Intro to the VPN Exploitation Process

[redacted]

OTP VPN Exploitation Team

S31176

September 13, 2010

Overview

- S31176 and the OTP VPN Exploitation Team
- How can we help you?
- VPN and Network Encryption Types
- Birth of the VPN Adventure
- Sustained Exploitation
- Exploitation Successes
- Conclusions

S31176

Branch Name:

Custom Thread Development for Network Encryption

Team Name:

OTP VPN Exploitation Team

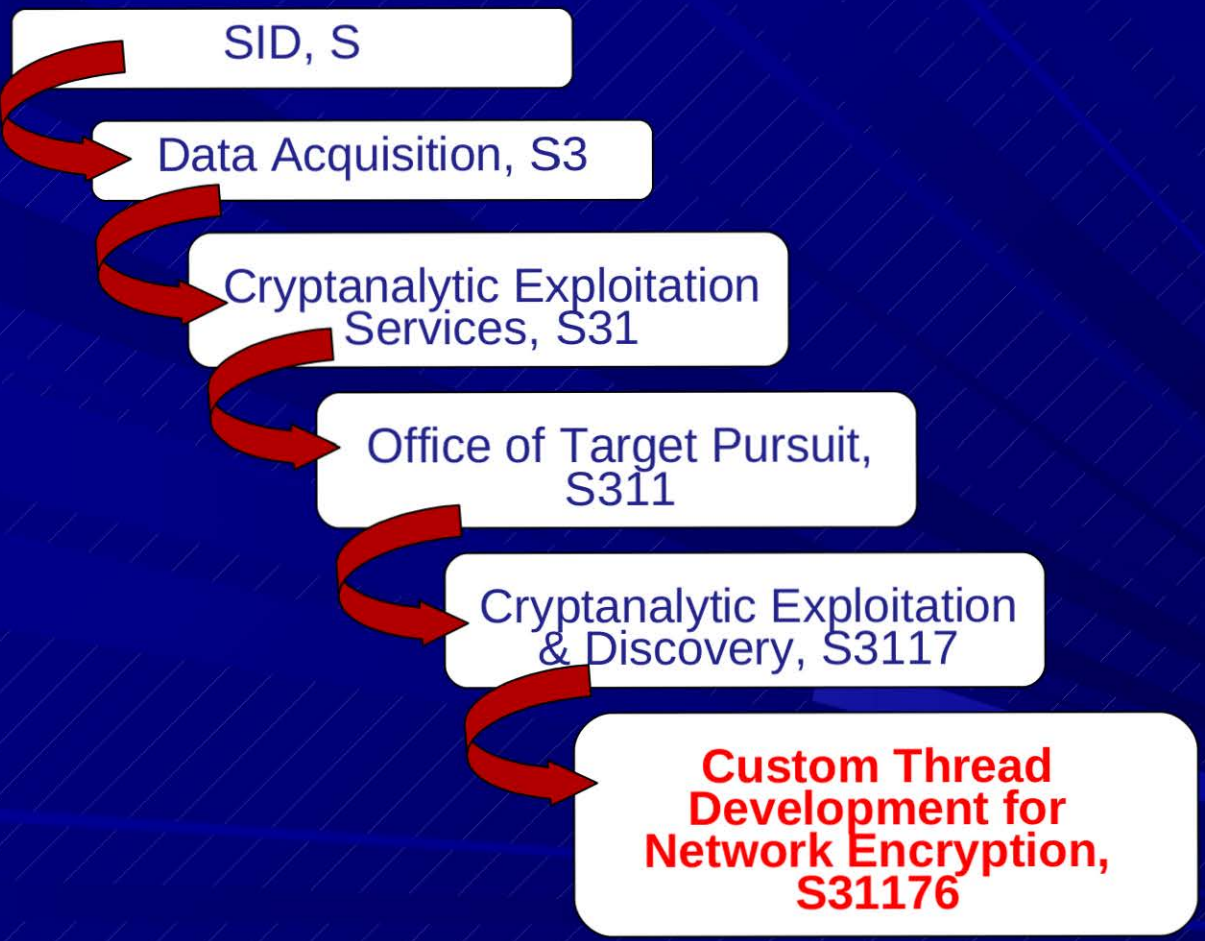
Mission Statement

S31176 provides cryptanalytic support services for many network encryption protocols, including, but not limited to: IPSec, SSL, PPTP, SSH and proprietary protocols. We are the front-door of CES for targeted vulnerability assessment and custom interim end-to-end exploitation flows for these protocols. In conjunction with various agency SIGDEV counterparts and target organizations, we engage in discovery to find TOPI targets of interest. By maintaining contact with field sites, TAO, and NCSC, we endeavor to guide and direct development and access through both active and passive means in order to make exploitation possible and enable full prosecution of the target…

Purpose in a Nutshell

- Act as your one stop shop for all VPN and network encryption exploitation related issues!
- Act as a liaison for SIGDEVers and TOPIs to other areas of the VPN community
- Perform some SIGDEV and target discovery

Where are we positioned?



S31176 Branch Members

- [redacted] - Collection
- [redacted] – CMP Intern
- [redacted] – Team Lead, IPSec, SSH
- [redacted] – IPSec
