The Bro Monitoring Platform

Robin Sommer
International Computer Science Institute, &
Lawrence Berkeley National Laboratory

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

The Bro Monitoring 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

The Bro Monitoring Platform
“What Is Bro?”

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

The Bro Monitoring Platform
“What Is Bro?”

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

“Domain-specific Python”
The Bro Monitoring Platform

Network

Tap
The Bro Monitoring Platform

Platform

Programming Language

Standard Library

Packet Processing

Tap

Network
The Bro Monitoring Platform

Apps
- Intrusion Detection
- Vulnerability Mgmt
- File Analysis
- Traffic Measurement
- Traffic Control
- Compliance Monitoring

Platform
- Programming Language
- Standard Library
- Packet Processing

Tap
Network
The Bro Monitoring Platform

Open Source
BSD License

Apps
- Intrusion Detection
- Vulnerability Mgmt
- File Analysis
- Traffic Measurement
- Traffic Control
- Compliance Monitoring

Platform
- Programming Language
- Standard Library
- Packet Processing

Tap
- Network

The Bro Monitoring Platform
“Who’s Using It?”

Installations across the US
Universities
Research Labs
Supercomputing Centers
Government Organizations
Fortune 50 Enterprises

Examples
Lawrence Berkeley National Lab
National Center for Supercomputing Applications
Indiana University
Carnegie Mellon
National Center for Atmospheric Research

... and many more sites I can’t talk about.

Fully integrated into Security Onion
Popular security-oriented Linux distribution

Community
50/90/150 attendees at BroCon ’12/’13/’14
60 organizations at BroCon ‘14
2,500 Twitter followers
800 mailing list subscribers
70 users average on IRC channel
10,000 downloads / version
from 150 countries
> 30,000 Onion downloads (’12)
“What Can It Do?”

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

Log Files

Alerts

Custom Logic

“Network Ground Truth”
> bro -i eth0
[ ... wait ... ]
Bro Logs

> bro -i eth0
[ … wait … ]
> ls *.log

<table>
<thead>
<tr>
<th>log file</th>
<th>log file</th>
<th>log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>app_stats.log</td>
<td>irc.log</td>
<td>socks.log</td>
</tr>
<tr>
<td>communication.log</td>
<td>known_cert.log</td>
<td>software.log</td>
</tr>
<tr>
<td>conn.log</td>
<td>known_host.log</td>
<td>ssh.log</td>
</tr>
<tr>
<td>dhcp.log</td>
<td>known_service.log</td>
<td>ssl.log</td>
</tr>
<tr>
<td>dns.log</td>
<td>modbus.log</td>
<td>syslog.log</td>
</tr>
<tr>
<td>dpd.log</td>
<td>notice.log</td>
<td>traceroute.log</td>
</tr>
<tr>
<td>files.log</td>
<td>reporter.log</td>
<td>tunnel.log</td>
</tr>
<tr>
<td>ftp.log</td>
<td>signatures.log</td>
<td>weird.log</td>
</tr>
<tr>
<td>http.log</td>
<td>smtp.log</td>
<td></td>
</tr>
</tbody>
</table>

The Bro Monitoring Platform
The Bro Monitoring Platform

Bro Logs

```bash
> 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
#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  5OKnoww6x14  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   [...]
-haired]
```

