Exposing the Rat in the Tunnel:

Using Traffic Analysis for Tor-based Malware Detection

Priyanka G. Dodia : Qatar Computing Research Institute (QCRI)
Mashael S. Al-Sabah: Qatar Computing Research Institute (QCRI)
Omar Alrawi: Georgia Institute of Technology
Tao Wang: Simon Fraser University

QCRI
معهد قطر لبحوث الحوسبة
Qatar Computing Research Institute
جامعة حمد بن خليفة
HAMAD BIN KHALIFA UNIVERSITY

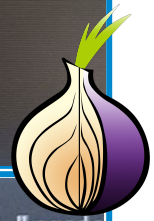
Motivation: The ‘WannaCry’ Ransomware Case Study

Enterprise Logs

- Real network traffic from industry partners in Qatar
  - Zeek logs with 600 million TCP/ICMP/UDP connections
- Hundreds of Tor connections
- High frequency of C&C Tor hidden service (**.onion**) **leaks** and kill switch domain accesses in the data

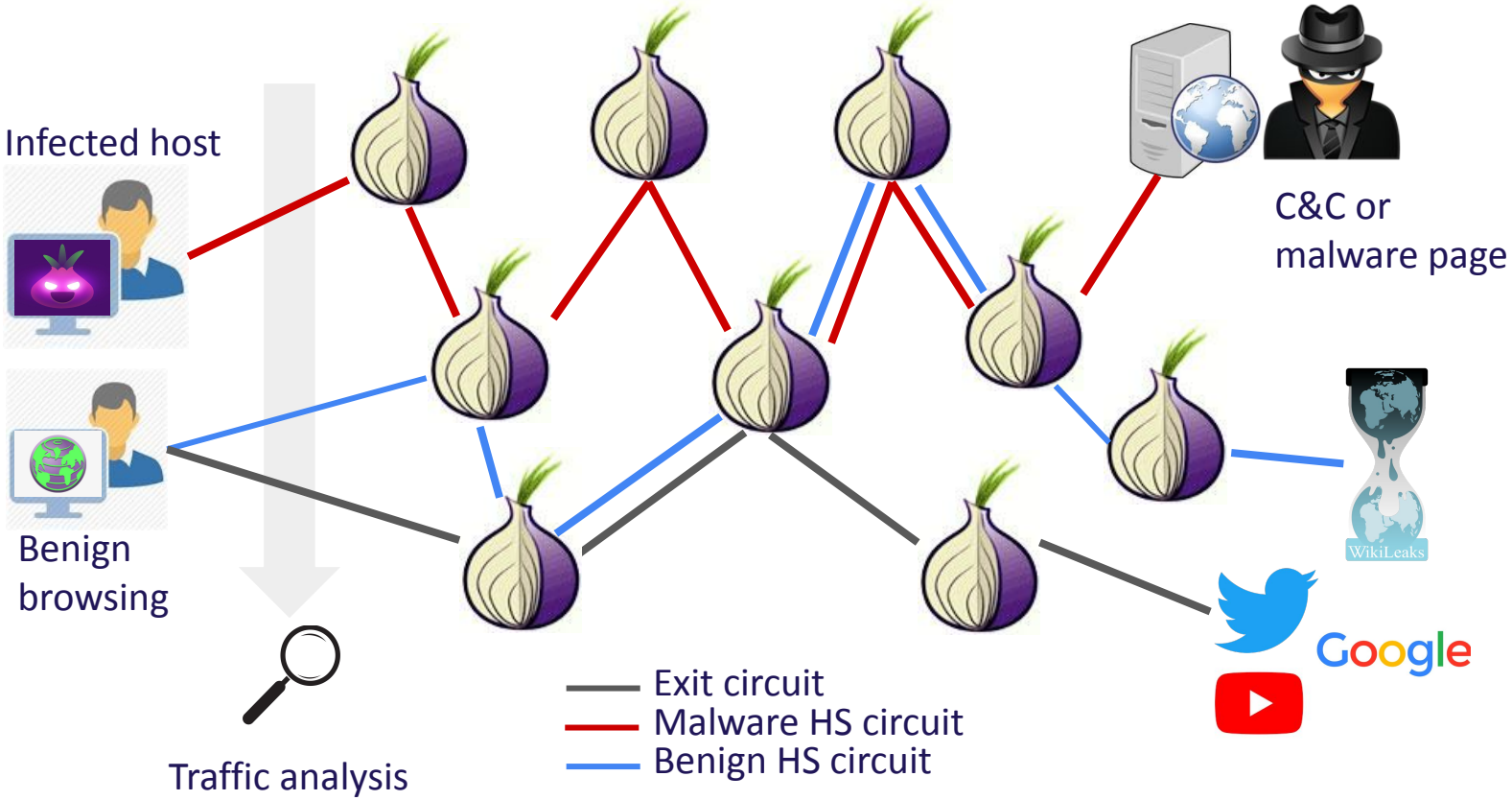
Command line snapshots of malware traces in network logs

```
175 "57g7spgrzlojinas.onion"
170 "76jdd2ir2embyv47.onion"
168 "cwwnhwhlz52ma.onion"
172 "cwwnhwhlz52maqm7.onion"
167 "gx7ekbenv2riucmf.onion"
170 "sqjolphimrr7jqw6.onion"
173 "xxlvbrloxvriy2c5.onion"
```



```
iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.org.qa" killswitch_domain.logs
{"AA":false,"id.resp_h":"82.148.111.11","TC":false,"qclass":1,"path":"/usr/local/bro/logs/current/dns.log","rcode
ame":"NXDOMAIN","rejected":false,"ts":1543901925.566,"query":"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.org.q
,"qtype":1,"RD":true,"@version":"1","Z":0,"id.resp_p":53,"id.orig_h":"213.130.112.178","id.orig_p":57353,"@timest
p":"2018-12-04T05:38:45.566Z","rcode":3,"host":"[redacted]","client":"[redacted]","RA":false,"qclass_name":"C_INTERNET","qtyp
name":"A","proto":"udp","uid":"Cu3G2j2VvqFzlDEkG9","logtype":"bro-dns","type":"bro-dns","trans_id":36655}
```

