Broverview

Robin Sommer

Corelight, Inc., &
International Computer Science Institute

robin@icsi.berkeley.edu
http://www.icir.org/robin

The Bro Platform

Open Source
BSD License

Apps

- Intrusion Detection
- Vulnerabilit. Mgmt
- File Analysis
- Traffic Measure-ment
- Traffic Control
- Compliance Monitoring

Platform

- Programming Language
- Standard Library
- Packet Processing

Tap

- Network

Bro's been around for a while …

1995

Vern writes first line of code.

1998

Best Paper Award at USENIX Security

2006

1st Bro Workshop, Supercomputing, Tampa, FL

2016

BroCon '16, TACC, Austin, TX

Organizations using Bro

Information about usage of Bro from public sources, mailing lists, job postings, public talks, etc.

Why has Bro become popular?

The legacy cyber security stack

Opaque, proprietary,

fueled by fear

The modern cyber security stack

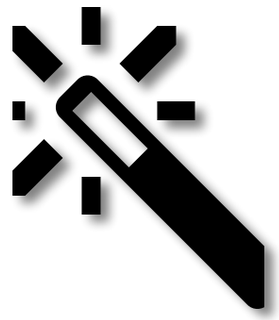
Open-source, based on science,

fueled by data & analytics

"What Can It Do?"

"Network Ground Truth"

Alerts



Custom Logic

Bro Logs

```
> bro -i eth0
[ … wait … ]

> ls *.log
app_stats.log                   irc.log                     socks.log
communication.log               known_certs.log             software.log
conn.log                        known_hosts.log             ssh.log
dhcp.log                        known_services.log          ssl.log
dns.log                         modbus.log                  syslog.log
dpd.log                         notice.log                  tracerouter.log
files.log                       reporter.log                tunnel.log
ftp.log                         signatures.log              weird.log
http.log                        smtp.log

> cat *conn.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2018-04-28-23-47-26
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       […]
#types  time    string  addr    port    addr    […]
1258531221.486539   arKYeMETxOg   192.168.1.102   68      192.168.1.1     […]
1258531680.237254   nQcgTWjvg4c   192.168.1.103   37      192.168.1.255   […]
1258531693.816224   j4u32Pc5bif   192.168.1.102   37      192.168.1.255   […]
1258531635.800933   k6kgXLOoSKl   192.168.1.103   138     192.168.1.255   […]
1258531693.825212   TEfuqmmG4bh   192.168.1.102   138     192.168.1.255   […]
1258531803.872834   5OKnoww6xl4   192.168.1.104   137     192.168.1.255   […]
1258531747.077012   FrJExwHcSal   192.168.1.104   138     192.168.1.255   […]
1258531924.321413   3PKsZ2Uye21   192.168.1.103   68      192.168.1.1     […]
[…]
```

Connections Logs

conn.log

ts	**1393099191.817686**	Timestamp
uid	**Cy3S2U2sbarorQgmw6a**	Unique ID
id.orig_h	**177.22.211.144**	Originator IP
id.orig_p	**43618**	Originator Port
id.resp_h	**115.25.19.26**	Responder IP
id.resp_p	**25**	Responder Port
proto	**tcp**	IP Protocol
service	**smtp**	App-layer Protocol
duration	**1.414936**	Duration
orig_bytes	**9068**	Bytes by Originator
resp_bytes	**4450**	Bytes by Responder
conn_state	**SF**	TCP state
local_orig	**T**	Local Originator?
missed_bytes	**0**	Gaps
history	**ShAdDaFf**	State History
tunnel_parents	**(empty)**	Outer Tunnels

HTTP

http.log

ts	1393099291.589208
uid	CKFUW73bIADw0r9pl
id.orig_h	17.22.7.4
id.orig_p	54352
id.resp_h	24.26.13.36
id.resp_p	80
method	POST
host	com-services.pandonetworks.com
uri	/soapservices/services/SessionStart
referrer	-
user_agent	Mozilla/4.0 (Windows; U) Pando/2.6.0.8
status_code	200
username	anonymous
password	-
orig_mime_types	application/xml
resp_mime_types	application/xml