[...]
## Connections Logs

### conn.log

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts</td>
<td>1393099191.817686</td>
<td>Timestamp</td>
</tr>
<tr>
<td>uid</td>
<td>Cy3S2U2sbarorQgmw6a</td>
<td>Unique ID</td>
</tr>
<tr>
<td>id.orig_h</td>
<td>177.22.211.144</td>
<td>Originator IP</td>
</tr>
<tr>
<td>id.orig_p</td>
<td>43618</td>
<td>Originator Port</td>
</tr>
<tr>
<td>id.resp_h</td>
<td>115.25.19.26</td>
<td>Responder IP</td>
</tr>
<tr>
<td>id.resp_p</td>
<td>25</td>
<td>Responder Port</td>
</tr>
<tr>
<td>proto</td>
<td>tcp</td>
<td>IP Protocol</td>
</tr>
<tr>
<td>service</td>
<td>smtp</td>
<td>App-layer Protocol</td>
</tr>
<tr>
<td>duration</td>
<td>1.414936</td>
<td>Duration</td>
</tr>
<tr>
<td>orig_bytes</td>
<td>9068</td>
<td>Bytes by Originator</td>
</tr>
<tr>
<td>resp_bytes</td>
<td>4450</td>
<td>Bytes by Responder</td>
</tr>
<tr>
<td>conn_state</td>
<td>SF</td>
<td>TCP state</td>
</tr>
<tr>
<td>local_orig</td>
<td>T</td>
<td>Local Originator?</td>
</tr>
<tr>
<td>missed_bytes</td>
<td>0</td>
<td>Gaps</td>
</tr>
<tr>
<td>history</td>
<td>ShAdDaFf</td>
<td>State History</td>
</tr>
<tr>
<td>tunnel_parents</td>
<td>(empty)</td>
<td>Outer Tunnels</td>
</tr>
<tr>
<td>Key</td>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>ts</td>
<td>1393099291.589208</td>
<td></td>
</tr>
<tr>
<td>uid</td>
<td>CKFUW73bIADw0r9pl</td>
<td></td>
</tr>
<tr>
<td>id.orig_h</td>
<td>17.22.7.4</td>
<td></td>
</tr>
<tr>
<td>id.orig_p</td>
<td>54352</td>
<td></td>
</tr>
<tr>
<td>id.resp_h</td>
<td>24.26.13.36</td>
<td></td>
</tr>
<tr>
<td>id.resp_p</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>method</td>
<td>POST</td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>com-services.pandonetworks.com</td>
<td></td>
</tr>
<tr>
<td>uri</td>
<td>/soapservices/services/SessionStart</td>
<td></td>
</tr>
<tr>
<td>referrer</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>user_agent</td>
<td>Mozilla/4.0 (Windows; U) Pando/2.6.0.8</td>
<td></td>
</tr>
<tr>
<td>status_code</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>anonymous</td>
<td></td>
</tr>
<tr>
<td>password</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>orig_mime_types</td>
<td>application/xml</td>
<td></td>
</tr>
<tr>
<td>resp_mime_types</td>
<td>application/xml</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>ts</td>
<td>1392805957.927087</td>
<td></td>
</tr>
<tr>
<td>uid</td>
<td>CEA0512D7k0BD9Dda2</td>
<td></td>
</tr>
<tr>
<td>id.orig_h</td>
<td>2a07:f2c0:90:402:41e:c13:6cb:99c</td>
<td></td>
</tr>
<tr>
<td>id.orig_p</td>
<td>40475</td>
<td></td>
</tr>
<tr>
<td>id.resp_h</td>
<td>2406:fe60:f47::aeb:98c</td>
<td></td>
</tr>
<tr>
<td>id.resp_p</td>
<td>443</td>
<td></td>
</tr>
<tr>
<td>version</td>
<td>TLSv10</td>
<td></td>
</tr>
<tr>
<td>cipher</td>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</td>
<td></td>
</tr>
<tr>
<td>server_name</td>
<td><a href="http://www.netflix.com">www.netflix.com</a></td>
<td></td>
</tr>
<tr>
<td>subject</td>
<td>CN=www.netflix.com,OU=Operations, O=Netflix, Inc., L=Los Gatos, ST=CALIFORNIA, C=US</td>
<td></td>
</tr>
<tr>
<td>issuer_subject</td>
<td>CN=VeriSign Class 3 Secure Server CA, OU=VeriSign Trust Network, O=VeriSign, C=US</td>
<td></td>
</tr>
<tr>
<td>not_valid_before</td>
<td>1389859200.000000</td>
<td></td>
</tr>
<tr>
<td>not_valid_after</td>
<td>1452931199.000000</td>
<td></td>
</tr>
<tr>
<td>client_subject</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>client_issuer_subject</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>cert_hash</td>
<td>197cab7c6c92a0b9ac5f37cfb0699268</td>
<td></td>
</tr>
<tr>
<td>validation_status</td>
<td>ok</td>
<td></td>
</tr>
</tbody>
</table>

