Network Security Monitoring with the Bro Platform

Adam Slagell
National Center for Supercomputing Applications

Content borrowed from Robin Sommer
International Computer Science Institute
“What Is Bro?”
“What Is Bro?”

Packet Capture
“What Is Bro?”

Packet Capture

Traffic Inspection
“What Is Bro?”

- Packet Capture
- Traffic Inspection
- Attack Detection
“What Is Bro?”

- Packet Capture
- Traffic Inspection
- Attack Detection
- Log Recording
“What Is Bro?”

- Packet Capture
- Traffic Inspection
- Attack Detection
- Log Recording
- Flexibility
- Abstraction
- Data Structures

Network Security Monitoring with the Bro Platform
“What Is Bro?”

- Packet Capture
- Traffic Inspection
- Attack Detection
- Log Recording
- Flexibility
- Abstraction
- Data Structures

Network Security Monitoring with the Bro Platform
“What Is Bro?”

- Packet Capture
- Traffic Inspection
- Attack Detection
- Log Recording
- Flexibility
- Abstraction
- Data Structures
“What Is Bro?”

Packet Capture
Traffic Inspection
Attack Detection
Log Recording
Flexibility
Abstraction
Data Structures

“Domain-specific Python”
Bro History

1995

Vern writes 1st line of code
Network Security Monitoring with the Bro Platform

Bro History

- **1995**: Vern writes 1st line of code
- **1996**: LBNL starts using Bro operationally
- **1997**: 1st CHANGES entry
- **1996**: v0.2
- **1998**: v0.4
- **1999**: v0.6
- **2000**: v0.7a90
- **2001**: v0.7a175/0.8aX
- **2002**: v0.7a48
- **2003**: v0.8a37
- **2004**: v0.8aX/0.9aX
- **2005**: v1.0
- **2006**: v1.1/v1.2
- **2007**: v1.3
- **2008**: v1.4
- **2009**: v1.5
- **2010**: v2.0
- **2011**: v2.1
- **2012**: v2.2
- **2013**: v2.3
- **2014**: v2.4
- **2015**: v2.5
- **2016**: v2.6

**Bro Lite**: Deprecated

**Bro Center**: New Analyzers

**Bro SDCI**: IPv6

**v2.4 Broker**: Input Framew.

**v2.5/2.6**: New Scripts

**v2.2 Summary Stat.**
Bro History

- **1995**: Vern writes 1st line of code
- **1996**: LBNL starts using Bro operationally
- **2001**: 1st CHANGES entry
- **2002**: v0.6 RegExps Login analysis
- **2003**: v0.7a90 Profiling State Mgmt
- **2004**: v0.8aX/0.9aX SSL/SMB STABLE releases BroLite
- **2005**: v0.1/v1.2 when Stmt Resource tuning Brocoli DPD
- **2006**: v1.0 BinPAC IRC/RPC analyzers 64-bit support Sane version numbers
- **2007**: v1.1 BroControl New Scripts
- **2008**: v1.4 BinPAC HTTP/BitTorrent
- **2009**: v1.5 BroSDC HTTP entities
- **2010**: 0.8a37 Consistent CHANGES
- **2011**: 0.8a37 Communication Persistence Namespaces Log Rotation
- **2012**: NetFlow
- **2013**: v2.0 File Analysis Summary Stat.
- **2014**: v2.3 New Analyzers
- **2015**: v2.4 Brocker
- **2016**: v2.5 IPv6 Input Framew.
Bro History

Beyond Pattern Matching: A Concurrency Model for Stateful Deep Packet Inspection

Count Me In: Viable Distributed Summary Statistics For Securing High-Speed Networks

Academic Publications

v2.0
v2.1
v2.2
v2.3
v2.4
v1.5
v1.4
v1.3
v1.2
v1.1
v0.9a
v0.8a
v0.7a
v0.6
v0.4
v0.2
Vern writes 1st line of code
LBNL starts using Bro operationally

Network Security Monitoring with the Bro Platform
“Who’s Using It?”