Syslog & DHCP

syslog.log

ts	1392796803.311801
uid	CnYivt3ZONHOuBALR8
id.orig_h	12.3.8.161
id.orig_p	514
id.resp_h	16.74.12.24
id.resp_p	514
proto	udp
facility	AUTHPRIV
severity	INFO
message	sshd[13825]: Accepted publickey for harvest from xxx.xxx.xxx.xxx

dhcp.log

ts	1392796962.091566
uid	Ci3RM24iF4vIYRGHc3
id.orig_h	10.129.5.11
id.resp_h	10.129.5.1
mac	04:12:38:65:fa:68
assigned_ip	10.129.5.11
lease_time	14400.000000

Files

files.log

ts	1392797643.447056
fuid	FnungQ3TI19GahPJP2
tx_hosts	192.168.187.33
rx_hosts	10.1.29.110
conn_uids	CbDgik2fjeKL5qzn55
source	SMTP
analyzers	SHA1,MD5
mime_type	application/x-dosexec
filename	Letter.exe
duration	5.320822
local_orig	T
seen_bytes	39508
md5	93f7f5e7a2096927e06e[…]1085bfcfb
sha1	daed94a5662a920041be[…]a433e501646ef6a03
extracted	-

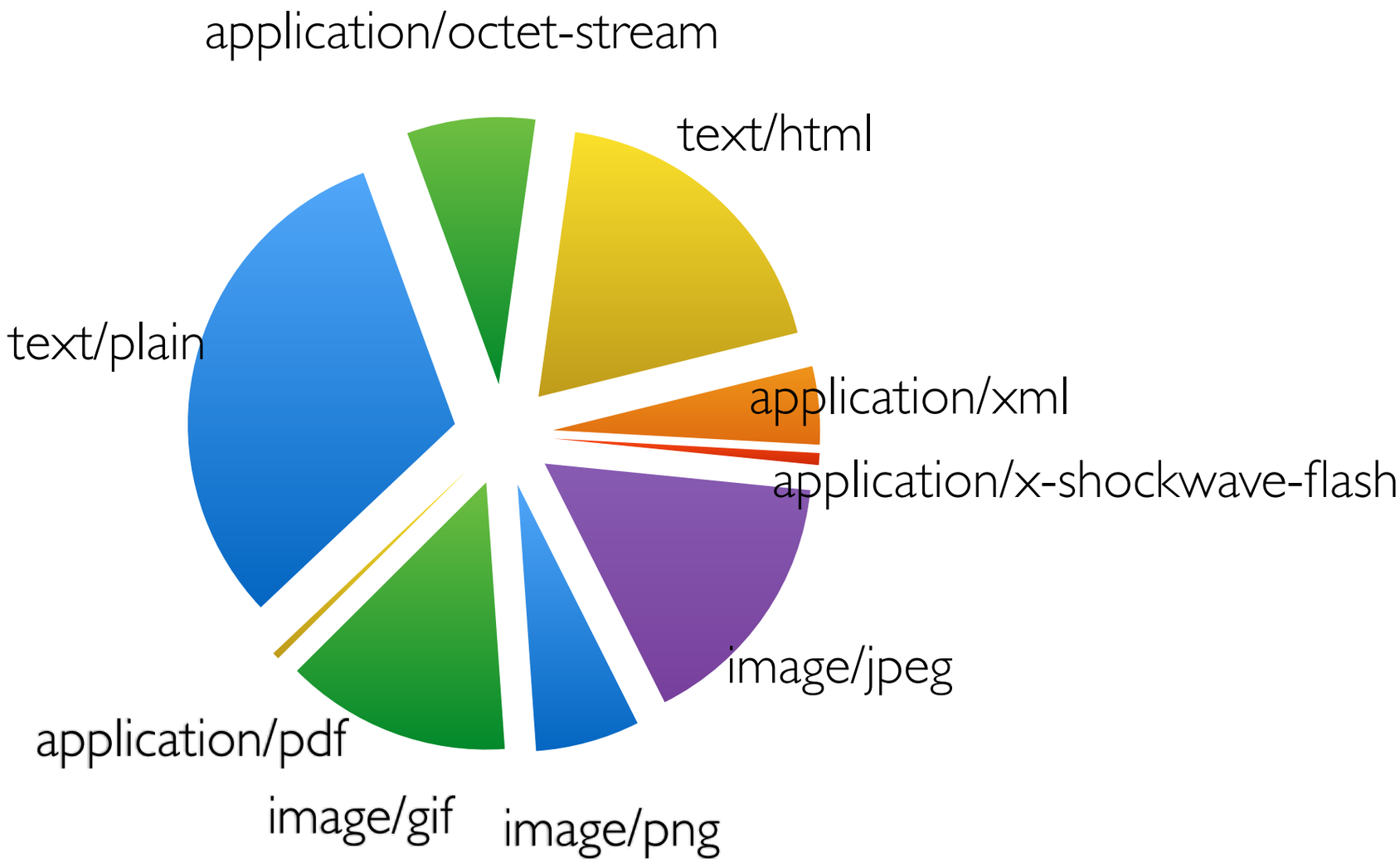
Software

software.log

ts	1392796839.675867
host	10.209.100.2
host_p	-
software_type	HTTP::BROWSER
name	DropboxDesktopClient
version.major	2
version.minor	4
version.minor2	11
version.minor3	-
version.addl	Windows
unparsed_version	DropboxDesktopClient/2.4.11 (Windows; 8; i32; en_US; Trooper 5694-2047-1832-6291-8315)

Help Understand Your Network

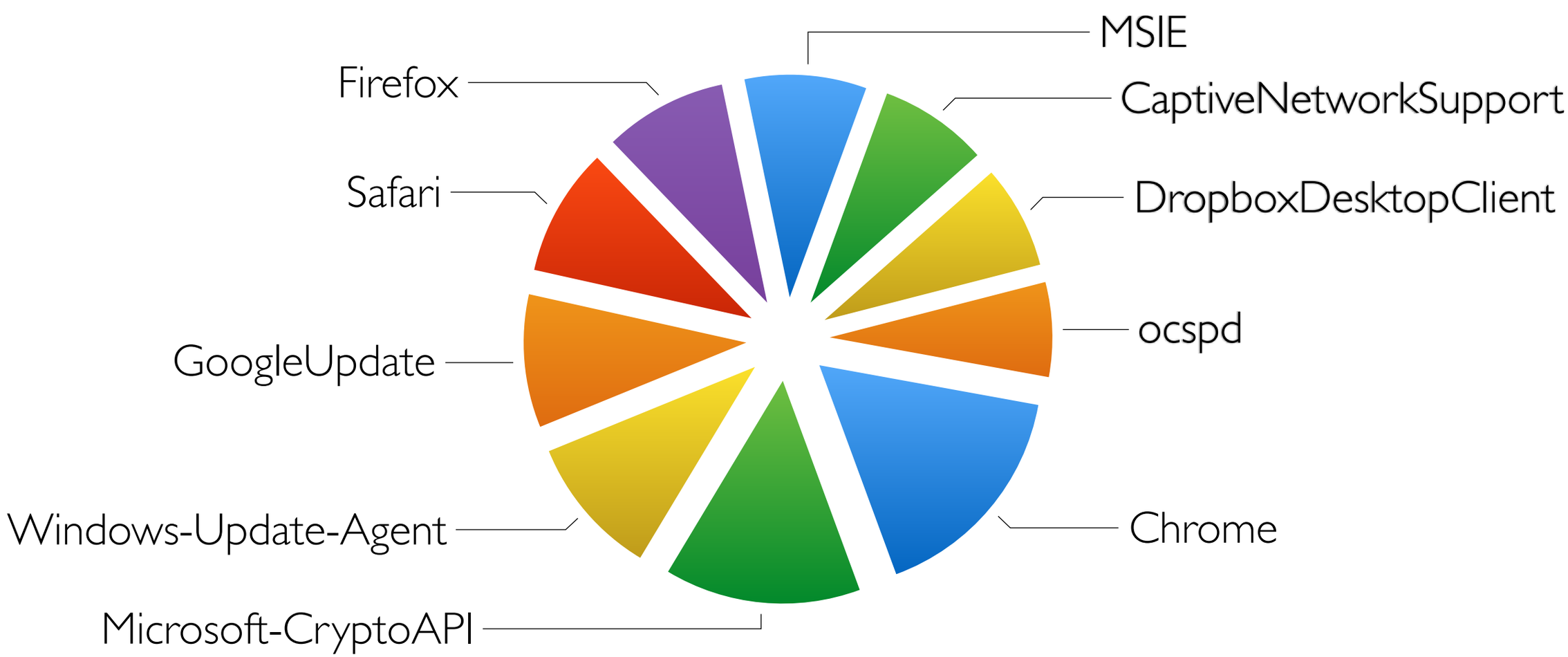
Top File Types




```
cat files.log | bro-cut mime_type | sort | uniq -c | sort -rn
```

