Public

Enterprise Advanced Security Ransomware Security Testing Methodology

Contents

1. Test framework

The test framework collects threats, verifies that they work against unprotected targets and exposes protected targeted 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 adversary techniques and tools used to emulate real world threat actors. Test cases are applied to the Threat Verification Network (TVN).

1.2 Threat Verification Network (TVN)

Threats sourced from the TMS are sent to vulnerable target system to ensure the validity of each test case.

1.3 Initial attack vectors

The following attack vectors are considered valid:

a) Private e-mail attachments (social engineering attacks)
b) Private direct-download web threats (social engineering attacks)
c) Private exploit-based web threats (exploitation attacks)
d) Access with compromised credentials (using credentials stolen via spear phishing attacks, enabling initial access to target devices)
e) Previously compromised endpoints (replicating an attacker with foothold on a network that was established before the tested security solution was deployed)
f) Local removable media

1.4 Targeted systems and targeted locations

The targeted systems will replicate vulnerable systems to the attack vectors present in the test. The target systems must contain enough files and a variety of file types for encryption. Targeted files may include:

a) Office file types - .docx, .doc, .docm, .xlsx, .xlsm, pptsx etc
b) Picture - .jpg , .png, .raw, .tiff, .gif
c) Video - .mkv , .mp4, .wmv
d) Miscellaneous - .html, .sln , .psd, .pproj

At least 1,000 files spread across the categories named above are present on the target system. The target locations can be considered in scope:

a) Common personal user folders. E.g. Desktop, Documents, Videos, Pictures
b) Local Network Shares
c) Cloud Accessible Folders
d) Removable Devices

1.5 Scenario selection

Publicly sourced and their derivatives are deployed on the endpoints any of the initial attack vectors. A subset of samples from each ransomware family will be chosen to be deployed using APT-style attacks including living of the land techniques and supply chain techniques.

APT-style scenarios are based on publicly available information. SE Labs will map key points of attacks to MITRE's ATT&CK Matrix for Enterprise.

2. Measuring success

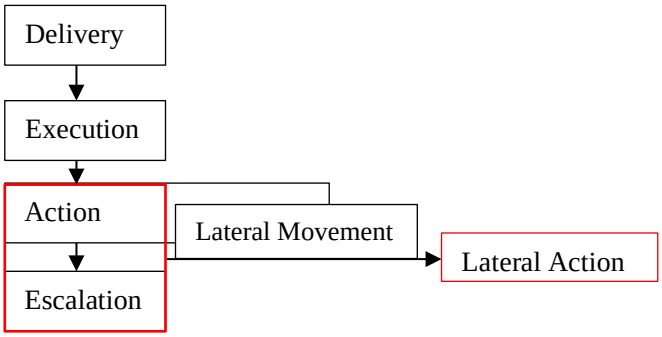
The test is performed in two stages, commodity Ransomware and APT-style Ransomware deployment.

2.1.1 Commodity ransomware

Commodity Ransomware is defined as publicly sourced malware and derivatives based on it. These will focus on the delivery and execution stages of an attack. Detection will be credited upon successful attribution of ransomware behaviour by the product under test.

2.1.2 APT-style ransomware attacks:

Assuming the following basic attack flow allows us to identify key stages where Ransomware can be deployed. Stages in red are critical to ransomware deployment.



All attack stages are performed to accurately represent the behaviour of a real-life attacker. Detections will be noted at each stage where applicable however the stages in red are considered as critical to ransomware deployment as such this is when detection will be measured.

As the attack is performed the TTPs used will be represented for each scenario under the ATT&CK framework as such:

Delivery	**Execution**	**Action**	**Escalation**	**Lateral Movement**	**Lateral Action**
Technique A	Technique B	Technique C	Technique D	Technique E	Technique F
Technique G	Technique H	Technique I		Technique X	Technique Y

2.2 Reported details

How the solution reports the threat when detected. For example, the threat's name or an attack type.

2.3 Unsuccessful threat detection

When the solution fails to detect the threat, this is recorded.

2.4 Anomalies

Testers record any strange or inconsistent behaviour shown by the solution.

3.0 Legitimate sample selection

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

When testing business grade products, the delivery method of the legitimate applications reflects real-world conditions. A system image with all business applications installed is created and the product under test is then installed on this new corporate image. If the product performs any full disk scanning during the installation process, any detections resulting from this will be noted. After the product is deployed each application will be executed for at least 60 seconds, with as many features of the application used as possible.

Potentially unwanted programs, which are not clearly malicious but that exhibit dubious privacy policies and behaviours, will be excluded from the test.

4.0 Change Log

04/09/2023 v1.0 Document created.