THE MISSING PIECE IN THREAT INTELLIGENCE

$ whoami

Frank Denis <f [at] 00f [.] net>
GitHub/Twitter: @jedisct1
Malware hunter @OVH

#malware #crypto #oss #appsec #bigdata
#distributedsystems #ml #dns #clang #rustlang #ruby
#js #lowlevelstuff #openbsd #bitrig #dragonflybsd

OVH.com

- Leading ISP in Europe
- Operating 17 data centers, 220 000 physical servers (current capacity: 1 million)
- Registrar, managing 3.7+ million domains
- 18 million host names mapping to OVH servers
- 3,000+ resellers
- Connectivity, enterprise telephony, dedicated servers, VPS, web hosting, public and private cloud services, cloud storage/backup
- Startup incubator


THREAT INTELLIGENCE
IS JUST AN RSS
FEED
BATMANCOMIC.COM

Threat Intelligence

Threat Intelligence

Defense

Combine is awesome

https://github.com/mlsecproject/combine

Trying out Combine with 41 popular feeds:

518

IP addresses

17

could be blocked right away

(but Combine is still awesome)

What about the rest?

- No evidence found
- Servers that had been taken down since the incident actually happened
- Previously compromised servers that had been cleaned or reinstalled
- IP addresses that had been reassigned to different customers
- IP addresses that had not been assigned

What about the rest?

- False positives
- Sinkholes
- VPNs, Tor exit nodes and proxies
- STUN servers and services returning information about HTTP clients and their IP addresses
- CDN and load balancers for shared services

CDNs / Shared hosting

104.24.126.62 - 104.24.127.62 - 104.27.148.231 - 104.27.149.231 - 104.27.184.206 - 104.27.185.206 - 104.27.188.177 - 104.27.188.62 - 104.27.189.177 - 104.27.189.62 - 104.28.12.63 - 104.28.17.114 - 104.28.20.37 - 104.28.21.37 - 104.28.4.65 - 104.28.5.65 - 104.28.9.177 - 108.162.215.150 - 108.162.225.142 - 108.162.226.173 - 108.162.229.50 - 141.101.112.193 - 141.101.75.125 - 141.101.81.56 - 141.101.97.38 - 141.101.97.40 - 141.101.98.120 - 162.158.94.150 - 198.41.182.215

CDNs / Shared hosting

104.24.126.62 - 104.24.127.62 - 104.27.148.231 - 104.27.149.231 - 104.27.184.206 - 104.27.185.206 - 104.27.188.177 - 10[illegible]2 - 104.27.189.177 - 104.27.189.[illegible] - [illegible].28.17.114 - 104.28.2[illegible] - [illegible]28.4.65 - 104.28[illegible] - [illegible]215.150 - [illegible]3 - 108.162.229.50 - 141.101.112.193 - 141.101.75.125 - 14[illegible].10[illegible].81[illegible]6 - 4[illegible].10[illegible]7.38 - 14[illegible].10[illegible]9[illegible]4[illegible] - 141.101.98.120 - 162.158.94.150 - 198.41.182.215

CLOUDFLARE®

Estyle.lt

estyle.lt
Internetinė elektronikos parduotuvė

Paieška...

Prekių krepšelis (0)

8 618 45840 info@estyle.lt Prisijungti Registruotis

Vaizdo ir garso technika | Kompiuterinė technika | Buitinė technika | Smulki buitinė technika | Telefonai ir navigacijos | Foto ir video technika | Žaidimai ir pramogos | Pirkite pagal gamintoją

Nešiojamieji kompiuteriai

Vaizdavimas: Eiliškumas: Populiariausios prekės viršuje Rodyti puslapyje: 60 rezultatų