Traffic Analysis for Tor-based Malware Detection



Research Questions

- Can we distinguish between benign and malware related Tor connections?
- Can we deduce the **type** of malware?
- Can we do this for unknown ‘zero-day’ malware accurately?

Tor-based Malware Binary Collection

1. Binary Collection

VIRUSTOTAL

33 / 71

Community Score

33 security vendors and 3 sandboxes flagged this file as malicious

fe61b7e86b36434229c393ff08855254174d29a69980f2760848dae487288c82

dcwwvwf

direct-cpu-clock-access | executes-dropped-file | malware | peexe | self-delete | upx

222.00 KB Size

2021-01-04 01:34:40 UTC 1 year ago

DETECTION | DETAILS | RELATIONS | BEHAVIOR

Crowdsourced IDS Rules

Matches rule ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 682 from Proofpoint Emerging Threats Open
↳ Misc Attack

Matches rule ET POLICY TLS possible TOR SSL traffic from Proofpoint Emerging Threats Open
↳ Misc activity

File System Actions

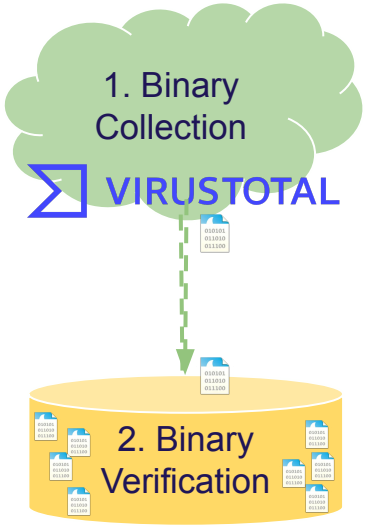
Files Dropped

- %LOCALAPPDATA%\699f3df3\tor\data\cached-certs
- %LOCALAPPDATA%\699f3df3\tor\data\cached-certs.tmp
- %LOCALAPPDATA%\699f3df3\tor\data\cached-microdesc-consensus
- %LOCALAPPDATA%\699f3df3\tor\data\cached-microdesc-consensus.tmp
- %LOCALAPPDATA%\699f3df3\tor\data\cached-microdescs.new
- %LOCALAPPDATA%\699f3df3\tor\data\state

