



# APEX VPN Phases

- ▶ **VPN Phase 1: IKE Metadata Only (Spin 15)**
  - IKE packets are exfiled to TURMOIL APEX.
  - APEX reconstructs/reinjects IKE packets to the TURMOIL VPN components.
  - TURMOIL VPN extracts metadata from each key exchange and sends to the CES TOYGRIPPE metadata database. This database is used by SIGDEV analysts to identify potential targets for further exploitation.
  
- ▶ **VPN Phase 2: Targeted IKE Forwarding (Spin 15)**
  - TURMOIL VPN looks up IKE packet IP addresses in KEYCARD.
  - If either IP address is targeted, the key exchange packets are forwarded to the CES Attack Orchestrator (POISON NUT) for VPN key recovery.
  
- ▶ **VPN Phase 3: Static Tasking of ESP**
  - HAMMERSTEIN receives static tasking to exfil targeted ESP packets.
  - APEX reconstructs/reinjects ESP packets to the TURMOIL VPN components.
  - TURMOIL VPN requests VPN key from CES and attempts decryption.
  
- ▶ **VPN Phase 4: Dynamic Targeting of ESP**
  - Based on the value returned by KEYCARD, the ESP for a particular VPN may be targeted as well.
  - TURMOIL sends to HAMMERSTEIN (via TURBINE) the parameters for capturing the ESP for the targeted VPN.



# APEX VoIP Phases

- ▶ **VoIP Phase 1: Static Tasking of VoIP (Spin 16)**
  - HAMMERCHANT monitors VoIP SIP/H.323 signaling and exfiltrates only targeted VoIP RTP sessions to TURMOIL.
  - APEX reconstructs and bundles the voice packets into a file, attaches appropriate metadata, and delivers to PRESSUREWAVE.
  - This triggers a modified VoIP analytic to prepare the VoIP for corporate delivery.
  
- ▶ **VoIP Phase 2. VoIP Call Survey**
  - HAMMERCHANT monitors VoIP SIP/H.323 signaling and exfiltrates all call signaling metadata to TURMOIL.
  - APEX inserts call signaling metadata into an ASDF record and publishes it to the TURMOIL AsdfReporter component for target SIGDEV.
  
- ▶ **VoIP Phase 3. Dynamic Targeting of VoIP**
  - HAMMERSTEIN captures/exfils all VoIP signaling
  - APEX reconstructs/reinjects the signaling to the TURMOIL VoIP components.
  - TURMOIL VoIP extracts call metadata and sends to FASCIA; checks KEYCARD for hits.
  - If called/calling party is targeted for active exfil, then TURMOIL sends to HAMMERSTEIN (via TURBINIE) the parameters to capture the targeted RTP session.
  
- ▶ Implementation of VoIP Phase 2 and 3 will be driven by mission need.
  - Phase 3 leverages all TURMOIL VoIP signaling protocol processors to expand beyond SIP and H.323 (e.g. Skype) without additional development on the implant.



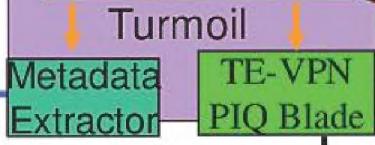
# APEX VPN Exploitation



Key exchange

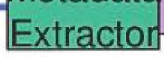
Encrypted Data

**FASHIONLEFT**  
Wrapped  
Exfil



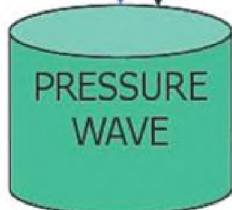
Look Up IP  
Address For  
Content Targeting

IKE Full take  
Metadata  
(Files)



Socket Connection (SSL) IKE Exchanges  
Socket Connection (SSL) Key Requests/Responses

Selected Decrypted  
Content



Cryptovvariable  
Management



# APEX VoIP Exploitation