Help Understand Your Network (2)

Top Software by Number of Hosts




```
cat software.log  | bro-cut host name | sort | uniq |
 awk -F '\t' '{print $2}' | sort | uniq -c | sort -rn
```

Bro Creates Visibility

Rich, structured, real-time data
for incident response, forensics, & analytics.

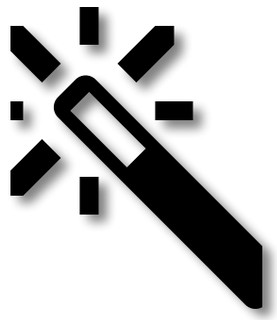
This data is what draws people to using Bro.

They have the analytics tools already, but they need high-quality input.

"What Can It Do?"

Log Files

Alerts



Custom Logic

"Watch this!"

Recorded in notice.log.
Can trigger actions.

Notices

Address_Scan
Certificate_Expired
Certificate_Expires_Soon
Certificate_Not_Valid_Yet
Content_Gap
Count_Signature
Dropped_Packets
External_Name
FTP::Bruteforcing
Intel::Notice
Interesting_Hostname_Login
Invalid_Ocsp_Response
Invalid_Server_Cert
Match
Multiple_Signatures
Multiple_Sig_Responders
Old_Version
Password_Guessing
Port_Scan
Protocol_Found
Retransmission_Inconsistency
Sensitive_Signature
Server_Found
Signature_Summary
Site_Exec_Success
Software_Version_Change
SQL_Injection_Attacker
SQL_Injection_Victim
SSL_Heartbeat_Attack
SSL_Heartbeat_Attack_Success
SSL_Heartbeat_Attack
SSL_Heartbeat_Attack_Success
SSL_Heartbeat_Many_Requests
SSL_Heartbeat_Odd_Length
Suspicious_Origination
Traceroute::Detected
Vulnerable_Version
Watched_Country_Login
Weak_Cipher
Weak_Key

Watching for Suspicious Logins

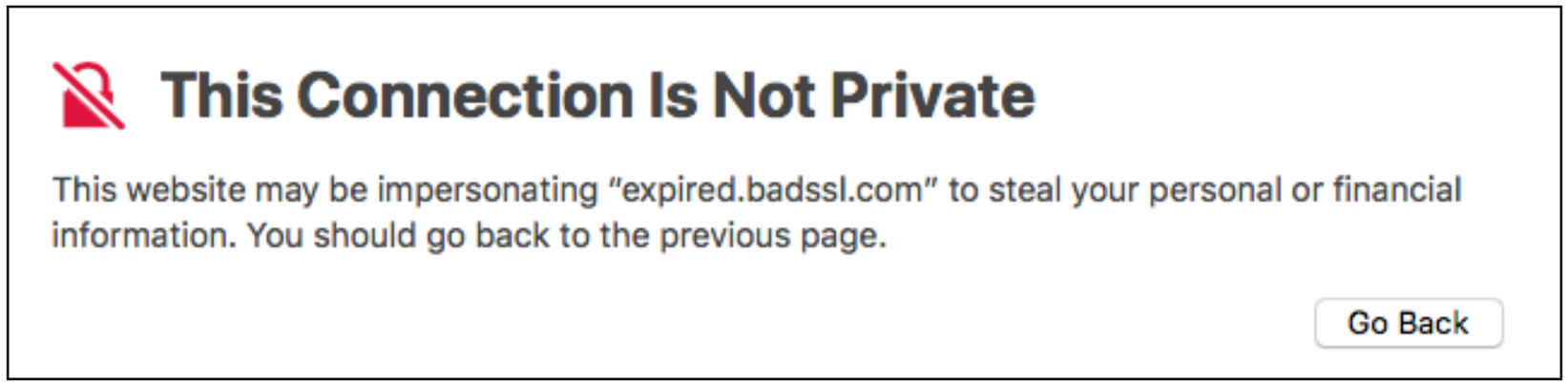
`SSH::Watched_Country_Login`

Login from an unexpected country.

