I2P Monitoring and Filtration

David Dagon[1]

[1]Georgia Institute of Technology
Atlanta, Georgia

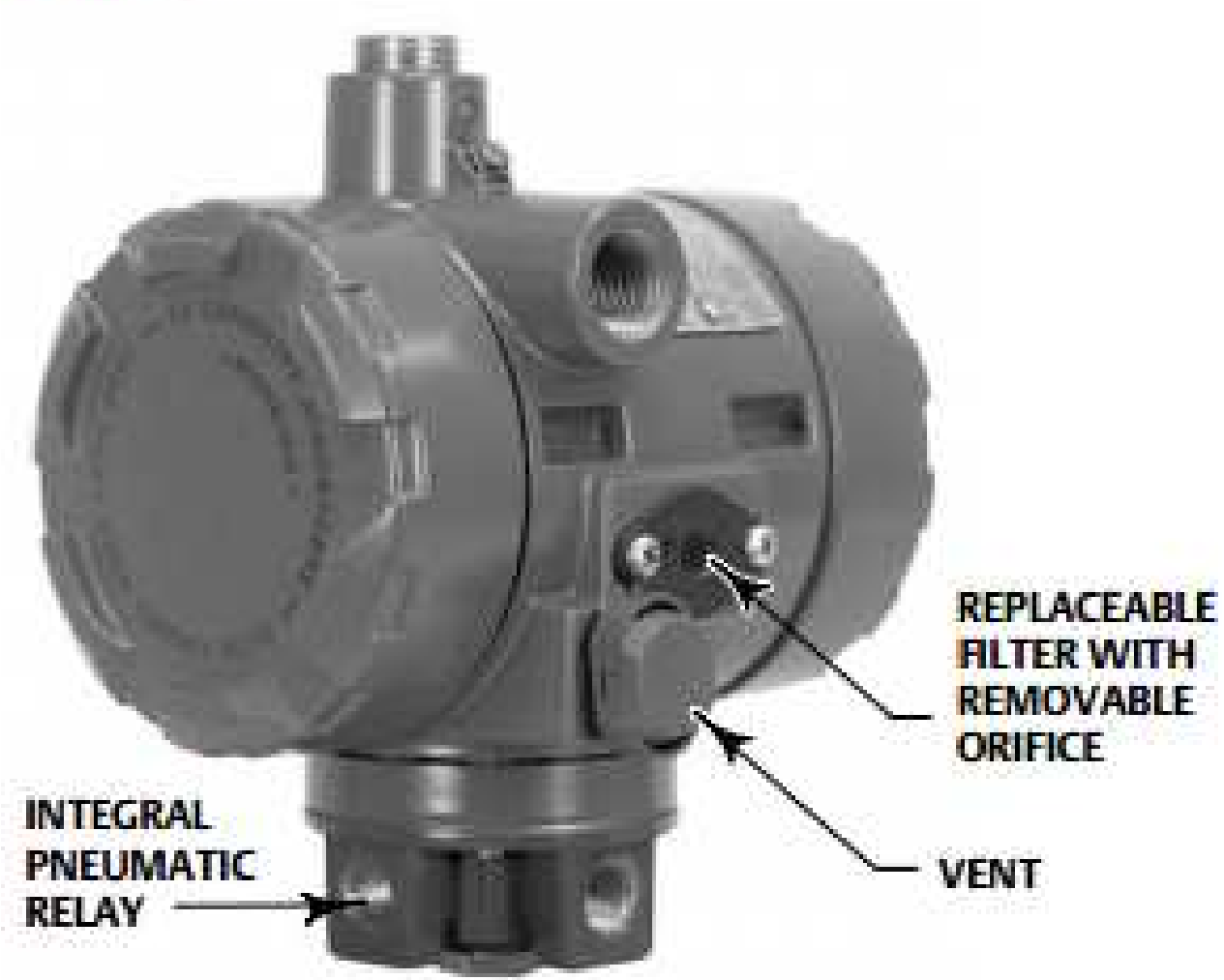
I2PCon Aug 2015


20 WEST
Birmingham
20 EAST
Augusta
Fulton St
Central Ave
Ga State Univ

Georgia Tech: Come Visit

Today's Topic: I2P Filtering

Figure 1. Fisher i2P-100 Electro-Pneumatic Transducer



Outline

- Overview of Online Community Abuse
- I2P monitoring
- Filtration: Commercial Efforts
- Filtration: I2P Suggestions