Installations across the Country

- Universities
- Research Labs
- Supercomputing Centers
- Government Organizations
- Fortune 20 Enterprises

Community

- 50/90/150/180 attendees at BroCon ’12/’13/’14/’15
- 110 organizations at BroCon ’15
- 4,500 Twitter followers
- 1,000 mailing list subscribers
- 100 users average on IRC channel
- 10,000 direct downloads / version from 150 countries

Fully integrated into Security Onion

Popular security-oriented Linux distribution

[Image of BroCon 2015, MIT]
Architecture

Network

Packets
Network Security Monitoring with the Bro Platform

Architecture

- Network
  - Packets
  - Protocol Decoding
    - Events
  - Event Engine
Network Security Monitoring with the Bro Platform

Architecture

- Network
- Protocol Decoding
  - Network
- Event Engine
  - Events
  - Notification
  - Logs
- Policy Script Interpreter
  - Events
- Analysis Logic
  - Logs
  - Notification
Network Security Monitoring with the Bro Platform

Architecture

- **Network**
  - **Packets** → **Event Engine**
  - **Analysis Logic**
    - **Protocol Decoding**
      - **Packets** → **Event Engine**
    - **Policy Script Interpreter**
      - **Events** → **Event Engine**
      - **Logs** → **Notification**
      - **User Interface**

"User Interface"
“What Can It Do?”

Log Files  Alerts  Custom Logic
“What Can It Do?”

- **Log Files**
- **Alerts**
- **Custom Logic**

“Network Ground Truth”
Bro’s Log Files

Rich, structured, real-time activity streams.
> bro -i eth0
[ ... wait ... ]
> bro -i eth0
[ ... wait ... ]
> ls *.log

app_stats.log  irc.log  socks.log
communication.log known_certs.log software.log
cconn.log  known_hosts.log  ssh.log
dhcp.log  known_services.log  ssl.log
dns.log  modbus.log  syslog.log
dpd.log  notice.log  traceroute.log
files.log  reporter.log  tunnel.log
ftp.log  signatures.log  weird.log
http.log  smtp.log
> bro -i eth0
[ ... wait ... ]
> cat conn.log

#separator \x09
#set_separator ,
#empty_field  (empty)
#unset_field -
#path  conn
#open  2013-04-28-23-47-26

| ts         | uid         | id.orig_h   | id.orig_p | id.resp_h | [...]
|------------|-------------|-------------|-----------|-----------|--------
| 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 | 50Knoww6x14 | 192.168.1.104 | 137       | 192.168.1.255 | [...]
| 1258531747.077012 | FrJEywHcSal | 192.168.1.104 | 138       | 192.168.1.255 | [...]
| 1258531924.321413 | 3PKsZ2Uye21 | 192.168.1.103 | 68        | 192.168.1.1 | [...]

[...]

Network Security Monitoring with the Bro Platform
## Connections Logs

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts</td>
<td>1393099191.817686</td>
</tr>
<tr>
<td>uid</td>
<td>Cy3S2U2sbarorQgmw6a</td>
</tr>
<tr>
<td>id.orig_h</td>
<td>177.22.211.144</td>
</tr>
<tr>
<td>id.orig_p</td>
<td>43618</td>
</tr>
<tr>
<td>id.resp_h</td>
<td>115.25.19.26</td>
</tr>
<tr>
<td>id.resp_p</td>
<td>25</td>
</tr>
<tr>
<td>proto</td>
<td>tcp</td>
</tr>
<tr>
<td>service</td>
<td>smtp</td>
</tr>
<tr>
<td>duration</td>
<td>1.414936</td>
</tr>
<tr>
<td>orig_bytes</td>
<td>9068</td>
</tr>
<tr>
<td>resp_bytes</td>
<td>4450</td>
</tr>
<tr>
<td>conn_state</td>
<td>SF</td>
</tr>
<tr>
<td>local_orig</td>
<td>T</td>
</tr>
<tr>
<td>missed_bytes</td>
<td>0</td>
</tr>
<tr>
<td>history</td>
<td>ShAdDaFf</td>
</tr>
<tr>
<td>tunnel_parents</td>
<td>(empty)</td>
</tr>
</tbody>
</table>
### HTTP