- [redacted] – Branch Chief
- [redacted] – Diversity Tour
- [redacted] – CADP Intern
- [redacted] – PPTP
- [redacted] – BLEAKINQUIRY, SSL

How to Contact us (May be changing soon):

[redacted]

go vpn-xft

Branches within OTP

- S31171 – PRC, N Korea, SE Asia, Japan
- S31172 – Iran, Hamas, Iraq, Saudi Arabia
- S31173 – Africa, Levant, Latin America, India, Pakistan, Afghanistan
- S31174 – Russia, Counter-Intel, Europe, FTM
- S31175 – Cross-Target Support Branch
- S31176 – Custom Thread Development

Exploitation in the OTP Branches

- Each branch has a VPN representative
  - We inform them about attacks, they inform us about targets
  - If you have a target-specific inquiry, they may be able to help
  - S31171 (Eastern and Southeast Asia)
  - [redacted], [redacted]
  - S31172 (Iran, Iraq, Arabian Peninsula)
  - [redacted], [redacted]
  - S31173 (Levant, Central Asia, Africa, Latin America)
  - [redacted]
  - S31174 (Russia, Europe, International Targets)
  - [redacted]

How can we help you?

Provide Exploitation Support

- Provide VPN vulnerability analysis
- Engage Network Security Products, TAO, ESO, etc
- Convey meaningful feedback to customer
- Develop sustained exploitation threads when possible
- Suggest alternative approaches if passive exploitation is unrealistic
- DECRYPTS, DECRYPTS, DECRYPTS!!!!!!

Additional Services

We can assist with the following:

- Collection problems
- Tasking
- Data flow
- Plaintext analysis
- Metadata interpretation
- Tip-off vulnerable VPN links
- VPN SIGDEV
- Target Discovery and Development

How can you help you?