E-parduotuvė › Kompiuterinė technika › Nešiojamieji kompiuteriai

Pirkite pagal

Akcijos / naujienos
- Akcijos
- Naujienos

Kaina

230.00 € - 2600.00 €

Gamintojas
- ACER
- APPLE
- ASUS
- DELL
- HP
- LENOVO
- MSI

-37% NEMOKAMAS PRISTATYMAS

Nešiojamasis kompiuteris SAMSUNG XE500T1C-A01 WIN8

499,99 €
~~799,06 €~~

Palyginti

-22% NEMOKAMAS PRISTATYMAS

Nešiojamasis kompiuteris ACER S5-391 WIN8 CI5-3317U 13 ENG

699,99 €
~~897,82 €~~

Palyginti

NEMOKAMAS PRISTATYMAS

Nešiojamasis kompiuteris SAMSUNG XE300TZC-K01 WIN8

639,99 €
~~695,09 €~~

Palyginti

-15% NEMOKAMAS PRISTATYMAS

Nešiojamasis kompiuteris ACER E1-522 A4-5000/4GB/320GB

319,99 €
~~376,50 €~~

Palyginti

-14% NEMOKAMAS PRISTATYMAS

-11% NEMOKAMAS PRISTATYMAS

-15% NEMOKAMAS PRISTATYMAS

-26% NEMOKAMAS PRISTATYMAS

188.165.25.153

Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset.**

3/39	2013-09-21 01:28:28	http://radio-mixport.ru/engine/opensearch.php
3/39	2013-09-04 17:50:33	http://bit-torrentsmd.ru/
5/39	2013-08-08 16:27:54	http://enemschool25.ru/
2/38	2013-07-11 04:41:17	http://vladzol.ru/
4/39	2013-07-07 01:20:09	http://radio-mixport.ru/video-klipy/797-modnyy-top-hits-letnyaya-tusovochka-2013.html
1/39	2013-06-25 00:57:33	http://188.165.25.153/
1/38	2013-06-24 10:15:51	http://vladzol.ru/td/go.php?sid=3
3/39	2013-06-21 05:54:28	http://big.torrentslife.ru/
4/39	2013-05-27 05:04:36	http://stroucity.ru/
1/38	2013-05-25 07:05:05	http://torrentslife.ru/

More

Latest undetected files that were downloaded from this IP address

Latest files that are **not detected by any antivirus solution and were downloaded by VirusTotal from the IP address provided.**

0/44	2013-07-11 04:41:38	fe691ae329612cb67336bcf3ba8750110d55ba88cd65cc0010f2dd60563ac5d1
0/47	2013-07-04 09:57:55	74e19d8b62ec24cf6cf8f3f8a8b7829e3c003a9220340977728319fab926ff60
0/45	2013-06-24 10:00:59	7921a6035cc8a0981a5dee737dd3d29b150ddd48407717d3fca4b6376f2b0e70
0/43	2013-05-27 05:05:40	8f9bcaf2108af8933b2a16dbdfd87d0f89114d1befab749aca3f9bcf76cfa7ca

Dirt Jumper C&C

188.165.25.153

- May 2013 - January 2014: Shady customer
- January 2014 - October 2014: Unassigned
- October 15, 2014: Assigned to a new customer

The Forest's Edge

Home

Welcome to the home of The Forest's Edge MUD.

If you're here, you've probably got a good idea of what a MUD is, and if you don't check out our handy guide to MUDding. TFE has a rich history spanning over 15 years with a vibrant player base. We have some players who have been with us the whole time, and others who are only recently joining our ranks – all are welcome. Over the years our unique and evolving world has grown bigger due to the hard work and dedication of our players, Avatars, and Immortals who continue to invest time and energy into the game.

Come, join us; immerse yourself into the vibrant world of TFE.

Connection Information

Host: theforestsedge.com [198.50.225.126]

Recent News:

- Server Move and IP Change February 19, 2015
- Want to Support TFE? July 6, 2013
- Updates June 2, 2013

Top Players

```
Top 10 Players
     [1] ???
     [2] ???
     [3] ???
     [4] ???
     [5] ???
     [6] ???
     [7] ???
```

198.50.225.126

- Nuclear Exploit Kit in September 2013
- Unassigned until January 2015
- Reassigned to a completely unrelated customer

How long should it be blocked?

No more observations of known indicators

DOESN'T MEAN

that

it has become safe

Empirically defined TTLs?

Until it returns a 404?

~~Forever~~

Until a customer complains?

Handling unblock requests is tricky

and the current situation doesn't encourage ISPs to care about cybercrime

The ISP can help!

