APEX
Active/Passive Exfiltration
“go apex”

STDP: S32354 & T112, NCSC/C91
August 2009
This presentation is classified

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123
Motivation: CES needs VPN keys!

NCC Increment 3 Planning

1. NCC CA Service Requests (Decrypt) per hour (aggregate for all VPN exploitation-enabled systems).
   - Q4 FY09 (Risk Reduction) 1,000
   - Q4 FY10 10,000
   - Q4 FY11 100,000

2. NCC front end systems shall fully process (i.e. decrypt and re-inject) at least 20% of CA service requests (~20% Reinject Rate?)
3. For tasked IP addresses, NCC front end systems shall identify relevant IPSec sessions and generate attack requests (Rates?)
4. NCC front end systems shall buffer VPN data for up to 15 minutes (900 seconds) while waiting for response from Attack Orchestrator (AO)
5. After successful key recovery and decryption PIQ services shall re-inject decrypted VPN for Stage1 & Stage2 processing
6. Aggregate VPN buffering and processing rate per TML system (Assumptions – LPT? T16? U64?)
   - Q4 FY09 (Risk Reduction) 4 VPN Systems 25 Concurrent VPN Flows / System 100 Mbps Aggregate VPN Data / System
   - Q4 FY10 10 VPN Systems 100 Concurrent VPN Flows / System 100 Mbps Aggregate VPN Data / System
   - Q4 FY11 100 VPN Systems 100 Concurrent VPN Flows / System 500 Mbps Aggregate VPN Data / System

- CES receives VPN IKE packets from passive collection (TURMOIL) and recovers VPN keys.
- TURMOIL receives VPN ESP packets and decrypts them using the keys recovered by CES.
- But there are many VPNs that TURMOIL(s) can’t see.
Motivation: Leverage TAO

- TAO/DNT active implants have a powerful Man-in-the-Middle capability to access data deep within target networks.
  - They can select packets and exfiltrate them back to the Common Data Receptor (CDR) at the Remote Operations Center (ROC).
  - HAMMERSTEIN: target any 5-tuple packet
    - \{SrcIP, SrcPort, DstIP, DstPort, Protocol\}
      - IKE: VPN key exchanges
      - ESP: VPN encrypted tunnels
  - HAMMERMERCHANT: target VoIP phone numbers
    - Process SIP/H.323 VoIP signaling
    - Forward targeted phone call RTP media sessions
- But CDR has limited input bandwidth.
Hmmmm...

Maybe… Combine Active & Passive?
Agenda

- Motivation: Why?
- TURBULENCE High Level Concept: What?
- Details: How?
  - FASHIONCLEFT Exfiltration Protocol
    - Definition
    - Processing Required
  - Turmoil Architecture
  - Turmoil Implementation
    - Packet Reinjection: Stage 1 Prime
    - Packet Processing Framework: AEG/SEG
    - Packet Routing: different Transform Engines
- Complexity
- Challenges
- Phased Development
(U) TURBULENCE Architecture

**SENSORS**
- TURMOIL: Passive SIGINT
- TUTELAGE: Active Defense
- TURBINE: Active SIGINT

**INFRASTRUCTURE**
- PRESSUREWAVE: Data Storage
- EITC: Networking

**FOR THE ANALYSTS**
- TRAFFICTHIEF: Tipping
- X-KEYSCORE: Session
- ANALYTICS: Analysis/Survey

**TURBULENCE INTEGRATION**
(U) Sensors: Passive Collection

Accesses

- TURMOIL
- TUTELAGE
- Implants (TAO)

(SI/SI/REL) High-speed passive collection systems intercept foreign target satellite, microwave, and cable communications as they transit the globe.
(TS//SI//REL) TURBINE enables the automated management and control of a large network of active implants.
APEX VoIP Mission

Internal Network

The Internet

VolP server or VPN

Exfil Path

TAO Inside

Tasking

Tailored Access Office Remote Operations Center

TURBINE NSAW

PRESSUREWAVE
FASHIONCLEFT Exfiltration Protocol
**Definition:** TAO/DNT protocol used by implants to exfiltrate collected network packets to the Common Data Receptor (CDR, aka FLAXENPRECEPT).