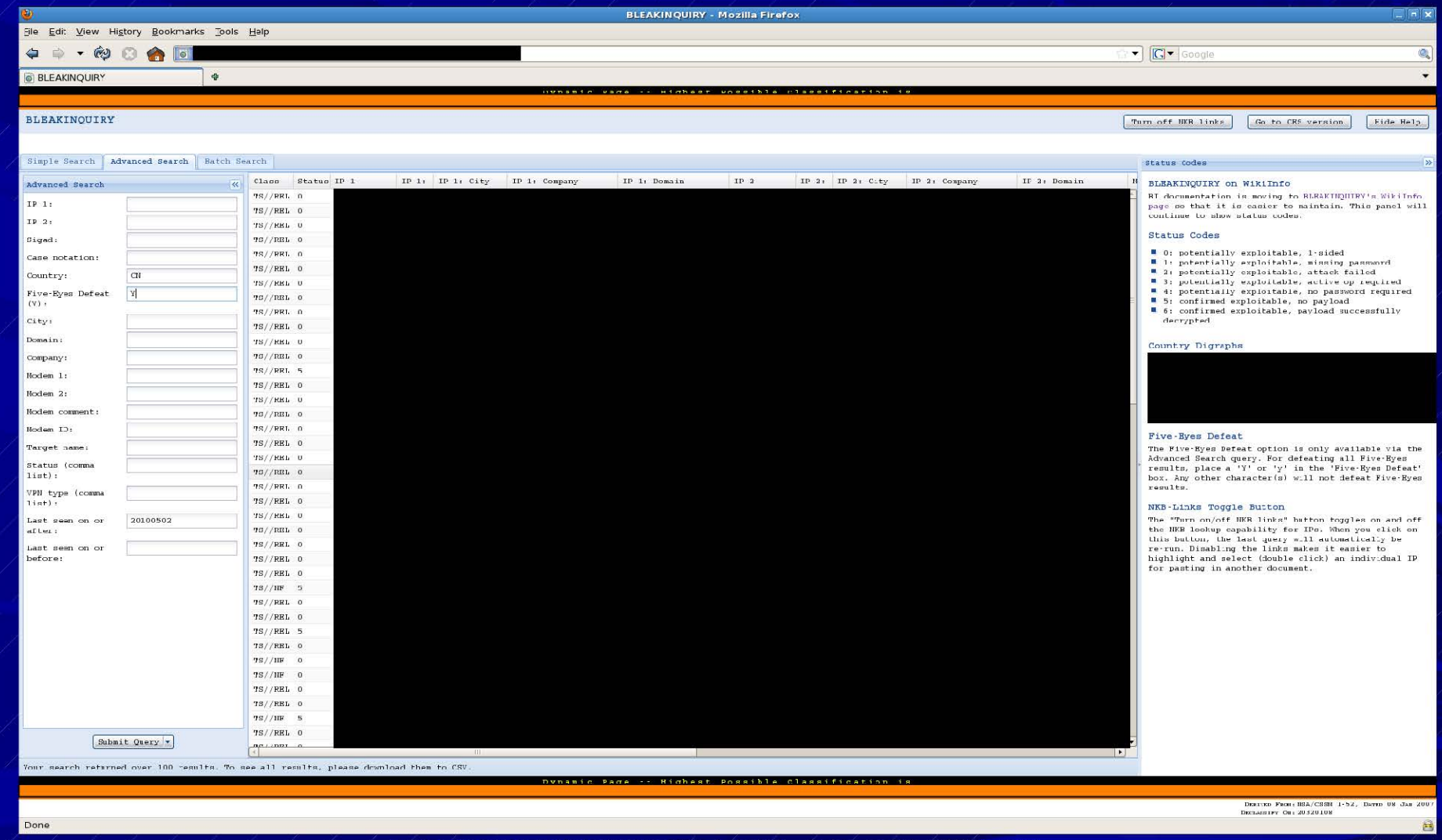
Glad you asked!

- Familiarize yourself with appropriate search criteria
  - [redacted]
- Get a BLEAKINQUIRY account
- If you find VPN-related data, let us know.
  - The existence of a VPN on a network of interest
  - Configuration/setup information about the VPN

