Zeeking the net

“Big Brother is Watching You”

Victor Salazar
Global Cybersec

Bro / Zeek

“The Open Source Network Security Monitoring Tool”

- Herramienta *Open Source* de *monitoreo y análisis pasivo* de tráfico de redes
- Licencia BSD: Uso libre, virtualmente sin restricciones

https://zeek.org
https://github.com/zeek/zeek/blob/master/COPYING

Vern Paxson

Co-fundador y Científico en Jefe

- 1995, Universidad de California, Berkeley
- Profesor de Ciencias de la Computación
- Co-fundador de Corelight

https://corelight.com/company/about-corelight

BUGCON 2022

s/Bro/Zeek/g

- *Big Brother*, El Gran Hermano (1984, George Orwell)
  - *Recordatorio Orweliano de que el software de monitoreo va de la mano con potenciales violaciones a la privacidad*
  - Connotación negativa

- 2018: se cambia el nombre a *“Zeek”*
  - Refleja mejor los valores de la comunidad

https://docs.zeek.org/en/current/about.html

BUGCON 2022

Para qué sirve?

“Si está sucediendo en la red, Zeek lo ve”

- Analiza el tráfico de red
- Extrae metadatos
- Genera logs específicos por protocolo
  - Más de 60 protocolos distintos
  - Más de 400 distintos campos
- Extrae archivos

https://docs.zeek.org/en/current/about.html

BUGCON 2022

- barnyard2
- broker
- capture loss
- cluster
- config
- conn
- conn history
- conn state
- dce rpc
- dhcp
- dnp3
- dns
- dpd
- files
- ftp
- http
- intel
- irc
- kerberos
- known certs
- known hosts
- known modbus
- known services
- loaded scripts
- modbus
- modbus register change
- mysql
- netcontrol
- netcontrol catch release
- netcontrol drop
- netcontrol shunt
- notice
- notice alarm
- ntlm
- ocsp
- openflow
- packet filter
- pe
- radius
- rdp
- reporter
- rfb
- signatures
- sip
- smb cmd
- smb files
- smb mapping
- smtp
- snmp
- socks
- software
- ssh
- ssl
- stats
- syslog
- traceroute
- tunnel
- unified2
- weird
- weird stats
- x509

BUGCON 2022

conn.log | IP, TCP, UDP, ICMP connection details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the first packet
uid	string	Unique ID of the connection
id.orig_h	addr	Originating endpoint's IP address (Orig)
id.orig_p	port	Originating endpoint's TCP/UDP port (or ICMP code)
id.resp_h	addr	Responding endpoint's IP address (Resp)
id.resp_p	port	Responding endpoint's TCP/UDP port (or ICMP code)
proto	proto	Transport layer protocol of connection
service	string	Detected application protocol, if any
duration	interval	Connection length
orig_bytes	count	Orig payload bytes; from sequence numbers if TCP
resp_bytes	count	Resp payload bytes; from sequence numbers if TCP
conn_state	string	Connection state (see conn.log > conn_state)
local_orig	bool	Is Orig in Site::local_nets?
local_resp	bool	Is Resp in Site::local_nets?
missed_bytes	count	Number of bytes missing due to content gaps
history	string	Connection state history (see conn.log > history)
orig_pkts	count	Number of Orig packets
orig_ip_bytes	count	Number of Orig IP bytes (via IP total_length header field)
resp_pkts	count	Number of Resp packets
resp_ip_bytes	count	Number of Resp IP bytes (via IP total_length header field)
tunnel_parents	set	If tunneled, connection UID of encapsulating parent(s)
orig_l2_addr	string	Link-layer address of the originator
resp_l2_addr	string	Link-layer address of the responder
vlan	int	The outer VLAN for this connection
inner_vlan	int	The inner VLAN for this connection

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
orig_fuids	vector	File unique IDs from Orig
orig_filenames	vector	File names from Orig
orig_mime_types	vector	File types from Orig
resp_fuids	vector	File unique IDs from Resp
resp_filenames	vector	File names from Resp
resp_mime_types	vector	File types from Resp
client_header_names[1]	vector	The names of HTTP headers sent by Orig
server_header_names[1]	vector	The names of HTTP headers sent by Resp
cookie_vars[2]	vector	Variable names extracted from cookies
uri_vars[2]	vector	Variable names extracted from the URI

[1] *If policy/protocols/http/header-names.bro is loaded*

[2] *If policy/protocols/http/var-extraction-uri.bro is loaded*

dns.log | DNS query/response details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the DNS request
uid & id		Underlying connection info > See conn.log
proto	proto	Protocol of DNS transaction—TCP or UDP
trans_id	count	16 bit identifier assigned by DNS client; responses match
rtt	interval	Round trip time for the query and response
query	string	Domain name subject of the query
qclass	count	Value specifying the query class
qclass_name	string	Descriptive name of the query class (e.g., C_INTERNET)
qtype	count	Value specifying the query type
qtype_name	string	Descriptive name of the query type (e.g., A, AAAA, PTR)
rcode	count	Response code value in the DNS response
rcode_name	string	Descriptive name of response code (e.g., NXDOMAIN, NODATA)
AA	bool	Authoritative answer: T = server is authoritative for the query
TC	bool	Truncation: T = the message was truncated
RD	bool	Recursion desired: T = recursive lookup of query requested
RA	bool	Recursion available: T = server supports recursive queries
Z	count	Reserved field, should be zero in all queries and responses
answers	vector	List of resource descriptions in answer to the query
TTLs	vector	Caching intervals of the answers
rejected	bool	Whether DNS query was rejected by server
auth[1]	set	Authoritative responses for the query
addl[1]	set	Additional responses for the query