- Provides support for:
  - Metadata Authentication/Integrity + AntiReplay + Encryption
  - Data Encryption
  - Uses 1024-bit RSA, 128-bit RC6, SHA-1

- Based on DNT standards:
  - FOGYNULL (DNT Exfiltration Protocol)
  - FUNNELAPS (DNT Exfiltration Data Format)
  - SHELLGREY (DNT Exfiltration Metadata Format)
How To Exfiltrate IP Packets

1. Select packet based on tasking.
2. Make a copy of the selected packet.
3. **Modify** packet IP destination address.
4. **Modify** other protocol fields (IP, UDP, TCP) as needed to bypass firewalls and to tag packets for ID.
5. Optionally **encrypt/munge** Transport layer payload.
6. Send modified Data Packet (DP) to new destination.
Receiver: Needs Metadata

- Metadata explains how to:
  1. Identify an exfil packet and the implant source.
  2. Recover original IP destination address.
  3. Recover other original protocol fields (IP, UDP, TCP).
  4. Contains Key to decrypt/unmunge transport layer payload.

- Metadata sent in a Session Announcement (SA)
  - SAs is an IP/UDP packet sent to a destination IP/port.
  - Multiple copies of SA sent to mitigate dropped SA packets.

- Receiver is dynamically configured with:
  - SA IP/ports, Infrastructure & Implant Private Keys
  - Processing Mode: Reconstruct or Reinject
FASHIONCLEFT

Session Announcement Format

- IP Header
- UDP Header
- SA Payload in UDP Transport Layer
  - Infrastructure Header (128 bytes)
    - RSA Encrypted w/ Infrastructure Public Key
    - Contains SHA-1(INF-HDR), Cryptold
      - Cryptold = [DeploymentId, TargetId, ImplantId]
  - Implant Header (128 bytes)
    - RSA Encrypted w/ Cryptold 's Public Key
    - Contains SHA-1(IMP-HDR)
    - 128-bit CV, MI, and CRC-16 checksum for Exfil/Metadata Block
  - Exfil/Metadata Block (variable)
    - RC6 Encrypted w/ CV & MI
- Minimum packet length = 344 bytes
FASHIONCLEFT

Session Announcement Processing

1. Look for SA packets:
   1) at destIP/destPort; protocol=UDP,
   2) that are at least 344 bytes long, and
   3) whose first 128-bytes of Transport Payload “look random”.
      • (Easy/quick initial checks)
2. RSA Decrypt INF-HDR w/ Infrastructure Private Key.
   • Authenticate w/ SHA-1
   • (Slow secondary check; can’t withstand much non-SA traffic on IP/port)
3. RSA Decrypt IMP-HDR w/ Cryptold ’s Private Key.
   • Authenticate w/ SHA-1
4. RC6 Decrypt Exfil/Metadata w/ CV and MI
   • Perform CRC-16 integrity check.
5. Anti-Replay Check & New Session/Retransmit Check
6. Extract Metadata and create Collection Filter rule for DPs
   • Metadata contains either 5-tuples or pattern/mask/offset that match DPs
   • PpfEvent.DfceCF.tuple (5-tuple)
Data Packet Processing

1. **Identify** an exfil packet that matches DP filter rule.
2. **Modify** to original IP destination address.
3. **Modify** to original protocol fields (IP, UDP, TCP).
4. **Decrypt/unmunge** transport layer payload.
   - Have now recovered the original captured packet.

1. Associate metadata with recovered packet.
   - agentCaseNoteation, Turmoil link caseNoteation
1. Perform protocol specific processing.
   - Pre-selected: forward all traffic to TUBE/PWAVE
   - Re-inject back into Turmoil Stage-1
TAO Remote Operations Center
Common Data Receptor

FIGBUILD
SURPASSPIN Outer -> ROOTKNOT Pitcher

OPTICPINCH
ROOTKNOT Catcher -> SURPASSPIN Inner -> SEAGULFARO

One-Way Link

Collection
CONVEY
PINWALE

Collection & Logs
Office of Target Pursuit (Forensics Lab)
Manual Processing and FTP

K7 LAN
/TARGETS

VINYLEASE (Email)
OLYMPUS (Files)
UNITEDRAKE (Email/Files/...)
Streaming Packets

Common Data Receptor
TURMOIL Architecture

Crucial for SSO and the desire of dynamic tasking.

What we are currently focused on

What we promised to also do for NSA/A&P

Stage 0: Physical
- Examines sequences of associated packets assessing the value of their associated sessions

Stage 1: Packet

Stage 2: Session
- Examines sequences of associated sessions assessing the value of their associated applications

Stage 3: Persona
- Examines sequences of associated applications assessing the value of their associated entities (targets/people).