`SSH::Interesting_Hostname_Login`

Login from an unusual host name.

Invalid SSL Certificates



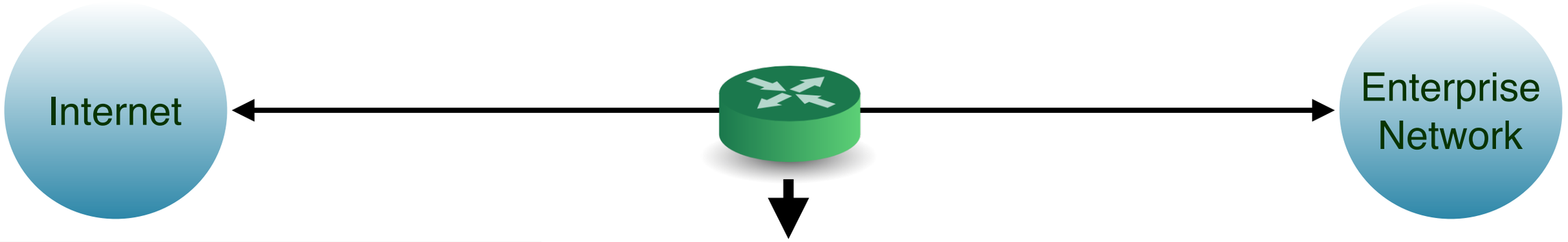
ssl.log

ts	1392805957.927087
uid	CEA0512D7k0BD9Dda2
id.orig_h	2a07:f2c0:90:402:41e:c13:6cb:99c
id.resp_h	2406:fe60:f47::aaeb:98c
version	TLSv10
cipher	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
server_name	www.netflix.com
subject	CN=www.netflix.com,OU=Operations, O=Netflix, Inc.,L=Los Gatos, ST=CALIFORNIA,C=US
issuer_subject	CN=VeriSign Class 3 Secure Server CA, OU=VeriSign Trust Network,O=VeriSign, C=US
cert_hash	197cab7c6c92a0b9ac5f37cfb0699268
not_valid_before	1389859200.000000
not_valid_after	1452931199.000000
validation_status	ok

notice.log

```
SSL::Invalid_Server_Cert
Certificate_Expired
Certificate_Expires_Soon
```

Intelligence Integration




```
Conn::IN_ORIG
Conn::IN_RESP
Files::IN_HASH
Files::IN_NAME
DNS::IN_REQUEST
DNS::IN_RESPONSE
HTTP::IN_HOST_HEADER
HTTP::IN_REFERRER_HEADER
HTTP::IN_USER_AGENT_HEADER
HTTP::IN_X_FORWARDED_FOR_HEADER
HTTP::IN_URL
SMTP::IN_MAIL_FROM
SMTP::IN_RCPT_TO
SMTP::IN_FROM
SMTP::IN_TO
SMTP::IN_RECEIVED_HEADER
SMTP::IN_REPLY_TO
SMTP::IN_X_ORIGINATING_IP_HEADER
SMTP::IN_MESSAGE
SSL::IN_SERVER_CERT
SSL::IN_CLIENT_CERT
SSL::IN_SERVER_NAME
SMTP::IN_HEADER
```

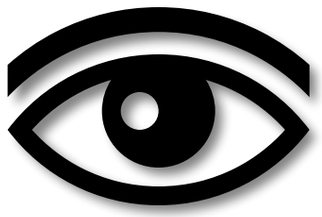
Traffic Monitoring

HTTP, FTP, SSL, SSH, FTP,
DNS, SMTP, …

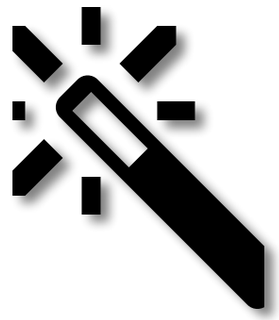
ts	1258565309.806483
uid	CAK677xaOmi66X4Th
id.orig_h	192.168.1.103
id.resp_h	192.168.1.1
note	Intel::Notice
indicator	baddomain.com
indicator_type	Intel::DOMAIN
where	HTTP::IN_HOST_HEADER
source	My-Private-Feed

notice.log

"What Can It Do?"