The Bro Monitoring Platform
## Syslog & DHCP

<table>
<thead>
<tr>
<th>ts</th>
<th>1392796803.311801</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>CnYivt3ZONHOuBALR8</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>ts</th>
<th>1392796803.311801</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>CnYivt3ZONHOuBALR8</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>ts</th>
<th>1392796962.091566</th>
</tr>
</thead>
<tbody>
<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>FnungQ3TI19GahPJP2</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[…]1085bfefb</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>ts</th>
<th>1392796839.675867</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>10.209.100.2</td>
</tr>
<tr>
<td>host_p</td>
<td>-</td>
</tr>
<tr>
<td>software_type</td>
<td>HTTP::BROWSER</td>
</tr>
<tr>
<td>name</td>
<td>DropboxDesktopClient</td>
</tr>
<tr>
<td>version.major</td>
<td>2</td>
</tr>
<tr>
<td>version.minor</td>
<td>4</td>
</tr>
<tr>
<td>version.minor2</td>
<td>11</td>
</tr>
<tr>
<td>version.minor3</td>
<td>-</td>
</tr>
<tr>
<td>version.add1</td>
<td>Windows</td>
</tr>
<tr>
<td>unparsed_version</td>
<td>DropboxDesktopClient/2.4.11 (Windows; 8; i32; en_US; Trooper 5694-2047-1832-6291-8315)</td>
</tr>
</tbody>
</table>
The Bro Monitoring Platform

Help Understand Your Network

Top File Types

- application/octet-stream
- text/html
- text/plain
- application/xml
- application/x-shockwave-flash
- application/pdf
- image/gif
- image/jpeg
- image/png

Command:
```
cat files.log | bro-cut mime_type | sort | uniq -c | sort -rn
```
Help Understand Your Network (2)

Top Software by Number of Hosts

- CaptiveNetworkSupport
- Firefox
- MSIE
- 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>Category</th>
<th>Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>CaptureLoss</td>
<td>too much loss</td>
</tr>
<tr>
<td>Conn: Ack Above Hole</td>
<td></td>
</tr>
<tr>
<td>Conn: Content Gap</td>
<td></td>
</tr>
<tr>
<td>Conn: Retransmission Inconsistency</td>
<td></td>
</tr>
<tr>
<td>DNS: External Name</td>
<td></td>
</tr>
<tr>
<td>FTP: Brute forcing</td>
<td></td>
</tr>
<tr>
<td>FTP: Site Exec Success</td>
<td></td>
</tr>
<tr>
<td>HTTP: SQL Injection Attacker</td>
<td></td>
</tr>
<tr>
<td>HTTP: SQL Injection Victim</td>
<td></td>
</tr>
<tr>
<td>Intel: Notice</td>
<td></td>
</tr>
<tr>
<td>PacketFilter: Dropped Packets</td>
<td></td>
</tr>
<tr>
<td>ProtocolDetector: Protocol Found</td>
<td></td>
</tr>
<tr>
<td>ProtocolDetector: Server Found</td>
<td></td>
</tr>
<tr>
<td>SMTP: Blocklist Blocked Host</td>
<td></td>
</tr>
<tr>
<td>SMTP: Blocklist Error Message</td>
<td></td>
</tr>
<tr>
<td>SMTP: Suspicious Origination</td>
<td></td>
</tr>
<tr>
<td>SSH: Interesting Hostname Login</td>
<td></td>
</tr>
<tr>
<td>SSH: Login By Password Guesser</td>
<td></td>
</tr>
<tr>
<td>SSH: Password Guessing</td>
<td></td>
</tr>
<tr>
<td>SSH: Watched Country Login</td>
<td></td>
</tr>
<tr>
<td>SSL: Certificate Expired</td>
<td></td>
</tr>
<tr>
<td>SSL: Certificate Expires Soon</td>
<td></td>
</tr>
<tr>
<td>SSL: Certificate Not Valid Yet</td>
<td></td>
</tr>
<tr>
<td>SSL: Invalid Server Cert</td>
<td></td>
</tr>
<tr>
<td>Scan: Address Scan</td>
<td></td>
</tr>
<tr>
<td>Scan: Port Scan</td>
<td></td>
</tr>
<tr>
<td>Signatures: Count Signature</td>
<td></td>
</tr>
<tr>
<td>Signatures: Multiple Sig Responders</td>
<td></td>
</tr>
<tr>
<td>Signatures: Multiple Signatures</td>
<td></td>
</tr>
<tr>
<td>Signatures: Sensitive Signature</td>
<td></td>
</tr>
<tr>
<td>Software: Software Version Change</td>
<td></td>
</tr>
<tr>
<td>Software: Vulnerable Version</td>
<td></td>
</tr>
<tr>
<td>TeamCymruMalwareHashRegistry: Match</td>
<td></td>
</tr>
<tr>
<td>Traceroute: Detected</td>
<td></td>
</tr>
<tr>
<td>Weird: Activity</td>
<td></td>
</tr>
</tbody>
</table>
Watching for Suspicious 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)

Internet → Enterprise Network

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

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

Feeds
- CIF
- JC3
- Spamhaus
- Custom/Proprietary
Intelligence Integration (Passive)

Internet ———————————— Enterprise Network

Intelligence
IP addresses
DNS names
URLs
File hashes

Traffic Monitoring
HTTP, FTP, SSL, SSH, FTP,
DNS, SMTP, ...