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts</td>
<td>1393099291.589208</td>
</tr>
<tr>
<td>uid</td>
<td>CKFUW73bIADw0r9p1</td>
</tr>
<tr>
<td>id.orig_h</td>
<td>17.22.7.4</td>
</tr>
<tr>
<td>id.orig_p</td>
<td>54352</td>
</tr>
<tr>
<td>id.resp_h</td>
<td>24.26.13.36</td>
</tr>
<tr>
<td>id.resp_p</td>
<td>80</td>
</tr>
<tr>
<td>method</td>
<td>POST</td>
</tr>
<tr>
<td>host</td>
<td>com-services.pandonetworks.com</td>
</tr>
<tr>
<td>uri</td>
<td>/soapservices/services/SessionStart</td>
</tr>
<tr>
<td>referrer</td>
<td>-</td>
</tr>
<tr>
<td>user_agent</td>
<td>Mozilla/4.0 (Windows; U) Pando/2.6.0.8</td>
</tr>
<tr>
<td>status_code</td>
<td>200</td>
</tr>
<tr>
<td>username</td>
<td>anonymous</td>
</tr>
<tr>
<td>password</td>
<td>-</td>
</tr>
<tr>
<td>orig_mime_types</td>
<td>application/xml</td>
</tr>
<tr>
<td>resp_mime_types</td>
<td>application/xml</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>ts</td>
<td>1392805957.927087</td>
</tr>
<tr>
<td>uid</td>
<td>CEA0512D7k0BD9Dda2</td>
</tr>
<tr>
<td>id.orig_h</td>
<td>2a07:f2c0:90:402:41e:c13:6cb:99c</td>
</tr>
<tr>
<td>id.orig_p</td>
<td>40475</td>
</tr>
<tr>
<td>id.resp_h</td>
<td>2406:fe60:f47::aaeb:98c</td>
</tr>
<tr>
<td>id.resp_p</td>
<td>443</td>
</tr>
<tr>
<td>version</td>
<td>TLSv10</td>
</tr>
<tr>
<td>cipher</td>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>server_name</td>
<td><a href="http://www.netflix.com">www.netflix.com</a></td>
</tr>
<tr>
<td>subject</td>
<td>CN=www.netflix.com,OU=Operations, O=Netflix, Inc.,L=Los Gatos, ST=CALIFORNIA,C=US</td>
</tr>
<tr>
<td>issuer_subject</td>
<td>CN=VeriSign Class 3 Secure Server CA, OU=VeriSign Trust Network,O=VeriSign, C=US</td>
</tr>
<tr>
<td>not_valid_before</td>
<td>1389859200.000000</td>
</tr>
<tr>
<td>not_valid_after</td>
<td>1452931199.000000</td>
</tr>
<tr>
<td>client_subject</td>
<td>-</td>
</tr>
<tr>
<td>client_issuer_subject</td>
<td>-</td>
</tr>
<tr>
<td>cert_hash</td>
<td>197cab7c6c92a0b9ac5f37cfe0699268</td>
</tr>
<tr>
<td>validation_status</td>
<td>ok</td>
</tr>
</tbody>
</table>
### Syslog & DHCP

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts</td>
<td>1392796803.311801</td>
</tr>
<tr>
<td>uid</td>
<td>CnYivt3ZONH0uBALR8</td>
</tr>
<tr>
<td>id.orig_h</td>
<td>12.3.8.161</td>
</tr>
<tr>
<td>id.orig_p</td>
<td>514</td>
</tr>
<tr>
<td>id.resp_h</td>
<td>16.74.12.24</td>
</tr>
<tr>
<td>id.resp_p</td>
<td>514</td>
</tr>
<tr>
<td>proto</td>
<td>udp</td>
</tr>
<tr>
<td>facility</td>
<td>AUTHPRIV</td>
</tr>
<tr>
<td>severity</td>
<td>INFO</td>
</tr>
<tr>
<td>message</td>
<td>sshd[13825]: Accepted publickey for harvest from xxx.xxx.xxx.xxx</td>
</tr>
</tbody>
</table>
### Syslog & DHCP

#### syslog.log

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts</td>
<td>1392796803.311801</td>
</tr>
<tr>
<td>uid</td>
<td>CnYivt3Z0NHoUBALR8</td>
</tr>
<tr>
<td>id.orig_h</td>
<td>12.3.8.161</td>
</tr>
<tr>
<td>id.orig_p</td>
<td>514</td>
</tr>
<tr>
<td>id.resp_h</td>
<td>16.74.12.24</td>
</tr>
<tr>
<td>id.resp_p</td>
<td>514</td>
</tr>
<tr>
<td>proto</td>
<td>udp</td>
</tr>
<tr>
<td>facility</td>
<td>AUTHPRIV</td>
</tr>
<tr>
<td>severity</td>
<td>INFO</td>
</tr>
<tr>
<td>message</td>
<td>sshd[13825]: Accepted publickey for harvest from xxx.xxx.xxx.xxx</td>
</tr>
</tbody>
</table>

