



# Egress Traffic Analysis



© Black Hills Information Security | @BHInfoSecurity

# MITRE and Egress

Command and Control	Exfiltration
Commonly Used Port	Automated Exfiltration
Communication Through Removable Media	Data Compressed
Connection Proxy	Data Encrypted
Custom Command and Control Protocol	Data Transfer Size Limits
Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Data Encoding	Exfiltration Over Command and Control Channel
Data Obfuscation	Exfiltration Over Other Network Medium
Domain Fronting	Exfiltration Over Physical Medium
Domain Generation Algorithms	Scheduled Transfer

Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service



# Need For Visibility



- Basic alerting is not enough
- The need for context
- further identifying gaps in endpoint coverage
- IoT, Shadow IT access
- When things go bad, you need answers
- This is why the mix between network and host-based data is key
- Even Gartner and I agree on this.



# Netflow



- Created by Cisco
- Collection of traffic statistics
- Quickly became a standard
- Exporter, Importer and Analysis
- Spawned off a lot of other companies creating their own flow
- Also, different implementations





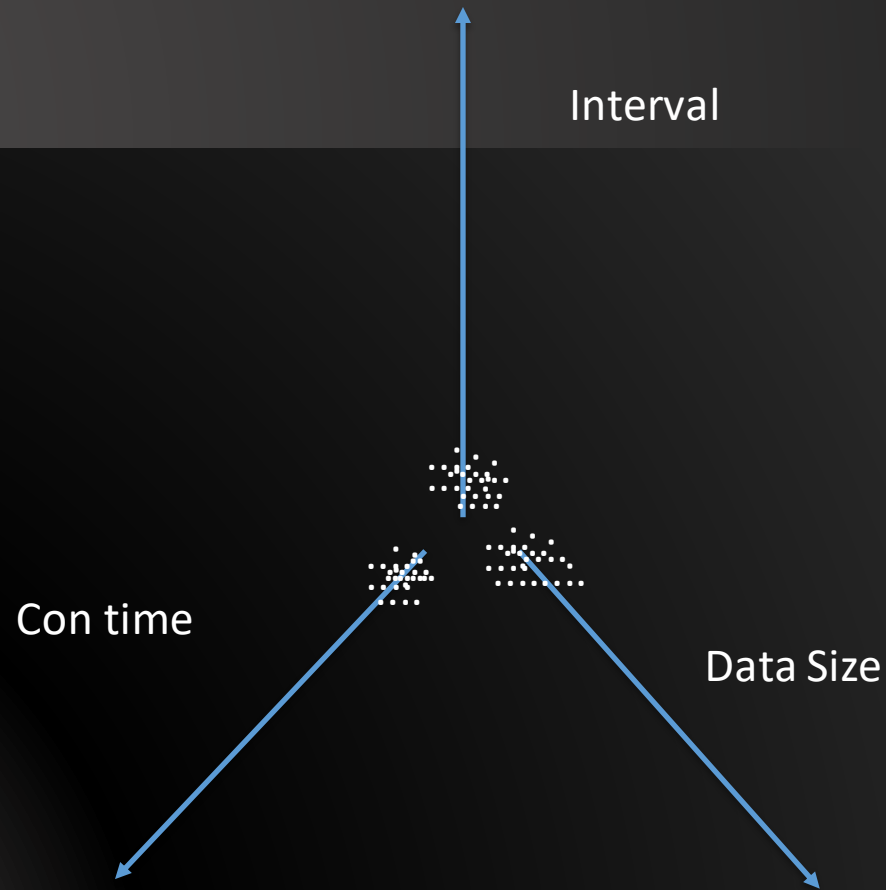
- Speed
- Large user base
- Lots of support
- Consistency
- Timestamps are key
- Many devices handle timestamps in different/odd ways
- Generates required log files
- We are moving away from signature-based detection
- Too many ways to obfuscate
- Encryption, Encoding, use of third-party services like Google DNS





- Finds patterns in network traffic
- Specifically looks for beacons
- Also, Denylist checking, DNS views, Long Connections
- All for free
- Check it out!
- <https://github.com/activecm/rita>





