Intrusion Analysis/JeAC

The IA team conducts all-source analysis both of emerging and current electronic attack types. It forms part of the Joint Electronic Attack Cell (JeAC). (Other JeAC elements are EITT, JTRIG and the EA Threat Team). SIGINT targeting by the IA team falls under EITT oversight (see Seth's email of 6/12/07). The IA team is responsible for the management and release of eA signatures.

PoCs: [redacted] (Team Leader)

Main Customers: SS, GCHQ, SIS, HMG, 2nd Parties.

Sources: where does the material come from?

- SIGINT
- HARUSPEX (though most first-line analysis is done by the Incident Response Team)
- MessageLabs data managed via the HARUSPEX network
- Tasking of CNE
- Open Source

"Target" location

HARUSPEX sensors monitor attacks against UK systems based on known attack signatures. These signatures typically reflect attack vectors, infrastructure or entity identifiers associated with attacks. While the signatures reflect our knowledge of FIS activities, UK-to-UK traffic may be collected if the attacker is using UK infrastructure.

SIGINT is used to detect attack activity associated with FIS or Foreign Governments. Selectors include IP addresses, web domains and email addresses. In general these are not associated with the UK, but where UK infrastructure is involved, appropriate SIGINT processes are followed.

Report Types: How are results reported?

JeAC reports are issued as standard EPRs via PROSPERO.

Report Distribution Mechanism

PROSPERO

Legal Authorities

Authorisation varies depending on the source of the information:
Any CNE will be authorised under ISA and (where necessary) either with a warrant issued under s5 or under s7, depending on where the target is located.
Use of the SIGINT system is under the direction of EITT – all normal Ops rules apply and intercept will have been acquired under Part I of RIPA.
Any HARUSPEX information has been lawfully acquired under the LBPR, as for the Response Team.

Local Policy statements/documentation

- [redacted]'s signature release policy (X/29373/7008/009/000/0 of 26 June 2007)

- [redacted]'s email of 6/12/07: "EITT/RCIT is accountable for eA use of the SIGINT system".
- [redacted] of EITT is working with OPPLEG on eA-specific authorisations for CNE (eg. to allow the targeting of UK-based victims).
- [redacted]'s description of the Signature Spreadsheet.

Auditing arrangements
The IA team has a fairly small number of selectors in CORINTH. Team members are prompted monthly to check the validity of their selectors. Formal audits are conducted under the auspices of EITT. HRA checking is enforced by the SIGINT system, in that selectors will age off if not re-validated. Use of SIGINT system for eA is covered by 2 MIRANDA numbers, corresponding to the separate JIC requirements for current and emerging electronic threats.

The team maintains a local spreadsheet of about 1500 eA signatures with associated information on nationality, release, likely false positive rate etc. The Signature Release Policy mentioned above controls the deployment of these signatures on HARUSPEX and their release to external agencies.

Number of reporters and their skill levels
There are 6 reporters in the IA team, of whom 2 are trained to Skill level 3 and 2 to Skill Level 2.

Other available legal/policy training
Operational Legalities Briefing.

Status:
Updated 23/7/08 with input from [redacted] and [redacted].