[1] *If policy/protocols/dns/auth-addl.bro is loaded*

files.log | File analysis results

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when file was first seen
fuid	string	Unique identifier for a single file
tx_hosts	set	Host(s) that sourced the data
rx_hosts	set	Host(s) that received the data
conn_uids	set	Connection UID(s) over which file transferred
source	string	An identification of the source of the file data
depth	count	Depth of file related to source (e.g., HTTP request depth)
analyzers	set	Set of analyzers attached during file analysis
mime_type	string	File type, as determined by Bro's signatures
filename	string	Filename, if available from source analyzer
duration	interval	The duration that the file was analyzed for
local_orig	bool	Did the data originate locally?
is_orig	bool	Was the file sent by the Originator?
seen_bytes	count	Number of bytes provided to file analysis engine
total_bytes	count	Total number of bytes that should comprise the file
missing_bytes	count	Number of bytes in file stream missed
overflow_bytes	count	Out-of-sequence bytes in the stream due to overflow
timedout	bool	If the file analysis timed out at least once
parent_fuid	string	Container file ID this was extracted from
md5/sha1	string	MD5/SHA1 hash of the file
extracted	string	Local filename of extracted files, if enabled
entropy	double	Information density of the file contents

smtp.log | SMTP transactions

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when message was first seen
uid & id		Underlying connection info > See conn.log
trans_depth	count	Transaction depth if there are multiple msgs
helo	string	Contents of the HELO header
mailfrom	string	Contents of the MAIL FROM header
rcptto	set	Contents of the RCPT TO header
date	string	Contents of the DATE header
from	string	Contents of the FROM header
to	set	Contents of the TO header
cc	set	Contents of the CC header
reply_to	string	Contents of the ReplyTo header
msg_id	string	Contents of the MsgID header
in_reply_to	string	Contents of the In-Reply-To header
subject	string	Contents of the Subject header
x_originating_ip	addr	Contents of the X-Originating-IP header
first_received	string	Contents of the first Received header
second_received	string	Contents of the second Received header
last_reply	string	Last server to client message
path	vector	Message transmission path, from headers
user_agent	string	Value of the client User-Agent header
tls	bool	Indicates the connection switched to TLS
fuids	vector	File unique IDs seen attached to message
is_webmail[1]	bool	If the message was sent via webmail

[1] *If policy/protocols/smtp/software.bro is loaded*

ts	Timestamps with microsecond accuracy, synchronized across logs
uid	Unique ID for every connection
md5/sha1	File hash of every file
fuid	Unique ID for every instance of every file seen on the network

corelight

BUGCON 2022

conn.log

IP, TCP, UDP and ICMP connection details

Field	Type	Description
ts	time	Timestamp
uid	string	Unique ID of Connection
id.orig_h	addr	Originating endpoint's IP address (AKA ORIG)
id.orig_p	port	Originating endpoint's TCP/UDP port (or ICMP code)
id.resp_h	addr	Responding endpoint's IP address (AKA RESP)
id.resp_p	port	Responding endpoint's TCP/UDP port (or ICMP code)
proto	transport_proto	Transport layer protocol of connection
service	string	Dynamically detected application protocol, if any
duration	interval	Time of last packet seen – time of first packet seen
orig_bytes	count	Originator payload bytes; from sequence numbers if TCP
resp_bytes	count	Responder payload bytes; from sequence numbers if TCP
conn_state	string	Connection state (see conn.log:conn_state table)
local_orig	bool	If conn originated locally T; if remotely F. If Site::local_nets empty, always unset.
missed_bytes	count	Number of missing bytes in content gaps
history	string	Connection state history (see conn.log:history table)
orig_pkts	count	Number of ORIG packets
orig_ip_bytes	count	Number of ORIG IP bytes (via IP total_length header field)
resp_pkts	count	Number of RESP packets
resp_ip_bytes	count	Number of RESP IP bytes (via IP total_length header field)
tunnel_parents	set	If tunneled, connection UID of encapsulating parent (s)
orig_cc	string	ORIG GeoIP Country Code
resp_cc	string	RESP GeoIP Country Code

conn.log: conn_state

State	Meaning
S0	Connection attempt seen, no reply
S1	Connection established, not terminated (0 byte counts)
SF	Normal establish & termination (>0 byte counts)
REJ	Connection attempt rejected
S2	Established, ORIG attempts close, no reply from RESP.
S3	Established, RESP attempts close, no reply from ORIG.
RSTO	Established, ORIG aborted (RST)
RSTR	Established, RESP aborted (RST)
RSTOS0	ORIG sent SYN then RST; no RESP SYN-ACK
RSTRH	RESP sent SYN-ACK then RST; no ORIG SYN
SH	ORIG sent SYN then FIN; no RESP SYN-ACK ("half-open")
SHR	RESP sent SYN-ACK then FIN; no ORIG SYN
OTH	No SYN, not closed. Midstream traffic. Partial connection.

conn.log: history

Orig UPPERCASE, Resp lowercase, uniq-ed

Letter	Meaning
S	a SYN without the ACK bit set
H	a SYN-ACK ("handshake")
A	a pure ACK
D	packet with payload ("data")
F	packet with FIN bit set
R	packet with RST bit set
C	packet with a bad checksum
I	Inconsistent packet (Both SYN & RST)

BUGCON 2022

Big Brother?

Como todo software de monitoreo, Zeek puede tener usos *WhiteHat o BlackHat*

- White Hat
  - Monitoreo de red
  - IDS
  - Threat Hunting
  - Forensics
  - Estadísticas
  - Troubleshooting

- Black Hat
  - Fase de Reconocimiento
    - Reconocimiento pasivo de la red

BUGCON 2022

Ventajas

- Código abierto
- Gratuito y de uso libre (Licencia BSD)
- Los logs contienen información específica para análisis de seguridad
- Logs tienen menor costo de almacenamiento que los archivos Pcap
- Fácil integración con herramientas existentes
- Extensible mediante scripts creados por la comunidad
- Automatización de procesos mediante herramientas del OS
- Facilita el análisis de amenazas
- Disminución drástica en los tiempos de respuesta a incidentes de seguridad

BUGCON 2022

Desventajas

- Curva de aprendizaje pronunciada
- No existe una GUI nativa
- GUI de Corelight es privativa

“Zeek es uno de los secretos mejor guardados”

* Information about an organization’s use of Zeek Network Security Monitor obtained from public sources such as mailing lists, job postings, public talks, etc.