# Long Connections



```
thunt@thunt-one-day:~/lab1$ rita show-long-connections lab1 | head
Source IP, Destination IP, Port: Protocol: Service, Duration
10.55.100.100, 65.52.108.225, 443: tcp: -, 86222.4
10.55.100.107, 111.221.29.113, 443: tcp: -, 86220.1
10.55.100.110, 40.77.229.82, 443: tcp: -, 86160.1
10.55.100.109, 65.52.108.233, 443: tcp: ssl, 72176.1
10.55.100.105, 65.52.108.195, 443: tcp: ssl, 66599
10.55.100.103, 131.253.34.243, 443: tcp: -, 64698.4
10.55.100.104, 131.253.34.246, 443: tcp: ssl, 57413.3
10.55.100.111, 111.221.29.114, 443: tcp: -, 46638.5
10.55.100.108, 65.52.108.220, 443: tcp: -, 44615.2
thunt@thunt-one-day:~/lab1$ _
```





# Beacons



```
thunt@thunt-one-day:~/lab1$ rita show-beacons lab1 | head
Score,Source IP,Destination IP,Connections,Avg Bytes,Intvl Range,Size Range,
Top Intvl,Top Size,Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl
Dispersion,Size Dispersion
1,192.168.88.2,165.227.88.15,108858,199,860,230,1,89,53341,108319,0,0,0,0
1,10.55.100.111,165.227.216.194,20054,92,29,52,1,52,7774,20053,0,0,0,0
0.838,10.55.200.10,205.251.194.64,210,308,29398,4,300,70,109,205,0,0,0,0
0.835,10.55.200.11,205.251.197.77,69,308,1197,4,300,70,38,68,0,0,0,0
0.834,192.168.88.2,13.107.5.2,27,198,2,33,12601,73,4,15,0,0,0,0
0.834,10.55.100.111,34.239.169.214,34,704,5,4517,1,156,15,30,0,0,0,0
0.833,10.55.100.106,23.52.161.212,27,940,38031,52,1800,505,19,19,0,0,0,0
0.833,10.55.100.111,23.52.162.184,27,2246,37828,52,1800,467,23,25,0,0,0,0
0.833,10.55.100.100,23.52.161.212,26,797,36042,52,1800,505,16,25,0,0,0,0
thunt@thunt-one-day:~/lab1$
```



# What Will You Find Other Than Malware?

## TeamViewer Confirms Undisclosed Breach From 2016

By Sergiu Gatlan

May 17, 2018 02:02 PM



TeamViewer confirmed today that it has been the victim of a cyber attack which was discovered during the autumn of 2016, but was never disclosed. This attack is thought to be of Chinese origins and utilized the Winnti backdoor.

## WY: Gillette hospital targeted in ransomware attack

SEPTEMBER 21, 2019 DISSENT

Seth Klamann reports:

Campbell County Health in Gillette was targeted in a ransomware attack Friday, according to an alert the state Department of Health sent to health care providers.

The attack occurred early Friday morning, at approximately 3 a.m. The hospital "experienced serious computer issues" due to the attack. This caused a "service disruption" at the facility.

Read more on [Casper Star-Tribune](#). Updates on the situation are provided on the [county's web site](#). At the time of this posting, there is a notice at the top of the home page saying:



## SALTED HASH- TOP SECURITY NEWS

By [Steve Ragan](#), Senior Staff Writer, CSO FEB 28, 2018 4:00 AM PST

About

Fundamental security insight to help you minimize risk and protect your organization

NEWS

## Nuance says NotPetya attack led to \$92 million in lost revenue

Recent SEC filings disclose losses, and predicts additional spend in 2018 for security enhancements and upgrades