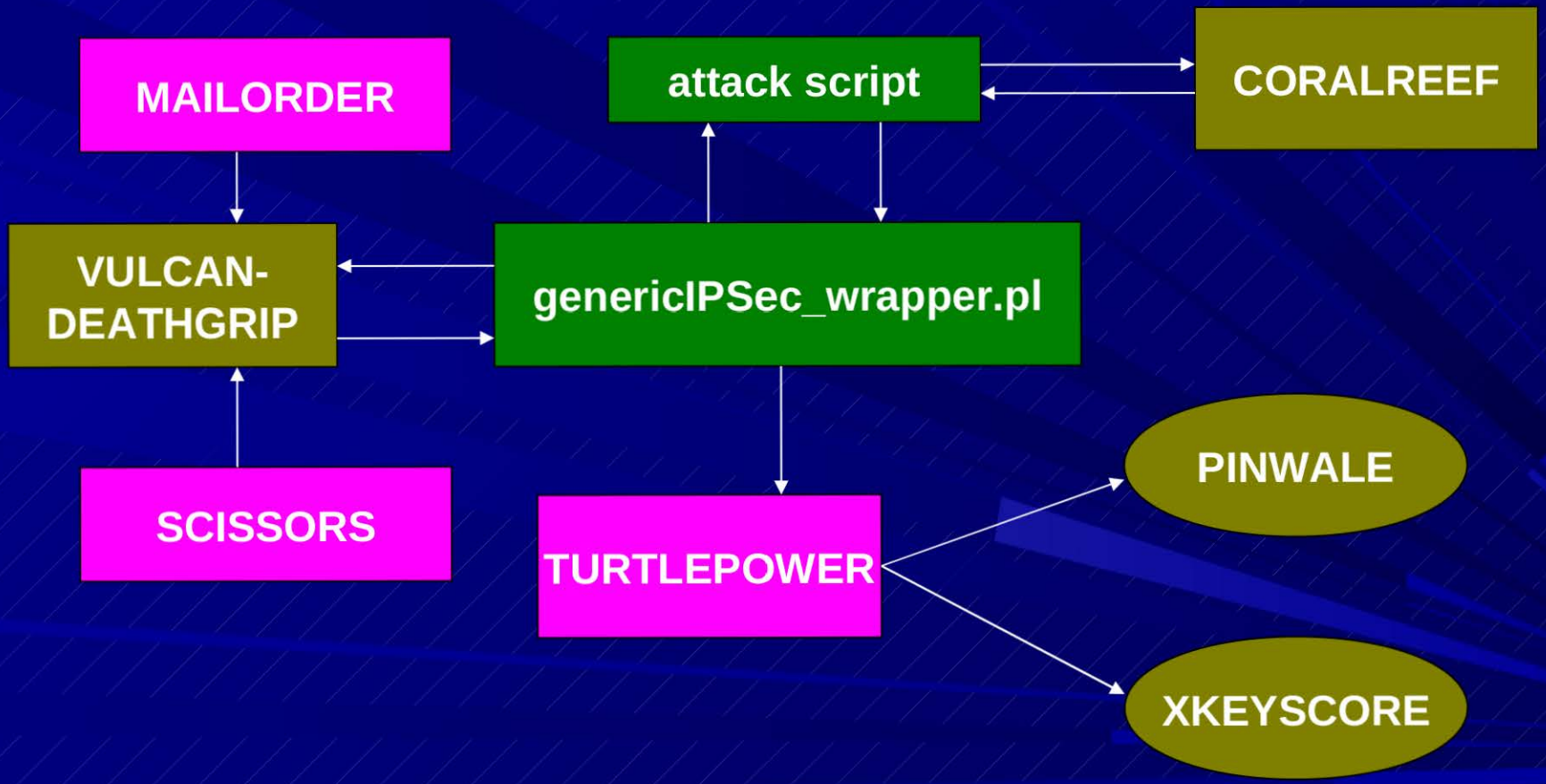
BLEAKINQUIRY

- Metadata database of potentially exploitable VPNs
- Data Sources
  - TOYGRIPPE metadata testing
  - XKEYSCORE fingerprints
  - Daily VPN exploitation
- Let us stress…"P-O-T-E-N-T-I-A-L"
- Want an account?
  - E-mail [redacted] or [redacted]

BLEAKINQUIRY



Local IPSec Processing



Type 1: IPSec

- IPSec: IP Security
- Complete paired IKE
  - Common UDP ports: 500 and 4500
- Pre-Shared Key (PSK)
  - Router configuration (good source for PSKs)
- Encrypted Payload (ESP or AH)
  - Next Protocol 50 or 51
  - XKEYSCORE Queries
  - Full log DNI search
  - AppID/Fingerprints: “vpn/*”, “vpn/esp”, “vpn/isakmp”, “vpn/ikev2”, “vpn/ikev2_content”

Type 2: PPTP

- PPTP: Point-to-Point Tunneling Protocol
- Paired collect
  - Next Protocol 47 = PPTP payload
  - TCP Port 1723 = PPTP tunnel set up, no payload
- One-sided collect, client side
- XKEYSCORE Queries
  - *Full log DNI search*
  - *Enter your IPs/casn/etc of interest*
  - *AppID/Fingerprint: “vpn/pptp_encr*”*
  - *Share your results with* [redacted]

