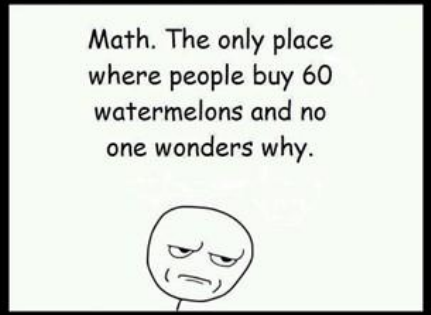
Introducing the RITA Framework

Hunting For Bad Guys On Your Network For Free Using Math!



Security Weekly

BLACK HILLS
Information Security

Breakdown

- Introduction – John Strand
- Hunting using DNS logs – Joff Thyer
- Hunting for C2 Beacons – Brian Fehrman
- Testing and Validation – Derek Banks
- Conclusions – John Strand

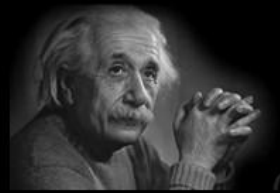
Security Weekly

BLACK HILLS
Information Security

Why Current Strategies Are Not Working

- Offensive: You will need to attack
- Defensive: Know our limitations
- Go back 5 or 6 years… What were they saying to defend networks?
  - Patch
  - AV
  - IDS/IPS
- What are they saying now?
  - Patch
  - AV
  - IDS/IPS
- Do you see the beginning of a bad pattern?
- This section is good for defense and for your attacks against the bad guys

Insanity: doing the same thing over and over again and expecting different results.



Albert Einstein
German Theoretical-Physicist
(1879-1955)

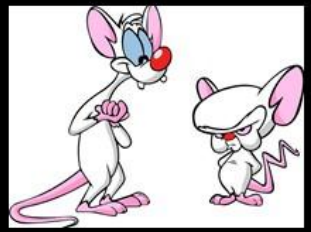
BLACK HILLS
Information Security

Just a Few Questions

- What are three AV companies?
- What are three IDS companies?
- What are three firewall companies?
- Who are the biggest?
- What is the total market share?

Just a Few More Questions

- Who are your main adversaries?
- China?
- Russia?
- The NSA?
- Organized crime?



Security Weekly

BLACK HILLS
Information Security

One Last Question

- Do you think these adversaries have the ability to bypass the limited technologies we just mentioned?

Hunt Teaming

- ***Actively*** looking for advanced attackers
- If we can bypass AV/IDS/IPS.. Attackers can too!
- We are looking for beaconing activity
- Involves close coordination with customer team
- Lots of logs and data to analyze
- Oh… And math, there is lots of math as well

Security Weekly

BLACK HILLS
Information Security

In Short…

Pictured…. Not Hunting.

