Mapping Out Cyber Crime Infrastructure
A Law Enforcement Approach

Jon Flaherty
UK National Cyber Crime Unit
13th May 2015
RIPE 70 - Amsterdam

Cyber Crime Infrastructure

"A Disposal Front End With A Static Stable Back End"

- Compromised and malicious domains hosting exploits
- Local log file tracing network intrusions / drops
- Leads to a common static and more stable IP infrastructure
- RIPE NCC members caught up in the middle of it ?

NCA
National Crime Agency

A New Approach
"Targeting the Infra not the Incident"

- **How does LE begin to map it ?**
- **Can we disrupt it ?**
- **Need for collaboration with RIPE community and service providers**

NCA
National Crime Agency

TEST CASE

AIM

Attribute a suspect ISP and reseller infrastructure to "Bullet Proof Hosting" activity

OBJECTIVES

Design an ISP mapping strategy that visualises target infrastructure to enhance attribution and operational strategy

NCA
National Crime Agency

Mapping Strategy
A 4 Stage Methodology

- Stage 1 : Collation of intelligence
- Stage 2 : IPv4 Network WHOIS research
- Stage 3 : Mapping IPv4 to DNS enrichment
- Stage 4 : Visualisation

NCA
National Crime Agency

Stage 1 - Collation of Intelligence

What do we know so far ?

- Hosting provider and suspects located in one country
- Operating under alias names
- Single strand IPv4 intelligence linked to lots of cyber crime

NCA
National Crime Agency

Stage 2 – IPv4 Network WHOIS Research

Mapping single strand intelligence across the WHOIS

- Find ISP & Reseller full IPv4 address ranges
- Dates of IP assignment
- Identify ASN / upstream providers who announce IP routes

NCA
National Crime Agency

Stage 2
Now what do we know ?

- Additional Hosting / Reseller IPv4 space
- Consistent hosting providers of reseller space
- Multiple RIPE NCC members announce target IP traffic
- Static IP infrastructure, small, consistent /27 IP address ranges
- RIPE WHOIS reveals more provider alias names and handles
- Small ARIN infrastructure

NCA
National Crime Agency

Stage 3 – Mapping IPv4 space to DNS Enrichment

What domain traffic and types of service point to these ranges ?

- Web, Mail, Name, VPN Servers
- Number of sites hosted
- Historic domains
- Bad Traffic
- Data Enrichment – Abuse feeds

Passive DNS

NCA
National Crime Agency

Stage 3
Now what do we know ?

- Target ISP ranges show legitimate web traffic
- UK reseller ranges carry known malicious traffic
- UK hosted GOZ and DGA activity across .eu ccTLD's
  - **.991ce.34691a9.832.1c.1736.ced.87.4050.xxxxxx.xxxxx.eu**
- GOZ privacy protected domains with a common registrar
- VPN end point servers and VPN over DNS traffic
  - **ln-037.rd-00004080.id-4934215.v0.tun.vpnoverdns.com**
- Beginning to see the bad from the good….

NCA
National Crime Agency

Stage 4 – Visualisation
Charting the infrastructure

- Bulk domain WHOIS lookups
- Geo locating IP ranges and records
- Colour coded clusters
- Layering ownership
- Pattern matching

NCA
National Crime Agency

AIM

Attribute a suspect ISP and reseller infrastructure to "Bullet Proof Hosting" activity

OBJECTIVES

Design an ISP mapping strategy that visualises target infrastructure to enhance attribution and operational strategy

NCA
National Crime Agency

BPH Picture

Clean Front v Malicious Reseller End Ranges

- Diversified infra of PVS hosted content and VPN end points
- Reseller architecture across more than one member / country
- Small IP blocks / multiple RIPE Database handles
- An attraction to cheap virtual hosting / IXP
- ASN commonalities / sponsoring org's for IP ranges
- Use of RIPE NCC tools gives LE more routes to best evidence……

NCA
National Crime Agency

Can We Disrupt The Abuse ?
Need For Collaboration - Mitigation@Scale

- Mapping infrastructure identifies abuse at greater scale
- LE migrating into proactive CERT prevention / outreach to Industry
- IP reseller intelligence mapped and shared to members
- PDNS entries notified as an ISP abuse issue / feed to Industry
- Malicious IP ranges become Spamhaus blacklist entries
- Privacy/Proxy abuse becomes an ICANN compliance submission

NCA
National Crime Agency

Questions

jonathan.flaherty@nca.x.gsi.gov.uk

NCA
National Crime Agency