BUGCON 2022

Press releases

Zeek is Now a Component of Microsoft Windows

World's leading open source network security monitoring platform now deployed on more than one billion global endpoints

San Francisco, Calif. — Oct. 12, 2022 — **Corelight**, the leader in open network detection and response (NDR), today announced the integration of **Zeek**®, the world's most popular open source network security monitoring platform, as a component of **Microsoft Windows** and **Defender for Endpoint**. The **integration** will help security teams respond to the most challenging attacks by providing "richer signals for advanced threat hunting, complete and accurate discovery of IoT devices, and more powerful detection and response capabilities."

Originally created by **Corelight** co-founder and chief scientist Dr. **Vern Paxson** while at Lawrence Berkeley National Laboratory (**Berkeley Lab**), Zeek transforms network traffic into compact and high-fidelity logs, file content, and behavioral analytics to accelerate security operations. Vital funding for Zeek came initially from the **National Science Foundation** and the US Department of Energy's **Office of Science**.

As adoption increased, Corelight was founded to provide a financial model and corporate sponsor for the project. This week in Austin, Texas, Corelight hosts the annual **ZeekWeek** user conference, where the community will gather and where Microsoft speakers will describe the new integration.

"Microsoft is strongly committed to supporting open source projects and ecosystems," said Rob Lefferts, corporate vice president for Microsoft. "We're proud to be working with Zeek and are thrilled to bring this level of network intelligence and monitoring to our customers."

"This is an amazing development for Zeek and its community of contributors and users," said Paxson. "I never imagined that the tool I developed for network monitoring would find broader application in defending endpoints - but that's part of the creative magic of open source development. We are grateful for Microsoft's contributions and support, and we are excited that the project's impact, and that of the community of contributors, will increase so dramatically."

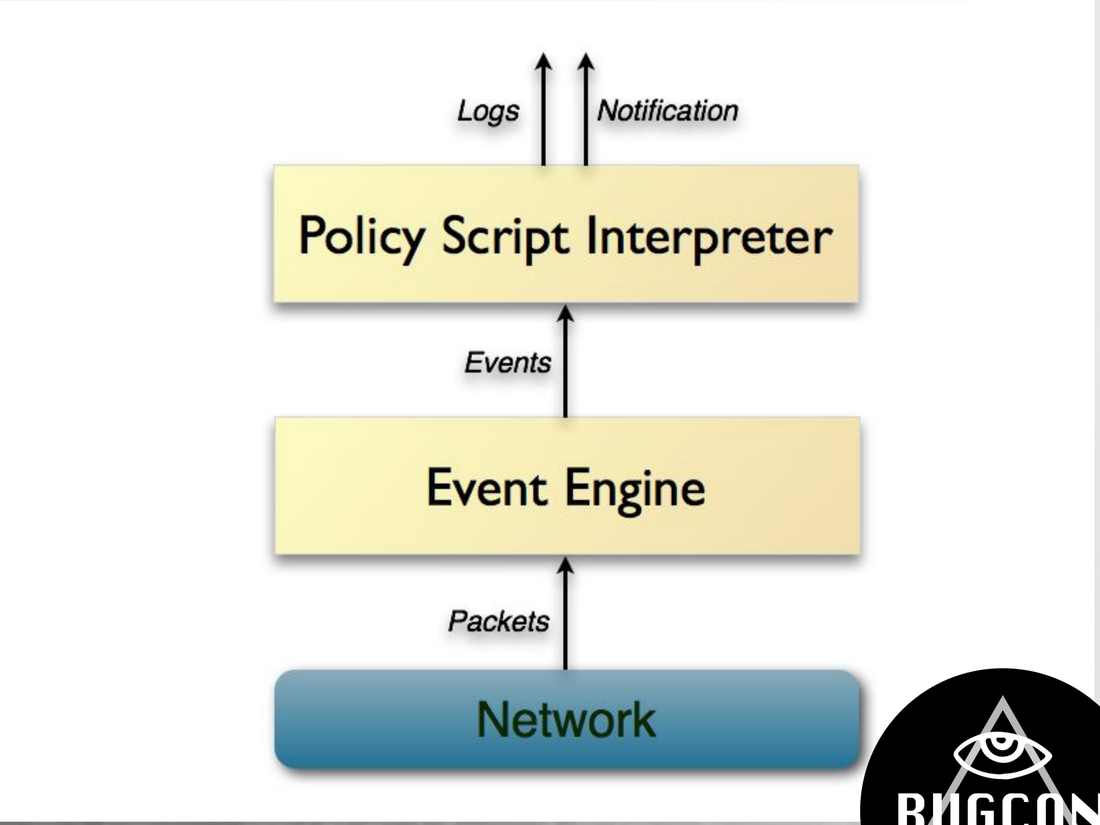
https://corelight.com/company/zeek-now-component-of-microsoft-windows

