Cyber Essentials Plus:Test files

Version 2

Created by : Cary Hendricks,
ID Cyber Solutions
18/05/2018

Introduction

The requirement for a standardised set of test files has been requested and as such a portal was created to enable the sharing of the current and new files when they become available. ID Cyber Solutions and QG Management Standards are sponsoring the portal and creation of the files, with valuable input from several other Accreditation Bodies.

Test Files

For test file criteria, we need to distinguish between two broad groups of test files:

• malware test files — anti-malware should detect these and block the user from accessing them

• executable test files — the user should at least see a warning and a prompt that allows them to decide whether or not to proceed

To create a standard set of test files that are representative of all the file types that applicants are likely to encounter, work has started to create these files. As time goes on, more and more files will become available and existing files be replaced to maintain fresh signatures.

The current set is quite small, but it forms a basis for any innovative ideas. We would encourage everyone to come up with ideas on how we could expand this set.

The full set of representative test files being provided must include:

• container formats (such as .zip and .gz) which the Applicant's environment is able to process

• a range of file types that are executable by default on common platforms — both native binaries and scripting languages

• files of types which users might regularly receive — such as documents and spreadsheets — but which contain inert malware samples

Also note that:

• *executable test files should launch obvious behaviour (such as launching a web browser to a known page, or creating an onscreen dialog) so that the Assessor can detect execution quickly and easily*

This behaviour will be implemented in the next iteration. Most likely **29/06/2018** via the portal.

• *malware samples should be specific inert files that are known to be flagged by the majority of common antivirus solutions*

This means the EICAR files as an example. We are working on other samples for the Next Generation AV engines.

The current inventory has mostly Microsoft binaries.

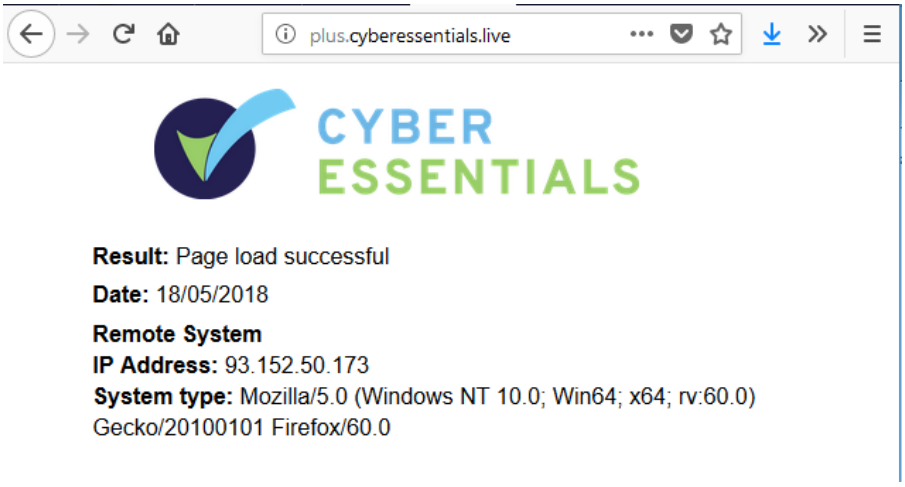
What's new?

The binaries now have active connections to the website http://plus.cyberessentials.live

The main file when launched, will present 2 buttons.

This will show the application has launched but at this stage it has not attempted to make any outbound connections.

On clicking the WEB button, it will make an outbound HTTP connection to http://live.cyberessentials.live using the **default browser.**



On clicking the EICAR button, it will make an outbound HTTP connection to http://live.cyberessentials.live/testfiles/eicar.com

This will allow control on capturing the download for the file.

Shell scripts

The following shell scripts have been updated.

Ceplus.ps1

This script will only launch when PowerShell has been enabled and can run *unrestricted scripts*. This script is not signed. On launch it will open up the default browser and attempt to load http://plus.cyberessentials.live If PowerShell has not been configured to run scripts, nothing will happen and an error may be displayed in the PowerShell command window.

Ceplus.bat

On launch it will open up Internet Explorer browser and attempt to load http://plus.cyberessentials.live

The reasoning is that if a malicious script can be saved to the system, it will try and find the most common browser on the system and use that.

Ceplus.py

This script will launch a Python based web browser included in Python and attempt to load http://plus.cyberessentials.live

Ceplus.docx

This document has a macro embedded that will launch the default web browser and attempt to launch http://plus.cyberessentials.live/macro.php

The page will also reflect that the page was invoked by a macro.

Ceplus.xlsm

This document has a macro embedded that will launch the default web browser and attempt to launch http://plus.cyberessentials.live/macro.php

The page will also reflect that the page was invoked by a macro.

Suggestions

Any suggestions will be most welcome. Please send them to me at cary@idcybersolutions.com