Sample signatures:

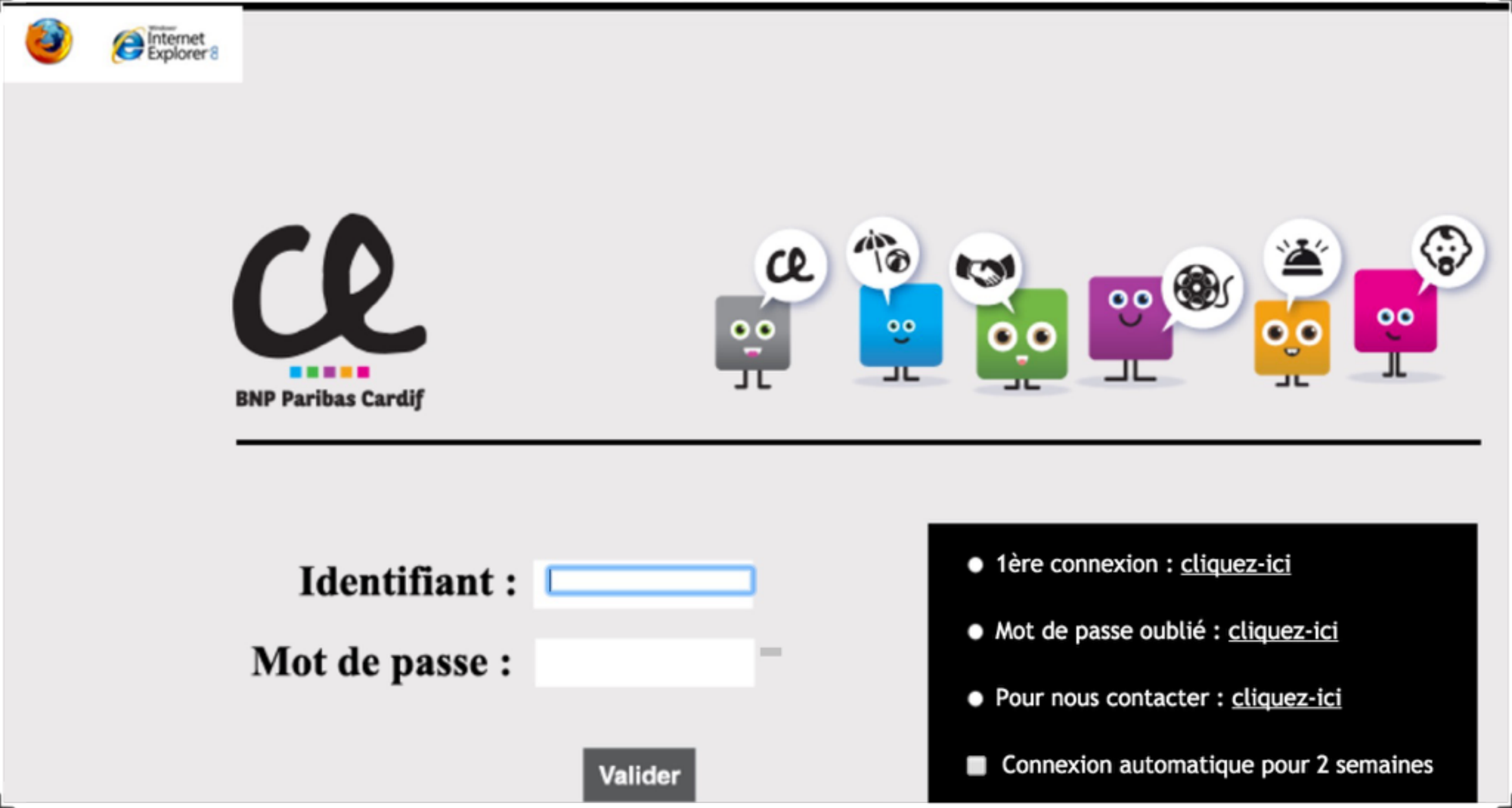
Forever relevant*

Network-based indicators:

Must be coupled with a time window

*ignoring collisions on the hash function

Phish or not?



ce-bnppass.com

A local ISP can help!

ISPs can also talk to their customers.

Live threats

vs

Indicators of Compromise

Permanently relevant

A command-and-control server IP being unintentionally contacted by a system remains a strong indicator that this system may have been infected.

Permanently relevant

A command-and-control server IP being unintentionally contacted by a system remains a strong indicator that this system may have been infected.

A domain name known for having served a payload after having exploited a local vulnerability should also immediately trigger an alert, even if the payload is not accessible any more.

Permanently relevant

A command-and-control server IP being unintentionally contacted by a system remains a strong indicator that this system may have been infected.

A domain name known for having served a payload after having exploited a local vulnerability should also immediately trigger an alert, even if the payload is not accessible any more.