BUGCON 2022

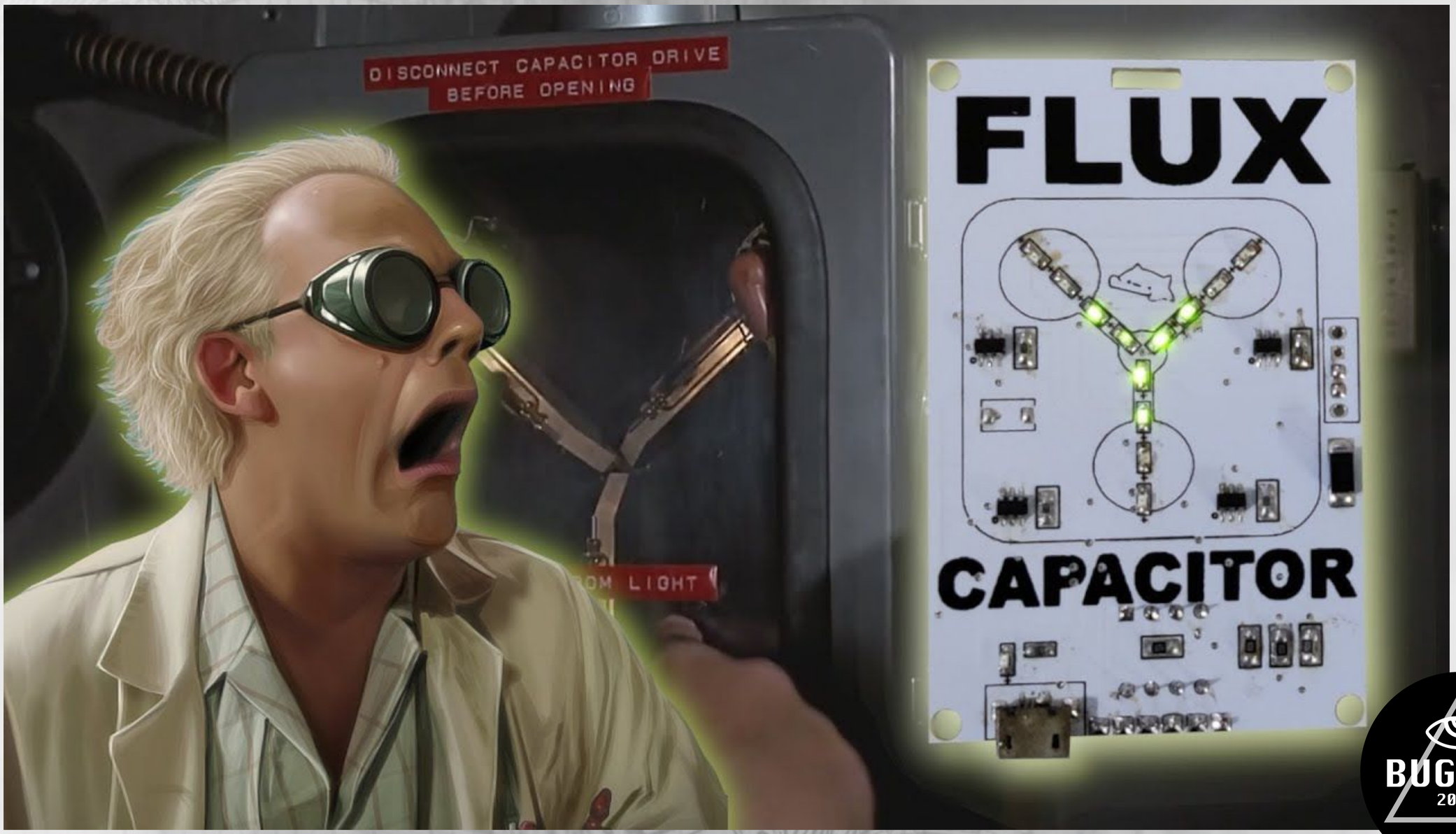
Arquitectura

- Funciona sobre una copia del tráfico de red (no es una herramienta *inline*)
  - Puerto Mirror/Span port
  - Archivos Pcap

