ENDPOINT MEMORY EXPLOITATION

Testing Methodology

SE Labs

SE Labs

Methodology version 1.0;
Created: 01/03/2017

CONTENTS

1.0 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.

1.1 Threat Management System (TMS)

The Threat Management System is a database of attacks including live malicious URLs; malware attached to email messages; and a range of other attacks generated in the lab using a variety of tools and techniques. Threats are fed to the Threat Verification Network (TVN).

1.2 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.

1.3 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.

1.4 Threat selection

All of the following exploitation attacks 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 email attachment threats
b) Private exploit-based web threats
c) Private email attachment threats

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.

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 popular and non-malicious applications downloaded directly from their source websites where possible.

1.5 Target System details

The Target Systems are identical Windows PCs specified as below.

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

Each system runs Windows 7 (64-bit), updated with security patches available up to Service Pack 1.

Popular but vulnerable third-party applications installed include Adobe Flash Player, Adobe Reader, Apple QuickTime and Oracle Java (32-bit).

A web session replay system will be used when exposing systems to web-based threats. This provides an accurate simulation of a live internet connection and allows each product to experience exactly the same threat. All products have real-time and unrestricted access to the internet.

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.

Automatic submission of data to vendors is disabled where possible unless this reduces the immediate effectiveness of the product.

All products are updated fully using the latest definitions, patches and any other available updates. These updates are made immediately prior to each exposure to a threat or legitimate application. Products may be upgraded to the latest version, if the version changes during the test period.

2.0 Threat selection and management

2.1 Sample numbers and sources

The Target Systems will be exposed to a selection of threats composed of exploits designed to corrupt memory with a view to subverting the system. The number of attacks used will vary according to the test's specific purpose.

2.2 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.

2.3 Attack stage

Threats will be introduced to the system in as realistic a method as possible. This means that threats usually found as email attachments will be sent to target systems in the same way – as attachments to email messages. Web-based threats are downloaded directly from their original sources. These downloads occur through a proxy system that includes a session replay service to ensure consistency.

Public threats that run on the Target System are allowed 10 minutes to exhibit autonomous malicious behaviour. This may include initiating connections to systems on the internet or making changes to the system to establish persistence.

3.0 Legitimate sample selection

Non-malicious application files are used to check for false positive detection. The number of these files will match or exceed the number of malware samples used, according to the test's specific purpose. 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.

4.0 Measuring success

The following occurrences during the attack stage will be recorded.

4.1 The point of detection

(e.g. before/after execution).

4.2 Detection categorisation, where possible

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

4.3 Details of the threat, as reported by the product

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

4.4 Unsuccessful detection of threats.

4.5 Legitimate files allowed to run without problems.

4.6 Legitimate files acted on in non-optimal ways

(e.g. accusations of malicious behaviour; blocking of installation) and at what stage (e.g. before/after execution).

4.7 User alerts/interaction prompts such as:

a) Pop-up information messages (even if non-interactive).
b) Requests for action (take default option or follow testing policy of 'naïve user' if no default provided).
c) Default suggestions.
d) Time-out details (e.g. record if an alert/request for action disappears/takes a default action after n seconds of no user response).

4.8 When an initial attack or attacker succeeds in downloading further malicious files, such downloads will be recorded along with the product's behaviour (if any).

This additional data will be presented alongside the main results, clearly labelled as representing a second attack. For statistical purposes, detection rates of these files will not be automatically added to the overall totals for each product (although doing so after the event will be possible).

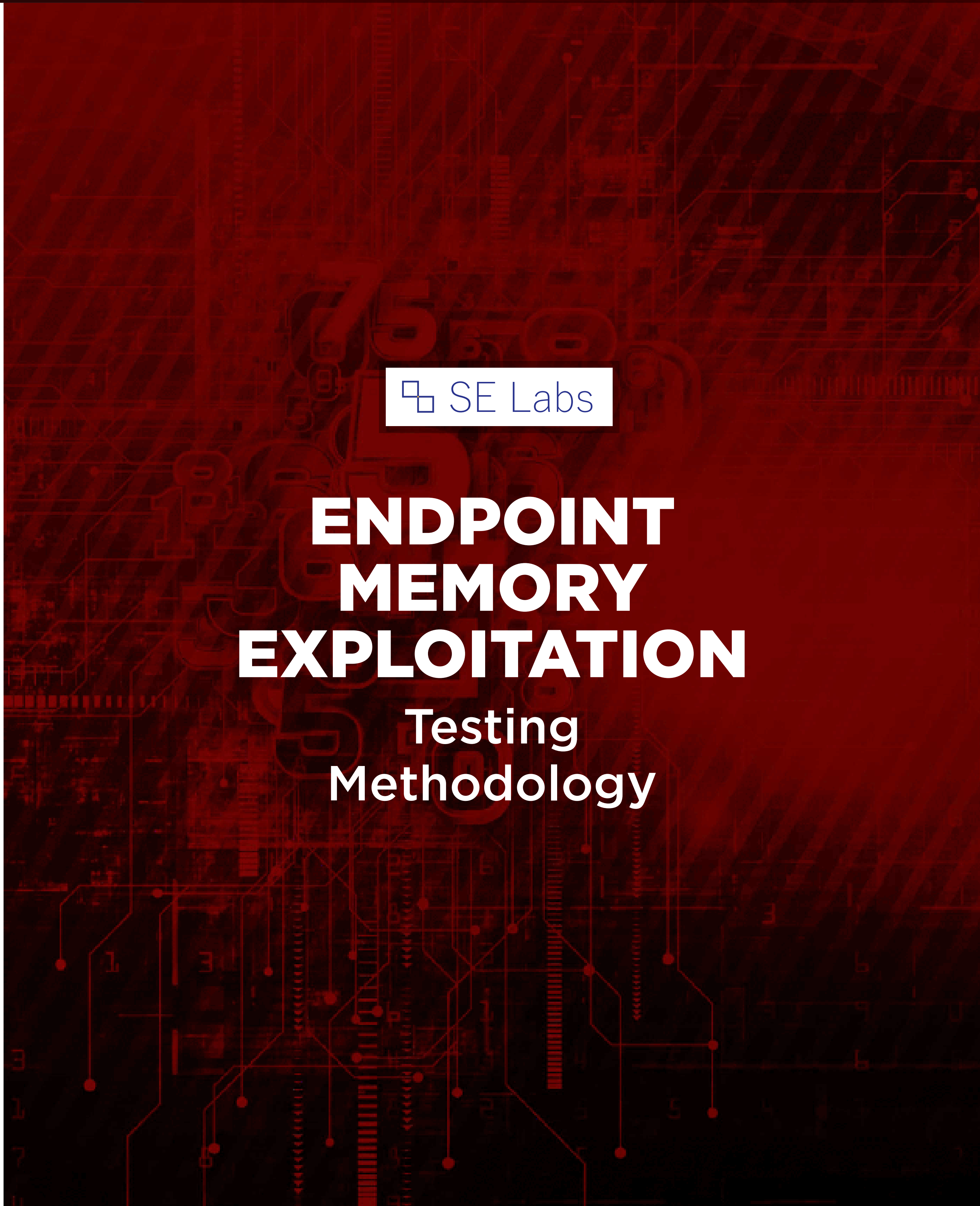
4.9 Any anomalies

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

5.0 Legitimate sample selection

Non-malicious application files are used to check for false positive detection. The number of these files will match or exceed the number of malware samples used, according to the test's specific purpose. 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.



SE Labs

ENDPOINT MEMORY EXPLOITATION

Testing Methodology