Tool Delivery Review

EZCheese
Version 6.2

IV&V

EDG Project Lead: XXXXX Y.
IV&V Lead: XXXXX Y
COG/OED/GB POC: XXXXX Y

IOC ERB:

IV&V Overview

- EZCheese v6.2 was tested in accordance with IMIS Requirement 2013-0090
- The test environment consisted of the following operating systems:
  - Windows XP Professional, SP3, 32-bit
  - Windows Vista Ultimate, SP2, 32 & 64-bit
  - Windows 7 Ultimate, SP1, 32 & 64-bit
- The MD5 hash values for EZCheese v6.2 are:

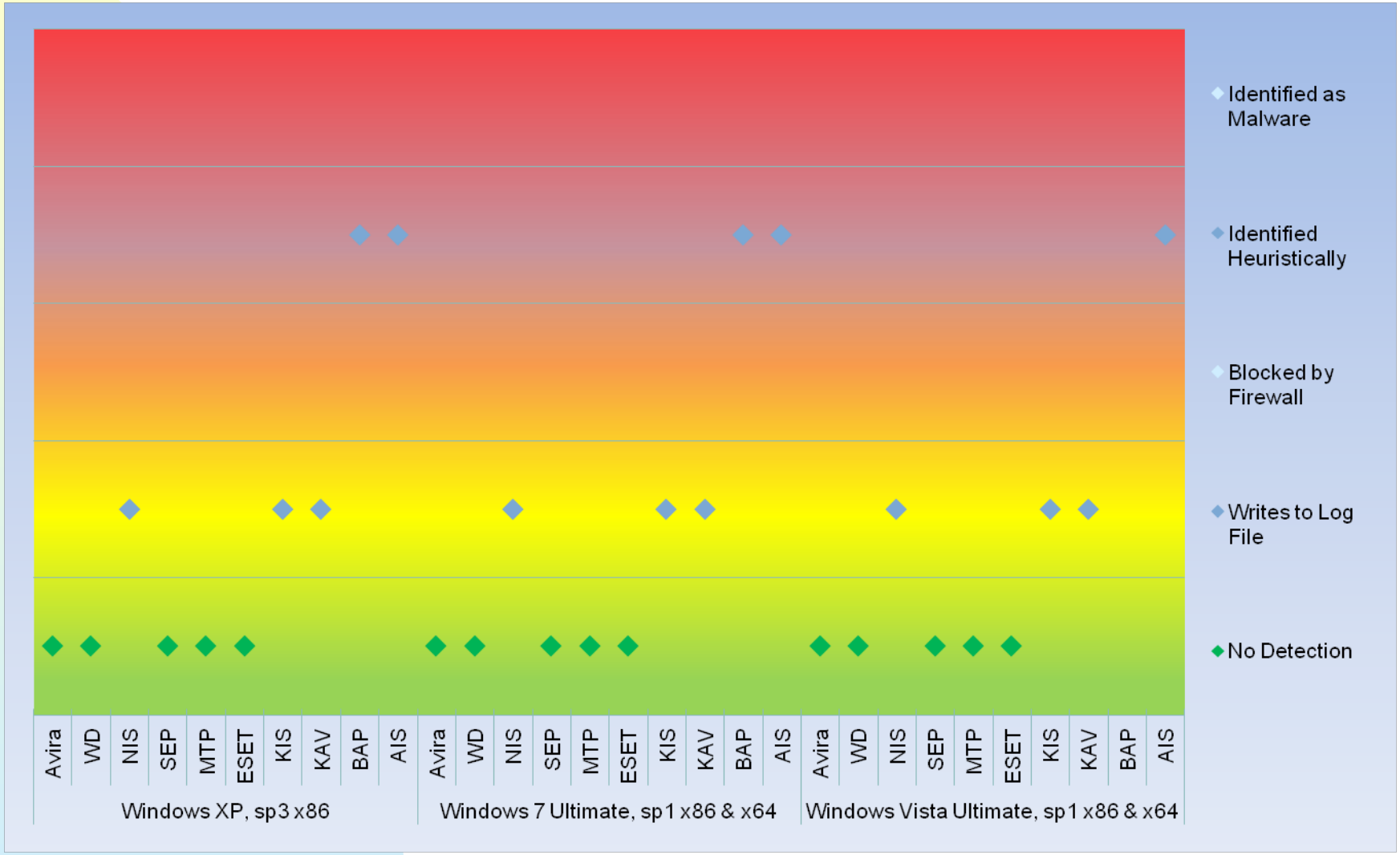
File Name	MD5 Hash Values
CheeseProcessor.exe	CBF54D4FA4BCBBA0AD3E970E1FF763FD
EZConfigUltimate.exe	7FE4255D334E69A4A74D449EA0BDB91D
Mac-n-Cheese.exe	050FB699F6915380029AAEC4FDBD60D0

IV&V Overview (cont.)