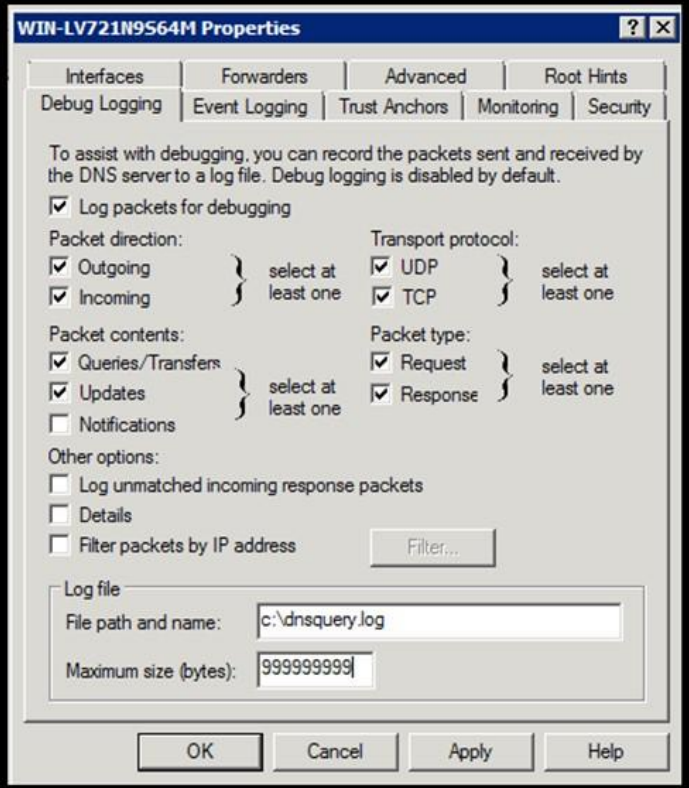
BLACK HILLS
Information Security

Hunting using DNS Logs

Joff Thyer

C2 hunting using DNS logs

- Compare peer workstation traffic
  - Majority of query types should be of type “A”, “CNAME”, and some “SVC”.
- What if we had an device that exhibited unusual behavior?
  - Receiving *many* NXDomain responses
  - Producing *many* TXT queries
  - Querying with a specific name pattern



Security Weekly

BLACK HILLS
Information Security

C2 hunting using DNS logs

- Sub-total all queries by
  - Response code
    - Examples: NOERROR, NXDOMAIN
  - Query and Response Types
    - A, CNAME, SRV, SOA, TXT, NS
- Create means, and standard deviations across whole dataset
  - An outlier differs from the mean by two standard deviations.

C2 hunting using DNS logs

```
[*] 192.168.1.21
    [+] ----------------------
    [+]         NOERROR:    409
    [+]        NXDOMAIN:     87
    [+] ----------------------
    [+]           TOTAL:    496
    [+] ----------------------
    [+] Query Types ..........
    [+]         [     A]:    106
    [+]         [   SRV]:    142 * >2 StdDev *
    [+] Response Types .......
    [+]         [     A]:    106
    [+]         [   SRV]:    142 * >2 StdDev *
    [+] ----------------------
```