Overview of Online Community Abuse

- Historical Lessons
  - Geocities $\Rightarrow$ “Digital Blight” ($3.57B acquisition, closed 10 years later)
  - SMTP $\Rightarrow$ Spam “Port 25 Management”
  - Tor $\Rightarrow$ Botnets (Predicted in 2012 by G-Data)
  - Bitcoin $\Rightarrow$ Ransom currency
  - Youtube $\Rightarrow$ Youtube comments
- What can I2P learn from these experiences?

Overview of Online Community Abuse

The New York Times

DealB%k WITH FOUNDER ANDREW ROSS SORKIN

For Ransom, Bitcoin Replaces the Bag of Bills

By NATHANIEL POPPER JULY 25, 2015

Email

Share

Tweet

Save

In the old days, criminals liked their ransom payments in briefcases full of unmarked bills.

These days, there's a new preferred method for hostage takers: the virtual currency Bitcoin.

Overview of Online Community Abuse

Tor networks: Stop employees from touring the deep Web

by
Adam Rice

Are employees using Tor to view blocked Web sites, or mining Bitcoins on corporate resources? Sinister or not, it needs to stop.

Examples of Network Abuse

- E.g., “bomb threats” via Tor
  - Tor community response largely focused on preparing exit node operators for legal and policy defense
- Snooping by exit nodes
- Anecdotes from sample collection: lost personal documents, life savings, and trust

Anonymity Community Responsibilities

- Anonymity networks must balance competing principles:
  - True: Anonymity technologies are morally neutral: they can be used for good or bad.
  - However, if that's the end of the analysis, the anonymity network will experience digital blight
- Working theory: If anonymity communities do not actively set standards, they will be set by others.

I2P: Symptoms of Abuse

- Dyre botnet (and related 'ransomware') abusing I2P
  - Security vendors will likely block *all* I2P traffic, good or bad.
  - Some filtration will take place using IP-based DNSBLs, based on member enumeration
- IP-based blocking may have implications for I2P tunnel creation (blocking host found in netdb, resulting failed tunnels without NACKs).

