Keywords: SE Labs; ESSP; email; filtering; assessment;

8th January 2020
Updated : 3rd February 2020

Version 1.2

Q1 2020 Email Security Service Protection Test Plan

AMTSO Standard Compliance Statement

This Test has been designed to comply with the Anti-Malware Testing Standards Organization, Inc. (“AMTSO”) Testing Protocol Standard for the Testing of Anti-Malware Solutions, Version 1.2 (the “Standard”). This Test Plan has been prepared using the AMTSO Test Plan Template and Usage Directions, Version 2.3. SE Labs is solely responsible for the content of this Test Plan.

Table of Contents

SELabs Test Plan for Q1 2020 ESSP

1. Introduction

SE Labs tests a variety of email filtering services to judge which are the most effective. Each service is exposed to the same threats at the same time. The threats are an equal mixture of commodity, social engineering, phishing, malware and legitimate samples. The malicious samples contained within the test are all generated from commodity samples discovered independently by SE Labs, thereby ensuring that they reflect reality to the highest degree. The legitimate samples are all generated in-house and are designed to be demonstrably benign. The resulting test reports show how effective each Test Subject Vendor's products are at detecting malicious samples while still allowing through legitimate ones. The most recent report is listed below:

Email Security Services October – November 2018
https://selabs.uk/download/enterprise/essp/2018/dec-2018-essp.pdf

2. Scope

The SE Labs ESSP test examines the ability to stop malicious email in various categories while also passing legitimate email, with the following companies and products comprising the latest Test Subject Vendors list.

Product Vendor	Product Name	Version Selected or Process Used
Fortinet	*FortiMail Cloud - Gateway Premium*	*Latest Version available by Test Commencement Date.*
Microsoft	*Office 365*	*Latest version available by Test Commencement Date.*
Microsoft	*Office 365 with Advanced Threat Protection*	*Latest version available by Test Commencement Date.*
Mimecast	*Secure Email Gateway*	*Latest Version available by Test Commencement Date.*
Perception Point	*Advanced Email Security*	*Latest Version available by Test Commencement Date.*

While SE Labs will work with Test Subject Vendors that become Participants to understand previous results and to suggest possible improvements to configurations based on those scores, Participants and Test Subject Vendors are wholly responsible for configuring the service they submit for testing by Test Commencement Date. In cases where no preferred configuration is presented by a Participant, default settings may be used.

3. Methodology and Strategy

To run the ESSP methodology, we send a Test Corpus of samples to a group of identical Office 365 accounts, each protected by a single Test Subject Vendor's product.

The Test Corpus is split into five categories as follows:

Category	Proportion
Commodity	20%
Targeted social engineering	20%
Targeted Phishing	20%
Targeted Malware	20%
Legitimate	20%

Scenarios group samples of the same threat type. For example, a scenario might concern a PayPal phishing scam, with the samples it contains all implementing different versions of that scam.

Commodity samples are emails sent by criminals as part of active, malicious campaigns. We use commodity samples in two ways. Firstly, we send fresh commodity samples as they come in during the testing period to examine the ability of Test Subject Vendor's products to respond to current real-world threats. Secondly, we use other commodity samples as the basis for targeted scenarios (social engineering, phishing and malware).

Targeted Social Engineering samples attempt to trick the recipient into willingly acting to afford some form of advantage to criminals. Examples include advanced fee fraud, sextortion, sexploitation, fake love, money mule, and so on.

Targeted Phishing samples attempt to trick the recipient into entering their credentials on a fake web site, to subsequently be either misused directly, or sold to other criminals for misuse.

Targeted Malware samples trick recipients into running malware payloads to either exploit or damage target computers. Payloads may be sent as attachments, or as links pointing to third-party servers and well-known document-sharing sites. Payloads and links to payloads may be disguised using a variety of techniques where those techniques are found being used in the wild.

Legitimate samples are generated in-house and are designed to be completely benign. These samples ensure the products under test are not configured to block every single sample we send as part of the test.

Commodity Sample Source: SE Labs independently collects commodity samples and uses various techniques to ensure relevance and variety.

Scenario Generation: Malicious scenarios are based on commodity samples discovered by SE Labs to ensure a high degree of realism. There are varying levels of sophistication added to or removed from these messages. For targeted and phishing scenarios, the original payloads and landing pages are either reused or replaced with obfuscated alternatives using real-world techniques, as required by individual scenarios.