Visualizing raw DNS stats

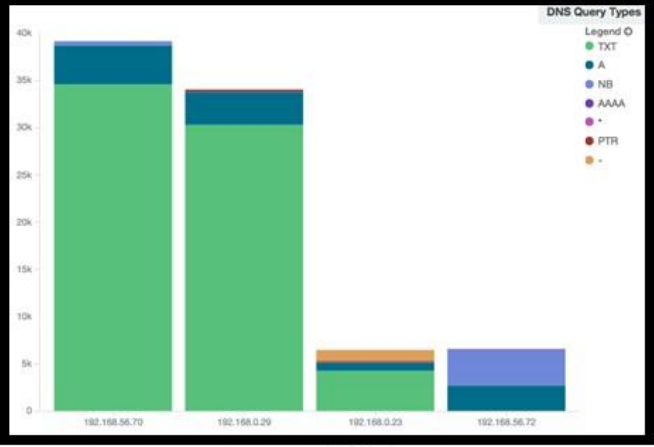


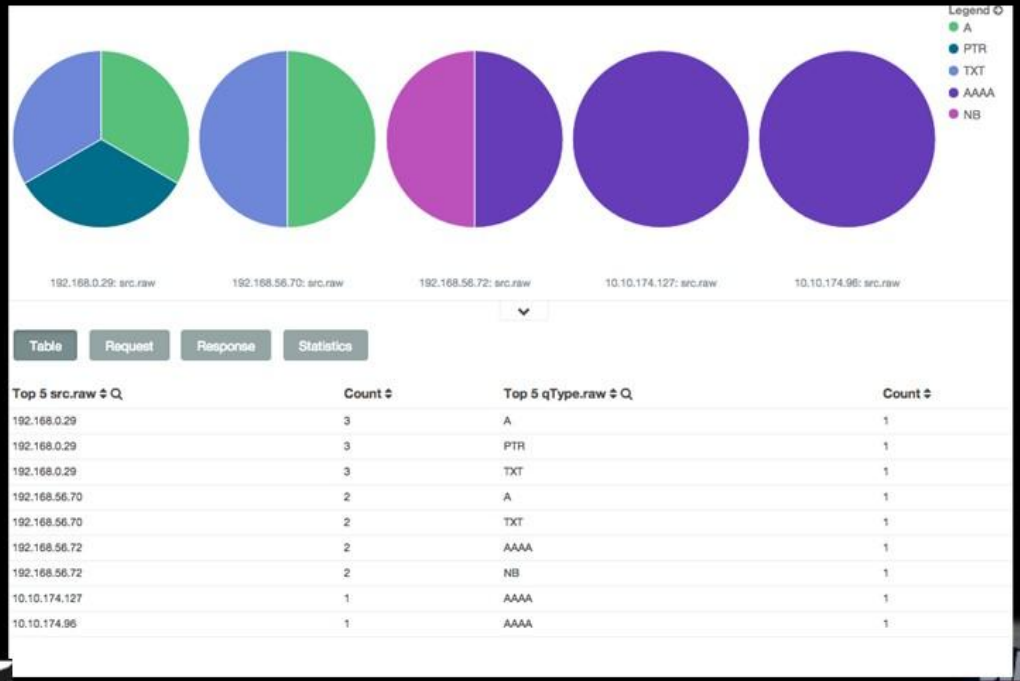
Table | Request | Response | Statistics

Top 4 src.raw	Top 5 qType.raw	Count
192.168.56.70	TXT	34571
192.168.0.29	TXT	30285
192.168.0.23	TXT	4284
192.168.56.70	A	4148
192.168.56.72	NB	3732
192.168.0.29	A	3481

Security Weekly

BLACK HILLS Information Security

Visualizing Analyzed DNS Data



Top 5 src.raw	Count	Top 5 qType.raw	Count
192.168.0.29	3	A	1
192.168.0.29	3	PTR	1
192.168.0.29	3	TXT	1
192.168.56.70	2	A	1
192.168.56.70	2	TXT	1
192.168.56.72	2	AAAA	1
192.168.56.72	2	NB	1
10.10.174.127	1	AAAA	1
10.10.174.96	1	AAAA	1

Hunting for Domain Name Generation Algorithms (DGA)

- "train" a classifier model using
  - Known good domains
    - OpenDNS top 10,000 domains
    - OpenDNS 10,000 random domain names
    - Alexa top 1 million domain names
  - Known DGA domain lists
    - Cryptolocker, and Game over Zeus botnets
  - About 500,000 known words
- Based on some published work from Click Security

DGA Hunt Feature Engineering

- Calculate
  - Length, and entropy
  - N-grams (3,4,5), and distance from legitimate domains and dictionary words
  - Difference between two n-gram distances
- Feed output data into a Random Decision Tree model, and serialize trained data to disk

Hunting for DGA

- Can re-train the classifier at any time with updated datasets
- Python script checks the classification of a domain for “dga”
  - If “dga” found, then update ElasticSearch variable to “behavior: dga”.
- Further experimentation with other feature engineering
  - Eg: Ratios of numbers to vowels/consonents
  - Proportion of domain matching dictionary word

Hunting for C2 Beacons

Brian Fehrman

Beaconing

- Not to be confused with baconing…

Equally Awesome

Beaconing

- Many types of malware call home
- Particularly C2 Channels
- Calls typically happen at predefined intervals

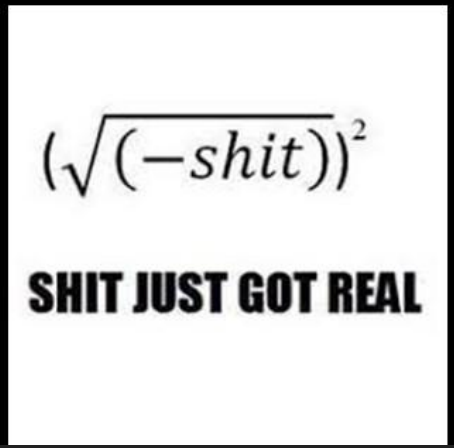
I guess you could say…
It was a dangerous callback.
YEAAAAAAAAAAAAA!

