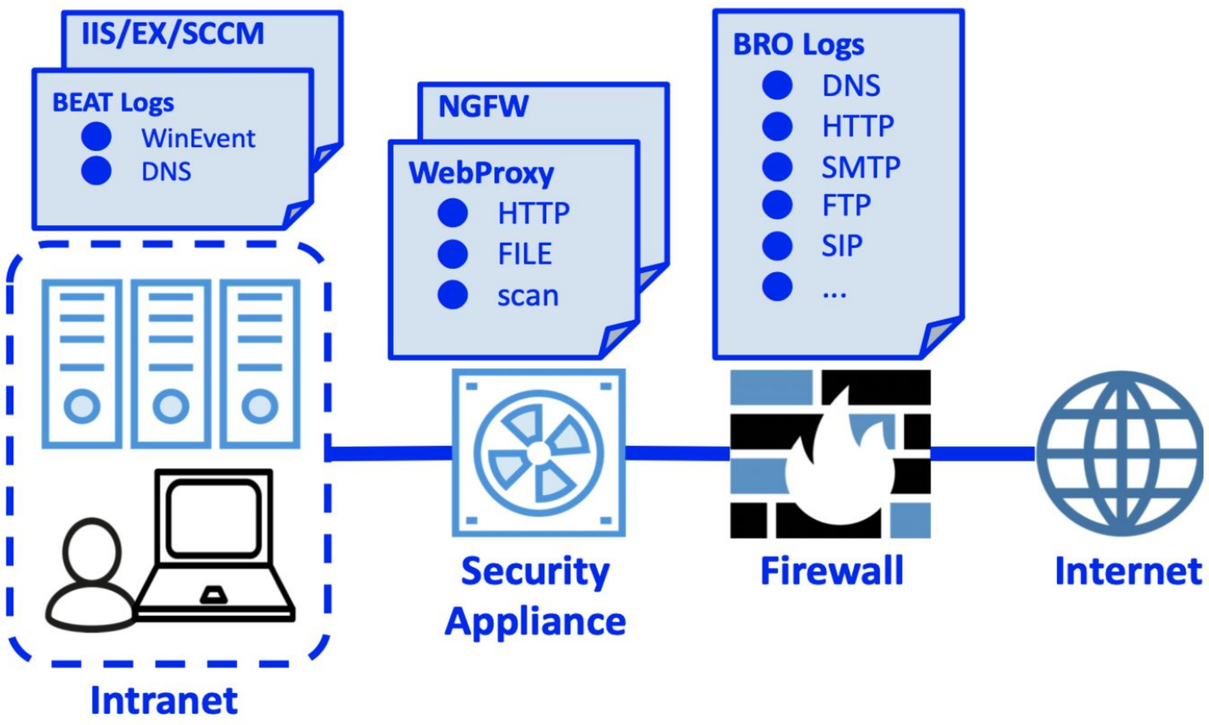
VPN and Tor Based Malware Activity in Ministry Of Interior Network Data

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)
MOJ	1 Billion	5318 (5)
MOPH	606 Million	162 (19)
MEI	159 Million	19 (2)

Tor Connections

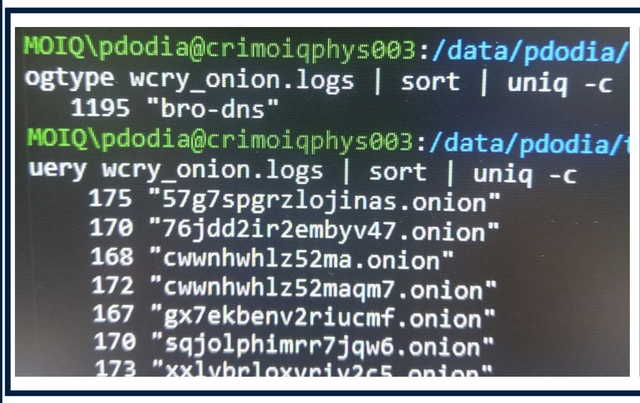
Ministry	Total DNS Entries Recorded	DNS Lookups for VPN Server (Unique Server)	VPN Related DNS Lookups (by "vpn" string search)
MOJ	2 Billion	18810 (12)	1Million 426K
MOPH	176 Million	59 (22)	57,765
MEI	34 Million	0	949

VPN Connections

Ministry	Onion Domains Found (dns.logs)	Unique Onion Domains	Malware Related Onion Domains
MOJ	2 Million 929 K	27,232	1
MOPH	1252	34	7

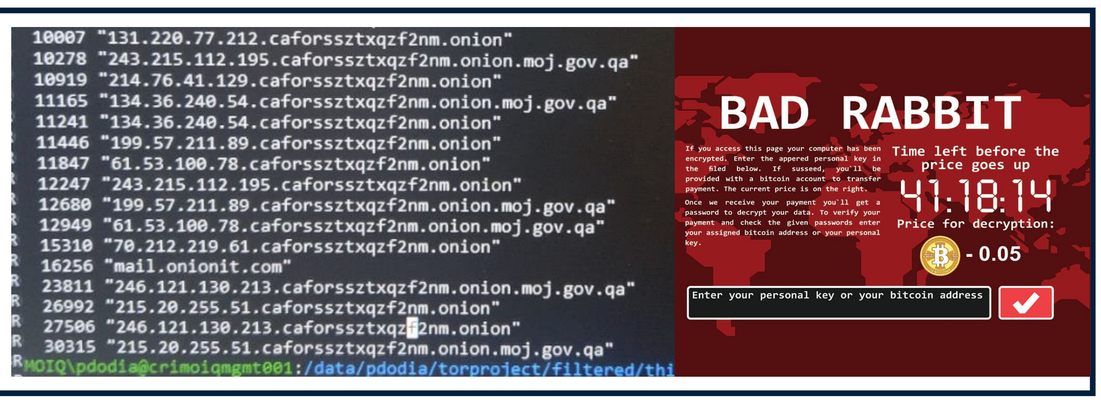
Onion Domains

Traces of Tor Malware in MOI Network



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.