#### dhcp.log

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts</td>
<td>1392796962.091566</td>
</tr>
<tr>
<td>uid</td>
<td>Ci3RM24iF4vIYRGHc3</td>
</tr>
<tr>
<td>id.orig_h</td>
<td>10.129.5.11</td>
</tr>
<tr>
<td>id.resp_h</td>
<td>10.129.5.1</td>
</tr>
<tr>
<td>mac</td>
<td>04:12:38:65:fa:68</td>
</tr>
<tr>
<td>assigned_ip</td>
<td>10.129.5.11</td>
</tr>
<tr>
<td>lease_time</td>
<td>14400.000000</td>
</tr>
</tbody>
</table>
## Files

**files.log**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts</td>
<td>1392797643.447056</td>
</tr>
<tr>
<td>fuid</td>
<td>FnungO3TI19GahPJP2</td>
</tr>
<tr>
<td>tx_hosts</td>
<td>191.168.187.33</td>
</tr>
<tr>
<td>rx_hosts</td>
<td>10.1.29.110</td>
</tr>
<tr>
<td>conn_uids</td>
<td>CbDgik2fjeKL5qzn55</td>
</tr>
<tr>
<td>source</td>
<td>SMTP</td>
</tr>
<tr>
<td>analyzers</td>
<td>SHA1,MD5</td>
</tr>
<tr>
<td>mime_type</td>
<td>application/x-dosexec</td>
</tr>
<tr>
<td>filename</td>
<td>Letter.exe</td>
</tr>
<tr>
<td>duration</td>
<td>5.320822</td>
</tr>
<tr>
<td>local_orig</td>
<td>T</td>
</tr>
<tr>
<td>seen_bytes</td>
<td>39508</td>
</tr>
<tr>
<td>md5</td>
<td>93f7f5e7a2096927e06e[...]1085bfcfb</td>
</tr>
<tr>
<td>sha1</td>
<td>daed94a5662a920041be[...]a433e501646ef6a03</td>
</tr>
<tr>
<td>extracted</td>
<td>-</td>
</tr>
</tbody>
</table>
## Software

<table>
<thead>
<tr>
<th><strong>software.log</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ts</strong></td>
</tr>
<tr>
<td><strong>host</strong></td>
</tr>
<tr>
<td><strong>host_p</strong></td>
</tr>
<tr>
<td><strong>software_type</strong></td>
</tr>
<tr>
<td><strong>name</strong></td>
</tr>
<tr>
<td><strong>version.major</strong></td>
</tr>
<tr>
<td><strong>version.minor</strong></td>
</tr>
<tr>
<td><strong>version.minor2</strong></td>
</tr>
<tr>
<td><strong>version.minor3</strong></td>
</tr>
<tr>
<td><strong>version.addl</strong></td>
</tr>
<tr>
<td><strong>unparsed_version</strong></td>
</tr>
</tbody>
</table>
Help Understand Your Network (2)

Top Software by Number of Hosts

- Firefox
- MSIE
- CaptiveNetworkSupport
- Safari
- DropboxDesktopClient
- ocspd
- GoogleUpdate
- Windows-Update-Agent
- Chrome
- Microsoft-CryptoAPI

```
cat software.log | bro-cut host name | sort | uniq |
awk -F \t '{print $2}' | sort | uniq -c | sort -rn
```
“What Can It Do?”

- Log Files
- Alerts
- Custom Logic
“What Can It Do?”

Log Files

Alerts

Custom Logic

“Watch this!”