Running the Test: Each test case is sent from a Sending Server using a standard email client in turn to each of the target accounts within a few seconds. Outcomes of sending a test case is recorded and scored according to the methodology.

At the end of the test, the results pertaining to each individual Participant are distributed to that Participant only for review, along with the Test Corpus that was used along with a description of the scenarios and the reasoning behind why the scenarios were chosen. The corpus is delivered in the same form that it was sent from the Sending Server, so that Participants can re-run samples under the same circumstances as the original test if desired.

4. Participation

SE Labs doesn’t charge for testing so there are no contracts to be considered in this section. Details of post-testing consultancy can be discussed with SE Labs directly.

The general process for participation in this, or any, test with SE Labs follows.

- SE Labs or Vendor approach one another in person, by email or on the phone.
- Both parties will then:
  - Discuss the desired testing methodology and configuration
  - SE Labs reserves the right that they may or may not test the product
  - Dispute processes proceed
  - Report publication

Please contact us at info@SELabs.uk. We will be happy to arrange a phone call to discuss our methodology and the suitability of your product for inclusion.

Opt-Out Policy: If any Vendor can supply sufficient reason as to why SE Labs should not include their product in an upcoming or on-going test, SE Labs will honor that request provided that there is agreement on the facts. As an example, an acceptable Opt-Out request would include the documented and pending release of a substantially newer version of Vendor software which would render the testing of the previous version meaningless.

Conflict of Interest Disclosure: No known conflicts of interest exist at this time. Post-test consultancy services are available to all participants for a fee.

Funding: Products we consider of key interest to our readers are included in our tests at no cost to the vendor. Post-test consultancy services, rights to use our logos, and re-promote our results are made available to all participants, subject to consultancy or licensing fees.

5. Environment

Physical Configuration: Each target account is hosted by the Microsoft Office Cloud and is protected by a single Test Subject Vendor's product using the configuration of their choosing. Each

Participant supplies setup details for their product and these are followed by SE Labs system administration staff. In each case, we send benign test messages to the target account to ensure that the path to the target account through the product protecting it is open and accepting traffic before Test Commencement Date. As stated in Section 2, it is the responsibility of the Participant or Test Subject Vendor to configure their product in the way they wish it to be tested by the Test Commencement Date.

Sample Relevance: During Test Corpus development, the developer maintains the Scenario Description document. This document gives a description of each of the five categories of test (commodity, legitimate, phishing, social engineering, and targeted). It then gives a description of each scenario in each category, explaining why it was included in the corpus and how the scenario develops across its ten samples.

Geographic Limitations: All samples in the Test Corpus, with the exception of Commodity samples, are written in English. Commodity samples may, in very rare cases, be written in other languages. From time to time, SE Labs observes campaigns typically in Polish, Spanish and Chinese, and so we reserve the right to occasionally include representative commodity samples reflecting this fact in the Test Corpus.

Curation Process: The curation process of the samples upon which scenarios is based is ongoing, with a shortlist being maintained prior and during scenario development, as stated above (Sample Relevance). This enables us to respond to new, widespread campaigns that appear during corpus development, and ensures we have several alternatives at the point at which the final scenario list is compiled.

Distribution of Test Data: Once the Test Corpus is sent to the target inboxes, and the results have been collated and checked, the corpus can be supplied to all Participants at the Calculated End Date, along with the results spreadsheet, and the Scenario Description document which explains the curation and selection process for each scenario and its base commodity sample.

Test Subject Vendors have the right to challenge results. This process is the subject of a dispute call, made after the Test Subject Vendor has received and analyzed their results and the Test Corpus themselves. Advice on remediating shortcomings in a Test Subject Vendor's product or configuration is provided, with possible follow-up technical calls with engineering staff being scheduled after that.

6. Schedule

Start Date Range: The testing period includes one week of setup and testing to ensure Participant accounts are set up and configured. This will commence on 27th January 2020. This will be followed immediately by 3 weeks of testing, beginning on 3rd February 2020, which will end on 21st February. The results spreadsheet, Test Corpus and scenario description document will be given to the Participants as soon as possible after 21st February. The dispute period begins on 9th March and lasts until 20th March.

Test Duration and Calculated End Date: The final report will be published in the week of March 30, 2020.

