Prevention Systems (IPS). The IPS were all up-to-date (e.g., software and signatures) and configured, using a best configuration scenario. This ensured that all attack attempts against the provided vulnerabilities, were being blocked while not using evasion techniques.

The findings provide some cause for concern and should be a warning to those organisations that rely on simple and/or outdated implementations of IPS, especially those that do not patch their systems. With advances in evasions occurring rapidly the time between discovery, publishing and usage is minimal, IPS vendors and organisations need to be able to protect against an ever-evolving threat and one that has the ability to employ evasion techniques in more complex attacks. In broad terms, evasion techniques involve the manipulation of certain circumstances that permit an attack to go unnoticed by the detection engine.

Malware developers constantly use evasion techniques to evade Antivirus engines. This report shows that it is still possible to make use of AETs to bypass IPS detection and successfully

[1] Hackers shift to outflanking the first line of defense
http://www.cso.com.au/article/435101/hackers_shift_outflanking_first_line_defense/#closeme

[2] Symantec defiant after New York Times hackers evade antivirus defences
http://news.techworld.com/security/3423783/symantec-defiant-after-new-york-times-hackers-evade-antivirus-defences/

launch an undetected attack on networked systems. As the threat continues to grow, these techniques will soon be widely adopted by opportunistic attackers.

Intrusion Prevention and Evasion

Intrusion Prevention Systems aim to protect networks by taking action, rather than simply acting as a warning for potential security threats, like an Intrusion Detection System. However, Intrusion Prevention Systems have a number of weaknesses, one being that they may not be able to recognise attacks when a payload, the part of the virus performing the malicious action, has been broken down into multiple packets. As a result of the attack being delivered in multiple packets the data is not recognised until the receiving host has correctly amassed the payloads and reconstructed the information, which then allows it to be correctly compared to a set rule. Based on this basic principal, researchers will continue to discover and evolve evasion techniques that will be capable of bypassing protection mechanisms in security appliances, unless IPS vendors start to address the problem more systematically.

The Threat to Business

Significant academic attention has been focused on investigating techniques for defeating IDS/IPS systems, with work dating back to the 1990's. This information has been accessible to the wider public including those who may wish to put the information to malevolent use. As the overwhelming majority of organisations now employ some form of security on their network, it is reasonable to suggest that in order to bypass security most forms of successful network attack employ some degree of evasion technique. This could range from being in the form of a simple single attack on the network to a more complex multi-staged one.

Designing and applying IT security within an organisation has, to some extent, always been something of an 'arms race'. Early evasion techniques were relatively simple methods that could be employed to evade an IDS/IPS. Protecting against them was as simple as the techniques used. Recent advances in the development of evasion techniques demonstrate how the attacker can close the gap in the race to access secured systems, with the ability to combine evasions that generate far more complex techniques, e.g., AET. This is further exacerbated as the evasion may occur at multiple levels of the ISO model, making the evasions more complex and harder to detect.

The current threat to businesses is therefore quite high, since evasion techniques and the combination of evasions may make them undetectable and very effective against any system they are targeting. An undetectable evasion creates the perfect opportunity for a successful intrusion which can then be used at a later stage, either to exfiltrate data or to use as a resource in a botnet.

Experiment Details

For testing purposes we had a set of Intrusion Prevention Systems at our disposal. These included appliances from the following companies: Sourcefire, IBM, PaloAlto, Fortigate, McAfee, Checkpoint, Juniper, Cisco and Stonesoft. As far as we were aware, at the point of testing, the systems had up-to-date software versions, detection engines and detection rules. This report will not include version numbers but they can be provided to the vendors upon specific request to the authors.

The experiment made use of Stonesoft's Evader tool[3] to generate the attacks and their evasions. Therefore the target systems had to have vulnerable versions of the software supported by the Evader tool. The vulnerabilities selected for the experiment were those as described in CVE-2008-4250 (i.e., MS08-067) and CVE-2004-1315. These are old vulnerabilities and should be easily blocked by all vendors, and by most recent versions of the tools.

Tests conducted using open source and third party tools confirmed that the target systems were vulnerable. All IPS systems were effective at protecting against simple attacks that did not include evasion techniques. However, tests were then conducted using Evader and any successful (i.e. undetected) evasions and combinations were noted. For both vulnerabilities, testing produced a number of pseudo-random evasion combinations over a fixed period of time, that were then filtered down to a common set that was consistent across all the IPS. A summary of these can be seen in Table 1 for CVE-2008-4250 and Table 2 for CVE-2004-1315.