Type 3: SSL

- SSL – Secure Sockets Layer
  - Renamed TLS (Transport Layer Security) but still often referred to as SSL
- Paired collect – Compare IP's and Ports
- Server Certificates
- Port Numbers: 443, 465, 989, 990, 992, 993, and 995
- XKEYSCORE Queries
  - *Full log DNI search or use SSL plugin*
  - *AppID/Fingerprints: "encryption/ssl/*" or "network_encryption/ssl/*"*

Type 4: SSH

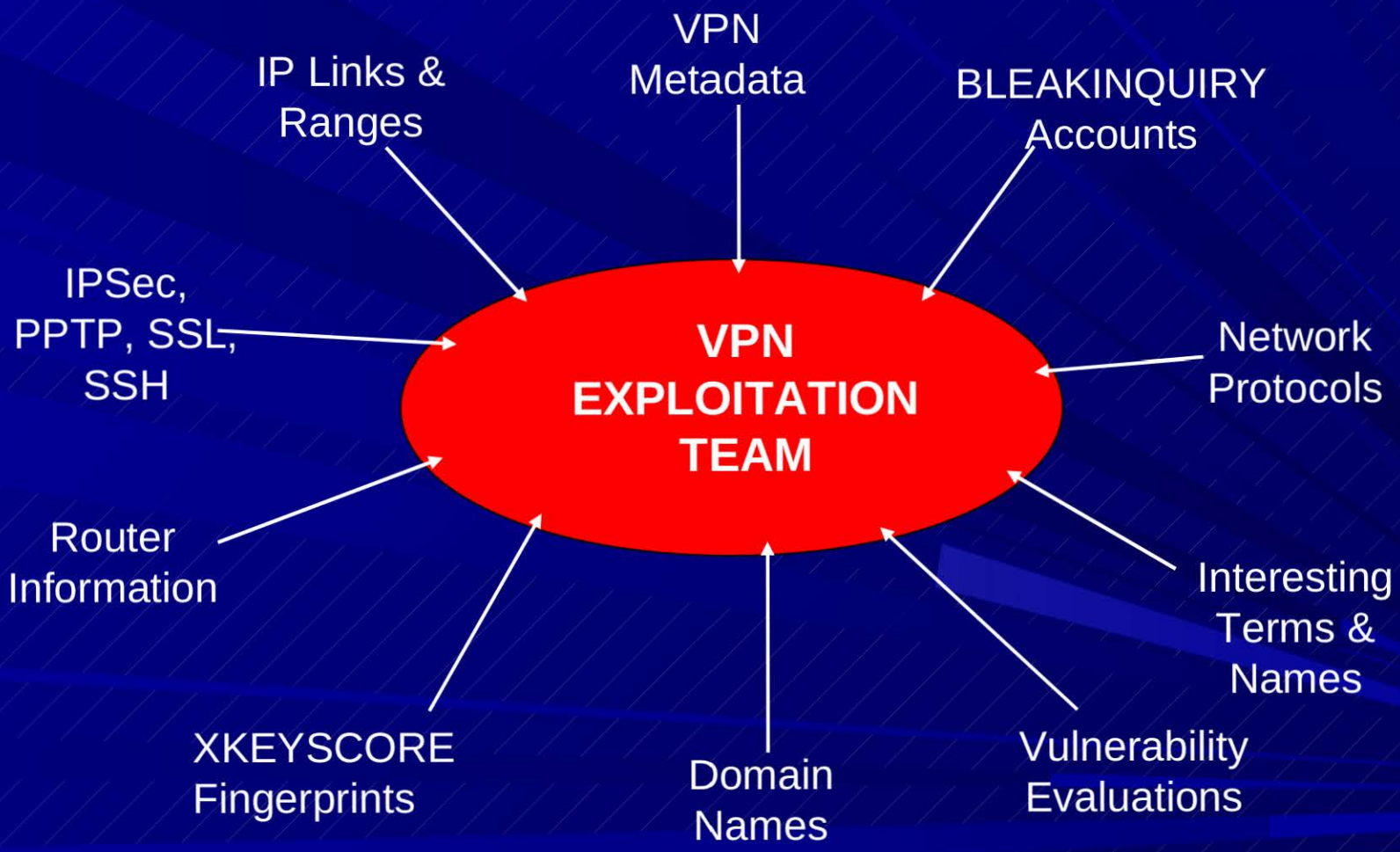
- SSH – Secure Shell
  - Industry-standard networking protocol for securely logging into other machines via a network.
  - Complete paired traffic
  - Port number 22
  - Potentially recover user names and passwords
    - Useful to TAO to access boxes and gather cryptographic information
- XKEYSCORE Queries
  - *Full log DNI search*
  - *AppID/Fingerprints: “terminal/ssh/*”*