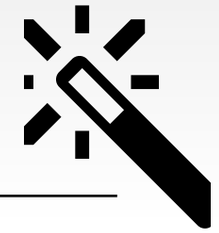
Log Files



Custom Logic

"Don't ask what Bro can do.
*Ask what you **want** it to do."*

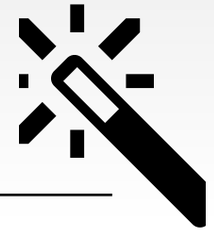
Script Example: Matching URLs



Task: Report all Web requests for files called "passwd".

```
event http_request(c: connection,           # Connection
                   method: string,          # HTTP method
                   original_URI: string,    # Requested URI
                   unescaped_URI: string, # Decoded URI
                   version: string)         # HTTP version
{
    if ( method == "GET" && unescaped_URI == /.*passwd/ )
        NOTICE(...); # Alarm.
}
```

Script Example: Scan Detector



Task: Count failed connection attempts per source address.

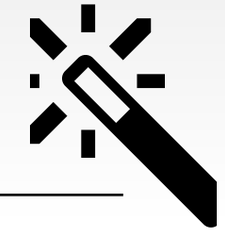
```
global attempts: table[addr] of count &default=0;

event connection_rejected(c: connection)
{
    local source = c$id$orig_h;      # Get source address

    local n = ++attempts[source];    # Increase counter

    if ( n == SOME_THRESHOLD )       # Check for threshold
        NOTICE(...);                 # Alarm
}
```

Scripts are Bro's "Magic Ingredient"



Bro comes with >10,000 lines of script code.

Prewritten functionality that's just loaded.

Scripts generate everything we have seen.

Amendable to extensive customization and extension.

Community writing 3rd party scripts.

Growing number of Bro *packages*

Bro Package Manager

bro_bitcoin

https://github.com/jsiwek/bro_bitcoin

5 ★ 25 2 0 Last Push 2/1/18, 6:30 PM

Bro Module for Detecting Cryptocurrency (Bitcoin) Mining Hosts

This script module for Bro can detect Bitcoin, Litecoin, PPCoin, or other cryptocurrency mining traffic that uses getwork <https://en.bitcoin.it/wiki/Getwork>, getblocktemplate <https://en.bitcoin.it/wiki/Getblocktemplate>, or Stratum <http://mining.bitcoin.cz/stratum-mining/> mining protocols over TCP or HTTP. Note that the module cannot currently detect the Bitcoin P2P protocol, which is different from the mining protocols.

See mining.bro for more details on how it works.

Installation

Via bro-pkg:

```
bro-pkg install jsiwek/bro_bitcoin
```

Thanks to Mozilla Open Source Support

So much more …

Bro is … a Platform

Intrusion Detection	Vulnerabilit. Mgmt	File Analysis	Traffic Measure-ment	Traffic Control	Compliance Monitoring

There's much more we can talk about …

Host-level integration
Data import and export
Active Response
Monitoring Internal Networks
Measurements
SDN integration
Industrial Control Systems
Embedded Devices

More File Analysis
More Protocols
100Gb/s Networks
Enterprise Protocols
Summary Statistics
Science DMZs
ICSL SSL Notary
Cluster Deployment

The U.S. National Science Foundation has enabled much of our work.

Bro is coming out of almost two decades of academic research, along with extensive transition to practice efforts. NSF has supported much of that, and is currently still funding a Bro Center of Expertise at the *International Computer Science Institute* and the *National Center for Supercomputing Applications*.

The Bro Project

www.bro.org

info@bro.org

@Bro_IDS