Unless it is Github. Or Dropbox. Or something you know of and trust.

Temporarily relevant

Compromised websites

starting a chain of infection

Compromised domains

EK landing pages

Are they safe now?

Live threats

Block them unconditionally.

They present an immediate security risk.

IOCs

Trigger an alert.

Think twice before blocking.

The role of an ISP in fighting botnets:

Essential

Can take down infrastructure,
help Law Enforcement and researchers

classification: suspicious

It's malicious!

It's malicious!

Private TX platforms

classification: malware

Users

Researchers

It's malicious!

Public TX platforms

#malware

IRC/Jabber

#malware

VT Comments

It's malicious!

W32/Malicious

Forums

Security vendors

Twitter

192.0.2.42

It's China!

Blocked

Blacklists

Malware?

Analysis of a new malware

Sysadmins

Mailing lists

Bloggers

"Malware on your network!"

"Nuked"

Incident reporter

Infrastructure provider

"Cool"

classification: malware

It's malicious!

It's malicious!

Private TX platforms

classification: dangerous

Users

Researchers

It's malicious!

Public TX platforms

#malware

IRC/Jabber

#malware

VT Comments

It's malicious!

W32/Malicious

Twitter

192.0.2.0/24

Forums

Security vendors

One of the Koreas!

Still blocked

Blacklists

Malware!

New malware is still around!

Sysadmins

Mailing lists

Bloggers

#sad

Service providers can answer these questions:

- Has the threat observed on this website been removed? And when?
- More generally, what actions have been taken after an incident report?
- Is the IP address previously observed during an incident still being operated by the same actor?

Service providers can answer these questions:

- When was a server, a domain name or an IP address assigned to a new customer?
- Is a given server, domain name or IP address dedicated to a single user or shared by multiple, unrelated customers?

➜ Law Enforcement and security researchers

Current tools and protocols are insufficient

Complementary information from ISPs

- is only shared on demand, after a threat was reported
- require one-on-one communications
- cannot be automatically processed


LET'S FIX THIS!
DIYLOL.COM

Introducing DIP

A minimal, machine-parseable language to describe changes made by an ISP.

Events are not observations, but actions having been performed as a response to an incident, as well as changes in associations between services and customers.

Requirements

Expose changes without disclosing personal customer information.

Events must be restricted to providing facts, not opinions.

Feeds can be public.

Requirements

Simple

to understand, implement, deploy

Properties

id	event identifier	mandatory
time	timestamp	mandatory
type	resource type	mandatory
resource	resource identifier	mandatory
state	new state after a change	mandatory
source	source identifier	mandatory
depth	source depth	mandatory
owner	resource owner	type-dependent
related	related events and indicators	optional

Resource type & identifier

domain	example.com
nsrec	asd.example.com
vhost	example.com
uri	http://example.com/wp-includes/x.php
email	user@example.com
ip	192.0.2.42
subnet	192.0.2.0/24

State

assigned

A new owner has been added to the resource,
in addition to the possibly already existing set of owners.

State

reserved

The resource has been reserved by the provider for its own use.

State

unassigned

A previous owner doesn’t control the resource any more, but the resource can only be reassigned by the entity who previously assigned it.

State

suspended

The resource is still assigned to its previous set of owners, but was temporarily suspended by the ISP.

State

resumed

The resource is still assigned to its previous set of owners, and is online again after having been suspended.

State

clean

The service provider attests that no known security issues exist regarding the resource.

This is used to report false positives.

State

notified

Owners of the resource have been notified by the service provider about a security issue.

State

cleaned

The service provider attests that known security issues regarding the resource have been addressed.

State

deleted

The resource doesn’t exist any more or is not being used any more.

Resource owner

An entity having full control over a resource.

The value of that property must change every time the actual owner of the resource changes.

