DYNAMIC PAGE—HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//COMINT//REL TO USA, FVEY

You are logged in a [redacted]

Search FlawMill

--- Jump to project ---

flawmillbeta

- (TS//SI//REL) ROC CT MAC NSAW DMW QUEUE
- Issues
- Projects
- Home

edit

Issue #12: (TS//SI//REL) AZTECTOMB32 DMW Install and ESH Package

8 months ago by [redacted] at 18:10, 13 Feb 2012

Votes

1

Actions

- Add an Update
- Add a Subscriber
- Subscribe to this Issue
- Adopt this Issue
- Assign this Issue
- Move this Issue

Project Actions

- Submit an Issue
- Return to Project

(TS//SI//REL) Please create a DEMENTIAWHEEL install for AZTECTOMB32 (Has a UR and VAL ID is 610104408). Target is Win 7 32-bit running PSP Kaspersky 2010.

Once DEMENTIAWHEEL is installed, please build a 12:3:1 ESH package (84 total possible infections) for deployment with AZTECTOMB32. Please make sure all USBs that are seen will be infected. Details:

ESH payload: DEMENTIAWHEEL (Version based off your install), VALIDATOR (32 and 64-bit)

VALIDATOR settings: LP: 50

Project Name: AZTECTOMB

32 and 64 bit VALIDATORs

Callback frequency: 1 hour

DEMENTIAWHEEL settings:

airgapLogFlag = 1

copyAirgapExfilToDiskFlag = 1

Details

Submitted by:
[redacted]
Owners:
[redacted]
Status:
closed
Priority:
high
Tags:

reply

(U) Starting Build

8 months ago by [redacted] at 11:33, 23 Feb 2012

(TS) Took ticket, the PSP is still unevaluated, awaiting testing. Had to change from 12:3:1 ESH to 10:3:1 because of ESH limitation.

Updates

- Status changed from "new" to "accepted"

reply

(U) Built

8 months ago by [redacted] at 11:36, 23 Feb 2012

(TS//SI//REL) Building complete and in [redacted]

Awaiting PSP testing and evaluation from lrivera.

Updates

- Status changed from "accepted" to "configured/awaiting testing"

reply

(U) On Hold

8 months ago by [redacted] at 14:53, 27 Feb 2012

(TS//SI//REL)The new guidance per ROC MD's and PSP Platform Champion is "NO NEW IMPLANTS ON KASPERSKY 2010+."

This is because Kaspersky 2010+ products have been updated to include the cloud functionality. Until the work around is fixed then nothing can be implanted on them. Any existing implants are ok to continue collection from, but no new installations!

This means for this project, DMW and ESH is a NO GO!

Sorry.

The following link is the PSP advisory from PORTALSIX:

https:/[redacted]

Updates

- Status changed from "configured/awaiting testing" to "on hold"

reply

(U) Closed

6 months ago by [redacted] at 13:33, 18 Apr 2012

(TS//SI//REL)Closed due to PSP, per analyst

Updates

- Status changed from "on hold" to "closed"

Add an Update

Summary

Details

preview

Details use WikiInfo-style markup (info).

Issue Status

closed

« re-open

Issue Priority

high

« low medium high critical

Add Tags

Tags should be comma separated

Attach

image patch file issue

Post Update Portion marking and **bold** fields are required.

Content Steward: (S//SI//REL) [redacted]
Page Publisher: (U//FOUO) [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108
An Innovations Working Group Project.
DYNAMIC PAGE—HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//COMINT//REL TO USA, FVEY