Security Weekly

BLACK HILLS
Information Security

Beaconing

- Bring on the math
- Network connections are time-varying signals
- Signal processing can be applied

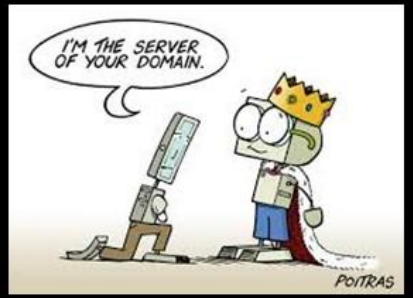


Security Weekly

BLACK HILLS
Information Security

Beaconing

- Two domains in signal processing



- Time Domain
  - Connections happening over time

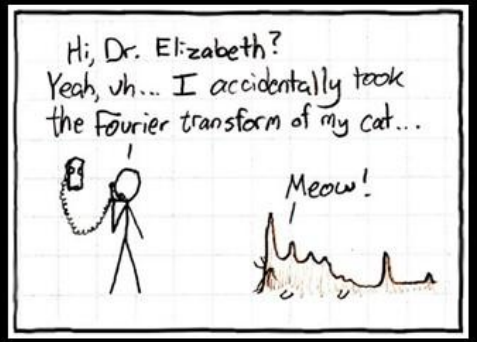
- Frequency Domain
  - The frequency at which the connections occur

Security Weekly

BLACK HILLS
Information Security

Beaconing

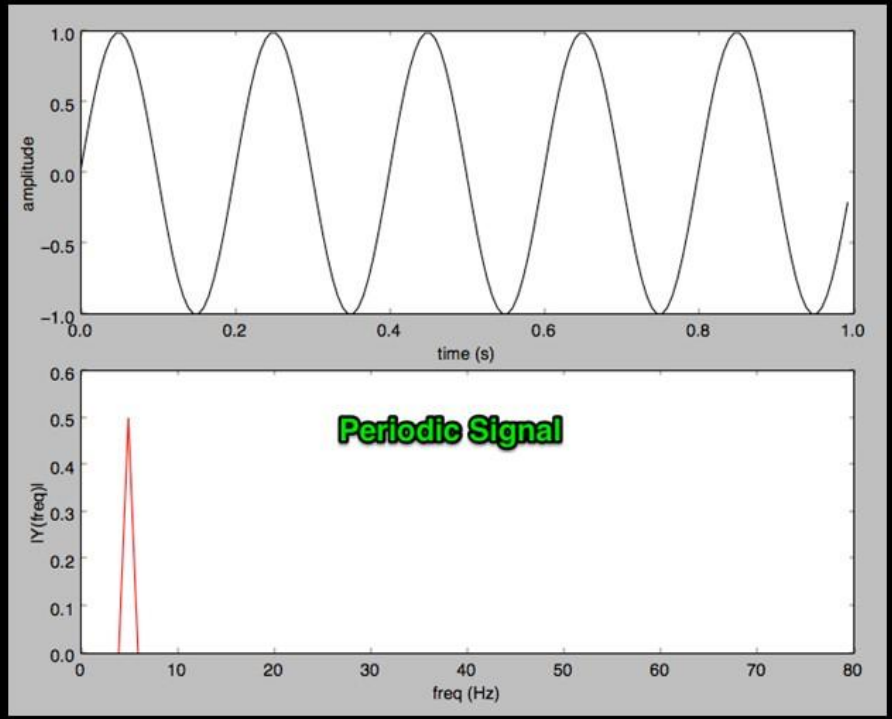
- How can we determine frequency?
- Enter…Fast Fourier Transforms (FFT)
  - technically DFT but lets not go there now
- Transforms signals from time/spatial domain to frequency domain



Beaconing

- So what?
- Most users interact randomly
- Most software does not…including malware
- If something happens at regular intervals, this sticks out in the frequency domain