- The test environment included the following PSPs:
  - Norton Internet Security 2013
  - Kaspersky Internet Security 2013
  - Kaspersky Antivirus 2013
  - Avira Internet Security 2012
  - McAfee Total Protection 2013
  - Bitdefender Antivirus Plus 2013
  - ESET NOD32 Antivirus 5
  - Avast Internet Security 2013
  - Windows Defender
  - Symantec Endpoint Protection

PSP Characterization

Default / High Settings



IV&V Findings

	CONTEXT	IMPACTS	WORK AROUND/ RECOMMENDATION
1.	None		

IV&V Observations

- Observation 1:
  - Context: Kaspersky ISS 2013, running on Windows 7 SP1, 32 & 64-bit, generates two popup alerts upon EZCheese execution, stating “Using program interfaces of other applications”, and an alert highlighting a file EZCheese is trying to read for its file collection. This particular file was located in the Kaspersky system directory, which consequently is shown in the popup alert message as being denied access. All activity was logged and all files accessed by EZCheese collection were logged. (Alerts are only displayed on high settings but all activity was also logged on default settings)
  - Impact: Increased risk and suspicion when using EZCheese in a Kaspersky environment
  - Workaround/Recommendation: Update the User Manual to note this behavior

IV&V Observations (cont.)

- Observation 2:
  - Context: Norton ISS 2013 (default and high settings), running on Windows 7 SP1 32 & 64-bit, causes the entire system to freeze for 4 to12 seconds upon EZCheese execution. Movement of the mouse is possible but no other actions are successful
  - Impact: Increased risk and suspicion when using EZCheese in a Norton ISS 2013 environment
  - Workaround/Recommendation: Update the User Manual to note this behavior

IV&V Observations (cont.)

- Observation 3:
  - Context: On Windows XP, SP3, 32-bit OS with Kaspersky Internet Security at default and high settings, four events are captured in the log file:
    - First: Log displayed actual name of the executable, which was classified by Kaspersky as a ‘Low Restricted Object’ that was heuristically calculated
    - Second: Log indicated that the executable accessed critical system objects
    - Third: Log highlighted that the executable used program interfaces of other applications
    - Fourth: Log indicated that the executable opened a service to write data
  - Impact: Unauthorized activity on the target may be discovered
  - Workaround/Recommendation: Update the User Manual to note this behavior

IV&V Observations (cont.)

- Observation 4:
  - Context: On Windows Vista, SP2, 32-bit OS with Kaspersky Internet Security at default and high settings, two events are captured in the log file:
    - First: Log displayed the actual name of the executable and is classified by Kaspersky as a ‘Low Restricted Object’ that was heuristically calculated
    - Second: Log highlighted that the executable used program interfaces of other applications
  - Impact: Unauthorized activity on the target may be discovered
  - Workaround/Recommendation: Update the User Manual to note this behavior

IV&V Observations (cont.)

- Observation 5:
  - Context: On Windows Vista SP2, 64-bit OS with Kaspersky Internet Security at default and high settings, seven events are captured in the log file:
    - First: Log showed the actual name of the executable and is classified by Kaspersky as a ‘Low Restricted Object’
    - The remaining six log events displayed the name of the executable and the path to the Google Chrome browser’s cache file. These log events presented a link between the executable and the browser’s cache file. EZCheese was still able to collect browser data
  - Impact: Unauthorized activity on the target may be discovered
  - Workaround/Recommendation: Update the User Manual to note this behavior

IV&V Observations (cont.)

- Observation 6:
  - Context: On Windows XP, SP3, 32-bit with ESET Smart Security at default and high settings:
    - Web information, system information and network data were not collected
    - The executable process ran for 15 minutes and the process did not terminate
  - Impact: Some desired data will not be collected for targets running Windows XP, SP3 with ESET Smart Security installed
  - Workaround/Recommendation: Update the User Manual to note this behavior

IV&V Observations (cont.)

- Observation 7:
  - Context: On Windows XP, SP3, 32-bit or Windows 7, SP1, 32-bit with BitDefender Total Security at high settings:
    - An alert pop-up window immediately appeared, stating ‘Intrusion Detection has detected and blocked a potentially malicious application’
    - The executable process did not run, hence the payload was not dropped
    - This alert is recorded in the log file
    - EZCheese did return survey and file collection data
  - Impact: The payload was not deployed on the target with the above configurations
  - Workaround/Recommendation: Update the User Manual to note this behavior

IV&V Observations (cont.)

- Observation 8:
  - Context: On Windows Vista, SP2, 64-bit OS with BitDefender Total Security at default and high settings:
    - An alert pop-up window immediately appeared, which stated ‘Active Virus Control has detected and blocked a potentially malicious application’
    - The executable process failed to run, hence the payload was not dropped
    - This alert is recorded in the log file
    - EZCheese did return survey and file collection data
  - Impact: The payload was not deployed on the target with the above configurations
  - Workaround/Recommendation: Update the User Manual to note this behavior

IV&V Observations (cont.)

- Observation 9:
  - Context: On Windows XP, SP3, 32-bit; Windows Vista, SP2, 32-bit; or Windows Vista, SP2, 64-bit with Norton Internet Security at high settings:
    - An entry is recorded in the log file. The log entry identified the EZCheese executable and notes that it is trying to access the Internet
    - The executable and its location are captured in the log file
  - Impact: Unauthorized activity on the target may be discovered
  - Workaround/Recommendation: Update the User Manual to note this behavior

IV&V Observations (cont.)

- Observation 10:
  - Context: On Windows XP, SP3, 32-bit; Windows Vista, SP2, 32-bit; or Windows Vista, SP2, 64-bit with Avast Internet Security at default and high settings:
    - Two alert pop-up windows appeared
    - After analysis, Avast determined that the executable was not malware but the executable was sandboxed
    - Only the file collection and payload drop actions were performed by the tool
  - Impact: Survey of the target will not be completed
  - Workaround/Recommendation: Update the User Manual to note this behavior