**BLACK HILLS** | Information Security

# SNR

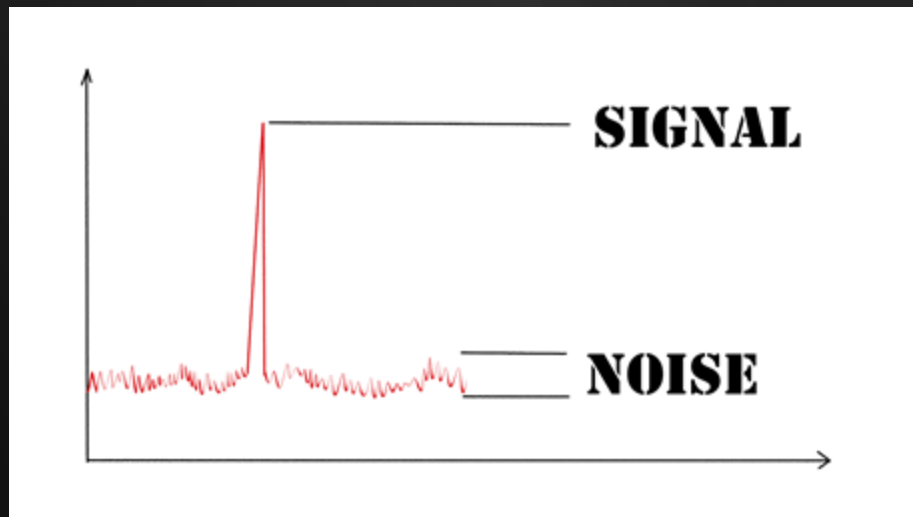


A special note on signal to noise....

Lets kill..