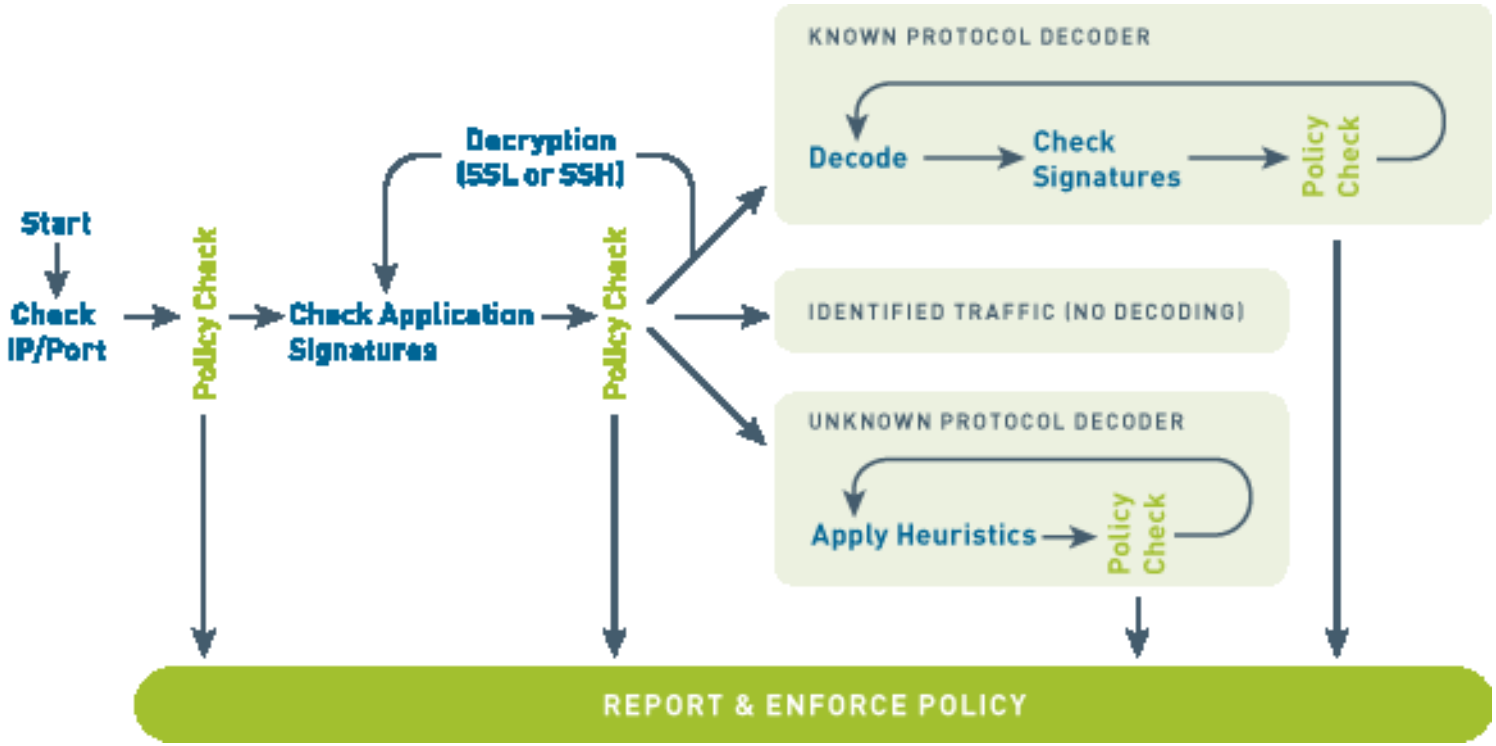
Commercial Filtration of I2P

- Companies offer modules that block I2P-related traffic
  - Some are (evidently) DPI-based
  - Some are based on crawls/enumerations