https://docs.zeek.org/en/current/about.html#architecture

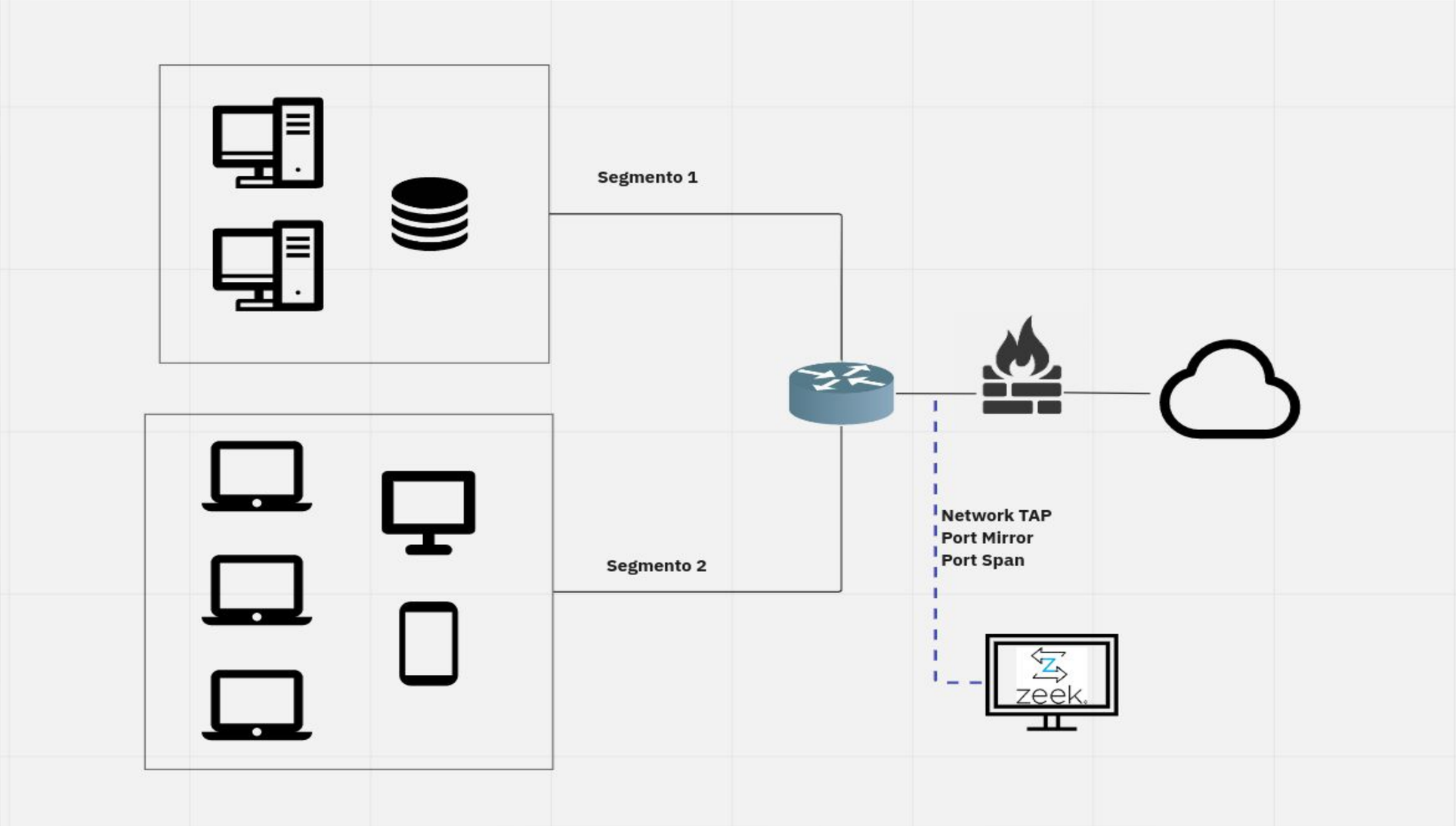


BUGCON 2022


DISCONNECT CAPACITOR DRIVE
BEFORE OPENING
FLUX
CAPACITOR

BUGCON
2022

Deployment


Segmento 1
Segmento 2
Network TAP
Port Mirror
Port Span
zeek

Instalación

- Linux
  - Paquetes binarios
    - apt
    - yum
  - Compilación e instalación desde código fuente
    - Instalación de dependencias
    - Descarga del paquete comprimido
    - `git clone`
    - `./configure && make && sudo make install`
- FreeBSD
  - `sudo pkg install -y zeek`
- Mac OS
  - `brew install zeek`
- Docker
  - `docker pull blacktop/zeek`
- Windows

Configuración

```
$ vim $PREFIX/etc/node.cfg

[zeek]
type=standalone
host=localhost
interface=eth0   #listening interface

$ zeekctl
[ZeekControl] > install
[ZeekControl] > start

[ZeekControl] > deploy
[ZeekControl] > restart
[ZeekControl] > status
```

Estructura de directorios

- $PREFIX:
  - /nsm/bro
  - /nsm/zeek
  - /opt/zeek
  - /usr/local/zeek

```
$ pwd
/nsm/zeek
$
$ ls
bin  etc  include  lib  logs  share  spool
$
$ ls bin
bifcl  binpac  bro  bro-config  broctl  bro-cut  capstats  trace-summary
$
$ ls etc
broctl.cfg  networks.cfg  node.cfg
$
$
```

$PREFIX/logs

```
$ pwd
/nsm/zeek/logs
$ ls
2022-09-01  2022-09-12  2022-09-23  2022-10-04  2022-10-15  2022-10-26  2022-11-06  2022-11-17
2022-09-02  2022-09-13  2022-09-24  2022-10-05  2022-10-16  2022-10-27  2022-11-07  2022-11-18
2022-09-03  2022-09-14  2022-09-25  2022-10-06  2022-10-17  2022-10-28  2022-11-08  2022-11-19
2022-09-04  2022-09-15  2022-09-26  2022-10-07  2022-10-18  2022-10-29  2022-11-09  2022-11-20
2022-09-05  2022-09-16  2022-09-27  2022-10-08  2022-10-19  2022-10-30  2022-11-10  2022-11-21
2022-09-06  2022-09-17  2022-09-28  2022-10-09  2022-10-20  2022-10-31  2022-11-11  2022-11-22
2022-09-07  2022-09-18  2022-09-29  2022-10-10  2022-10-21  2022-11-01  2022-11-12  2022-11-23
2022-09-08  2022-09-19  2022-09-30  2022-10-11  2022-10-22  2022-11-02  2022-11-13  current
2022-09-09  2022-09-20  2022-10-01  2022-10-12  2022-10-23  2022-11-03  2022-11-14
2022-09-10  2022-09-21  2022-10-02  2022-10-13  2022-10-24  2022-11-04  2022-11-15
2022-09-11  2022-09-22  2022-10-03  2022-10-14  2022-10-25  2022-11-05  2022-11-16
$
$ du -ch 2022-11-22
1.9G    2022-11-22
1.9G    total
$ du -ch * | tail -n 1
115G    total
$
```

$PREFIX/logs/current

```
$ pwd
/nsm/zeek/logs/current
$
$ ls
capture_loss.log  files.log           notice.log    ssh.log     stdout.log
conn.log          http.log            ntp.log       ssl.log     tunnel.log
dhcp.log          known_hosts.log     pe.log        stats.log   weird.log
dns.log           known_services.log  software.log  stderr.log  x509.log
$
$
```

$PREFIX/logs/$DATE

```
$ cd 2022-11-23
$ ls -1 | wc -l
396
$ ls *.13:00:00-14:00:00.*
capture_loss.13:00:00-14:00:00.log.gz  notice.13:00:00-14:00:00.log.gz
conn-summary.13:00:00-14:00:00.log.gz  ntp.13:00:00-14:00:00.log.gz
conn.13:00:00-14:00:00.log.gz          software.13:00:00-14:00:00.log.gz
dhcp.13:00:00-14:00:00.log.gz          ssh.13:00:00-14:00:00.log.gz
dns.13:00:00-14:00:00.log.gz           ssl.13:00:00-14:00:00.log.gz
files.13:00:00-14:00:00.log.gz         stats.13:00:00-14:00:00.log.gz
http.13:00:00-14:00:00.log.gz          tunnel.13:00:00-14:00:00.log.gz
known_hosts.13:00:00-14:00:00.log.gz   x509.13:00:00-14:00:00.log.gz
$
```