Recorded in notice.log.
Can trigger actions.
Alerts in Bro 2.2

<table>
<thead>
<tr>
<th>CaptureLoss::Too_Much_Loss</th>
<th>SSH::Password_Guessing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conn::Ack_Above_Hole</td>
<td>SSH::Watched_Country_Login</td>
</tr>
<tr>
<td>Conn::Content_Gap</td>
<td>SSL::Certificate_Expired</td>
</tr>
<tr>
<td>Conn::Retransmission_Inconsistency</td>
<td>SSL::CertificateExpires_Soon</td>
</tr>
<tr>
<td>DNS::External_Name</td>
<td>SSL::Certificate_Not_Valid_Yet</td>
</tr>
<tr>
<td>FTP::Bruteforcing</td>
<td>SSL::Invalid_Server_Cert</td>
</tr>
<tr>
<td>FTP::Site_Exec_Success</td>
<td>Scan::Address_Scan</td>
</tr>
<tr>
<td>HTTP::SQL_Injection_Attacker</td>
<td>Scan::Port_Scan</td>
</tr>
<tr>
<td>HTTP::SQL_Injection_Victim</td>
<td>Signatures::Count_Signature</td>
</tr>
<tr>
<td>Intel::Notice</td>
<td>Signatures::Multiple_Sig_Responders</td>
</tr>
<tr>
<td>PacketFilter::Dropped_Packets</td>
<td>Signatures::Multiple_Signatures</td>
</tr>
<tr>
<td>ProtocolDetector::Protocol_Found</td>
<td>Signatures::Sensitive_Signature</td>
</tr>
<tr>
<td>ProtocolDetector::Server_Found</td>
<td>Software::Software_Version_Change</td>
</tr>
<tr>
<td>SMTP::Blocklist_Blocked_Host</td>
<td>Software::Vulnerable_Version</td>
</tr>
<tr>
<td>SMTP::Blocklist_Error_Message</td>
<td>TeamCymruMalwareHashRegistry::Match</td>
</tr>
<tr>
<td>SMTP::Suspicious_Origination</td>
<td>Traceroute::Detected</td>
</tr>
<tr>
<td>SSH::Interesting_Hostname_Login</td>
<td>Weird::Activity</td>
</tr>
<tr>
<td>SSH::Login_By_Password_Guesser</td>
<td></td>
</tr>
</tbody>
</table>
Watching for Suspicous Logins
Watching for Suspicious Logins

SSH::Watched_Country_Login

Login from an unexpected country.
Watching for Suspicious Logins

**SSH::Watched_Country_Login**
Login from an unexpected country.

**SSH::Interesting_Hostname_Login**
Login from an unusual host name.

smtp.supercomputer.edu
Intelligence Integration (Passive)
Intelligence Integration (Passive)

Intelligence
- IP addresses
- DNS names
- URLs
- File hashes

Traffic Monitoring
- HTTP, FTP, SSL, SSH, FTP, DNS, SMTP, …

Feeds
- CIF
- JC3
- Spamhaus
- Custom/Proprietary
Network Security Monitoring with the Bro Platform

Intelligence Integration (Passive)

Internet

Traffic Monitoring

Enterprise Network

Intelligence

- IP addresses
- DNS names
- URLs
- File hashes

Feeds

- CIF
- JC3
- Spamhaus
- Custom/Proprietary

<table>
<thead>
<tr>
<th>ts</th>
<th>1258565309.806483</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>CAK677xaOmi66X4Th</td>
</tr>
<tr>
<td>id.orig_h</td>
<td>192.168.1.103</td>
</tr>
<tr>
<td>id.resp_h</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>note</td>
<td>Intel::Notice</td>
</tr>
<tr>
<td>indicator</td>
<td>baddomain.com</td>
</tr>
<tr>
<td>indicator_type</td>
<td>Intel::DOMAIN</td>
</tr>
<tr>
<td>where</td>
<td>HTTP::IN_HOST_HEADER</td>
</tr>
<tr>
<td>source</td>
<td>My-Private-Feed</td>
</tr>
</tbody>
</table>

Intelligence

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

Traffic Monitoring

HTTP, FTP, SSL, SSH, FTP,
DNS, SMTP,…

Notice.log
### Intelligence Integration (Passive)

**Internet**  
➡️  
**Enterprise Network**

### Traffic Monitoring

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

<table>
<thead>
<tr>
<th>ts</th>
<th>1258565309.806483</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>CAK677xaOmi66X4Th</td>
</tr>
<tr>
<td>id.orig_h</td>
<td>192.168.1.103</td>
</tr>
<tr>
<td>id.resp_h</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>note</td>
<td>Intel::Notice</td>
</tr>
<tr>
<td>indicator</td>
<td>baddomain.com</td>
</tr>
<tr>
<td>indicator_type</td>
<td>Intel::DOMAIN</td>
</tr>
<tr>
<td>where</td>
<td>HTTP::IN_HOST_HEADER</td>
</tr>
<tr>
<td>source</td>
<td>My-Private-Feed</td>
</tr>
</tbody>
</table>
Intelligence Integration (Active)
# cat files.log | bro-cut mime_type sha1 | awk '$1 ~ /x-dosexec/'

<table>
<thead>
<tr>
<th>mime_type</th>
<th>sha1</th>
</tr>
</thead>
<tbody>
<tr>
<td>application/x-dosexec</td>
<td>5fd2f37735953427e2f6c593d6ec7ae882c9ab54</td>
</tr>
<tr>
<td>application/x-dosexec</td>
<td>00c69013d34601c2174b72c9249a0063959da93a</td>
</tr>
<tr>
<td>application/x-dosexec</td>
<td>0d801726d49377bfe989dcca7753a62549f1ddda</td>
</tr>
</tbody>
</table>

[...]