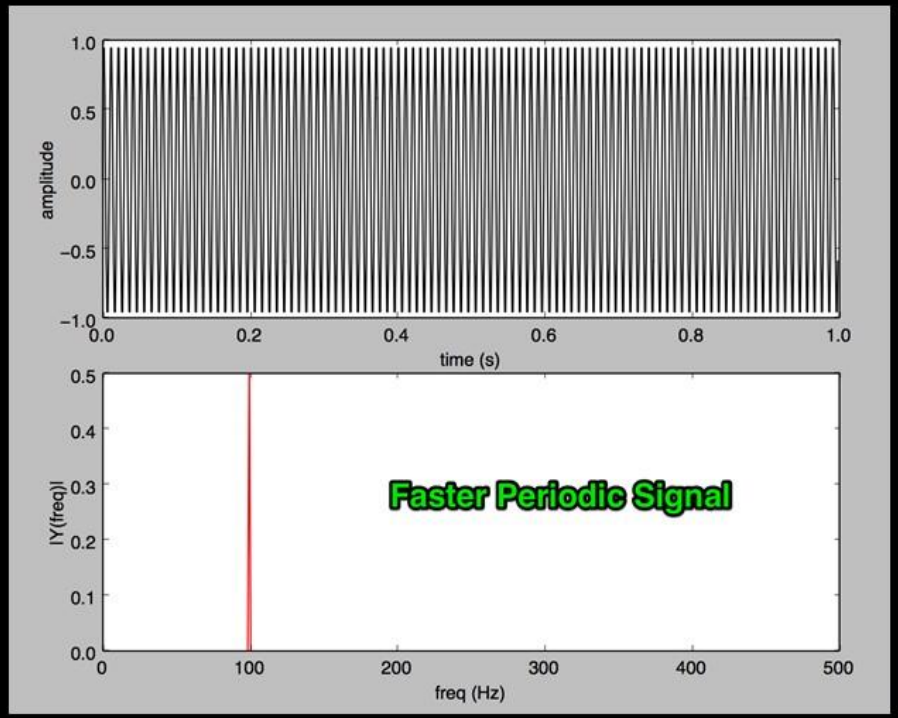
Beaconing



Security Weekly

BLACK HILLS
Information Security

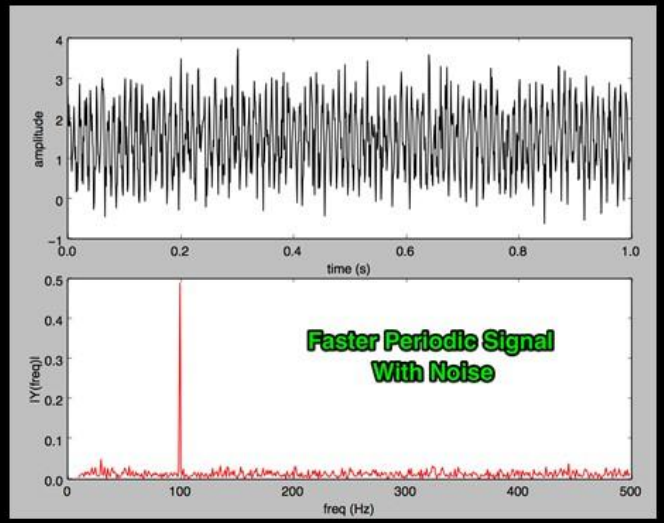
Beaconing

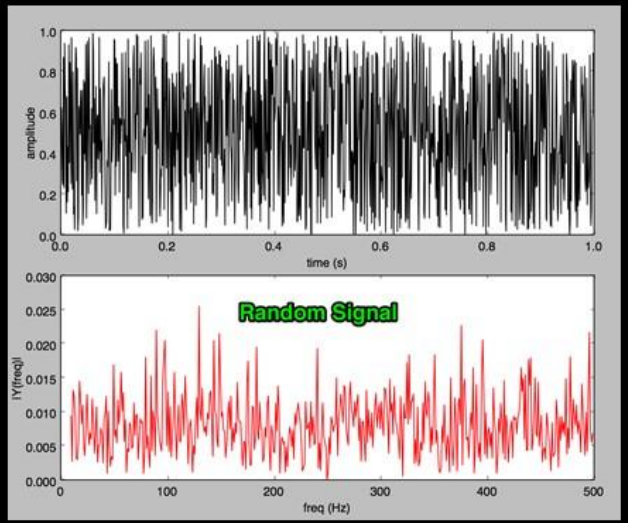


Security Weekly

BLACK HILLS
Information Security

Beaconing



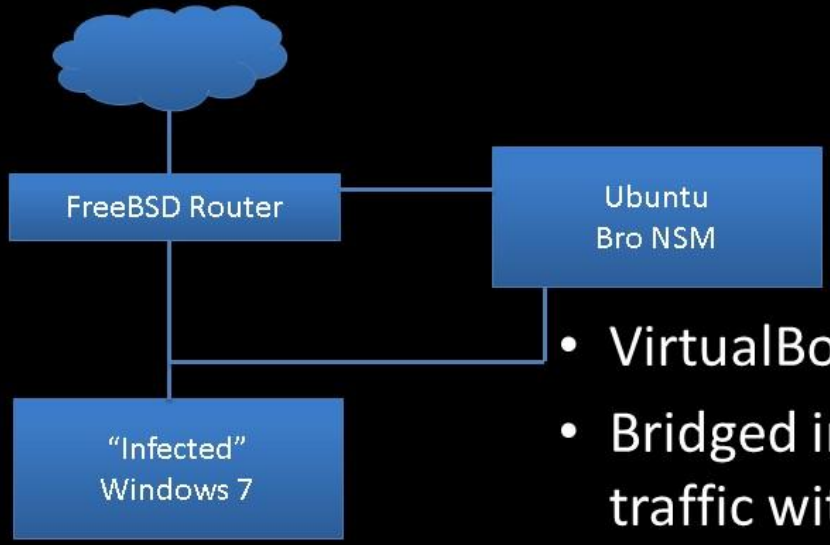


Security Weekly

BLACK HILLS
Information Security

Testing and Validation
Derek Banks