BUGCON 2022

Análisis de logs

- Es posible integrar los logs de Zeek a cualquier herramienta gráfica GUI:
  - Corelight
  - SIEM
  - Splunk
  - ELK

conn.log

```
$ head -n 12 conn.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2022-11-23-23-00-01
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service duration     o
rig_bytes       resp_bytes      conn_state      local_orig      local_resp      missed_bytes    history orig_pkts    o
rig_ip_bytes    resp_pkts       resp_ip_bytes   tunnel_parents
#types  time    string  addr    port    addr    port    enum    string  interval        count   count   string  bool b
ool     count   string  count   count   count   count   set[string]
1669244337.801155       CJs9Es3Z8jeslmZzkb      10.30.1.36      53798   239.255.255.250 1900    udp     -       3.0223
72      692     0       S0      T       F       0       D       4       804     0       0       -
1669244340.825736       CHiB1o1bsFltEfUAkf      10.30.1.195     35514   10.30.1.36      53798   udp     -       -    -
-       S0      T       T       0       D       1       547     0       0       -
1669244391.311135       C6Ltcz3hGbXTOm2xLb      10.30.1.195     54285   8.8.4.4 53      udp     dns     0.008197     3
2       48      SF      T       F       0       Dd      1       60      1       76      -
1669244391.849184       CupNi23M9EW9yGgiul      10.30.1.32      34396   10.30.1.151     8005    tcp     http    5.0057
34      1063    752     SF      T       T       0       ShADadfF        5       1331    5       1020    -
$
$
```

conn.log (json)

```
$ tail -n 1 conn.log
{"ts":1669244702.740363,"uid":"CDSsxedacqY9Pc2pa","id.orig_h":"10.30.1.77","id.orig_p":48142,"id.resp_h":"10.60
.3.110","id.resp_p":443,"proto":"tcp","service":"ssl","duration":5.263704061508179,"orig_bytes":1530,"resp_byte
s":2396,"conn_state":"SF","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"ShADadfF","orig_pkts"
:10,"orig_ip_bytes":2058,"resp_pkts":10,"resp_ip_bytes":2924,"community_id":"1:erS1XOjxJQxN7L/TmJto3RAPqdw="}
$
$ tail -n 1 conn.log | jq
{
  "ts": 1669244661.017066,
  "uid": "Cs0D0g4fsTdgYcVH5",
  "id.orig_h": "fe80::a6ba:dbff:fe2e:41f9",
  "id.orig_p": 131,
  "id.resp_h": "ff02::123",
  "id.resp_p": 130,
  "proto": "icmp",
  "conn_state": "OTH",
  "local_orig": false,
  "local_resp": false,
  "missed_bytes": 0,
  "orig_pkts": 1,
  "orig_ip_bytes": 72,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "community_id": "1:GUTJi45vo018QVSmr12UERugp/s="
}
$
```

zeek-cut

```
$ export PATH="$PATH:/opt/zeek/bin"
$
$ cat conn.log | zeek-cut -d ts id.orig_h id.resp_h id.resp_p | head -n 20
2022-11-24T19:57:20+0000        10.30.2.36      212.129.3.113   443
2022-11-24T19:59:50+0000        10.30.1.12      224.0.0.252     5355
2022-11-24T19:59:00+0000        10.30.2.254     10.30.2.55      161
2022-11-24T19:59:00+0000        10.30.1.224     10.30.2.55      161
2022-11-24T19:59:55+0000        10.30.1.151     10.30.1.34      55874
2022-11-24T19:59:50+0000        10.30.2.18      50.17.0.10      53
2022-11-24T19:58:32+0000        10.30.2.36      172.253.122.95  443
2022-11-24T19:59:00+0000        10.30.2.36      10.30.2.55      161
2022-11-24T19:59:00+0000        10.30.2.11      10.30.2.55      161
2022-11-24T19:59:01+0000        10.30.12.122    239.255.255.250 1900
2022-11-24T19:58:58+0000        10.30.2.18      239.255.255.250 1900
2022-11-24T19:59:01+0000        10.30.2.4       10.30.2.55      161
2022-11-24T19:59:51+0000        10.30.1.34      10.60.2.17      443
2022-11-24T19:59:01+0000        10.30.13.11     91.189.91.157   123
2022-11-24T19:54:25+0000        10.30.2.18      18.160.10.13    443
2022-11-24T19:59:57+0000        10.30.1.36      10.60.2.17      443
2022-11-24T19:59:52+0000        10.30.1.34      10.60.2.25      443
2022-11-24T19:59:02+0000        10.30.2.18      142.251.163.101 443
2022-11-24T19:59:53+0000        10.30.1.224     3.87.85.24      53
2022-11-24T19:59:53+0000        10.30.1.224     3.87.85.24      53
$
```

BUGCON 2022

Buscar una dirección IP

```
$
$ cat conn.log | zeek-cut -d ts id.orig_h id.resp_h id.resp_p | grep -Fw '10.30.1.34' | head -n 20
2022-11-24T19:59:55+0000        10.30.1.151     10.30.1.34      55874
2022-11-24T19:59:51+0000        10.30.1.34      10.60.2.17      443
2022-11-24T19:59:52+0000        10.30.1.34      10.60.2.25      443
2022-11-24T19:59:59+0000        10.60.2.24      10.30.1.34      45174
2022-11-24T20:00:00+0000        10.30.1.151     10.30.1.34      47990
2022-11-24T20:00:04+0000        10.60.2.24      10.30.1.34      45174
2022-11-24T20:00:05+0000        10.30.1.151     10.30.1.34      47990
2022-11-24T20:00:01+0000        10.30.1.34      3.87.85.24      53
2022-11-24T20:00:03+0000        10.30.1.34      10.60.3.110     443
2022-11-24T20:00:09+0000        10.60.2.24      10.30.1.34      51502
2022-11-24T20:00:04+0000        10.30.1.34      10.60.3.110     443
2022-11-24T20:00:10+0000        10.30.1.151     10.30.1.34      32890
2022-11-24T20:00:14+0000        10.60.2.24      10.30.1.34      51502
2022-11-24T20:00:10+0000        10.30.1.34      10.60.3.210     443
2022-11-24T20:00:15+0000        10.30.1.151     10.30.1.34      32890
2022-11-24T20:00:12+0000        10.30.1.34      10.60.2.19      443
2022-11-24T20:00:12+0000        10.30.1.34      3.87.85.24      53
2022-11-24T20:00:19+0000        10.60.2.24      10.30.1.34      53588
2022-11-24T20:00:20+0000        10.30.1.151     10.30.1.34      57088
2022-11-24T20:00:24+0000        10.60.2.24      10.30.1.34      53588
$
```