Intelligence Integration (Active)
Intelligence Integration (Active)

```bash
# cat files.log | bro-cut mime_type sha1 | awk '$1 ~ /x-dosexec/'
application/x-dosexec   5fd2f37735953427e2f6c593d6ec7ae882c9ab54
application/x-dosexec   00c69013d34601c2174b72c9249a0063959da93a
application/x-dosexec   0d801726d49377bfe989dcca7753a62549f1ddda
[...]  

# dig +short 733a48a9cb4[...]2a91e8d00.malware.hash.cymru.com TXT
"1221154281 53"
```
Intelligence Integration (Active)

```
# cat files.log | bro-cut mime_type sha1 | awk '$1 ~ /x-doseexec/
application/x-doseexec 5fd2f37735953427e2f6c593d6ec7ae882c9ab54
application/x-doseexec 00c69013d34601c2174b72c9249a0063959da93a
application/x-doseexec 0d801726d49377bfe989dcca775a62549f1ddda
[...]

# dig +short 733a48a9cb4[...]2a91e8d00.malware.hash.cymru.com TXT
"1221154281 53"
```

**notice.log**

<table>
<thead>
<tr>
<th>ts</th>
<th>1392423980.736470</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>CjKeSB45xa0mIo4Th</td>
<td>Connection ID</td>
</tr>
<tr>
<td>id.orig_h</td>
<td>10.2.55.3</td>
<td>Originator IP</td>
</tr>
<tr>
<td>id.resp_h</td>
<td>192.168.34.12</td>
<td>Responder IP</td>
</tr>
<tr>
<td>fuid</td>
<td>FEGVbAgcArRQ49347</td>
<td>File ID</td>
</tr>
<tr>
<td>mime_type</td>
<td>application/jar</td>
<td>MIME type</td>
</tr>
<tr>
<td>description</td>
<td><a href="http://app.looking3g.com/%5B%E2%80%A6">http://app.looking3g.com/[…</a>]</td>
<td>Source URL Bro saw</td>
</tr>
<tr>
<td>note</td>
<td>TeamCymruMalwareHashRegistry::Match</td>
<td>Notice Type</td>
</tr>
<tr>
<td>msg</td>
<td>2013-09-14 22:06:51 / 20%</td>
<td>MHR reply</td>
</tr>
<tr>
<td>sub</td>
<td><a href="https://www.virustotal.com/%5B%E2%80%A6">https://www.virustotal.com/[…</a>]</td>
<td>VirusTotal URL</td>
</tr>
</tbody>
</table>
“What Can It Do?”

Log Files

Alerts

Custom Logic
“What Can It Do?”

Log Files

Alerts

Custom Logic

“Scripts are Bro’s magic ingredient.”
Script Example: Matching URLs

Task: Report all Web requests for files called “passwd”.
Task: Report all Web requests for files called “passwd”.

```plaintext
event http_request(c: connection, 
    method: string,        # HTTP method.
    original_URI: string,  # Requested URL.
    unescaped_URI: string, # Decoded URL.
    version: string)       # HTTP version.
{
    if ( method == "GET" && unescaped_URI == /.*passwd/ )
    NOTICE(...); # Alarm.
}
```
Task: Count failed connection attempts per source address.
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.
}
Bro Ecosystem

Relationship Status:
It’s complicated
Bro Ecosystem

Internet -> Tap -> Internal Network

Bro
Bro Ecosystem

Internet  Tap  Internal Network

Bro  Control  Output

BroControl  User Interface

Network Security Monitoring with the Bro Platform
Bro Ecosystem

Internet \(\rightarrow\) Tap \(\rightarrow\) Internal Network

<table>
<thead>
<tr>
<th>External Scripts</th>
<th>Functionality</th>
<th>Bro</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>BroControl</th>
<th>Control</th>
<th>Output</th>
</tr>
</thead>
</table>