Test Environment



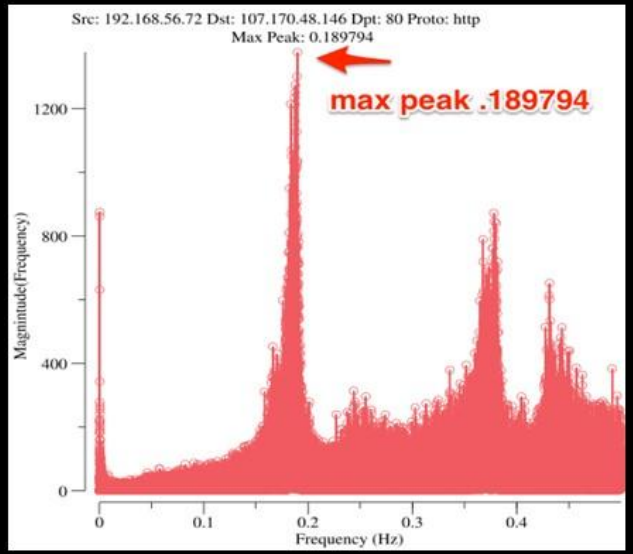
- VirtualBox on single host
- Bridged interface to sniff traffic with Bro
- Python Script to simulate additional traffic

Security Weekly

BLACK HILLS
Information Security

HTTP Beaconing

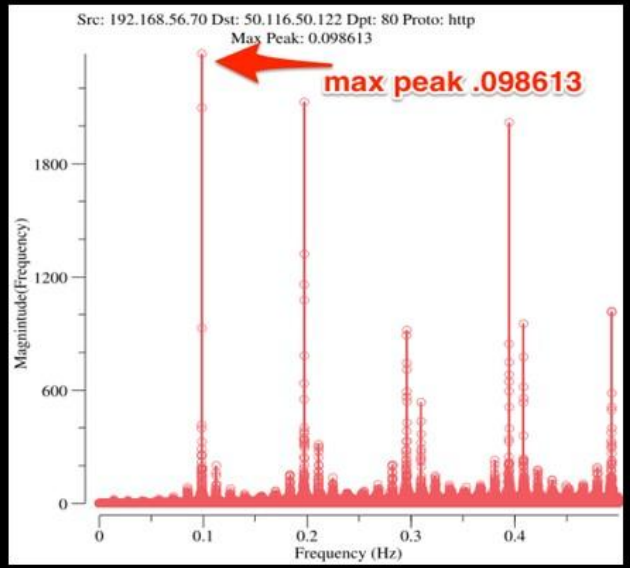
- Powershell Empire
  - C2 over HTTP
  - Default Five Second Interval Configuration
  - T=1/f (Hz)
    - 5.3 seconds