Stage 4: Social
- Examines sequences of associated entities assessing the value of their associated social network.
Inside Stage 1

Packet Processing Framework (PPF)

PreProc → Event Engine → State Engine

Detect

Delay Flow Control Engine

Message Bus

Data Bus

Operate

State Engine

Transform Engine

Key

Data
Delay Flow Control Engine
Delays packets for 3-30 sec then drops unwanted packets and sends the rest to requested Transform engines.
Event Engines: Detect

- **Stateless** - does not store data or metadata (Atomic Event Generator = AEG)
- Evaluation of traffic

- Publish observations
- Each engine can be specialized and optimized based on incoming speed
  - Software and/or Hardware

**Examples:**

1. Detect VPN setup: IKE key exchange.
2. Detect VPN tunnel: ESP packets.
3. Detect VoIP signaling: H.323, SIP, Skype, etc.
4. Detect FASHIONCLEFT Session Announcement.

**Key**

- Data
State Engines: Control

- Receives published events from Event Engines and makes processing decisions.
- Choreographs activity for data flows (Stateful Event Generator = SEG)
  - Correlates multiple published events
  - Starts/stops transform processing engines
  - Publishes decisions about the flow
- Each State Engine can be specialized and optimized

Examples:
1. Associate VPN IKE/ESP traffic with recovered VPN keys.
2. Associate VoIP signaling w/ phone call.
3. Track FASHIONCLEFTE SA’s: new, keepalive, replay?
Transform Engines: Grooming

- Receives orders from State Engines
- Operation applied to a data object that does not change its level of abstraction.
  - Packet ➔ Packet(s)
  - Session ➔ Session(s)
- Groomed data object can then be re-injected or sent forward

Examples:
1. Decompress/decrypt packet.
2. Reconstruct original packet from FASHIONCLEFT Data Packet.

Key:
- Data
TURMOIL Implementation
TURMOIL Stage 1’ (Stage One Prime)

**Stage 1: Packet Processing**

- **DFCE**
  - Delay → Flow Control Processor (FCP)
  - Selects Packet

- **First Stage** Packet Filter (FSPF)
  - First Stage Packet Filter (FSPF)
  - Packets Matching Criterion
  - Filter Criteria

- **Packet Processing Framework (PPF)**
  - Metadata
  - Sessions & Bundles (No Rejection Required)

- **Metadata Processor**
  - Sessions & Bundles
  - Metadata

- **Stage 2: Session Processing**
  - Rejected Packets (>2)
  - Sessions & Bundles (No Rejection Required)

**Stage 0:**

- **DFID Allocator**
  - SRI Metadata

**DFCE**

- Delay → Flow Control Processor (FCP)
  - Selects Packet

**Metadata Processor**

- Metadata
  - Sessions & Bundles
  - Metadata

**Sessions & Bundles (No Rejection Required)**

**SRI Metadata**

**Rejected Packets (>2)**
TURMOIL Stage 1 Packet Router

Stage 1: Packet Processing
Stage 1': Packet Re-Processing

- Sessionizing TE
- Bundling TE
- Detunneling TE
- APEX Bundling TE
- APEX Reinjecting TE
- VPN Decrypt TE

DFCE → Packet Router
Routing Rules Table

All Selected Packets → Sessionized Packets → Bundled VoIP Packets

Re-inject (Stage 1)
TURMOIL Stage 1 Sessionizing TE

Sessionizing TE

Packet Router
Fast IP Processor (FIP)
Appl'd
Metadata Injector
Selector Scanner
Stage 2
TDAL

Routed Packets
Selected Packets
All Packets

DFCE
PPF Event "Hits"

"Hits"

HTTP
POP3
SMTP
IMAP
Other
X.400
Lotus Notes
Demuxes

Sessionized Packets
Selectors
Selection Distribution Element
CoreSSC
TURMOIL Stage 1 APEX Bundling TE

Packet Router

Fast IP Processor (FIP)

Metadata Injector

APEX Bundle Reconstruct

Stage 2

Home

DFCE

All Packets

Selected Packets

APEX VoIP Routed Packets

PPF Event “Hits”

“Hits”

VoIP Bundles
TURMOIL Stage 1 Metadata Processor

Stage 1: Packet Processing

PPF Engines

Metadata

Atomic Event Generator (AEG)
Stateful Event Generator (SEG)
Event Filter (EF)

Metadata Processor

Stage1 ASDF Reporter
IKE Events to BME
ESP Events to BME
IVE Metadata Tabulator

ASDF Metadata to Stage 2
VPN IKE/ESP Metadata to Stage 2
IVE Metadata to Stage 2
EF Metadata to Stage 2
APEX Spin 15 Design

Stage 1

APEX Preselected TE

APEX Recursion TE

Recursive Stage 1'

Ike Metadata Event

Ike Event ToSbe (SSTE)