User Interface

Network Security Monitoring with the Bro Platform
Bro Ecosystem

Internet → Tap

Tap → Bro

Bro → Internal Network

Bro → External Scripts

External Scripts → Functionality

Functionality → Bro

Bro → Other Bros

Other Bros → Events

Events → State

State → Bro

Bro → BroControl

BroControl → Control

Control → Output

Output → User Interface

User Interface → BroControl

BroControl → Bro

Bro → BroControl

Bro → Internet

Bro → Internal Network
Bro Ecosystem

- Internet
- Internal Network
- Bro
- External Scripts
- Other Bros
- BroControl
- Broccoli
- Control
- Output
- Events
- State
- User Interface
- Functionality

Tap

Bro Client Communication Library

Network Security Monitoring with the Bro Platform
Network Security Monitoring with the Bro Platform
Bro Ecosystem

Internet — Tap — Internal Network

- External Scripts
  - Functionality
  - Control
  - Output

- Bro
  - Network Control
  - Events
  - State

- BroControl
  - User Interface

- Other Bros
  - Events

- Broccoli
  - Broccoli Ruby
  - Broccoli Python
  - (Broccoli Perl)

Bro Client Communication Library

Network Security Monitoring with the Bro Platform
Bro Ecosystem

- Internet
- Internal Network
- Bro
- External Scripts
- BroControl
  - User Interface
  - Control
  - Output
- Other Bros
  - Events
  - State
- Broccoli
  - Broccoli Ruby
  - Broccoli Python
  - Broccoli Perl
- Network Control
- Time Machine
- Functions
Bro Ecosystem

- **Internet**
- **Internal Network**
- **Tap**
- **Time Machine**
- **External Scripts**
  - Bro-aux
  - BinPAC
  - capstats
  - BTest
  - trace-summary
  - bro-out
- **Functionality**
- **Control**
- **Output**
- **Network Control**
- **Events**
  - State
  - Other Bros
  - Events
  - Bro Client Communication Library
  - Broccoli Ruby
  - Broccoli Python
  - (Broccoli Perl)
- **User Interface**
- **BroControl**
- **Bro**
Network Security Monitoring with the Bro Platform

**Bro Ecosystem**

- **Bro Distribution**
  - `bro-2.3.tar.gz`

- **Internal Network**

- **External Scripts**
  - `bro-aux`
  - `BinPAC`
  - `capstats`
  - `BTest`
  - `trace-summary`
  - `bro-cut`

- **Functionality**

- **BroControl**

- **Output**

- **Control**

- **User Interface**

- **Events**

- **Events State**

- **Broccoli**
  - `Broccoli Python`
  - `Broccoli Ruby`
  - `(Broccoli Perl)`

- **Bro Client Communication Library**

- **Other Bros**

- **Time Machine**

- **Network Control**

- **Network Security Monitoring with the Bro Platform**

25
Bro Cluster Ecosystem

Internet → Tap → Internal Network

External Scripts → Bro → BroControl → Broccoli

Functionality → Control → Output

BroClient Communication Library

Broccoli Ruby
Broccoli Python
(Broccoli Perl)

Events State

External Bro → Events

User Interface → BroControl

Network Security Monitoring with the Bro Platform
Network Security Monitoring with the Bro Platform

Bro Cluster Ecosystem

- Internet
- Internal Network
- External Scripts
- External Bro
- Broccoli
  - Broccoli Ruby
  - Broccoli Python
  - (Broccoli Perl)

Bro Client Communication Library

Tap
Network Security Monitoring with the Bro Platform
Bro Cluster Ecosystem
Bro Cluster Ecosystem

- Internet
- Internal Network
- Bro
- Bro
- Bro
- Bro
- Load-Balancer
- External Scripts
- BroControl
- Output
- Broccoli
  - Broccoli Ruby
  - Broccoli Python
  - (Broccoli Perl)
- BroClient Communication Library
- Tap
- External Bro
- Control
- Packets
- User Interface
- BroControl
- BroControl
- Output
- BroControl
- BroControl
- BroControl
- BroControl
- BroControl
Network Security Monitoring with the Bro Platform

Bro Cluster Ecosystem

- Internet
- Internal Network
- Load-Balancer
  - "Frontend"
  - "Workers"
  - "Manager"
- Bro
- External Scripts
- Broccoli Ruby
- Broccoli Python
- Broccoli Perl
- External Bro
- BroControl
- User Interface
- Control
- Output
- Bro Client Communication Library
  - Broccoli Python
  - Broccoli Ruby
  - (Broccoli Perl)
Foundation: Broker

Bro’s new unified communication library.
Foundation: Broker

Bro’s new unified communication library.

