

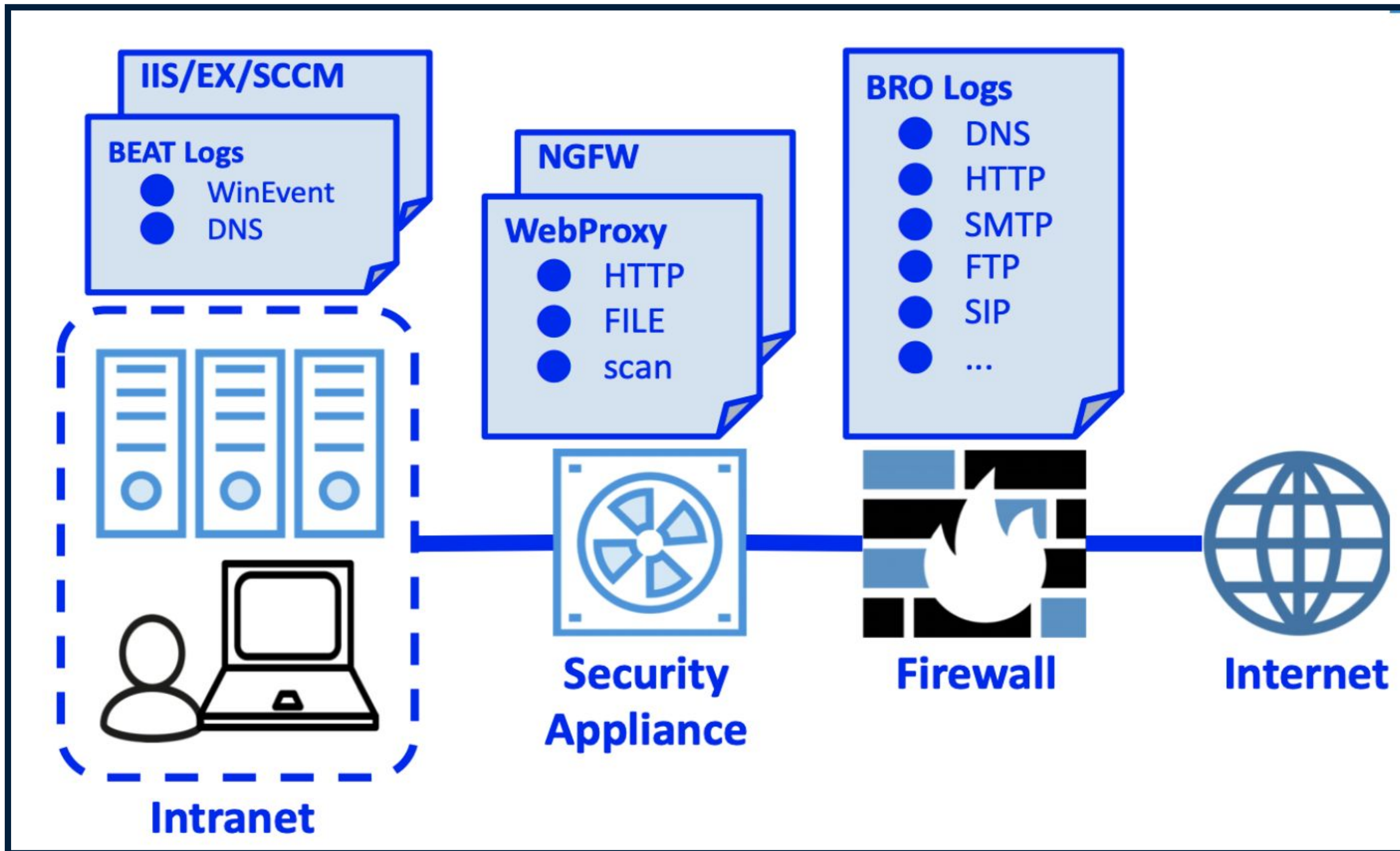
Priyanka Dodia

Qatar Computing Research Institute, HBKU
Doha, Qatar
pgdodia@hbku.edu.qa

Mashael S. Al Sabah

Qatar Computing Research Institute, HBKU
Doha, Qatar
msalsabah@hbku.edu.qa

MOI Log DATA

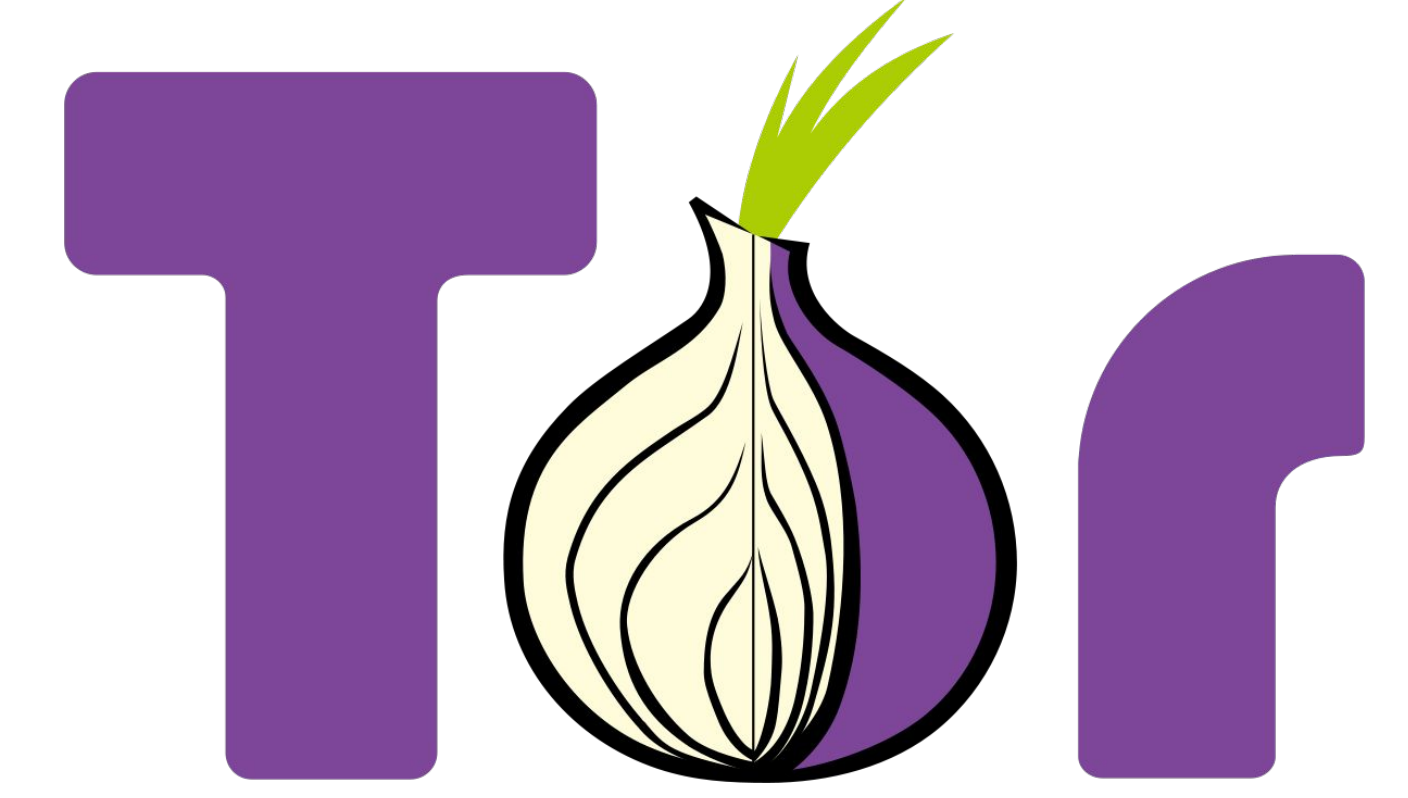


The Ministry of Interior data consists of system and network level activity logs. In this study we focus on network level activity recorded over 2 years (2018-19). Network traffic is recorded with BRO/Zeek analyzer which splits logs based on application protocols such as DNS, HTTP, FTP etc.

