An Alert has Fired. Now What?

Open-source Bro solves security problems traditional tools can't.

May 2017

Anyone who works in a security operations center understands the drill:

- An alert fires from a source that may be prone to false positives (next-generation firewall, intrusion detection/prevention system)
- The incident response team jumps into action

What happens next? For a large and growing number of organizations worldwide, analysts consult data produced by the Bro network monitoring platform to quickly arrive at the truth.

Bro is the world's most powerful framework for transforming network traffic into actionable data for **analysis, forensics, and real-time incident response.**

Why are enterprises adopting Bro *now*?

For the first 15 years of its history, Bro had the reputation of being a powerful but challenging tool, best suited for critical high-performance environments. That reputation is quickly changing as enterprise adoption of Bro has started to skyrocket. In fact, Bro's log format is becoming the de facto standard for network-based data. Organizations worldwide now rely on the security-based information that Bro provides for forensics, incident response, and threat hunting. Whether it's used to validate or disprove an alert from another tool, piece together a complex security incident, or support threat hunting teams, Bro's powerful, versatile, and actionable data is at the center of the world's most capable security operations.

INSIDE: See how Bro handles a threat.

corelight

The world's largest enterprises **now use Bro.**

Organizations are deploying Bro to tackle:

COMPLEXITY	Enterprise networks have become more complex, with thousands of global collaborations, a disappearing boundary between 'inside' and 'outside', new cloud service providers, and shifting traffic patterns that defy easy characterization.
EVOLVING THREATS	Threats are more challenging. Today, large enterprises plan for nation-state attacks in the same way that government and research organizations have for decades. Malware infections, denial of service attacks, exfiltration, phishing, misconfigurations, abuse, and many other security threats can be detected and investigated using Bro's powerful data.
SMB ANALYSIS	Bro itself is more capable with every release. In the past year the open-source development team added support for analyzing SMB (Windows) traffic. That's a game changer, because so much enterprise traffic runs over SMB.

Bro is a powerful **open source framework** first created 20 years ago by computer scientist Vern Paxson to study complex Internet traffic patterns.

Almost immediately, Vern's tool was adopted by network security teams in national laboratories, government agencies, and large research universities.

corelight

Analysis of an exploit:
It began with a click.

See how an incident responder might use Bro logs to quickly resolve an event:

START

A user receives an email.

And clicks a link in the email.

The browser loads a web page.

The web page automatically downloads a file.

Malware is loaded on the user's machine.

The loader reaches out to download stage 1 malware.

Malware loads and beacons.

Another security tool fires an alert.

smtp.log | Provides sender, recipient, subject and much more

```
192.168.1.104 1604 192.168.1.1 25
Wed, 18 Nov 2009 12:53:59 -0800
Charlie <charlie@m57.biz> Pat McGoo <pat@m57.biz> Re: Google patent
```

conn.log and **dns.log** | Provide connection and domain info

```
192.168.2.14 52947 192.168.1.1 53
udp 58652 click.malicious.com
1 C_INTERNET 1 A NOERROR 216.218.224.24
```

http.log | Provides details including URI and user-agent

```
GET click.malicious.com /page/view/1072708368/?loader=1258577832840&cv=6&fst=
1258577832840&num=1&hl=en&gl=US&guid=ON&ct_cookie_present=false
http://www.malicious.com/ Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
```

files.log | Shows rich file information

```
2.233.51.87 192.168.2.14 CaDoRe2fMgT5wHkgve
HTTP 0 PE application/x-dosexec
```

Possible integration with host monitoring in logs

```
192.168.2.14 3692 3484 "C:\temp\winword.exe"
```

conn.log and **dns.log** | Provide connection and domain info

```
192.168.2.14 52947 192.168.1.131 53 udp 14651 loader.badguy.com
1 C_INTERNET 1 A NOERROR 221.28.64.221
```

http.log | Provides detailed info about C&C traffic

```
Nov 18 10:32:50 GET checkin.badguy.com/js/
```

Bro logs supply context and help guide the investigation.

CORELIGHT, INC. | INFO@CORELIGHT.COM

Real-time data from Bro transforms the work of incident response, making it faster and **much more accurate**.

After deploying Bro, enterprises discover that security incidents can often be resolved with Bro data alone. When an alert fires in the SOC, incident responders turn immediately to Bro data for context and understanding.

