

Security Network Infrastructure  
@uwaterloo.ca

Mike Patterson

**WATERLOO**  
**INFORMATION SYSTEMS**  
**& TECHNOLOGY**  
Information Security Services

09 March 2016

# Outline

1. Who we are
2. What we do
3. How we do what we do
4. What we do after we do what we do

# Who

## **Mark Gaulton**

Security Operations Specialist

---

## **Terry Labach**

Information Security Specialist

---

## **Sean Mason**

IAM Specialist

---

## **Patrick Matlock**

Information Security Specialist

---

## **Mike Patterson**

Manager, IT Security Operations

---

## **Andy Redfearn**

Information Systems Specialist

---

## **Jason Testart**

Director, Information Security Services

---

## **Andrew Ward**

IAM Specialist

# What

## SOC work

1. IDS
2. Firewalls
3. Vulnerability management
4. LE and academic integrity requests
5. General scutwork

How



# Network Monitoring



ARISTA



# Snort

```
Sequence: 8:27952781
Timestamp: 2016-03-02 09:48:00 -0500
Signature: 2022482 Rev 1 (GID 1) | ET TROJAN JS/Nemucod
    requesting EXE payload 2016-02-01
Source: 129.97.xxx.yyy:55788
Destination: 91.196.50.241:80
Decoded payload (TCP):
----
GET /69.exe HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: soclosebutyetqq.com
Connection: Keep-Alive
```

## Bro Usage

```
$ jq -c '[.ts, .uid, ."id.orig_p", ."id.resp_h", \
."id.resp_p", .method, .host, .uri, .response_body_len, \
.status_code]' < dddd | grep 91.196.50.241
```

```
[1456930076.513924,"Cx6fTT1ckh1mXRvGX1",55788,
"91.196.50.241",80,"GET","soclosebutyetqq.com","/69.exe",
3844,200]
```

```
$
```



# Bro Likes CPU

```
1 [|||||100.0%] 6 [|||||85.2%] 11 [|||||100.0%] 16 [|||||91.4%]
2 [||||| 24.3%] 7 [|||||88.0%] 12 [|||||78.7%] 17 [|||||100.0%]
3 [|||||100.0%] 8 [|||||77.4%] 13 [|||||100.0%] 18 [||||| 20.6%]
4 [|||||82.6%] 9 [|||||100.0%] 14 [|||||92.9%] 19 [|||||100.0%]
5 [|||||100.0%] 10 [|||||100.0%] 15 [|||||100.0%] 20 [|||||100.0%]
Mem[|||||62391/386696MB] Tasks: 100, 94 thr; 32 running
Swp[ 0/0MB] Load average: 27.67 28.78 28.46
Uptime: 20 days, 05:12:58
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
137929	root	20	0	7760M	7508M	397M	R	100.	1.9	67h27:05	/fsys2/bro-2.4.
137993	root	20	0	7559M	7336M	425M	R	100.	1.9	67h14:41	/fsys2/bro-2.4.
137926	root	20	0	2964M	2725M	402M	R	100.	0.7	47h04:44	/fsys2/bro-2.4.
137969	root	20	0	2878M	2646M	408M	R	92.5	0.7	46h47:58	/fsys2/bro-2.4.
137773	root	25	5	126M	56736	960	R	91.6	0.0	4h18:05	/fsys2/bro-2.4.
137983	root	20	0	2827M	2594M	411M	S	89.2	0.7	46h06:38	/fsys2/bro-2.4.
137774	root	25	5	150M	81824	960	R	88.7	0.0	2h38:11	/fsys2/bro-2.4.
137954	root	20	0	2915M	2675M	404M	S	86.8	0.7	46h33:12	/fsys2/bro-2.4.
138012	root	20	0	2960M	2708M	390M	S	82.5	0.7	47h31:33	/fsys2/bro-2.4.
138017	root	20	0	2849M	2581M	388M	R	81.5	0.7	46h59:24	/fsys2/bro-2.4.
137965	root	20	0	2796M	2591M	433M	R	75.8	0.7	46h23:22	/fsys2/bro-2.4.
137997	root	20	0	2704M	2472M	397M	R	75.8	0.6	46h19:51	/fsys2/bro-2.4.

```
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit
```

## Firewalls



```
set security policies from-zone untrust to-zone Campus\  
policy TaurineWeirdSSH match source-address any  
set security policies from-zone untrust to-zone Campus\  
policy TaurineWeirdSSH match destination-address\  
taurine.csclub.uwaterloo.ca  
set security policies from-zone untrust to-zone Campus\  
policy TaurineWeirdSSH match application taurineSSH  
set security policies from-zone untrust to-zone Campus\  
policy TaurineWeirdSSH then permit
```

## Vulnerability Management: General



```
qualys=> select count(*) from vulns where last_detected  
> '2016-02-01';  
count  
-----  
19527  
(1 row)
```

## Vulnerability Management: Specific

```
qualys=> \d wordpress
```

```
Table "public.wordpress"
```

```
Column | Type | Modifiers
```

```
-----+-----+-----  
version | text |  
url      | text |  
first    | date |  
last     | date |
```

```
qualys=> select count(*) from xpfound where
```

```
last > '2016-03-01';
```

```
count
```

```
-----
```

```
117
```

```
(1 row)
```

# LE / Academic Integrity / Non-Academic Offenses

1. Stalking
2. Missing persons
3. Stolen laptops/mobiles
4. Somebody went to the bathroom with their phone
5. Somebody pulled their phone out *during* the exam
6. Somebody hired somebody else to *write* their exam



## Scutwork

Entity: CEG TEK International

Subject: Copyright Infringement - Case C123987

ISP: University of Waterloo

Copyright Owner: Awesome Movies Inc

IP Address: 10.20.30.40

Source Port: 780013

Date of Infringement: right down to .xx seconds

Infringing Work : Battlefield Earth

Filename : At\_Least\_Somebody\_Might\_Watch\_It.rar

Filesize : 4.3PB

# Responses

1. Implement ACLs or firewall policies
2. Sinkhole DNS
3. Disable switch ports
4. Lock accounts
5. Report to AssDeans, LE
6. Information sharing communities

End

Thanks for coming out.



# Attribution

Talk itself is CC-by-SA, except all logos are marks of their respective owners. These include:

- ▶ Snort, Pig logo are registered trade marks of Cisco
- ▶ Bro eye logo is a mark of The Bro Project
- ▶ Elastic logo is a trade mark of Elasticsearch BV
- ▶ QRadar logo is a mark of IBM
- ▶ Arista logo is a mark of Arista Networks
- ▶ Endace logo is a mark of Emulex Corporation
- ▶ Qualys logo is a mark of Qualys Inc