NETWORK LOG ANALYSIS

Goal: In this work, we analyse network logs in ministry data for VPN and Tor based suspicious activity.

- We investigate logs for
1. Tor connections
 2. Onion domains
 3. VPN



Summary of Findings:

- Found leaked onion domains in DNS logs related to **WannaCry Ransomware** in Ministry Of Public Health (MOPH) network.
- Suspicious DNS log entries with multiple VPN IPs accessing onion domain payment site for **BadRabbit Ransomware** in Ministry Of Justice (MOJ) logs.

FINDINGS

Ministry	Total Connections Recorded (2018-19; conn.logs)	TOR Connections Found (Unique TOR IPs)	Ministry	Total DNS Entries Recorded	DNS Lookups for VPN Server (Unique Server)	VPN Related DNS Lookups (by "vpn" string search)	Ministry	Onion Domains Found (dns.logs)	Unique Onion Domains	Malware Related Onion Domains
MOJ	1 Billion	5318 (5)	MOJ	2 Billion	18810 (12)	1Million 426K	MOJ	2 Million 929 K	27,232	1
MOPH	606 Million	162 (19)	MOPH	176 Million	59 (22)	57,765				
MEI	159 Million	19 (2)	MEI	34 Million	0	949	MOPH	1252	34	7

Tor Connections

VPN Connections

Onion Domains

TRACES OF TOR MALWARE IN MOI NETWORK

```
MOIQ\pdodia@crimoiqphys003:/data/pdodia/
ogtype wcry_onion.logs | sort | uniq -c
1195 "bro-dns"
MOIQ\pdodia@crimoiqphys003:/data/pdodia/
query wcry_onion.logs | sort | uniq -c
175 "57g7spgrzlojinaz.onion"
170 "76jdd2ir2embyv47.onion"
168 "cwwnhwhl252ma.onion"
172 "cwwnhwhl252maqm7.onion"
167 "gx7ekbenv2riucmf.onion"
170 "sqj0lphimrr7jqw6.onion"
173 "xxlvhrlaxvny2c5.onion"
```

```
10007 "131.220.77.212.caforssztxqzf2nm.onion"
10278 "243.215.112.195.caforssztxqzf2nm.onion.moj.gov.qa"
10919 "214.76.41.129.caforssztxqzf2nm.onion"
11165 "134.36.240.54.caforssztxqzf2nm.onion.moj.gov.qa"
11241 "134.36.240.54.caforssztxqzf2nm.onion"
11446 "199.57.211.89.caforssztxqzf2nm.onion"
11847 "61.53.100.78.caforssztxqzf2nm.onion"
12247 "243.215.112.195.caforssztxqzf2nm.onion"
12680 "199.57.211.89.caforssztxqzf2nm.onion.moj.gov.qa"
12949 "61.53.100.78.caforssztxqzf2nm.onion.moj.gov.qa"
15310 "70.212.219.61.caforssztxqzf2nm.onion"
16256 "mail.onionit.com"
23811 "246.121.130.213.caforssztxqzf2nm.onion.moj.gov.qa"
26992 "215.20.255.51.caforssztxqzf2nm.onion"
27506 "246.121.130.213.caforssztxqzf2nm.onion"
30315 "215.20.255.51.caforssztxqzf2nm.onion.moj.gov.qa"
```

WCry C&C Onion Domains

WCry Kill Switch Onion Domain

BadRabbit Ransom Payment Site Access Attempts using VPNs

WannaCry Ransomware in MOPH

BadRabbit Ransomware in MOJ

RESEARCH DIRECTION

- In this study we identify several Tor connections and accidental onion domain leaks that reveal presence of malware in the Ministry network.
- In the absence of accidental DNS leaks, it is a challenge to identify which Tor connections relate to malware activity.
- Our ongoing research efforts focus on developing a mechanism to detect Tor based malware from observed network activity using Artificial Intelligence, specifically Machine Learning techniques.