Commercial Filtration of I2P

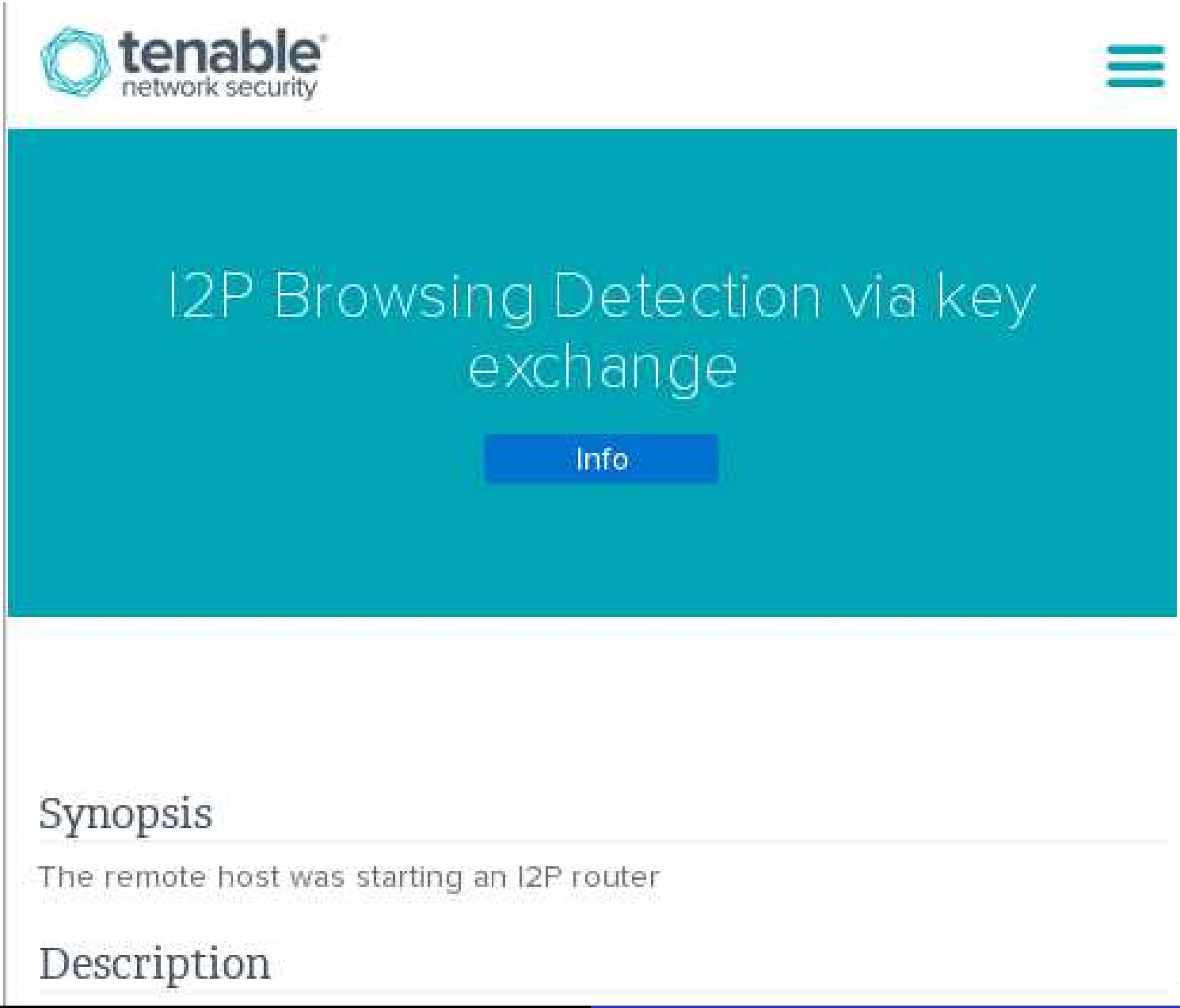
- Companies offer modules that block i2p-related traffic
  - PaloAlto Networks, DPI
  - Tenable DNS-based as well DPI-based
  - Dell/SonicWall App detection
  - Premium snort-based rules

Commercial Filtration of I2P: PAN App-ID



https://www.paloaltonetworks.com/products/technologies/app-id.html

Commercial Filtration of I2P: Tenable



Commercial Filtration of I2P: Tenable

I2P Outbound Connection Detection

http://www.tenable.com/pvs-plugins/7170

The remote host has just made a connection to the **i2p** network. The **i2p** network allows users to tunnel traffic anonymously and encrypted to ...

I2P Browsing Detection via SSDP

http://www.tenable.com/pvs-plugins/8798

The remote host was starting an **I2P** router Plugin ID: 8798 The remote host was starting an **I2P** router N/A Plugin Family: Internet Services ...

I2P Browsing Detection

http://www.tenable.com/pvs-plugins/8797

The remote host was starting an **I2P** router Plugin ID: 8797 The remote host was starting an **I2P** router N/A Plugin Family: Internet Services ...

I2P Browsing Detection via DNS

http://www.tenable.com/pvs-plugins/8800

The remote host was starting an **I2P** router Plugin ID: 8800 The remote host was starting an **I2P** router N/A Plugin Family: Internet Services ...