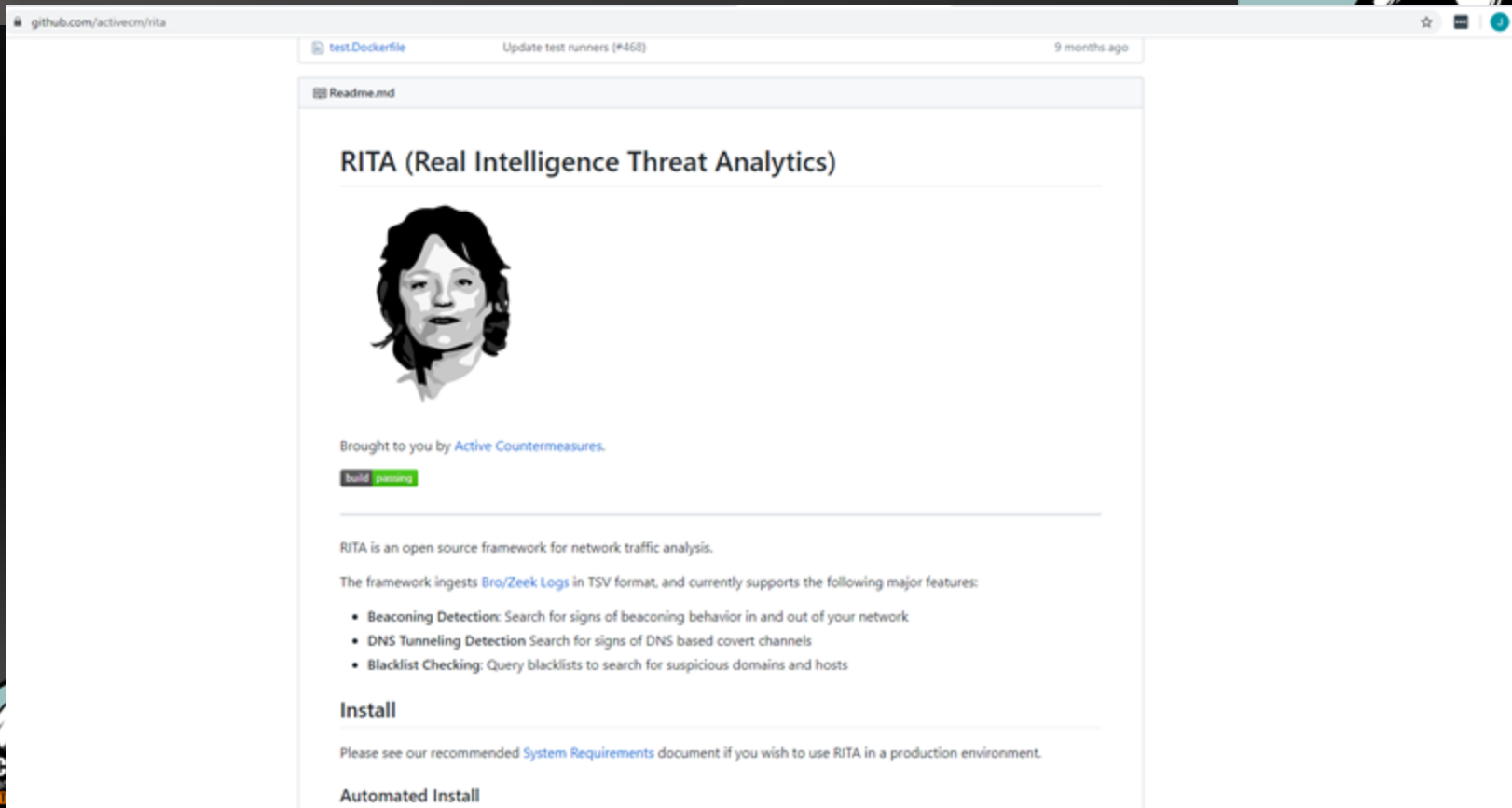
Ads

Weird beacons.



© Black Hills Information Security | @BHInfoSecurity

# It's Free




The screenshot shows the GitHub repository page for `activecm/rita`. The repository is titled "RITA (Real Intelligence Threat Analytics)" and is described as an open source framework for network traffic analysis. The page includes a profile picture of a woman, a "Brought to you by Active Countermeasures" note, and a "Build" status indicator showing "passing". The "Readme.md" file is selected, displaying the repository's description and features.

github.com/activecm/rita

test.Dockerfile Update test runners (#468) 9 months ago

Readme.md

## RITA (Real Intelligence Threat Analytics)



Brought to you by [Active Countermeasures](#).

Build passing

RITA is an open source framework for network traffic analysis.

The framework ingests [Bro/Zeek Logs](#) in TSV format, and currently supports the following major features:

- **Beaconing Detection:** Search for signs of beaconing behavior in and out of your network
- **DNS Tunneling Detection** Search for signs of DNS based covert channels
- **Blacklist Checking:** Query blacklists to search for suspicious domains and hosts

### Install

Please see our recommended [System Requirements](#) document if you wish to use RITA in a production environment.

#### Automated Install

# It Will Be Free.



UNITED STATES PATENT AND TRADEMARK OFFICE  
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT RECORDATION BRANCH OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE ASSIGNMENT RECORDATION BRANCH AT 571-272-3350. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, MAIL STOP: ASSIGNMENT RECORDATION BRANCH, P.O. BOX 1450, ALEXANDRIA, VA 22313.

RECORDATION DATE: 05/31/2018

REEL/FRAME: 045948/0205  
NUMBER OF PAGES: 4

BRIEF: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

DOCKET NUMBER: BHIS-P0001C1

ASSIGNOR:  
FEHRMAN, BRIAN

DOC DATE: 04/20/2017

ASSIGNEE:  
NETSEC CONCEPTS, LLC  
21148 TWO BIT SPRINGS RD  
STURGIS, SOUTH DAKOTA 57785

APPLICATION NUMBER: 15956933

FILING DATE: 04/19/2018

PATENT NUMBER:

ISSUE DATE:

TITLE: MALWARE BEACONING DETECTION METHODS

ASSIGNMENT RECORDATION BRANCH  
PUBLIC RECORDS DIVISION

© Black Hills Information Security | @BHInfoSecurity



# Full pcap



- Very portable
- Everything supports it
- Issues of size
- Encryption can cause issues
- Learning curve
- Tcpdump and Wireshark are the key tools to learn
- Let's play with it now.

```
root@pop-os:~# tcpdump -i wlp0s20f3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp0s20f3, link-type EN10MB (Ethernet), capture size 262144 bytes
08:46:28.184586 IP map2.hwcdn.net.http > pop-os.34009: Flags [.] , seq 4247888066
:4247890962, ack 3187269570, win 59, options [nop,nop,TS val 1138523834 ecr 1935
086224], length 2896: HTTP
08:46:28.185682 IP pop-os.34009 > map2.hwcdn.net.http: Flags [.] , ack 4294935440
, win 12299, options [nop,nop,TS val 1935086524 ecr 1138523832,nop,nop,sack 2 {4
294962952:2896}{4294945576:4294954264}], length 0
08:46:28.185878 IP map2.hwcdn.net.http > pop-os.34009: Flags [.] , seq 14480:1592
8, ack 1, win 59, options [nop,nop,TS val 1138523834 ecr 1935086224], length 144
8: HTTP
08:46:28.186944 IP pop-os.34009 > map2.hwcdn.net.http: Flags [.] , ack 4294935440
, win 12299, options [nop,nop,TS val 1935086525 ecr 1138523832,nop,nop,sack 3 {1
4480:15928}{4294962952:2896}{4294945576:4294954264}], length 0
08:46:28.187198 IP pop-os.56430 > _gateway.domain: 48232+ [1au] PTR? 38.0.0.10.i
n-addr.arpa. (51)
```