Bundled Files (6)

Scanned	Detections	File type	Name
2022-04-24	43 / 69	Win32 EXE	hvnc.exe
2022-01-13	49 / 67	Win32 EXE	BitRAT.exe
2022-04-15	2 / 69	Win32 EXE	tor.exe
2022-05-15	0 / 65	Win32 DLL	libcrypto-1_1.dll
2021-10-15	0 / 57	?	ipdb.bin
2022-08-13	0 / 69	Win32 DLL	libssl-1_1.dll

Tor-based Malware Binary Verification



Consensus

TLS

- www.2ahmrvssyrvsiyg3zc6l.com
- www.33rt6up6k7oexutgdtjuanf.com
- www.4g4ewmccgm337hggem4jgb.com
- www.6pr3k3djr.com
- www.7le5trltjeptd.com
- www.cednrx6tp3mtpn5lbp4uf26.com
- www.dphwwn6earpeyrm3d4d2.com
- www.duwax35nwqs7z3jub7xgddou.com

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Security Vendors' Analysis

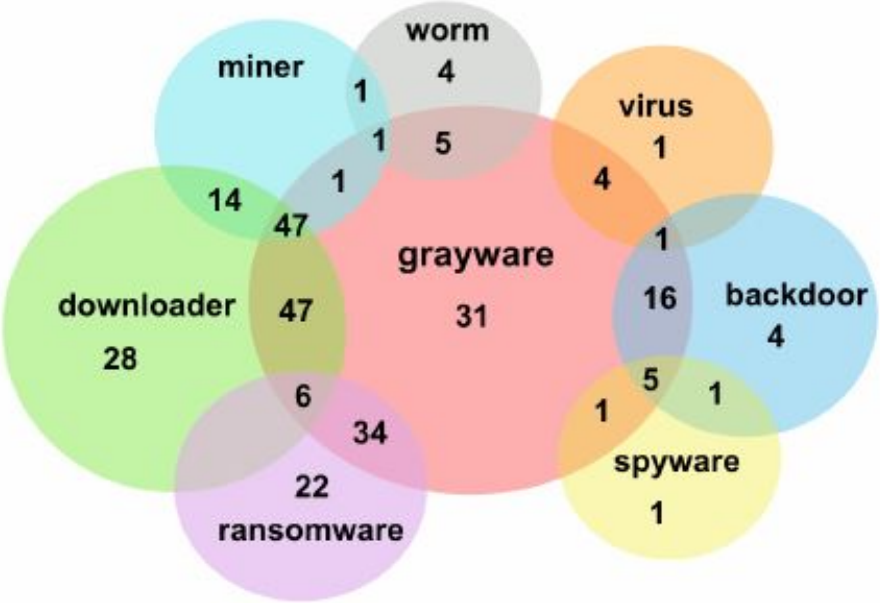
AegisLab	Trojan.Win32.Bulz.4!c
ALYac	Gen:Trojan.Heur.RP.cmGfb0qToep
Avast	Win32:Malware-gen
Avira (no cloud)	TR/Redcap.zxhpp
Cynet	Malicious (score: 85)
eScan	Gen:Variant.Bulz.316791
F-Secure	Trojan.TR/Dropper.Gen
GData	Gen:Trojan.Heur.RP.cmGfb0qToep
Kaspersky	HEUR:Trojan.MSIL.Injuke.gen
MAX	Malware (ai Score=87)
Microsoft	Trojan:Win32/Ymacco.AAFB
Qihoo-360	Win32/Trojan.Injuke.HqcASO8A
Sangfor Engine Zero	Trojan.Win32.Save.a
Sophos	Mal/Generic-S