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 Integration (Passive)

Traffic Monitoring
HTTP, FTP, SSL, SSH, FTP, DNS, SMTP, ...

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts</td>
<td>1258565309.806483</td>
</tr>
<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>

notice.log
Intelligence Integration (Active)
# cat files.log | bro-cut mime_type sha1 | awk '$1 ~ /x-dosexec/'
application/x-dosexec  5fd2f37735953427e2f6c593d6ec7ae882c9ab54
application/x-dosexec  00c69013d34601c2174b72c9249a0063959da93a
application/x-dosexec  0d801726d49377bfe989dcca7753a62549f1ddda
[...]

Intelligence Integration (Active)
Intelligence Integration (Active)

```
# 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 shal | awk '$1 ~ /x-dosexec/'
application/x-dosexec 5fd2f37735953427e2f6c593d6ec7ae882c9ab54
application/x-dosexec 00c69013d34601c2174b72c9249a0063959da93a
application/x-dosexec 0d801726d49377bfe989dcca7753a62549f1ddd

# 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>CjKeSB45xaOmiIo4Th</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

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

```python
event http_request(c: connection, method: string, original_URI: string, unescaped_URI: string, version: string) {
    if (method == "GET" && unescaped_URI == /.*passwd/) {
        NOTICE(...); # Alarm.
    }
}
```
Script Example: Scan Detector

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.
}
The Bro Monitoring Platform

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.

Growing community writing 3rd party scripts.
  Bro could report Mandiant’s APT1 indicators within a day.
Bro Ecosystem
Bro Ecosystem
Bro Ecosystem

Internet → Tap → Bro → BroControl → User Interface → Output

Internet

Bro

BroControl

Internal Network

Control
Bro Ecosystem

Internet

Tap

External Scripts

Functionality

Bro

Control

Output

BroControl

User Interface

Internal Network
Bro Ecosystem

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

- **Internet**
- **Internal Network**

**Tap**

**Bro**
- **Functionality**
- **Events**
- **State**
- **Control**
- **Output**

**External Scripts**

**BroControl**
- **User Interface**
- **Events**

**Other Bros**

**Broccoli**

*Bro Client Communication Library*
Bro Ecosystem

Internet → Bro → Internal Network

Internet → Tap → Internal Network

External Scripts → Bro → BroControl

Other Bros → Bro → BroControl

BroControl → Control → Bro

Output → BroControl → Events

BroControl → User Interface

Bro → Control → BroControl

Events → Bro → BroControl

State → Bro → BroControl

Bro Client Communication Library

Broccoli Ruby
Broccoli Python
(Broccoli Perl)
Bro Ecosystem

- **Internet**
- **Internal Network**
- **Tap**
- **Network Control**
- **Events**
- **State**
- **Other Bros**
- **External Scripts**
- **Functionality**
- **Bro**
- **Control**
- **Output**
- **BroControl**
- **User Interface**
- **Broccoli**
  - **Broccoli Ruby**
  - **Broccoli Python**
  - (Broccoli Perl)
- **Bro Client Communication Library**

The Bro Monitoring Platform
Bro Ecosystem

Internet \(\Rightarrow\) Bro \(\Rightarrow\) Internal Network

Internal Network \(\Rightarrow\) Bro \(\Rightarrow\) Internet

Bro \(\Rightarrow\) External Scripts \(\Rightarrow\) BroControl

BroControl \(\Rightarrow\) User Interface

Events \(\Rightarrow\) Other Bros

Other Bros \(\Rightarrow\) Events

Event Control \(\Rightarrow\) Output

Network Control \(\Rightarrow\) BroControl

Tap \(\Rightarrow\) Time Machine

Bro Client Communication Library:
- Broccoli Python
- Broccoli Ruby
- (Broccoli Perl)

The Bro Monitoring Platform
Bro Ecosystem

The Bro Monitoring Platform
Bro Ecosystem

Bro Distribution
bro-2.3.tar.gz

Time Machine
Internal Network
Tap
Network Control
Events State
Events