BUGCON 2022

AWK-wardly effective

```
$
$ awk -F'\t' '{print $3, $5, $6}' conn.log | tr ' ' '\t' | tail -n 20
10.30.2.20      239.255.255.250 1900
10.30.2.36      142.251.111.95  443
10.60.2.24      10.30.1.34      53012
10.30.2.20      142.251.163.95  443
10.30.2.20      172.253.62.101  443
10.30.2.6       10.30.2.55      161
10.30.12.214    224.0.0.252     5355
10.30.2.36      10.30.2.55      161
10.30.2.25      157.240.229.61  80
10.30.1.151     10.30.1.34      47348
10.30.2.4       10.30.2.55      161
10.30.1.1       10.30.1.150     8005
10.30.2.6       8.8.8.8 53
10.30.12.214    224.0.0.252     5355
10.30.2.11      10.30.2.55      161
10.30.2.6       10.30.1.56      161
fe80::dea5:f4ff:feaf:a58f       ff02::1:2       547
10.30.1.34      10.60.3.110     443
10.30.2.254     10.30.2.55      161
10.30.1.224     10.30.2.55      161
$
```

Buscar una dirección IP con AWK

```
$
$ awk -F'\t' '$3 == "10.30.1.34"  {print $1,$3, $5, $6}' http.log | tr ' ' '\t' | tail -n 20
1669320221.815711       10.30.1.34      35.224.170.84   80
1669320522.028377       10.30.1.34      185.125.190.17  80
1669320579.348348       10.30.1.34      23.205.105.176  80
1669320822.031808       10.30.1.34      185.125.190.18  80
1669320905.029681       10.30.1.34      142.251.111.94  80
1669320905.029739       10.30.1.34      142.251.111.94  80
1669320905.031538       10.30.1.34      142.251.111.94  80
1669320905.032082       10.30.1.34      142.251.111.94  80
1669320905.039287       10.30.1.34      142.251.111.94  80
1669321122.032321       10.30.1.34      185.125.190.48  80
1669321421.825403       10.30.1.34      35.224.170.84   80
1669321721.914529       10.30.1.34      91.189.91.48    80
1669322021.826483       10.30.1.34      35.232.111.17   80
1669322322.033889       10.30.1.34      185.125.190.18  80
1669322622.028924       10.30.1.34      185.125.190.49  80
$
```

Buscar peticiones DNS

```
$ grep 'tiktok.com' dns.log | awk -F'\t' '{print $3, $10}'
10.30.2.11 analytics.tiktok.com
10.30.2.11 analytics.tiktok.com
10.30.2.11 analytics.tiktok.com
10.30.2.11 analytics.tiktok.com
$
$ grep 'facebook.com' dns.log | awk -F'\t' '{print $3, $10}' | head -n 12
10.30.2.18 www.facebook.com
10.30.2.18 www.facebook.com
10.30.2.36 connect.facebook.com
10.30.2.36 www.facebook.com
10.30.2.18 www.facebook.com
10.30.2.18 www.facebook.com
10.30.2.18 www.facebook.com
10.30.2.18 www.facebook.com
10.30.2.36 connect.facebook.com
10.30.2.36 www.facebook.com
10.30.2.36 connect.facebook.com
10.30.2.36 www.facebook.com
$
```

BUGCON 2022

Buscar conexiones por UID

```
$ grep 'CqTDjk2VArkva6Awej' conn.log
1669323616.839869       CqTDjk2VArkva6Awej      10.249.2.5      30947   [redacted]      25      tcpsmtp
   1.398548        230408  492     RSTO    T       F       0       ShAdDaR 175     237420  422184     -
$ grep 'CqTDjk2VArkva6Awej' *.log
conn.log:1669323616.839869      CqTDjk2VArkva6Awej      10.249.2.5      30947   [redacted]      25tcp
   smtp    1.398548        230408  492     RSTO    T       F       0       ShAdDaR 175     237420     42
      2184    -
files.log:1669323617.299199     Fivofd3NHU4Y5oqGMg      10.249.2.5      [redacted]      CqTDjk2VArkva6Aw
ej SMTP    2       SHA1,MD5        text/plain      -       0.000000        T       T       448-       0
      0       F       -       1edf5193e5fa476d821014bdc624e542        4f7b23acd2015d65160d3dbfb09c445779
6c7b58   -       -       -       -
files.log:1669323617.299202     FsKMh03dS1suNiYuXi      10.249.2.5      [redacted]      CqTDjk2VArkva6Aw
ej SMTP    3       SHA1,MD5        application/vnd.ms-tnef winmail.dat     0.332597        T T165196  -
      0       0       F       -       8bd03429f018ee4a3c09301e1133d4d6        597333906d58a96de925e730b7
e2e13483bbc7c0   -       -       -       -
smtp.log:1669323617.010426      CqTDjk2VArkva6Awej      10.249.2.5      30947   [redacted]      251mail.
[redacted] com.mx [redacted]@[redacted].mx [redacted]@[redacted].mail.onmicrosoft.com Thu, 24 Nov 2
022 20:59:50 +0000 [redacted] <[redacted]@[redacted].com.mx>  =?utf-8?B?S2FyaW5h
IEFjdc0xYSBPcmRvw7Fleg==?= <[redacted]@[redacted]>  -  -  <006d0879d2124daa9a02baa335a[redacted]
6f@[redacted]>  <[redacted]@mail.gmail.
        RV: CONSTANCIA_VAFG.pdf 10.15.19.148    from [redacted] ([redacted]:
]) by [redacted] ([redacted]:1f0c%14]) with mapi id 15.00.1497.000; Thu, 24
```