Tor-based Malware Traffic Collection

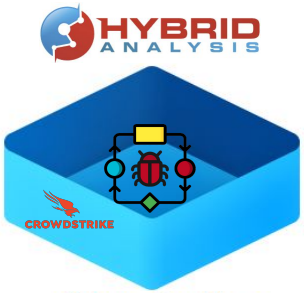
Traffic Characteristics

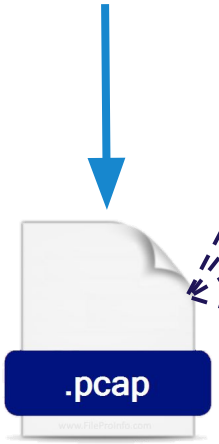
Malware

- Malware traffic
  - Collection period: 3 months
  - PCAPs: ~6000 (362 active/523 binaries)
  - Classes: 10
  - Families: 80
  - Tor connections: ~30,500



Classifier Features





Tor Connections

T1

T2

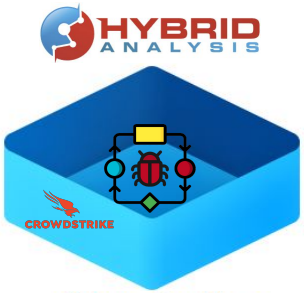
T3

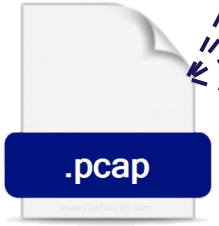
TN

Classifier Instances (CI)

Connection-level	Host-level	Class label
Connection-level	Host-level	Class label
Connection-level	Host-level	Class label
Connection-level	Host-level	Class label

Classifier Features





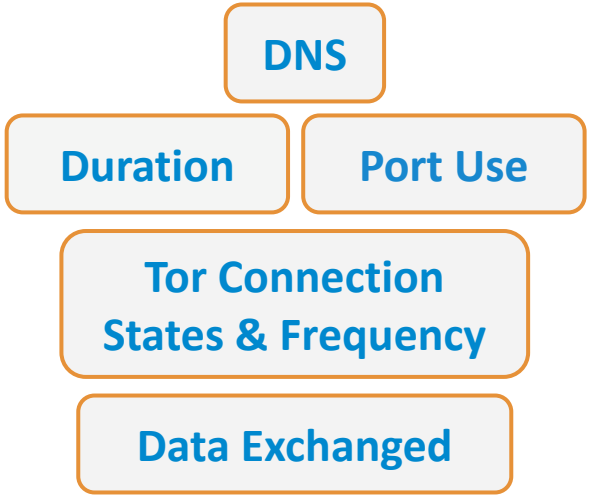
Tor Connections

Classifier Instances (CI)

T1	Connection-level	Host-level	Class label
T2	Connection-level	Host-level	Class label
T3	Connection-level	Host-level	Class label
⋮			
TN	Connection-level	Host-level	Class label

Classifier Features

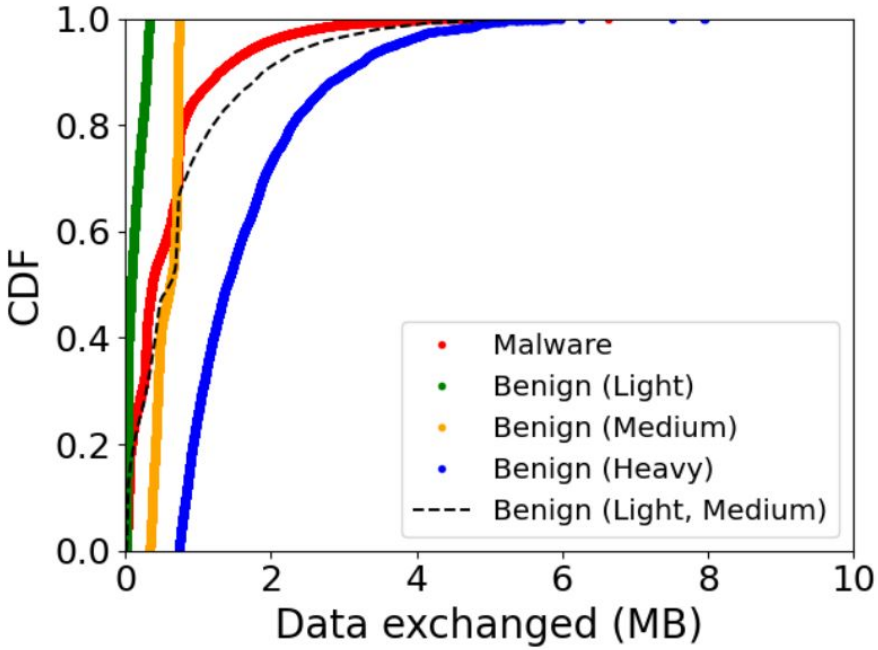
- **Host-level:** 40 global PCAP-level features [NOVEL]
- **Connection-level:** 150 WF features [USENIX 2016]
  - Packet inter-arrival time
  - Packet concentration
  - Outgoing packets
  - Rate of packets