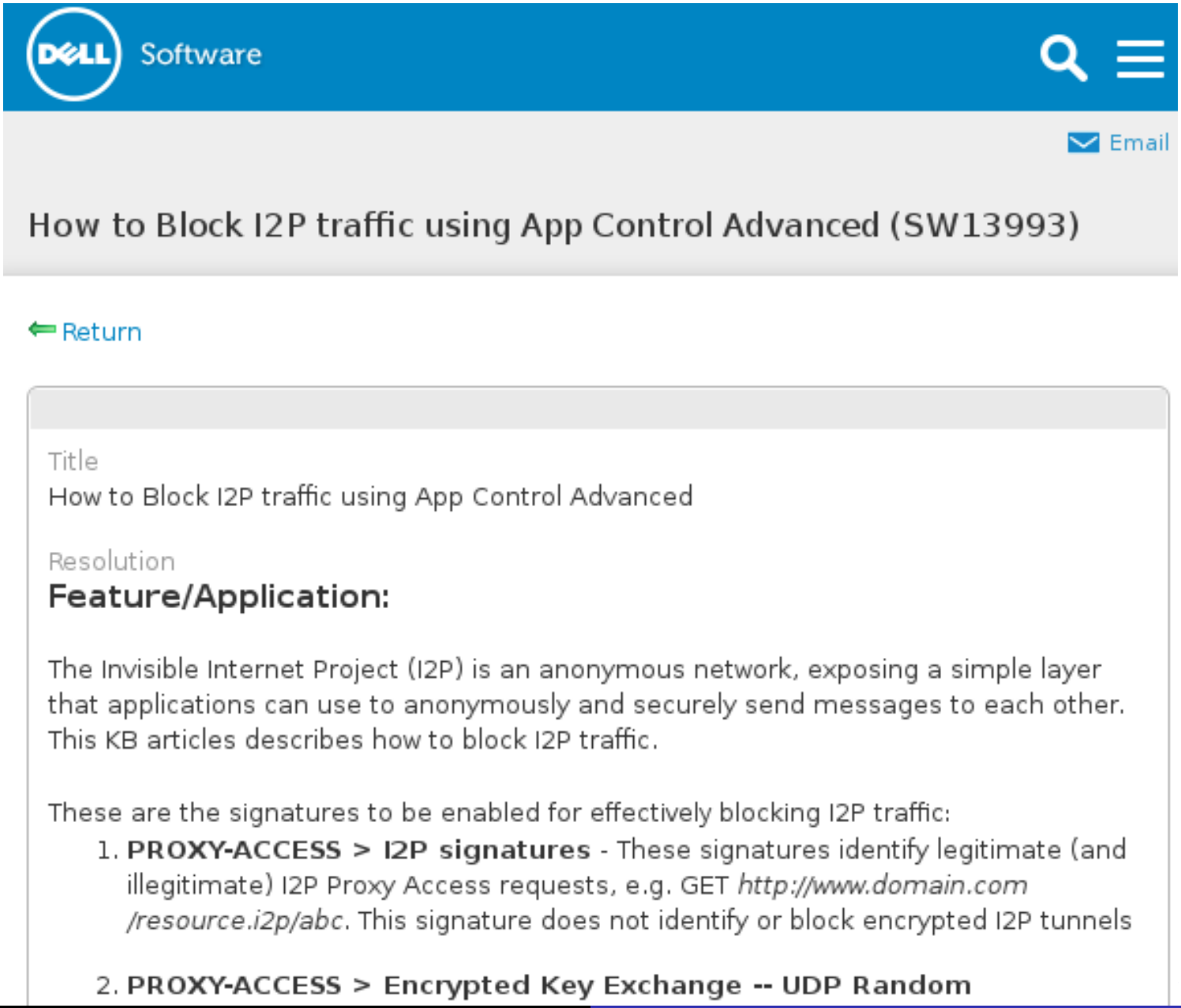
I2P Browsing Detection via key exchange

http://www.tenable.com/pvs-plugins/8799

The remote host was starting an **I2P** router Plugin ID: 8799 The remote host was starting an **I2P** router N/A Plugin Family: Internet Services ...

http://www.tenable.com/search/node/i2p

Commercial Filtration of I2P: Dell



DELL Software

Email

How to Block I2P traffic using App Control Advanced (SW13993)

Return

Title
How to Block I2P traffic using App Control Advanced

Resolution
Feature/Application:

The Invisible Internet Project (I2P) is an anonymous network, exposing a simple layer that applications can use to anonymously and securely send messages to each other. This KB articles describes how to block I2P traffic.