Resource owner

1. Personal information identifying the owner
2. A unique account identifier
3. A monotonically increasing counter
4. The output of a block cipher in counter mode
5. A randomly chosen unique identifier

Related events

OpenTPX identifiers

STIX identifiers

CRITS identifiers

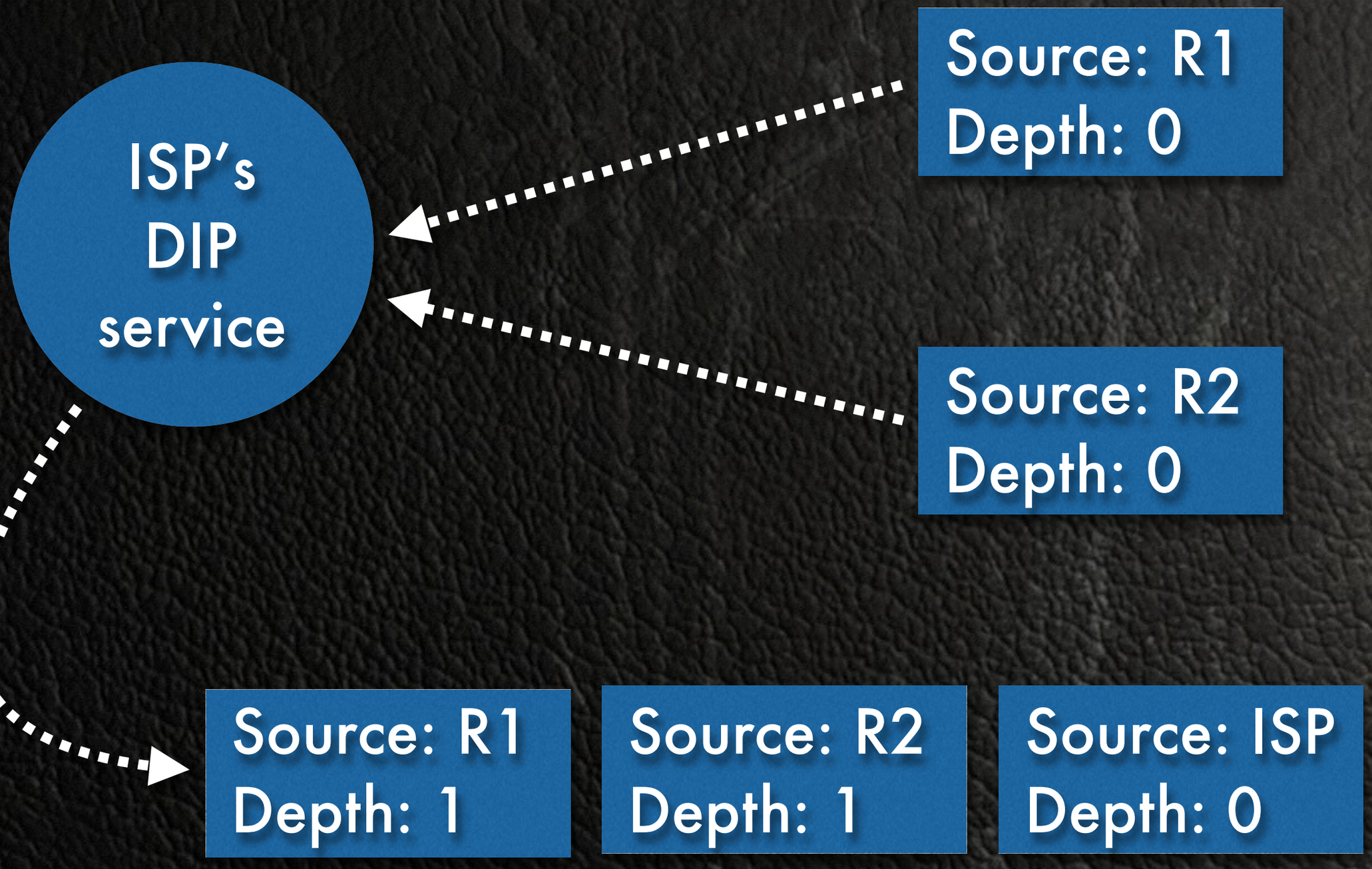
Ticket identifiers

URLs

Aggregation and relaying

Service providers can relay DIP events from their resellers

Aggregation and relaying



Aggregation and relaying

ISP's DIP service

Aggregators can review individual events, and raise their trust level by lowering the depth value

Source: R1
Depth: 1

Source: R2
Depth:0

Source: ISP
Depth: 0

A chain of trust

Feeds are decentralized and can be public.

Consumers explicitly choose the set of producers they trust.

This holds true for all consumers in the chain.