Functionality
Control
Output

BroClient Communication Library
Broccoli
Broccoli Python
Broccoli Ruby
(Broccoli Perl)

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

Bro

BroControl

User Interface

The Bro Monitoring Platform
**Bro Cluster Ecosystem**

- **Internet**
- **Internal Network**
- **Bro**
  - **Functionality**
  - **Control**
  - **Output**
- **External Scripts**
- **Events**
- **State**
- **External Bro**
- **Broccoli Ruby**
- **Broccoli Python**
  - **(Broccoli Perl)**
- **BroControl**
  - **User Interface**

**The Bro Monitoring Platform**
Bro Cluster Ecosystem
Bro *Cluster* Ecosystem

- Internet
- **Tap**
- *Load-Balancer*
- **Internal Network**
- **External Scripts**
- **External Bro**
- **Broccoli**
- *Bro Client Communication Library*
  - Broccoli Python
  - Broccoli Ruby
  - (Broccoli Perl)

The Bro Monitoring Platform
Bro Cluster Ecosystem

- Internet
- Internal Network
- Load-Balancer
  - Bro
  - Bro
  - Bro
  - Bro
- External Scripts
- External Bro
- Broccoli
  - Broccoli Ruby
  - Broccoli Python
  - (Broccoli Perl)
- Bro Control
  - User Interface
  - Output
- Bro Client Communication Library
Bro Cluster Ecosystem

- Internet
- Internal Network
- Load-Balancer
- Bro
- Bro
- Bro
- Bro
- BroControl
- External Scripts
- External Bro
- Broccoli
- Broccoli Ruby
- Broccoli Python
- (Broccoli Perl)
- User Interface
- Control
- Output
- Packets
- Tap
Bro Cluster Ecosystem

Internet

Tap

Internal Network

Bro

“Workers”

“Manager”

“Frontend”

LoadBalancer

Packets

Control

Output

User Interface

External Scripts

Bro Client Communication Library

Broccoli

Broccoli Ruby

Broccoli Python

Broccoli Perl

External Bro

BroControl

The Bro Monitoring Platform
Installing Bro

Here: We’ll use the VM (or Bro Live).
Comes with everything preinstalled.

Normally: Follow instructions on bro.org.
http://www.bro.org/sphinx/install

Building from source is pretty straight-forward:

> yum install cmake flex bison swig libpcap-devel [...]  
> wget http://www.bro.org/downloads/release/bro-2.2.tar.gz  
> tar xzvf bro-2.2.tar.gz  
> cd bro  
> ./configure --prefix=/usr/local && make && make install
Configuring Bro

In many cases, just two files to edit.

<prefix>/etc/node.cfg

# If you have a small network and only one interface to monitor, # this will do it. We’ll talk about cluster mode later.
[bro]
type=standalone
host=localhost
interface=eth0

<prefix>/etc/networks.cfg

# List of local networks in CIDR notation, optionally followed by a # descriptive tag.
# For example, "10.0.0.0/8" or "fe80::/64" are valid prefixes.

10.0.0.0/8     Private IP space
192.168.0.0/16 Private IP space

(There’s also <prefix>/etc/broctl.cfg with more options you can tweak.)
Using BroControl

Use “broctl” to start & stop.

```
# broctl install
# broctl start
starting bro ...
# broctl status

Name       Type       Host       Status   Pid    Started
bro        standalone localhost  running  16737  15 May 15:57:35

# ls <prefix>/logs/current/
conn.log http.log […]
```

Reinstall after changing Bro’s configuration.

```
# broctl check
bro is ok
# broctl install
# broctl restart
```
Using Bro from the Command Line

We’ll use the Bro binary directly.

```
# bro -r trace.pcap
# ls *.log
conn.log http.log [...]
```

“bro-cut” is a handy tool to work with logs.

```
# cat http.log | bro-cut -d ts id.orig_h host
2009-11-21T02:19:34-0800 192.168.1.105 download.windowsupdate.com
[...]
```

Generally, use your standard Unix tools. grep, awk, head/tail, sed, etc.
So much more …
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 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 funding a Bro Center of Expertise at the International Computer Science Institute and the National Center for Supercomputing Applications.