SE Labs

Email gateway testing methodology

Methodology version 1.1; Created: 30/11/2016

Contents

1.0 Introduction

This methodology provides a way to test email filtering services for prolonged periods using a variety of realistic approaches and to supply results on an on-going basis. A network of dedicated email honeypots enables us to utilise the latest campaigns in these tests.

Testers also generate targeted malicious attachments and malicious link tests using live malware from our continuous anti-malware endpoint testing service. A wide selection of legitimate messages is included to test for false positive rates.

Testing is conducted using regular endpoint clients configured to use popular email services such as Google Apps and Microsoft Office 365 that are, in turn, configured to use the email gateway products under test.

2.0 Test framework

The test framework collects threats, verifies that they will work against unprotected targets and exposes protected targets to the verified threats to determine the effectiveness of the protection mechanisms.

2.1 Threat Management System (TMS)

The Threat Management System is a database of attacks including live malicious URLs; malware attached to email messages; links to malware included in email messages; spear-phishing email messages; and a range of other attacks generated in the lab using a variety of tools and techniques. All attacks used are either real attacks found in the wild or otherwise highly realistic attack scenarios. Live malware threats are fed to the Threat Verification Network (TVN).

2.2 Threat Verification Network (TVN)

When threats arrive at the Threat Verification Network they are sent to Vulnerable Target Systems in a realistic way. For example, a target would load the URL for an exploit-based web threat into a web browser and visit the page; while its email client would download, process and open email messages with malicious attachments, downloading and handling the attachment as if a naïve user was in control.

Replay systems are used to ensure consistency when using threats that are likely to exhibit random behaviours and to make it simpler for other labs to replicate the attacks.

2.3 Target Systems (TS)

Target Systems (TS) are identical to the Vulnerable Target Systems used on the Threat Verification Network, except that they also have endpoint protection software installed.

2.4 Service configuration

Services will be configured according to each vendor's recommendations. Additional changes may be made to take into account the issues surrounding IP address reputation. These may include, but are not limited to:

a) Adding header metadata to provide original source IP address values
b) Adding source IP address values into the SMTP negotiation (e.g. XCLIENT)
c) Whitelisting the attacking systems' IP address(es) to allow reputation systems to accept the message for analysis, after which it may block the message based on the source IP address (see a) and b) above)

2.5 Threat selection

All of the following threats are considered valid for inclusion in the test, although the distribution of the different types will vary according to the test's specific purpose:

a) Public exploit-based web threats (exploitation attacks)
b) Public direct-download web threats (social engineering attacks)
c) Public email attachment threats (exploitation and social engineering attacks)
d) Private exploit-based web threats (exploitation attacks)
e) Private direct-download web threats (social engineering attacks)
f) Private email attachment threats (exploitation and social engineering attacks)

Public threats are sourced directly from attacking systems on the internet at the time of the test and can be considered 'live' attacks that were attacking members of the public at the time of the test run. Multiple versions of the same prevalent threats may be used in a single test run, but different domain names will always be used in each case.

Private threats are generated in the lab according to threat intelligence gathered from a variety of sources and can be considered as similar to more targeted attacks that are in common use at the test of the test run.

All threats are identified, collected and analysed independently of security vendors directly or indirectly involved in the test.

The full threat sample selection will be confirmed by the Threat Verification Network as being malicious.

False positive samples will be messages containing popular and non-malicious website URLs, text-based messages with no harmful content and attached legitimate applications. These will comprise real legitimate email messages and generated messages that are clearly legitimate and will not easily be confused with malicious messages.

2.6 Target System details

The Target Systems are Windows PCs, deployed either as physical or virtual systems.

Each system has unrestricted internet access and it isolated from other Target Systems using Virtual Local Area Networks (VLANs).

The email client used will be configured to access the test's email samples via the email gateway undergoing test, according to instructions provided by each email gateway supplier.

Products run with the default settings. Additional logging may be enabled if requested by the vendor of the product in question. Vendors of business software are invited to make configuration recommendations.

3.0 Threat selection and management

3.1 Sample numbers and sources

The Target Systems will be exposed to a selection of undesirable email messages. These are weighted heavily (~75 per cent) towards public email-based threats, specifically those including malware, links to malware and other malware-related incidents. Spear-phishing and other social engineering attacks will also be included. A smaller set of the samples will include private, targeted attacks delivered as email attachments.

3.2 Sample verification

Threats will be verified using Vulnerable Target Systems, as outlined above (see 1.0 Test framework).

Threat verification occurs throughout the test period, with live public threats being used on shortly after they are verified as being effective against the Vulnerable Target Systems on the Threat Verification Network.

In cases where a threat is initially verified to be effective, but which is found not to be effective during testing (e.g. its C&C server becomes unavailable) the threat sample will be excluded from the test results of each product.

3.3 Attack stage

Threats are introduced to the system in as realistic a method as possible. This means that threats found as email attachments are sent to target systems in the same way – as attachments to email messages. Links to web-based threats are downloaded directly from their original sources, via clicking through in the email.

4.0 Legitimate sample selection

Non-malicious email test messages, website URLs and application files are used to check for false positive detection. The number of these URLs and files will be proportional to the number of threat samples used. Candidates for legitimate sample testing include newly released applications, ranging from free software to the latest commercial releases.

Potentially unwanted programs, which are not clearly malicious but that exhibit dubious privacy policies and behaviours, will be excluded from the test. Email body content will be clearly legitimate and not closely resembling harmful messages.

5.0 Measuring success

The following occurrences during the attack stage will be recorded.

5.1 The point of detection

(e.g. on arrival at the gateway).

5.2 Detection categorisation, where possible

(e.g. URL reputation, signature or heuristics).

5.3 Details of the threat, as reported by the product

(e.g. threat name; attack type).

5.4 Action on threat

(e.g. deletion, quarantine, delivered with warning, delivered without warning)

5.5 Legitimate files allowed to pass without problems

5.6 Legitimate files acted on in non-optimal ways

(e.g. accusations of malicious behaviour; blocking of installation)

5.7 Any anomalies

(e.g. strange or inconsistent behaviour by the product.)

6.0 Measuring product effectiveness

Each email gateway product is monitored to detect its ability to detect, block or warn against threats. Malware and legitimate application samples that are allowed to pass are checked to ensure that they are still valid and have not been corrupted. Corruption of malware is allowed, while corruption of legitimate applications is not.

Products are scored according to their success in warning users against threats or preventing such users from downloading these threats.

SE LABS LTD
ONE Croydon, CR0 0XT, United Kingdom.
Registered in England: 9688006.
Tel: +44(0)203 875 5000; Email: info@selabs.uk