The findings

As seen in Table 1, for the host, vulnerable to CVE-2008-4250, out of a total of 2759 attack attempts the majority of IPS tools detected 98.5% of the attacks. Only 1.5% or less of the attacks using evasion techniques was successful. Only Sourcefire detected less than 94% of the evaded attacks compared to the other vendors tested, failing to detect 6.669% of the attacks. The best two systems during testing were found to be Cisco with a success rate for detection of 99.928% and Stonesoft with a 99.565% rate.

IPS	CVE-2008-4250 Successful evasion(s)	Successful evasion(s) %	Detection rate %
Sourcefire	184	6.669%	93.331%
IBM	41	1.486%	98.514%
Palo Alto	38	1.377%	98.623%

[3] http://evader.stonesoft.com/

Fortigate	36	1.305%	98.695%
McAfee	30	1.087%	98.913%
Checkpoint	25	0.906%	99.094%
Juniper	12	0.435%	99.565%
Stonesoft	12	0.435%	99.565%
Cisco	2	0.072%	99.928%

Table 1. - CVE-2008-4250 (out of 2759 attempts)

Out of the 2638 attack attempts against the CVE-2004-1315 vulnerability, the results in Table 2. were slightly more surprising. Detection rates for most systems ranged between 50.569% and 65.883% (successful evasion attacks between 34.117% and 49.431%). Only two vendors achieved a detection rate of 99% or higher (i.e. less than 1% successful evasions.) These were Fortigate and Stonesoft with a detection rate of 99.242% and 99.735%, respectively.

The major concern is that seven out of the nine IPS systems tested failed to detect 34%-49% of attacks that used evasion techniques and this particular vulnerability.

IPS	**CVE-2004-1315 Successful evasion(s)**	**Successful evasion(s) %**	**Detection rate %**
McAfee	1304	49.431%	50.569%
Juniper	1303	49.393%	50.607%
Palo Alto	1294	49.052%	50.948%
Cisco	1292	48.976%	51.024%
Checkpoint	1132	42.911%	57.089%
Sourcefire	997	37.794%	62.206%
IBM	900	34.117%	65.883%
Fortigate	20	0.758%	99.242%
Stonesoft	7	0.265%	99.735%

Table 2. - CVE-2004-1315 (out of 2638 attempts)

Taking into consideration both tables, it can be safe to conclude that Fortigate, with 98.695% and 99.242%, and Stonesoft, with 99.565% and 99.735%, generally fared the best overall, scoring high detection rate percentiles. Stonesoft demonstrated consistency in both tests, unlike other tested systems.

The number of attack attempts has been normalised[4] to include common attacks tested across all IPS. We had Evader operating for a fixed length of time, and since every IPS performed differently, some processed more events than others. As a consequence, in some cases above, there has been a reduction of successful evasions. It should be noted that a committed attacker with enough resources and time could have access to any number of IPS. The attacker could then find the best combination of evasion techniques across all the systems and make use of this combination to bypass all IPS.

Overall, the work presented in this report should be a wider call to the network security community that IPS systems need to become more aware and reactive in relation to the use of possible evasion techniques, exploiting both previous and current vulnerabilities, during an attack.

Executive Summary

Evasion techniques are a recognised problem in network security. Advanced Evasion Techniques, on the other hand, are overlooked by many in the IPS industry, which is leading to attacks that are hard to detect. We believe that AET should be a key concern for IT Security practitioners as they enable attackers to circumvent security measures and gain unauthorized access to restricted assets.

The overall outcome of the experiment is troubling. As we have seen with Advanced Persistent Threats, attackers are opportunistic and will expend considerable effort to gain access. Once on the inside they then may be capable of exfiltrating information. Therefore even the success of one single evasion is enough to allow an active payload through placing a network and the information it contains at risk.

Currently companies are investing extensive amounts of money on securing networked systems. In the present financial climate companies need to be sure they are providing the best protection possible, this now includes attackers employing advanced techniques used to evade Intrusion Prevention Systems.

In this experiment we have shown that some of the IPS installed and available offer limited protection against attacks using advanced evasion techniques.

The key requirement of a successful system is to provide the broadest possible protection for a network. Based on the experiments presented in this paper, the Stonesoft system offers the best protection against complex evasion attempts.

[4] Due to the varied number of attack attempts across the different IPS, we have normalized the set to include only the attacks that were common across all IPS.