Host-level Feature Categories

Traffic Characteristics

Malware & Benign



- Benign traffic
  - Different browsing profiles
  - Overlapping distribution with malware traffic
    - Unbiased training data
    - Representative of real world scenario

Performance Evaluation: Binary Classification

Features	Best Performing Model	Precision (%)	Recall (%)	False Positive Rate (%)
Connection-level only	XGBoost	86.13	63.37	1.53
Host-level only	LightGBM	90.96	76.34	1.45

Performance Evaluation: Binary Classification

Features	Best Performing Model	Precision (%)	Recall (%)	False Positive Rate (%)
Connection-level only	XGBoost	86.13	63.37	1.53
Host-level only	LightGBM	90.96	76.34	1.45

Performance Evaluation: Binary Classification

Features	Best Performing Model	Precision (%)	Recall (%)	False Positive Rate (%)
Connection-level only	XGBoost	86.13	63.37	1.53
Host-level only	LightGBM	90.96	76.34	1.45

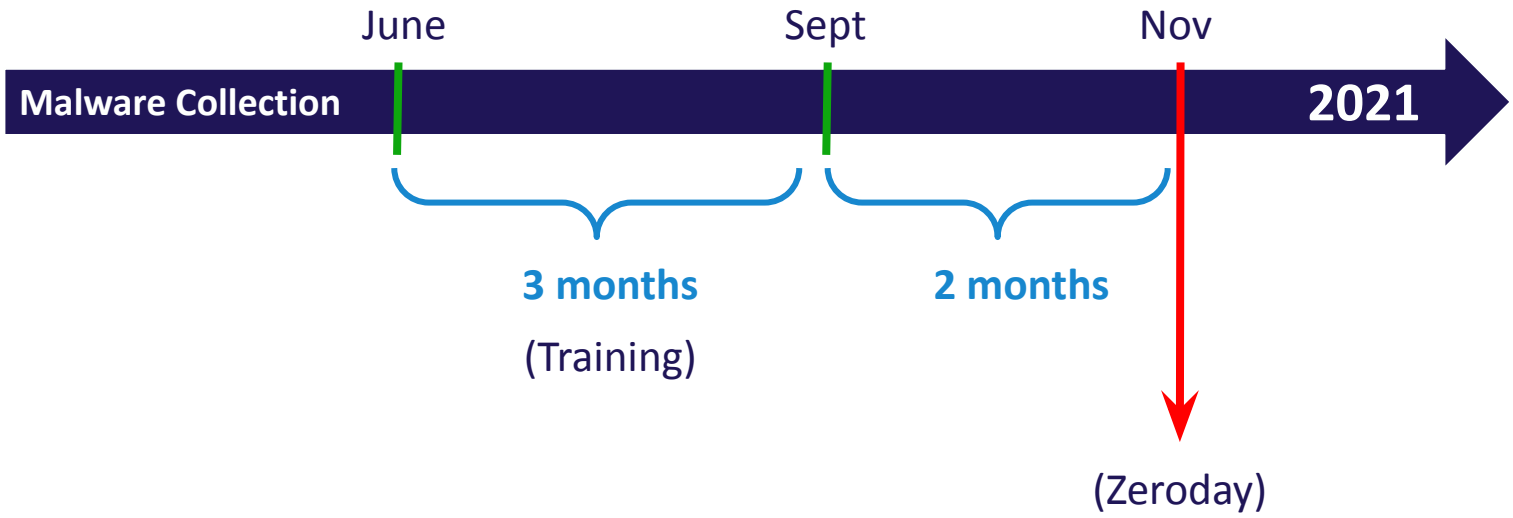
Useful for detection in the absence of raw PCAPs!