Home
Complexity
Complexity

- **APEX Sequence Diagram**
  - Tasking
    - Look for: FASHIONCLEFT Session Announcements.
  - Recognize SA
    - Look for: FASHIONCLEFT Data Packets
  - Recognize DP
    - Route DP to Bundling or Packet Reinjection TE
    - Reconstruct, Attach Metadata, Output/Reinject

- **VPN Dataflow & Sequence Diagram**
  - Recognize VPN IKE Packets
    - Send all IKE Metadata to CES TOYGRIPPE database
    - Send targeted IKE to CES POISON NUT for VPN key recovery.
  - Recognize VPN ESP Packets
    - Save targeted ESP in big buffer and request VPN key from CES.
    - If receive VPN key, decrypt and Reinject.
VPN Decrypt Sequence Diagram
Challenges
Challenges

- SIGDEV
  - Find target networks/devices with desired traffic.
    - TAO/R&T
  - Exfiltration path discovery from device to Turmoil.
    - COALSHOVEL

- End-to-End Metadata & Processing
  - Provide CES with appropriate metadata for VPN mission.
  - Provide TUBE/PRESSUREWAVE with appropriate metadata for VoIP analytic.
  - Two Case Notations:
    - Link collected by Active Implant: “new” agentCaseNotation
    - Link collected by Passive System: “current” caseNotation.
Challenges

- Classification & Legal Authority
  - Some TAO implants/accesses are compartmented.
    - The highest priority VPNs are likely on compartmented accesses.
  - We’d like to exfil packets to high-bandwidth SSO sites
    - Ensure compliance with FISA / FAA / PAA / USSID SP0018.

- Future Automation
  - Turbine tasks both Active & Passive collectors
  - Automated Path Discovery
  - Dynamically task Active system using Passive selectors
    - Exfil VoIP signaling to Turmoil for selection:
      - task selected calls for exfil.
    - Exfil VPN ESP tunnel starts to Turmoil for selection:
      - task exploitable tunnels for exfil.
    - Apply automated OPSEC policy to manage exfil bandwidth & CPU utilization on implanted device.
APEX Phased Development

- Command & Control
- VPN
- VoIP
APEX Command & Control Phases

- **C&C Phase 1: Manual Configuration (Spin 15)**
  - HAMMERMILL is configured via existing command interface.
  - Simultaneously TURMOIL APEX is provided a configuration file for this HAMMERMILL mission.
  - A human is responsible for keeping the two in sync.

- **C&C Phase 2: Semi-automatic Configuration**
  - TURBINE receives mission parameters and automatically configures both the HAMMERMILL implant and the TURMOIL APEX components.
  - TURBINE-HAMMERMILL interface uses CHIMNEYPOOL RPC commands and requires HAMMERMILL version 2.5.
  - TURBINE-TURMOIL interface uses ISLANDTRANSPORT.

- **C&C Phase 3: Dynamic Targeting**
  - TURBINE sets initial configuration as in Phase 2.
  - Exfiled traffic is evaluated by TURMOIL components+KEYCARD for selection decisions.
  - TURMOIL messages to TURBINE to dynamically target a particular flow through the implant.
  - Example:
    - TURMOIL receives an IKE key exchange (and possibly a few initial packets)
    - TURMOIL evaluates the IP addresses to decide if the VPN being set up corresponds to a target
    - If so, TURMOIL message to HAMMERMILL via TURBINE to capture/exfil corresponding ESP traffic.
  - This phase must be managed so that router exfil does not exceed the tolerable bandwidth limits set by OPSEC and operational concerns. TURBINE may need to implement additional workflows to monitor and control exfil volume.
Tasking ICF (Implant Control File)