Bro parses dozens of network protocols (including SMB, HTTP, DNS, and SMTP), extracts files directly from network traffic, speaks IPv4 and IPv6 natively, and is capable of controlling network devices such as routers and switches. Bro also includes a dedicated programming language for building applications, plus the ability to ingest intelligence feeds and log streams. And this brief description barely scratches the surface. Bro is simply the most flexible and powerful platform for network traffic analysis in the world.

How does Bro work?

Unlike a conventional IDS that characterizes traffic as good or bad, Bro is not generally configured to send alarms when it sees a predetermined pattern. Instead, it watches all network traffic and extracts the essential content from every flow, packing that content into data streams expressly designed for incident responders.

Think of Bro as a 'flight data recorder' for your network, always working in the background to characterize everything on the wire, without preconceptions about what traffic is normal in your environment. When you need definitive information about what happened on your network in the past, Bro data is available. In fact, many organizations retain a data archive for months or years, to assist forensic investigations.

Bro is versatile.

As you might imagine, Bro data is useful for many things besides incident response and forensics, including performance monitoring, network and host characterization, compliance, and vulnerability assessment. Multiple teams can benefit from the very same data set.

SMB
NTLM
DCE_RPC
CONN
DHCP
DNS
FILES
FTP
HTTP
IRC
MODBUS
RDP
RFB
SIP
SMTP
SOCKS
SSH
SSL

Bro parses dozens of network protocols.
For a complete list visit:
github.com/corelight/bro-cheatsheets

http.log | HTTP request/reply details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the HTTP request
uid & id		Underlying connection info > **See conn.log**
trans_depth	count	Pipelined depth into the connection
method	string	HTTP Request verb: GET, POST, HEAD, etc.
host	string	Value of the Host header
uri	string	URI used in the request
referrer	string	Value of the "Referer" header
user_agent	string	Value of the User-Agent header
request_body_len	count	Uncompressed content size of Orig data
response_body_len	count	Uncompressed content size of Resp data
status_code	count	Status code returned by the server
status_msg	string	Status message returned by the server
info_code	count	Last seen 1xx info reply code by server
info_msg	string	Last seen 1xx info reply message by server
tags	set	Indicators of various attributes discovered
username	string	Username if basic-auth is performed
password	string	Password if basic-auth is performed
proxied	set	Headers indicative of a proxied request

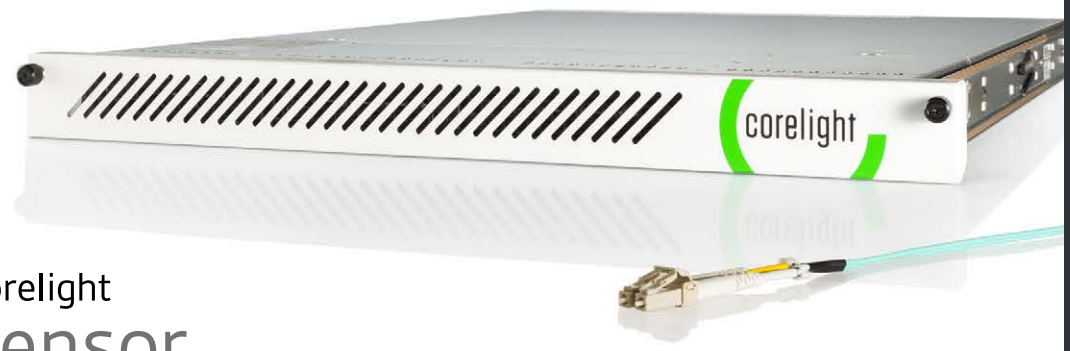
An Alert has Fired. Now What?

A **simple shortcut** to deployment.

Although it's relatively easy to get started with Bro, it's much more challenging to run the software efficiently and at scale—especially when deployment goals include monitoring high-speed links, managing a fleet of distributed sensors, minimizing packet loss, and controlling SIEM licensing costs.

The inventor and core technologists behind Bro have created a company, Corelight, to take the mystery and pain out of critical open-source Bro deployments. Corelight's flagship product—the Corelight Sensor—is shipping now, and more solutions are in the pipeline. Contact us for more information!

We ♥ Bro



Corelight
Sensor

Transform network traffic into high-fidelity data for your security teams. Designed by the creators of open source Bro, the Corelight Sensor is a turn-key solution tuned for performance at enterprise scale. Configure in minutes, and gain exceptional visibility into your network activity.

Evaluate a unit for 30 days. Call us.

Monitoring interfaces

4 SFP/SFP+ ports. Support for copper and optical modules at 1G and 10G.

Contact:

info@corelight.com

510-281-0760

corelight.com

bro.org