Performance Evaluation: Binary Classification

Features	Best Performing Model	Precision (%)	Recall (%)	False Positive Rate (%)
Connection-level only	XGBoost	86.13	63.37	1.53
Host-level only	LightGBM	90.96	76.34	1.45
Connection- & Host-level	LightGBM	93.33	81.60	0.88

Zeroday Malware: Identifying Tor Connections

- **Zeroday Test:** New zeroday binaries collected **2 months after** training binaries
- Not used in training



Zeroday Malware: Identifying Tor Connections

- **Zeroday dataset:** New zeroday binaries 2 months after training binaries

- Binaries with active Tor traffic from **'EternalRocks'** family
  - Use Tor browser for C&C
  - Bonus Challenge!

Malware Instances in Test	False Positive Rate (%)	Precision (%)	Recall (%)
1%	1.1	54.5	100
5%	0.7	87.5	
10%	1.0	91.3	
20%	1.2	95.4	

Zeroday Malware: Identifying Malware Classes

- Evaluate Random Forest models trained with multi labelling techniques

- **Class prediction performance:**
  - At least one correct class label
  - High precision (94 - 100%) & Low *Hamming Loss* (false labels in predictions)

Takeaways

- Goal: Identify Tor-based malware connections
- **Traffic analysis** to fingerprint Tor-based malware activity
- **Malware class labels** can be deduced using **connection- & host-level features**
- Validate usability with **zeroday test and real world enterprise data**

Expose the Rats Yourself!

- Code and datasets available at Github:

  https://github.com/malfp/tormalwarefp

- Contact us for full malware corpus, PCAPs and more:

Priyanka Dodia
pgdodia@hbku.edu.qa
Cybersecurity
Qatar Computing Research Institute (QCRI)

Supplementary Slides

Classifying Real Ransomware Connections

Enterprise Logs

- Examine best performing LightGBM model trained using D5
- **Enterprise test dataset:**
  - Tor connections: **207** (Infected host: **197**, Benign hosts: 10)
  - Classification Instances: **63**
    - Features used: **Host-only**
- **Classification results**: **16**/63 >= 80% confidence trace back to malicious host with onion leaks
  - **Misidentified:** 29/63 with very low confidence (< 64%) belonging to benign hosts

Malware Class Identification

Multi-class classifier performance trained with D5

Classification technique	Hamming loss	Micro-average precision(%)	Micro-average recall(%)
Binary Relevance	0.1	68.12	70.77
Classifier Chains	0.1	67.77	71.05
Label Powerset	0.1	66.81	72.37

Existing Malicious Traffic Detection Efforts

Related work	Detection point	Detection artifact	Detection approach	Scope	Class detection
BotMiner [34]	Network (client side)	TCP/UDP flow size DNS, SMTP, C&C IP	Unsupervised network flow clustering	Coordinated bots	✗
Jackstraws [39]	End Host	System calls	Supervised system call behaviour graph clustering	Generic malware	✗
TorWard [41]	Network (Tor exit OR)	TCP flow DPI, DNS C&C IP	Signature-based DPI	Tor exit traffic abuse	✓
BOTection [22]	Network (client side)	TCP/UDP/ICMP connection state, protocols (eg. DNS)	Connection state stochastic modeling	Bots w/ bursty connection behavior	✓
This work	Network (client side)	Tor cell sequences (TCP), connection states, DNS	Traffic analysis on encrypted flows	Tor-based malware	✓