

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

# Web Forum Exploitation using XKEYSCORE

[REDACTED] S2I7

July 2009

Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20340701

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## What forum data do we have in XKEYSCORE?

- FISA – full take\* for U.S. web forum servers under FISA coverage
- Passive collection for OCONUS web forum server traffic
- Passive collection for individual forum users located OCONUS

# Content

- Posts and private messages
  - When FISA is available – PINWALE is best for content (large amount of encrypted traffic)
  - Time sensitive threats – XKEYSCORE may be faster

# All posts/ threads on one forum

- HTTP Activity query form
- AppID + Fingerprints:
  - mail/webmail/vbulletin/post\*
- IP address (either): web forum server IP

# All Private Messages for a Forum

- HTTP Activity query form
- AppID + Fingerprints:
  - Mail/webmail/vbulletin/private\_message\*
- IP address (either): web forum server IP



# SysAdmin Activity

- CPanel:
  - All web forum IP addresses
  - AND
  - Ports for CPanel (2082 or 2083 or 2086 or 2087)
- AdminCP:
  - All web forum IP addresses
  - AND
  - Application Info - \*admincp\*

# Applications Used on Forums

- Example: all forum users with MS v2.0 encrypted private messages:
  - AppID+FP: mail/webmail/vbulletin/private\_message\*
- And
  - AppID+FP: encryption/mojahaden2\*