BLUVECTOR®

TARGETED LOGGING

Feature Review

The process of forensic analysis can be a tedious one, at best. Generally, an analyst must collect all logs surrounding an event and use a set of scripts and queries to identify those entries which are relevant to the investigation.

With version 3.0, BluVector has enhanced its targeted logging function to go beyond the collection and correlation of relevant network log entries (the HTTP header, HTTP log, DNS log, etc.). This has been accomplished through the introduction of two new, intuitive Event Metadata and Network-Centric displays. These displays make it possible to further summarize and prioritize the information required by analysts to speed decision making, thus improving forensic process efficiency and reducing time to detection.

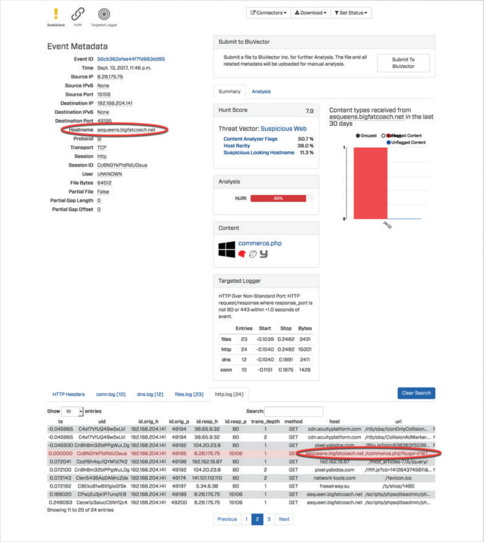
Q: How Does It Work?

When a BluVector detection engine identifies a suspicious event, it targets all Bro or Suricata logs containing entries recorded within a 15-minute time window of that event. Next, these targeted logs are scanned for matching criteria (host IP, domain, etc.). Currently, these criteria are fully-configurable by the user. BluVector also provides a large set of extensible Suricata rules that can be applied as additional matching criteria. All matching log entries are then stored with the flagged event and displayed within the BluVector dashboard.

Q: What's New in Version 3.0?

In addition to the log targeting and event enrichment engine improvements, BluVector 3.0 provides two new, more intuitive ways of viewing and assessing suspicious events.

1. **Event Metadata view:** Analysts can quickly determine whether an event is evidence of an attack or an example of legitimate network activity that should be filtered and omitted from further targeting.
2. **Network Graph view:** SOC teams can visualize not only the event itself, but also the traffic flows associated with that event.



Event Metadata

Event ID	56cb362afae44f7fd663dd95
Time	Sept. 13, 2017, 11:46 p.m.
Source IP	8.28.175.75
Source IPv6	None
Source Port	15106
Destination IP	192.168.204.141
Destination IPv6	None
Destination Port	49195
Hostname	asqueens.bigfatcoach.net
Protocol	ip
Transport	TCP
Session	http
Session ID	CcBNGYkP1dRdUOaua
User	UNKNOWN
File Bytes	64512
Partial File	False
Partial Gap Length	0
Partial Gap Offset	0

Submit to BluVector

Submit a file to BluVector Inc. for further Analysis. The file and all related metadata will be uploaded for manual analysis.

Submit To BluVector

Summary | Analysis

Hunt Score 7.9

Threat Vector: Suspicious Web

Content Analyzer Flags	50.7 %
Host Rarity	38.0 %
Suspicious Looking Hostname	11.3 %

Content types received from asqueens.bigfatcoach.net in the last 30 days

● Grouped ○ Flagged Content ● Unflagged Content

Analysis

hURI 89%

Content

commerce.php

Targeted Logger

HTTP Over Non-Standard Port: HTTP request/response where response_port is not 80 or 443 within +1.0 seconds of event.

	Entries	Start	Stop	Bytes
files	23	-0.1039	0.2482	3431
http	24	-0.1040	0.2482	15001
dns	12	-0.1040	0.1891	2411
conn	10	-0.1151	0.1875	1426

HTTP Headers | conn.log [10] | dns.log [12] | files.log [23] | http.log [24]

Clear Search

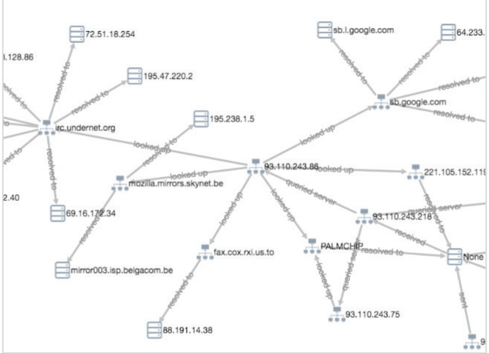
Show 10 entries Search:

ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	trans_depth	method	host	uri
-0.045965	C4xf7VfUQ49w5xLVi	192.168.204.141	49194	38.65.9.32	80	1	GET	cdn.acuityplatform.com	/rtb/oba/IconOnlyCollision...
-0.045965	C4xf7VfUQ49w5xLVi	192.168.204.141	49194	38.65.9.32	80	2	GET	cdn.acuityplatform.com	/rtb/oba/CollisionAdMarker...
-0.045930	CnBhBm32blPPgWuLDg	192.168.204.141	49192	104.20.23.8	80	1	GET	pixel.yabidos.com	/fitiu.js?pid=838363f5039...
0.000000	CcBNGYkP1dRdUOaua	192.168.204.141	49195	8.28.175.75	15106	1	GE	asqueens.bigfatcoach.net	/commerce.php?bugs=2187...
0.072041	Codf6h4qu1QYM1d7K2	192.168.204.141	49198	192.162.19.87	80	1	GET	192.162.19.87	/mod_articles-7.15/jquery/
0.072100	CnBhBm32blPPgWuLDg	192.168.204.141	49192	104.20.23.8	80	2	GET	pixel.yabidos.com	/iftfl.js?cb=14126437456118...
0.072143	Clen5436AqDAMrcZde	192.168.204.141	49174	141.101.112.110	80	2	GET	network-tools.com	/favicon.ico
0.072182	C9EkoB1wBXfgloGf5k	192.168.204.141	49197	5.34.6.38	80	1	GET	freeairway.su	/b/shoe/1480
0.189020	CPxq2u3js1P7unq1E8	192.168.204.141	49199	8.28.175.75	15106	1	GET	asqueen.bigfatcoach.net	/scripts/phpsqliteadmin/ph...
0.248093	Cecw1p3aiucC5NYQc4	192.168.204.141	49200	8.28.175.75	15106	1	GET	asqueen.bigfatcoach.net	/scripts/phpsqliteadmin/ph...

Showing 11 to 20 of 24 entries

Previous 1 2 3 Next

Event Metadata view



Network Graph view

BLUVECTOR®

To learn more visit bluvector.io