These are the signatures to be enabled for effectively blocking I2P traffic:

1. **PROXY-ACCESS > I2P signatures** - These signatures identify legitimate (and illegitimate) I2P Proxy Access requests, e.g. GET *http://www.domain.com /resource.i2p/abc*. This signature does not identify or block encrypted I2P tunnels

2. **PROXY-ACCESS > Encrypted Key Exchange -- UDP Random**

Commercial Filtration of I2P: Dell

- Documentation:
  - “PROXY-ACCESS > Encrypted Key Exchange - UDP Random Encryption
  - SID 7 blocks UDP tunnel traffic. Enabling this signature will not only block encrypted I2P traffic over UDB but also block other encrypted UDP traffic like IPSec VPN traffic passing through the SonicWALL. Before enabling this signature, exclude the outside or inside IP addresses of legitimiate IPSec traffic.”
- https://support.software.dell.com/kb/sw13993

Crawling of I2P: Researchers

JOURNAL OF NETWORKS, VOL. 9, NO. 9, SEPTEMBER 2014

Empirical Measurement and Analysis of I2P Routers

Peipeng Liu[a,b,c,d], Lihong Wang[d], Qingfeng Tan[b,c,d], Quangang Li[d], Xuebin Wang[d], Jinqiao Shi[c,d]
[a] Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China
[b] Graduate University of Chinese Academy of Sciences, Beijing 100049, China
[c] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[d] National Engineering Laboratory for Information Security Technologies, Beijing 100093, China

***Abstract*—With the increased focus on Internet privacy, especially after the exposure of PRISM(an Internet surveillance program), anonymous communication have been get-**

allow a fully anonymous communication between t
parties within the I2P network. On the contrary to T
[21, another popular anonymous system, I2P doesn't a

http://www.ojs.academypublisher.com/index.php/jnw/ article/viewFile/jnw090922692278/10045

Proposal: Filtration Module for I2P

- Users may create and publish their own IP-based and peer-based BLs
  - Similar to existing Blockfile Naming addressbooks
    - Note: “Blockfile” refers to the slab allocation strategy, not policy blocking
    - Provides metadata capabilities (notes, rationale for blocking etc)
  - May be destributed via, e.g., SusiDNS
  - Design principle: actively refuse tunnel creation rather than perform IP-based edge/DPI blocking, and explain the refusal
  - Perhaps a new reject value, `TUNNEL_REJECT_BL = 60`
- These slides refer to this DNSBL as “Block2File”

Block2File content: C2 DNSBL

- E.g., SSLBL
  - SSL fingerprinting of botnet C&C hosts
  - https://sslbl.abuse.ch/blacklist/
- May be augmented with other user analysis (example)

Block2File content: Augmented DNSBL

- E.g., examining hosts associated with i2p node
  `root.gator4084.hostgator.com.`
  `dns1.sweb.ru.`
  `mahdi.blackhat.gmail.com.`
  `parking.nic.ru.`
- Passive DNS associates this i2p node with other behavior

Block2File content: Augmented DNSBL

Hacked By IRAN Security Group http://selby.org/wp-content/uploads/

..:: In The Name Of Allah ::..

Hacked By IRAN Security Group

M4hdi Was Here ...

We Are Soldiers From Allah

Our New Project : Delete Israel From World Maps

Fuck Israel , America And All Terrorists

Team Members : Root SmasheR , Mr.Moein , Hektor , UmPire , ALIREZA_PROMIS , M4hdi , N-Kod , Social Enginner And All ISG Members

Home : IranSec.Net

E-Mail : Mahdi.BlackHat@GMail.com

Conclusion: Filtration Module for I2P

- Unwanted traffic should be addressed
  - Historic lessons: “No policy” means abuse will grow
  - Cat-and-mouse games with vendors will result in crawl-based DNSBLs and IP-level bans
- Proposed: policy-based Block2File may permit NACKs for tunnel builds
- **Principle 1**: Block systems should be opt-in (voluntary)
- **Principle 2**: Blocks should be explicit to avoid network failures
- **Principle 3**: Refusal errors should be justified to the end users
- Efficiencies through subscription model (SusiDNS-style propagation)
- If widely used on an opt-in basis, blocklists may encourage i2p abusers to go elsewhere or change their behavior