FARSIGHT SECURITY

Security Information Exchange (SIE) Channel Guide as of January 1, 2017 (subject to change without notice)

Channel #	Channel Name	Channel Description
Base Channel Package -- Select Content Providers		
14	Darknet - Farsight	Evidence of Internet address space scanning and unsolicited connection attempts to unlit networks, as detected by BGP routers
25	Spam (selected fields only) - Farsight	Data extracted from emails sent to spamtrap addresses
27	Phishing URLs - PhishLabs	URLs and other metadata related to malicious sites involved in phishing campaign
42	IDS and Firewall Log Data - ThreatStop	Anonymized evidence of blocking action from IDS and Firewall devices managed by ThreatStop (All source IP addresses are replaced with RFC1918 IP addresses)
80	Sinkhole Data - Conficker Working Group (CWG)	Requests to sinkhole web servers that capture web requests from infected clients
114	Sinkhole Data - Game Over Zeus (GoZ)	DNS command and control activity related to an FBI-directed takedown of GameOver Zeus botnet infrastructure. Also contain HTTP requests to sinkholes.
Raw Passive DNS Channel Package -- Farsight Security		
202	Passive DNS - Raw Sensor Array Input	Raw data collected through Farsight Security's Passive DNS sensor array
Value Added Passive DNS Channel Package -- Farsight Security		
204	Passive DNS - De-duplicated / Filtered / Verified	Channel 208 data filtered to remove extraneous, non-DNS-specific data prior to insertion into Farsight Security's DNSDB
206	Passive DNS - Processing Rejects (Chaff)	Any data rejected by the filtering and verification processes for channels 204, 207, and 208
207	Passive DNS - Deduplicated RRSETS	Channel 202 data de-duplicated
208	Passive DNS - Verified RRSETS	Channel 207 data verified for integrity and to be "in bailiwick"

Newly Observed Base Domains Channel Package

212	Newly Observed Base Domains (NOD)	Derivative work containing RRSET information for domains not seen in Ch. 204 (nor in gTLD zone file listings) during the entire history of DNSDB (starting June 2010)

Newly Observed Fully Qualified Domain Names Channel Package

213	Newly Observed Fully Qualified Domain Names	Fully qualified domain names (FQDN) seen in channel 204 that are new from the perspective of DNSDB

DNS Changes Channel Package

214	DNS Changes	Whenever a new FQDN is written to Ch213, or whenever a previously observed FQDN gets a new value

DNS Errors Channel Package

220	DNS Errors	Queries where the authoritative DNS servers answered with an error code.

NXDOMAINS Channel Package

221	NXDOMAINS	Queries answered with NXDOMAIN. The domain request could not resolve to an IP. The domain does not exist

Spam (Full Specimens) Channel Package

24	Spam (full specimens)	Full copies of e-mails sent to spamtrap addresses

SIE Heartbeat Channel Package

255	SIE Heartbeat Channel - Farsight	Repeating nmsg datagram used for SIE health monitoring

DDOS Events Channel Package

115	DDoS Events - Concordia University	DDoS and DRDoS attack event anomaly notification as the result of analysis