Birth of the VPN Adventure

We receive VPN-related requests from across the Globe

- TOPIs
- SIGDEV Analysts
- OTP Analysts
- Cryptologic Centers
- Field Sites
- Second Parties

The Many Flavors of Requests



1. Initial Steps

VPN Info Found/Question Arises

Task Assigned to Team Analyst

Gather Background Info About Request

2. Consult Repositories

- BLEAKINQUIRY – Metadata database of potentially exploitable VPNs

- TOYGRIPPE – VPN metadata repository
- PINWALE - Long-term repository for tasked SIGINT collect
- XKEYSCORE - Processes and databases DNI collect from various field sites
  - Full-take feed (tasked and untasked)
- VULCANDEATHGRIP - Repository for tasked, full-take VPN collection
- FOURSCORE – PPTP repository

3. Scripts: IPSec Focus

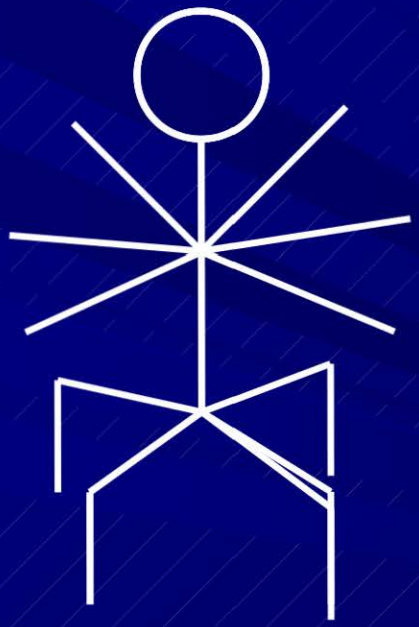
- Format downloaded repository files
- Create intermediate processing files
- Check for potential vulnerabilities
- Search for PSKs in CORALREEF
- Run attacks to recover PSK
- Decrypt traffic

4. Communicate Results

Can we decrypt the VPN traffic?

- If the answer is “No” then explain how to turn it into a “YES!”
- If the answer is “YES!” then…

Happy Dance!!



YES! We Have Decrypt!

- Notify customer of success
- Send decrypt through post-processing and deliver to TOPI
- Have TOPI determine the priority level of the resulting plain text
- Get IPs on sustained collect
- Set up and transition sustained decryption process to OTP VPN Branch Rep

Turn that Frown Upside Down! From "No" to "YES!"

- Depends on why we couldn't decrypt it
- Find Pre-Shared Key
- Locate complete paired collect
- Locate both IKE and ESP traffic
- Have collection sites do surveys for the IP's
- Find better quality collect with rich metadata

Contact Our Friends for Help

- Network Security Products
  - Develop decryption algorithms
- Tailored Access Operations
  - Computer Network Exploitation to create access points
- Collection Sites
  - Perform surveys for the IPs of interest

More Friends

- NSA/CSS Commercial Solutions Center
  - Manage industrial relationships
- SIGDEV
  - Develops tools and methods to help you find the traffic you desire
- OTP VPN Representatives
  - Assist in locating traffic of interest
- TOPI
  - Target knowledge

Sustained Exploitation

- Develop sustained exploitation thread AFTER the TOPI confirms the decrypts are interesting
  - TOPI must task IP in CADENCE
    - Task Port and IP
    - UTT does not have boolean logic
    - Categories
      - IPSec: 6640 (protocols) and 6648 (ports)
      - PPTP: 6648 (ports)
      - SSL: 6647 (ports)
  - Get the crypt system title
    - Work with the OTP VPN Regional Branch representative