Streaming API

JSON	SSE
Protobuf	TAXII
Cap'n Proto	AMQP
MessagePack	HTTP file transfer
XML	Kafka
LTSV	NATS
CSV	Redis

Examples

A subnet owner change


```
{
  "id": "86be9a55762d316a3026c2836d044f5fc7",
  "time": 1446289736,
  "type": "subnet",
  "resource": "192.0.2.0/28",
  "state": "unassigned",
  "source": "Infrastructure Provider Corp",
  "depth": 0,
  "owner": "ffe679bb831c95b67dc17819c63c509"
}
{
  "id": "a83dd0ccbffe39d071cc317ddf6e97f5c6",
  "time": 1446290241,
  "type": "subnet",
  "resource": "192.0.2.0/28",
  "state": "assigned",
  "source": "Infrastructure Provider Corp",
  "depth": 0,
  "owner": "e7cf46a078fed4fafd0b5e3aff1448"
}
```

A response to a phishing report


```
{
  "id": "7f71e4b6070f36e6c7e9c4b6f3d3bf1b",
  "time": 1446292030,
  "type": "uri",
  "resource": "http://phish.example.com/phish",
  "state": "suspended",
  "source": "Infrastructure Provider Corp",
  "depth": 0,
  "related": ["example:Observable-160b1cd"]
}
{
  "id": "a2f95be4d1d7bcfa89d7248a82d9f111",
  "time": 1446292750,
  "type": "uri",
  "resource": "http://phish.example.com/phish",
  "state": "deleted",
  "source": "Infrastructure Provider Corp",
  "depth": 0,
  "related": ["example:Observable-160b1cd"]
}
```

A response to a phishing report


```
{
  "id": "a5193e54cd52837ed91e32008ccf41ac",
  "time": 1446292941,
  "type": "vhost",
  "resource": "example.com",
  "state": "deleted",
  "source": "Infrastructure Provider Corp",
  "depth": 0,
  "related": ["example:Observable-160b1cd"]
}
{
  "id": "ba241029d241394997265a1a25aefc6",
  "time": 1446293713,
  "type": "domain",
  "resource": "example.com",
  "state": "deleted",
  "source": "Infrastructure Provider Corp",
  "depth": 0,
  "related": ["example:Observable-160b1cd"]
}
```

A response to a spam report


```
{
  "id": "3ad4e44a4306fb62b2df0ab7069c672a",
  "time": 1446295166,
  "type": "ip",
  "resource": "10.0.2.1",
  "state": "notified",
  "source": "Infrastructure Provider Corp",
  "depth": 0
  “related": ["http://spamtrap.example/4928"]
}
{
  "id": "fe1dcd3abfcd6b1655a026e60a05d0",
  "time": 1446295996,
  "type": "ip",
  "resource": "10.0.2.1",
  "state": "clean",
  "source": "Infrastructure Provider Corp",
  "depth": 0,
  “related": ["http://spamtrap.example/4928"]
}
```

A response to a compromised server


```
{
  "id": "e4ff5e7d7a7f08e9800a3e25cb774534",
  "time": 1446293747,
  "type": "uri",
  “resource": "http://example.com/wp-includes/",
  "state": "cleaned",
  "source": "Reseller Inc",
  "depth": 1,
  "related": ["example:Observable-160b1cd"]
}
{
  "id": "d0752b60adb148ca0b3b4d2591874e2d",
  "time": 1446294279,
  "type": "uri",
  “resource": "http://example.com/wp-includes/",
  "state": "cleaned",
  "source": "Reseller Inc",
  "depth": 0,
  "related": ["example:Observable-160b1cd"]
}
{
  "id": "88aa3e3b1f22c616b1817981215e7d1",
  "time": 1446295013,
  "type": "vhost",
  "resource": "example.com",
  "state": "cleaned",
  "source": "Infrastructure Provider Corp",
  "depth": 0,
  "related": ["example:Observable-160b1cd"]
}
```

Query API

Feeds represent incremental changes, not final states.

"When was this IP address assigned to the current owner?"

"How many incidents were reported and addressed on this website in a given time frame?"

"Is the same subnet shared by many customers?"

These can only be answered by replaying a sequence of events.

ERIS

https://github.com/dip-proto/eris

Why DIP?

- Law Enforcement Agencies can have instant access to valuable information regarding resources linked to suspicious activities, including on past data.
- Security researchers and SIEM operators can get instant feedback on reported threats and get more context to improve their models and products.
- Service providers and incident responders can save time by reducing the need for one-on-one communications.
- Users gets more visibility on the responsiveness of service providers regarding security threats.

dip-proto.github.io