Anton Baskov <*ab@architecturebureau.org*>
AB Architecture Bureau

Prospects of content blocking in light of future internet technologies development

Panel “Impact of content blocking on internet infrastructure”, ENOG 14

Текущие вызовы

- Текущие вызовы
  - Эффективность / стоимость / сопутствующий ущерб
  - Точечная блокировка, чтобы минимизировать сопутствующий ущерб
  - Игра в прятки (смена адресов, идентификаторов, перенаправления)
  - Скрытие цели (например, за легитимным сервисом) или доступ посредством скрытых сетей; Распределенный контент
  - Ложные срабатывания (в том числе и специально наведенные, для нецелевого использования системы блокировок)
  - «Использование» инфраструктуры системы блокировок для выведения из строя сегментов сети или элементов критической инфраструктуры
- Блокировка будет невозможной без системы всеобъемлющего контроля (pervasive monitoring) и систем внешнего мониторинга

Challenges

- Challenges
  - Efficiency vs. cost
  - Targeted blocking in order to minimize collateral damage
  - Hide-and-seek (changing IP, changing identifiers, decentralised content)
  - Hidden services (incl. accessed through other ones) and covert networks
  - False positives (incl. cases of blocking mechanisms abuse in order to DoS some targets)
  - Blocking system misuse in order to disable critical infrastructure or connectivity between networks
- Blocking will be impossible without pervasive monitoring
  - including external monitoring to obtain additional data for analysis

IETF view

- RFC 6973 – Privacy Considerations for Internet Protocols, July 2013
- RFC 7258 – Pervasive Monitoring Is an Attack, May 2014
  - *… PM … needs to be mitigated where possible, via the design of protocols that make PM significantly more expensive or infeasible*
- RFC 7624 – Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement, August 2015
- RFC 7754 – Technical Considerations for Internet Service Blocking and Filtering, March 2016

TLS SNI Encryption

- TLS Server Name Indication, RFC 3564
  - Monitoring tools might use SNI transmitted in plain text to determine requested service among others, collocated on the same host.
- TLS SNI Encryption
  - https://tools.ietf.org/id/draft-ietf-tls-sni-encryption-00.html

DNS

- DNS Privacy Considerations, RFC 7626
  - DNS requests are able to give information not only about websites we using, but also for people we send an email and much more
    - For example, OPENPGPKEY & SMIMEA RR
- Encryption
  - DNS over TLS and DTLS, RFC 7858 & RFC 8094
  - The EDNS(0) Padding Option, RFC 7830
- Authoritative servers
  - DNS Query Name Minimisation to Improve Privacy, RFC 7816
- Recursive servers
  - DNSSEC signed answers embedded in application level protocol?
  - …

Opportunistic IPSec using DNSSEC

- Opportunistic Encryption using the Internet Key Exchange, RFC 4322
- Current implementations:
  - Resolve and validate both A/AAAA and IPSEKKEY resource records
  - If signed IPSECKEY record found, IKE daemon negotiates IPSec tunnel using specified key
  - Application obtains A/AAAA records and send data over IPSec tunnel provided
  - IPSECKEY may be also stored in in-addr.arpa., ip6.arpa. zones

Opportunistic Security for HTTP/2

- RFC 8164 from May 2017
  - Intended to avoid passive pervasive monitoring, downgrade attack is possible
    - e.g. removing Alt-Svc: HTTP header
  - Uses concept of alternative services as in RFC 7838

Similarly for other protocols

- Encryption triggers:
  - DNS-based authentication of named Entities: TLSA, SMIMEA, OPENPGPKEY RR
  - SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS), RFC 7672
  - …
- …

Summary

- Effects
  - Efficiency (detectability) ↓
  - Granularity ↓
  - Cost, Collateral damage ↑
- «Block-and-forget» approach no longer works

Итого

- Эффекты
  - Эффективность (способность обнаружить) ↓
  - Точность ↓
  - Стоимость, сопутствующий ущерб ↑
- Подход «заблокировал и забыл» более не работает

What's next?

- Pervasive monitoring
  - Statistical analysis
  - Behaviour analysis
- External monitoring tools
- Collaborators (as defined in RFC 7624)
  - ISP, Service providers (infrastructure, advertisers, CDN, etc.), Software vendors

Что дальше?

- Средства отслеживания (pervasive monitoring)
  - Статистический анализ
  - Поведенческий анализ
- Средства внешнего мониторинга
- Информаторы
  - ISP, операторы сервисов (инфраструктурные, реклама, CDN и т.п.), разработчики ПО

Выводы

- Простых механизмов ограничения доступа достаточно для минимального ограничения доступа в большинстве случаев
- В остальных случаях необходима оперативная работа
  - и соответствующие средства оперативной разработки

Summary

- Simple content blocking mechanisms are sufficient to get adequate results for most cases
- Other cases require targeted measures
  - and corresponding tools for operative investigative activities

*
EN

Questions?

Anton Baskov <*ab@architecturebureau.org*>

RU

Вопросы?

Anton Baskov <*ab@architecturebureau.org*>