Milestones: Interim schedule milestones are listed below.

Sample Schedule Summary for Test Project

Index	Test Activity	Start Date	Dependencies
1	*Test Commencement*	*January 27, 2020*	
2	*Confirm Vendor Configuration Feedback*	*February 2, 2020*	
3	*Milestone 1 – Testing Commencement*	*February 3, 2020*	*(2)*
4	*Milestone 2 –End of Testing Period*	*February 21, 2020*	*(3)*
5	*Feedback and Dispute Resolution Time – Retests as Needed*	*March 9, 2020 - March 20, 2020*	*(4)*
6	*Milestone 3 – Issue Final Report – End Date for Test*	*March 30, 2020*	*(5)*

Communications: All Participants will be notified when the schedule wanders by four week or more.

Risks and Risk Management: No additional risks are known at this time

7. Control Procedures

Connectivity Validation: Prior to test commencement, connectivity from the Sending Server to the target inboxes will be tested by sending identical, benign test messages to those inboxes. The Products under test are all cloud-bases, so during the testing period it is expected that information will be transmitted and retained in the cloud.

Logging: Products typically run with the default logging settings. Additional logging may be enabled vendors.

Updates: Configuration updates must not be applied after Testing Commencement.

8. Dependencies

Participant and Test Subject Vendors Required Actions: Vendors may contact SE Labs for inclusion, exclusion or to respond to an invitation, either accepting or declining.

9. Scoring Process

The following table records the possible outcomes of an individual test case, along with the associated score.

Result Code	Description	Threat	Legitimate
Inbox	Message delivered to target's inbox	-10	10
Junk Folder	Message delivered to target's junk folder	5	-5
Quarantined (admin)	Kept by the service for release by administrator	8	-8
Quarantined (user)	Kept by the service for release by end user	6	-6
Notified	Original not available for release by user.	10	-10
Stopped	Silently stopped from being delivered	10	-10
Rejected	The filtering service rejected the message with a reply.	10	-10
Blocked	Blocked on route to service under test	10	-10
Edited (Allow)	URLs or other potentially harmful components changed	-10	10
Edited (Deny)	URLs or other potentially harmful components changed	10	-10
Junk (Deny)	URLs or other potentially harmful components changed	10	-10
Junk (Allow)	URLs or other potentially harmful components changed	-7	7

10. Dispute Process

The dispute process runs for two weeks from the end of the test. Please see Section 6 covering the Test Schedule for additional details and timing. The general Dispute Process works as follows.

1. The Participant's results and the Test Corpus are provided to the Participant.

2. Participant responds within two weeks, arguing why some results are wrong.

3. A dispute call is arranged, accepting or denying the disputes.

Although discussions will follow, ultimately the data speaks for itself.

Evidence Sharing Policy: After the test is complete the dispute (results review) process begins with the provision to participants of details of missed threats and misclassified legitimate messages. Hashes of malware and URLs will be provided, as well as the body of legitimate messages. Service-side logs may also be provided in contentious cases.

11. Attestations

I understand and agree that I am submitting this Test Plan, and the following Attestations, on behalf of the entity listed below, and I represent and warrant that I have authority to bind such entity to these Attestations. All references to "I" or "me" or similar language refer to such entity. I represent and warrant that the following Attestations are true, to the best of my knowledge and belief, and each of the following commitments will be upheld to the best of my ability.

1. I will provide public notification on the AMTSO website covering my obligation for notification of a Public Test, regardless of whether a potential Participant is in actual receipt of such notification prior to the Commencement Date of a Test. (Section 1, Section 4, Section 6)

2. All products included in this Test will be analyzed fairly and equally. (Section 2, Section 3, Section 5)

3. I will disclose any anticipated or known imbalance or inequity in the Test design to all Participants in the Test. (Section 2, Section 3)

4. Although I may charge for participation in a Test, I will not charge any additional fees for a vendor to be a test subject under the Standards. (Section 4)

5. I will disclose any material conflicts of interest or other information that could materially impact the reliability of the Test. (Section 4)

6. I will disclose how the Test was funded. (Section 4)

I hereby affirm, to the best of my knowledge and belief that this Test Plan complies with the AMTSO Testing Standards, as of the date hereof.

Signature: /s/

Name: Marc Briggs

Test Lab: SE Labs

AMTSO Test ID: [AMTSO-LS1-TP022]