Establish the Data Flow

- Establish the correct corporate data flow
  - CES data flow guru [redacted]
  - Make sure the correct routing tags and categories are appended to the data
  - Direct tasked traffic to correct data repository
    - PINWALE
    - VULCANDEATHGRIP – IPSec
    - VULCANMINDMELD – SSL
    - FOURSCORE - PPTP
    - Try to avoid relying on XKS workflows due to legal and logistical issues
      - XKEYSCORE – SSH using XKS workflows directed to a file directory

Data Flow Integrity

- Evaluate data integrity, quality, & quantity
  - Different collectors produce different metadata formats
  - Need rich metadata
  - Need all the pieces (IKE and ESP for IPSec)
  - Ensure that the data is not garbled and headers attached appropriately
  - Check that the data volume is what is expected

Collection Sites

- Contact Collection Sites if there are data issues
  - Malformed headers
  - Missing metadata
  - Missing payload
  - Garbled data
  - Low volume
  - Single-sided traffic
- Collection sites sometimes only collect one-side of the VPN traffic
  - Need to collaborate with both sites

Decrypt Processing

- Decrypt the VPN traffic
- Create SRI files for decrypts
- Send the decrypt and SRI files to TURTLEPOWER (IPSec, PPTP) or CAPRI OS (SSL, SSH) for post-processing
  - Decryption of payload
  - Decompression
  - Unrar files
- Route to appropriate data repository according to the crypt system title and type of decrypt (text, voice, etc)

Decrypt Repositories

- PINWALE
  - Tasked IPSec, PPTP, and SSL
  - Must be placed in the correct partition according to classification (REL FVEY, NOFORN, FISA)
- XKEYSCORE
  - SSH - often have router configurations and user credentials which are easier to view in XKS than PINWALE
  - Still developing the process

TOPI Evaluation

- Analyst locates the decrypts in PINWALE and/or XKEYSCORE
  - Viewing the decrypts
    - PINWALE,
    - XKEYSCORE
    - AGILITY
    - DNI PRESENTER
  - Contact TURTLEPOWER or CAPRI OS if there are file rendering issues
    - Also try the Unidentified Protocols team in s S31122 for help identifying unknown protocols

Thread Monitoring

- Responsibility for monitoring these exploitation threads are transferred to the OTP VPN Regional Branch representative
  - After the thread is established and stabilized
  - Trouble shoots decryption and collection issues
- Set up a cron job to run the decryptor every day
- Hopefully the TOPI continues to identify and report mission-critical intelligence from these decrypts

Success 1: IPSec

Follow-the-Money and TAO Targets

- TOPI (S2C22) has had a close relationship with TAO for quite some time
- FTM Target 1
  - Not susceptible to any of NSP's implants
  - TAO got the configuration files which provided us the PSKs to enable passive exploitation

Success 1: IPSec

- FTM Target 2
  - TAO got on the router through which banking traffic of interest flows
  - NSP had an implant which allows passive exploitation with just ESP
  - Successful exploitation for the past two years

Success 2: PPTP

- Airlines
  - Iran Air, IRTAA
  - Royal Jordanian Air, JOTAA
  - Transaero Airlines, RUCAC
  - Telecommunications
    - Mir Telematiki (pending system title)
    - Afghani Wimax (pending system title)
  - Government
    - Mexican Diplomatic, MXDBB
    - Pakistani General Intelligence, PKRAQ
    - Turkish Diplomatic, TUDAT
    - Afghanistan Government, AFYAD

Success 2: PPTP

- Banking and Financial
  - Zaad Financial
    - Ewallet transactions of a principal financial node for Somali terrorist activity
    - Follow-the-Money customer
  - Kabul Bank
  - BNI Banking, Indonesia
    - Formed and owned by the Indonesian government
    - Banking transactions over “Flexy,” Telkom Indonesia’s fixed wireless network
    - Other
  - IRGC cyber attacker
  - Nigerian power company’s internal network

Reminders

- If it's not exploitable now, that doesn't mean it won't be later
- We collaborate and communicate with our friends to produce decrypts
- Traffic must be both good quality and the correct type