Contents

What is CNE?

" Computer & Network Exploitation delivers to GCHQ data of intelligence value by remote access to computers, computer networks and telecom networks without the knowledge or consent of their owners and users, within the appropriate legal framework"

PTD "We penetrate targets' defences."

OR….

Legally accessing computers/networks remotely without the owners permission to:

- Produce Intelligence
- Do Effects
- Support others: PTD, CND, Partners

Why do CNE?

Passive Sigint won't always work

- Can overcome crypt or collection difficulties
- Access to data at rest

To <u>enable</u> conventional Sigint

- Used as an enabler of crypt
- Redirect traffic

PTD "We penetrate targets' defences."

CNE teams

PTD “We penetrate targets’ defences.”

Legalities & Policy

CNE must comply with current legislation:

• Computer Misuse Act (CMA) 1990 states that unauthorised access or modification is illegal when:

- person in UK and computer in UK
- person overseas and computer in UK
- person in UK and computer overseas

Legal & Policy

Exemption is obtained from the CMA using Intelligence Services Act (ISA) warrants:

- Section 5: UK targets (requires at least Foreign Secretary signature)
- Section 7: overseas targets (can be signed by DO unless sensitive)

European Human Rights Act

Covert Infrastructure, Access & Dataflow

All CNE activity must be UK deniable

- Intermediary machines/Covert Infrastructure used to:
  - gain **access** to targets via the internet
  - bring data back into corporate repositories

PTD "We penetrate targets' defences."

Infrastructure

Implementation/maintenance CNE core infrastructure

- CNE Desktop
- Network
- Servers
- Storage
- Sys Admin

CNE Operations

- Network End Points
- Counter Terrorism
- Single End Points
- Data Harvesting
- Effects
- CNE Scarborough

Types of Operation

Masquerades

- Use credentials obtained from CNE or passive collection to gain access to email, chat rooms etc

Content Delivery

- Individually crafted email attacks that dupe target into visiting an exploitation web server

Types of Operation

Router Ops

- Targeting network infrastructure via gaining access to Admin machines

Remote Access

- Use security weaknesses to survey and gain access to computers/devices using public/private tools

Effects

Making something happen a target's computer.

- Degrading comms to slow network.
- Bringing down target's web browser.
- Changing users' passwords on extremist website.

EREPO

- EREPO is the covername for router operations
- Provides access to in country collection through exploitation of routers
- Target data more accessible to SIGINT collection
- Provides crypt material, event tip-offs, target metadata

Capability - Implants

Develops techniques and technical assets, mainly software, for use in CNE Operations.

- Teams:
  - Microsoft
  - UNIX
  - Hardware
  - Mobiles

Capability - Research

- **Vulnerabilities Research and Exploit development**
  - Find the holes/weaknesses
  - Use them to gain execution
- **Future Techniques**
  - QUANTUM
  - MUGSHOT

Capability - Prototyping

- Analyst and Operator Tools
- Automation
- STARGATE
- HIGHNOTE

Joint working

- 2nd Parties, SIS and Security Service
  - all do CNE but have different targets and toolsets

- Close working with OPD-GNE, OPC-TDSD, OPD-JS and other teams within Active Approaches

Deconfliction

Deconfliction carried out with Second Parties:

- Implants may interfere with each other
- More activity increases risk of being found

Deconfliction by IP addresses, not target.

'Primacy' agreed and tasking shared.

CNE support PTD

Includes:

- Password Cracking
- VPN Exploitation
- CV/Key Extraction
- WHARFRAT

Challenges

- Avoiding detection by target or another agency
- Remaining within the law while increasing pace
- Staying ahead of the game
- Diversifying toolkit
- Meeting increasing customer demands
- Demystifying what we do
- Co-existing with partners

Contacts

- Email [redacted]
- Call [redacted]
- Visit A3c
- [redacted]