BUGCON 2022

“Las 20 direcciones IP más visitadas”

```
$ cat conn.log | zeek-cut id.resp_h id.resp_p | sort -n \
> | uniq -c | sort -nr | head -n 20
    500 8.8.8.8 53
    404 224.0.0.252     5355
    359 10.30.1.151     8005
    226 [redacted]      1900
    112 208.67.220.220  53
     94 ff02::1:2       547
     48 ff02::1:3       5355
     48 10.30.1.25      38043
     46 10.30.12.235    53
     38 255.255.255.255 11050
     38 10.30.1.151     22
     35 8.8.8.8 0
     33 10.30.1.249     0
     30 10.30.12.255    138
     23 40.119.6.228    123
     23 224.0.0.251     5353
     22 ff02::2 134
     19 10.30.1.151     443
     18 10.30.2.255     138
     17 172.217.2.132   443
$
```

“Los 20 sitios web más visitados”

```
$ cd /opt/zeek/logs/2022-11-23
$ zcat dns.*.gz | zeek-cut query | sort \
> | uniq -c | sort -nr | head -n 20
  17146 1.12.30.10.in-addr.arpa
   3716 www.google.com
   3540 [redacted]
   3174 [redacted]
   3144 [redacted]
   2939 WPAD
   2894 tp-link.com
   2869 a.root-servers.net
   1964 ISATAP
   1879 scontent.xx.fbcdn.net
   1834 star-mini.c10r.facebook.com
   1689 isatap
   1681 _nomachine._tcp.local
   1576 www.facebook.com
   1156 [redacted]
    965 msgr-latest.c10r.facebook.com
    889 star.c10r.facebook.com
    876 win10.ipv6.microsoft.com
    870 gateway.facebook.com
    834 static.xx.fbcdn.net
$
```

BUGCON 2022

Enumeración de la red

```
$ zcat conn.*.gz | awk -F\\t '$6 == 3306 {print $5, $6}' \
> | sort -u | tr ' ' '\t'
[redacted].63.64    3306
[redacted].63.79    3306
$
$ zcat conn.*.gz | awk -F\\t '$6 == 22 {print $5, $6}' \
> | sort -u | tr ' ' '\t' | head -n 5
10.247.1.2       22
10.250.150.59    22
10.250.150.79    22
10.250.160.210   22
10.250.160.212   22
$
```

Actividad sospechosa

```
$ zcat conn.*.gz | awk -F\\t '$6 == 4444 {print $5, $6, $7, $8}' \
> | sort -u | tr ' ' '\t'
[redacted]170.82   4444    tcp     -
[redacted].63.64   4444    tcp     -
[redacted].63.64   4444    udp     -
[redacted].63.79   4444    tcp     -
[redacted].63.79   4444    udp     -
$
```

```
$ zcat conn.*.gz | awk -F\\t '$6 == 1337 {print $5, $6, $7, $8}' \
> | sort | uniq -c
      2 [redacted].63.64 1337 tcp -
      2 [redacted].63.79 1337 tcp -
$
```

BUGCON 2022

RITA: Análisis de Amenazas

activecm / rita Public

Notifications | Fork 325 | Star 2k

Code | Issues 68 | Pull requests 6 | Actions | Projects 8 | Wiki | Security | Insights

master | rita / Readme.md | Go to file | ···

lisaSW Migrate beacons analysis to using full timestamp list (#745) ··· Latest commit ea1007d on Aug 19 History

14 contributors +2

156 lines (99 sloc) | 9.25 KB | Raw | Blame

RITA (Real Intelligence Threat Analytics)

If you get value out of RITA and would like to go a step further with hunting automation, futuristic visualizations, and data encrichment take a look at AC-Hunter.

Sponsored by Active Countermeasures.

https://github.com/activecm/rita

BUGCON 2022

RITA | Viewing: VSAGENT-2017-03-15 | Beacons | DNS | BL Source IPs | BL Dest. IPs | BL Hostnames | BL URLs | Scans | Long Connections | Long URLs | User Agents | RITA on

Score	Source	Destination	Connections	Avg. Bytes	Intvl. Range	Size Range	Intvl. Mode	Size Mode	Intvl. Mode Count	Size Mode Count
0.997	10.234.234.100	138.197.117.74	4532	1317.207	8	935	10	544	3921	445
0.994	10.234.234.100	65.52.108.210	28	633.679	471	2674	1680	197	19	27
0.994	10.234.234.101	65.52.108.211	28							
0.992	10.234.234.103	65.52.108.194	28							
0.986	10.234.234.102	65.52.108.186	28							
0.986	10.234.234.104	131.253.34.232	28							
0.984	10.234.234.103	131.253.34.248	26							
0.984	10.234.234.105	40.77.224.145	28							

RITA | Viewing: DNSCat-2017-03-21 | Beacons | DNS | BL Source IPs | BL Dest. IPs | BL Hostnames | BL URLs | Scans | Long Connections | Long URLs | User Agents | RITA on

Subdomain	Visited	Domain
25185	63995	com
23362	40799	nanobotninjas.com
23361	40799	cat.nanobotninjas.com
1960	33139	net
270	9746	akamaiedge.net
221	682	edgekey.net
200	2466	org
183	2612	akadns.net
173	478	uk
164	371	co.uk

BUGCON 2022

Más información

- zeek.org
- corelight.com
- zeekorg.slack.com
- github.com/zeek
- github.com/activecm/rita
- github.com/ksaver/zeek-bugcon-2022
- vsalazar@globalcybersec.com

Hacking:
Computing Power to the People

Gracias :)

BUGCON
2022