- Log forwarding.
- Event exchange.
- Global key/value stores.
- Publish/subscribe.
- APIs for Bro, C++, C, Python.
- BSD license.

http://github.com/bro/broker
Global Coordination with Broker

Network Security Monitoring with the Bro Platform
Global Coordination with Broker

Global state through persistent data stores.
Global Coordination with Broker

Global state through persistent data stores.

Global correlation through message passing.
Integrating Host Monitoring

Leverage control over end hosts.
Integrating Host Monitoring

Leverage control over end hosts.

Diagram:

- Bro
  - Bro
    - Bro
      - Host
    - Bro
      - Host
  - Bro
  - Bro
  - Bro
  - Bro
Integrating Host Monitoring

Leverage control over end hosts.

https://osquery.io
Integrating Host Monitoring

```plaintext
#fields t       host  pid    path          uid    gid    argv
1453849601.880629 127.0.0.1 40136 /usr/bin/git  10000  10000  git diff --no-ext-diff --quiet --exit-code
1453849643.924678 127.0.0.1 40397 /usr/bin/git  10000  10000  git push
1453849643.924678 127.0.0.1 40404 /usr/bin/ssh  10000  10000  ssh git@github.com git-receive-pack '/bro-osquery'
```

https://osquery.io
From Passive to Active

Bro is not an inline solution.
But it can still talk to your network.
From Passive to Active

Bro is not an inline solution.
But it can still talk to your network.

Examples
Shunting
Dynamic Firewall
Cluster with Shunting
Cluster with Shunting

Internet

100G

Border

100G

Load-balancer

10G 10G 10G 10G

LAN

10G

Bro Cluster
Cluster with Shunting

Network Security Monitoring with the Bro Platform
Shunting for Supercomputers
Shunting for Supercomputers

Source: Lawrence Berkeley National Laboratory
Shunting for Supercomputers

![Graph showing network traffic over time with peaks on specific dates.](image-url)
Cluster with Dynamic Firewall

Internet

100G

Border Gateway

100G

LAN

Load-balancer

10G 10G 10G 10G

Bro Cluster

Network Security Monitoring with the Bro Platform
Cluster with Dynamic Firewall

- Internet
- LAN
- Load-balancer
- Bro Cluster
- Border Gateway
- API

100G
10G
10G
10G
10G
100G
10G
100G
10G

“Block it!”

Blocking
Dynamic Firewall Example

Managing 1000s of blocks with “catch & release”.
Dynamic Firewall Example

Managing 1000s of blocks with "catch & release".

Source: Indiana University
Foundation: Bro’s NetControl Framework

High-level script API to talk to network equipment.
Foundation: Bro’s NetControl Framework

High-level script API to talk to network equipment.

- drop_connection (connection, timeout)
- drop_address (host, timeout)
- shunt_flow (flow, timeout)
- redirect (flow, port, timeout)

https://github.com/bro/bro-netcontrol
Foundation: Bro’s NetControl Framework

High-level script API to talk to network equipment.

- `drop_connection (connection, timeout)`
- `drop_address (host, timeout)`
- `shunt_flow (flow, timeout)`
- `redirect (flow, port, timeout)`

Current Backends

OpenFlow, iptables, acld.

https://github.com/bro/bro-netcontrol
Bro is ... a Platform

There’s much more we can talk about ...

- Host-level integration
- Data import and export
- Automatic Reaction
- Monitoring Internal Networks
- Measurements
- SDN integration
- Industrial Control Systems
- Embedded Devices
- Current Research
- More File Analysis

- More Protocols
- More File Analysis
- 100Gb/s Networks
- Enterprise Protocols
- Summary Statistics
- Science DMZs
- ICSL SSL Notary
- Cluster Deployment
The U.S. National Science Foundation has enabled much of Bro.

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

The Bro Project is a member of Software Freedom Conservancy.

Software Freedom Conservancy, Inc. is a 501(c)(3) not-for-profit organization that helps promote, improve, develop, and defend Free, Libre, and Open Source Software projects.

The Bro Project

www.bro.org
info@bro.org
@Bro_IDS
The NSF Bro Center of Expertise

We are there to help you!

http://nsf.bro.org   mailto:nsf@bro.org