# Egress Capture



- First, you will need to have a system to capture the traffic
- Second, RITA is free and awesome



Pre NAT:



Zeek, RITA



# Dedicated Capture Devices



- Gigamon
- Corelight
- Plug and Play
- Very expensive
- How much time?





# User Agent Strings



Useragent String	Seen	Requests	Sources
Microsoft-Delivery-Optimization/10.0	48	au.download.windowsupdate.com, 2.tlu.dl.delivery.mp.microsoft.com	192.168.99.10, 192.168.99.52
Windows-Update-Agent/10.0.10011.16384 Client-Protocol/2.0	98	download.windowsupdate.com	192.168.99.10
Microsoft-WNS/10.0	720	tile-service.weather.microsoft.com	192.168.99.53, 192.168.99.51, 192.168.99.54, 192.168.99.52, 192.168.99.55
Microsoft-CryptoAPI/10.0	795	www.microsoft.com, ocsp.msocsp.com, ocsp.digicert.com, ctldl.windowsupdate.com	192.168.99.53, 192.168.99.10, 192.168.99.51, 192.168.99.52, 192.168.99.54, 192.168.99.55
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	7059	wilfredcostume.bamoon.com	192.168.99.52





README.md

## JA3 - A method for profiling SSL/TLS Clients

JA3 is a method for creating SSL/TLS client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence.

Before using, please read this blog post: [TLS Fingerprinting with JA3 and JA3S](#)

This repo includes JA3 and JA3S scripts for [Zeek](#) and [Python](#).

JA3 support has also been added to:

[Moloch](#)

[Trisul NSM](#)

[NGINX](#)

[MISP](#)

[Darktrace](#)

[Suricata](#)

[Elastic.co](#) [Packetbeat](#)

[Splunk](#)

[MantisNet](#)

[ICEBRG](#)

[Redsocks](#)

[NetWitness](#)

[ExtraHop](#)

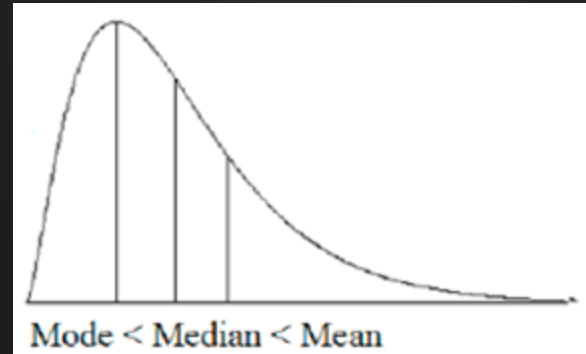
[Vectra Cognito Platform](#)



# Long Tail



- Key for any hunting is looking for outliers
- Never go looking for a needle in a haystack
- Sort, and look for anomalies
- True for endpoint
- True for Network
- A simple sort on connections



# Denylists



RESULTS

Total Bytes Exchanged (▼)

Sort

search

165.227.88.15

165.227.216.194

ADDRESS	CONNS	BYTES	COMM
192.168.88.2	108858	21.73 MB	53:udp:dns,53:tcp:-

165.227.88.15

asn: 14081

org: DIGITALOCEAN-ASN

range: 165.227.0.0/16

city: North Bergen

country: United States

postal: 07047

location: 40.793N, -74.0247W

fqdn: baddns.r-1x.com

total connections: 108858

unique connections: 1

total bytes transferred: 21.73 MB

inbound bytes: 9.78 MB

outbound bytes: 11.95 MB

1/1

# Security Onion



- Security Onion is free and kicks most commercial tools to the curb
- They offer training
- Zeek, Suricata and so much more are included
- Works with RITA!!!





# LAB: Zeek/RITA



© Black Hills Information Security | @BHInfoSecurity