(U//FOUO) TURMOIL GALLANTWAVE

From WikiInfo

(U//FOUO) VALIANTSURF: TURMOIL GALLANTWAVE

(U//FOUO) The **TURMOIL CIET** (Common Internet Encryption Technologies) Thrust's mission is to ensure that the GALLANTWAVE team's TURMOIL-related requirements are fulfilled. Two sub-projects under CIET are VALIANTSURF and GALLANTWAVE.

(TS//SI//REL) GALLANTWAVE (GW) is a CES Mission Application hosted on TURMOIL that enables exploitation of target communications that employ Data Network Session Cipher (DNSC) technologies. The GALLANTWAVE mission application integrates with TURBULENCE-based solutions at the front end. After interacting with T5's LONGHAUL key recovery service via ISLANDTRANSPORT, it exploits the cipher at the front end, exposing the plain text to follow-on selection and collection.

BULLRUN

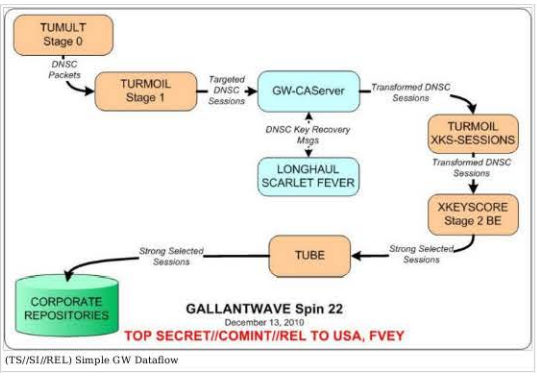
(S//SI//REL) Information revealing any capability NSA has to exploit a specific target's or company's implementation of encryption for GALLANTWAVE technologies is BULLRUN.

Contents

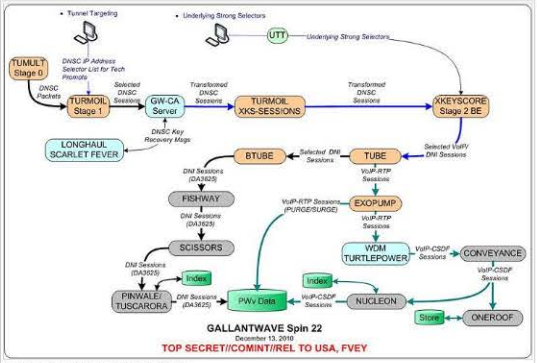
GALLANTWAVE Detailed Description

(TS//SI//REL) GALLANTWAVE (GW) implements TML Stage 1 PPF graphs (1 per host) with dedicated instances of the TechPromote (GWAeg) and the PSPSeg (GWSeg). GW PPF graphs identify and promote DNSC packets that meet criteria specified in a Rules.cfg file. A TE_GALLANTWAVE graph subsequently sessionizes the selected traffic, injects control-flow metadata, and forwards targeted DNSC Sessions to a GW mission-application hosted on a CA Server. The GW-CAServer interacts with SCARLET FEVER (a CES LONGHAUL component) to transform those sessions for IP-addresses within an approved set of target IP-addresses. The GW-CAServer transformed sessions are sent to XKEYSCORE via a modified TURMOIL XKS-SESSIONS graph for session processing, strong-selection, and forwarding to follow-on processing systems and Corporate Repositories.

Data Flow Diagrams



(TS//SI//REL) Simple GW Dataflow



(TS//SI//REL) Complex GW Dataflow

(U) Open GALLANTWAVE DRs

(U) Note: This table can be dynamically-edited (cells edited; rows added). Changes are saved to CIET/Gallantwave_DRs.

Headline	DR Number (TU or TML)	Date Submitted	Description Version	Resolution/Status	Responsible component/project	TML version	Testing/Deployment notes
DnscPromotionFilterEngine is part of FspfProcess and should not be	X7I-T00054264 [redacted]	Apr 2013	The GwModule as delivered start the DnscPromotionFilterEngine as part of the FspfProcess. According to the TURMOIL Core team, no processes should be added to the FspfProcess, as this 'strictly forbidden'. Due to this configuration, we have observed a number of occurrences where the message queues for DnscPromotionFilter are not created, and this results in 100% loss of Dnsc misson for the affected Fspf.	Medium State: fixed	Assigned: [redacted]	GW 4.0.0-3.0	Fixed with the release of GW 4.0.0-3.1 (MF#109912)
XKS HttpDemux Problem at DGO	DNCA Ops ticket 99481 [redacted]	Dec 2012	For several months, GW transformed sessions requiring http decompression and detunneling have been rendered useless by an XKS 1.5.7 deficiency			XKS 1.5.7	Submitted By: [redacted] Adddate: 2013-03-28 15:05:06 Correction to the previous statement: tjse t3 does in fact have XKS 1.5.10 installed, and querying in XKEYSCORE has

							shown that, for the past week, there have been successful GALLANTWAVE decrypts that have resulted in hits on 'compression/http_decompressed' but not any results that are still in the gzip compressed state. Thus, we can feel confident that **XKS 1.5.10 also resolves this issue**, though it has not been deployed to any live sites as of yet.
Memory allocation errors	[redacted]	Mar 2013	Both the TtSessionToPacketEngine and TtPacketInjectorEngine engines have multiple crashes and restarts due to memory allocation errors (see below). TUMMS graph showing restarts is attached. /c2/run.d/cemetery/TepidTsunamiProcess /2013-03-13_04:48:19.487/process.log:2013-03-13 04:48:18,249 ERROR tdk.adapter.spte.SessionToPacketTransformEngineAdapter Root cause: St9bad_alloc; Calling SessionToPacketTransformEngine::processSession: Unexpected bad_alloc exception caught: St9bad_alloc	High State: Open	Assigned: [redacted]	Tt 4.0.0-1.3	

(U) Old GALLANTWAVE DRs

- see Old GALLANTWAVE DRs for closed, resolved, rejected etc DRs

Spin 12.2

- GW 3.1-3.1 uses UTT/Core SSC or Static Target files to target.

(U) GALLANTWAVE and NetDef Brief

Spin 12.1

(U//FOUO) Feathers

- GW 3.1-2.0 uses KEYCARD to target and has the SLIDETACKLE capability.
- GW 3.1-3.0 uses Core SSC and IPCollector to target and works at both U and NET Def sites

Spin 22

Stories

(U//FOUO) Support GALLANTWAVE Deployments
(U//FOUO) Prototype Stage 1' Reinjection US131 TA1563

(U) RFCs

RFC Number (TU or TML)	Description	Related DR(s)	Resolution/ Status	Date Submitted
2981	Instructions to change targeting file	None		week of 6 Dec 2010
3120	Instructions to change MHS Live targeting file	None		week of 17 Jan 2011

Spin 21

Stories

GALLANTWAVE
(U//FOUO) Feather Deliveries
(U//FOUO) Deploy/activate CA Servers to POLARSTARKEY
(U//FOUO) Interagency pairing
(U//FOUO) GALLANTWAVE 3.0 Design

Retrieved from '[redacted]'
Category: Wikiclass