# TEST-APEX-1 INFRASTRUCTURE CONFIGURATION FILE
ICF_NAME TEST-APEX-1
ICF_DTG Wed Jan 28 14:38:59 2009
ICF_INFO Test ICF for Apex Development
IMPLANT_ID 0x0001
IMPLANT_VER 1
TARGET_ID 0x00000002
DEPLOYMENT_ID 0x00000003
TARGET_CN TESTTECHNIQUE_TESTHOST
TARGET_IP 10.0.0.1
TARGET_HOST TESTHOST
#
# IMPLANT_LP[1-9] [<Tunnel-Id>:]<ip-address>[:port(s)]
# Tunnel-Id: 1-TCP_Redir, 2-Fashioncleft, 3-HTTP_BT_S, 4-UDP_S
# ./genkey -l 128
IMPLANT_LP1 2:10.1.1.2:10002
IMPLANT_RC6_CV1 5366fbe1 7f7a05fd 33d66a6f 3581de48
#
IMPLANT_RSA_INF
RSANAME TEST_APEX_INF_KEY-1
RSAINFO Wed Jan 28 14:38:59 2009, ./rsagenkey v2.0
RSASIZE 1024
RSAMOD 32
  0xdb532e9d, 0x93c792fc, 0x4459fc40, 0x07744c65, ...
RSAMU 33 ...
RSAPRIV 32 ...
RSAPUB 32 ...
#
IMPLANT_RSA_IMP
RSANAME TEST_APEX_IMP_KEY-1
...
<?xml version="1.0" encoding="UTF-8"?>
<dc:dc>
  <header>
    <fullyQualifiedId>
      <protocol>
        <protocolName>FN</protocolName>
        <protocolVersion>2.0</protocolVersion>
      </protocol>
    </fullyQualifiedId>
    <targetId>2</targetId>
    <techniqueId>1</techniqueId>
    <techniqueVersion>1</techniqueVersion>
    <instanceId>0</instanceId>
  </header>
  <configurationVersion>2</configurationVersion>
  <revisionDate>2009-01-30T12:19:05.910-05:00</revisionDate>
</header>
<commands>
  <command name="fogynullControls" identifier="FN_CONTROL">
    <parameters>
      <parameter name="replayPrevent">1</parameter>
      <parameter name="historyLimit">100</parameter>
      <parameter name="antiDelay">0</parameter>
      <parameter name="timeWindow">1800</parameter>
    </parameters>
  </command>
  <command name="implantLP" identifier="IMPLANT_LP">
    <parameters>
      <parameter name="tunnelId">2</parameter>
      <parameter name="ip">10.1.1.2</parameter>
      <parameter name="port">10002</parameter>
    </parameters>
  </command>
  ...
</commands>
<?xml version="1.0" encoding="UTF-8"?>
<task:message schemaVersion="1.0" xmlns:task="urn://control.exo/TaskingInterface/v1">
  <task:taskAdd>
    <task:msgUuid>00110000-1111-2222-3333-444455556666</task:msgUuid>
    <task:timestamp>2</task:timestamp>
    <sessionConfigTask>
      <task:SecurityMarking classification="TS" coi="COMINT" disseminationControls="REL"
      scIcontrols="SI" releasableTo="USA AUS CAN GBR NZL" legalAuthority="RAWSIGINT"/>
    </sessionConfigTask>
    <header> ... </header>
    <commands>
      <fogynullControls>
        <replayPrevent>1</replayPrevent>
        <historyLimit>100</historyLimit>
        <antiDelay>0</antiDelay>
        <timeWindow>1800</timeWindow>
      </fogynullControls>
      <apexControls>
        <taskUuid>00100001-1111-2222-3333-444455556666</taskUuid>
        <agentUuid>80010001-1111-2222-3333-444455556666</agentUuid>
        <agentCaseNotation>UA.AAABBBCCCMM1</agentCaseNotation>
        <processingMode>Reinject</processingMode>
      </apexControls>
      <implantLp>
        <tunnelId>2</tunnelId>
        <ip>10.1.1.2</ip>
        <port>10002</port>
      </implantLp>
    </commands>
  </task:taskAdd>
</task:message>
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.
Performance & Status Metrics

HMS/nmdc-apex: Turmoil Input [2009-08-17 15:30:47]

- Avg packet size Bytes [10 minutes old]
- Input Max Moits/sec [10 minutes old]
- Input Avg Mb/s [5 minutes old]
- Input Packets/sec [10 minutes old]

HMS/nmdc-apex: Apex Sessions [2009-08-17 15:30:52]

- Decrypted Session Announcements / 5min [5 minutes old]
- New Session Announcements / 5min [5 minutes old]
- Replay Session Announcements / 5min [5 minutes old]
- # Active Sessions [10 minutes old]
- # Active Users [10 minutes old]
- # Session Exits / 5min [10 minutes old]
- BFQX (ER) Cache Mispkts / 5min [5 minutes old]
Performance & Status Metrics

MHS/nodo-apex: Apex Sessions [2009-08-17 15:30:52]

- Decrypted Session Announcements / 5min (5 minutes old)
- New Session Announcements / 5min (5 minutes old)
- Replay Session Announcements / 5min (5 minutes old)
- Active Sessions / 10min (10 minutes old)
- Session Exp. Causes / 10min (10 minutes old)
- BFU2 (ERR) Cache Misses / 5min (5 minutes old)

Time: 08/11 00:00 - 08/17 00:00
Questions?

“go apex”
apex chat room on LINKUP

STDP: S32354 & T111, NCSC/C91