Sep 16	00:00:04	CTibsBQrPD21kqrk4	192.168.56.72	49828	107.170.48.146	80	1	GET	107.170.48.146	/admin/get.php	-
Sep 16	00:00:09	CbS6RR2XvFqstlaZS	192.168.56.72	49829	107.170.48.146	80	1	GET	107.170.48.146	/login/process.jsp	-
Sep 16	00:00:15	CMAOx54cahdZ8AWMFh	192.168.56.72	49830	107.170.48.146	80	1	GET	107.170.48.146	/news.asp	-
Sep 16	00:00:20	Cnktgv45Sys7WQm4v8	192.168.56.72	49832	107.170.48.146	80	1	GET	107.170.48.146	/news.asp	-
Sep 16	00:00:26	CpCJi02n633bq8fRYa	192.168.56.72	49834	107.170.48.146	80	1	GET	107.170.48.146	/login/process.jsp	-
Sep 16	00:00:31	CkFhSQuaOFLoa2rPf	192.168.56.72	49835	107.170.48.146	80	1	GET	107.170.48.146	/admin/get.php	-
Sep 16	00:00:37	CV4Y1W1nsW5l2i1WW1	192.168.56.72	49836	107.170.48.146	80	1	GET	107.170.48.146	/login/process.jsp	-

HTTP Beaconing

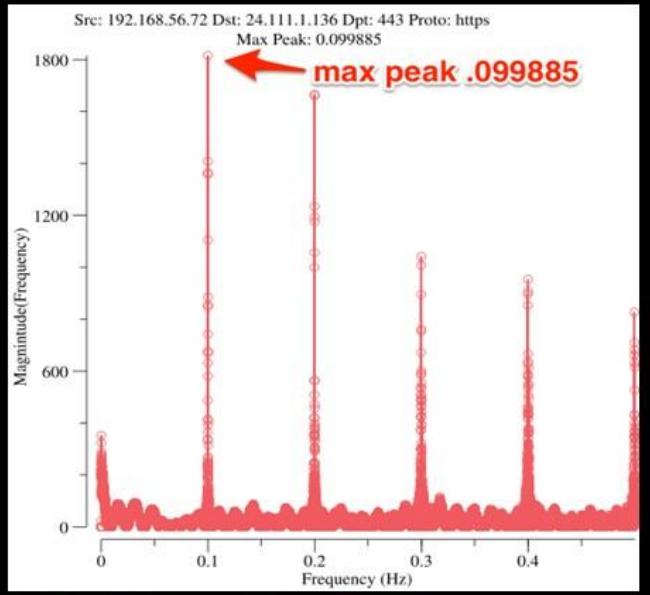
- VSAgent
  - Custom written malware
  - C2 via HTTP Viewstate
  - T=1/f (Hz)
    - 10.2 seconds



Sep 16	19:00:06	CWQSKa480hAaDFYpK9	192.168.56.70	49725	50.116.50.122	80	1	POST	vsagent.blackhillsinfosec.com
Sep 16	19:00:16	CKIW5k4dgXMDLfhKG5	192.168.56.70	49726	50.116.50.122	80	1	POST	vsagent.blackhillsinfosec.com
Sep 16	19:00:26	CLml964iCOIugWVOF6	192.168.56.70	49727	50.116.50.122	80	1	POST	vsagent.blackhillsinfosec.com
Sep 16	19:00:36	CZGvp2lavczMBUgHd	192.168.56.70	49728	50.116.50.122	80	1	POST	vsagent.blackhillsinfosec.com
Sep 16	19:00:46	CPPdMfiMCObMFAYoc	192.168.56.70	49729	50.116.50.122	80	1	POST	vsagent.blackhillsinfosec.com
Sep 16	19:00:56	CosWA81DeXhW9taC3e	192.168.56.70	49730	50.116.50.122	80	1	POST	vsagent.blackhillsinfosec.com
Sep 16	19:01:07	CaSa9B3x1fCY9gMk57	192.168.56.70	49731	50.116.50.122	80	1	POST	vsagent.blackhillsinfosec.com

HTTPS Beaconing

- Meterpreter
  - reverse_https module
  - TLS Encrypted C2 Channel
  - T=1/f (Hz)
    - 10 seconds

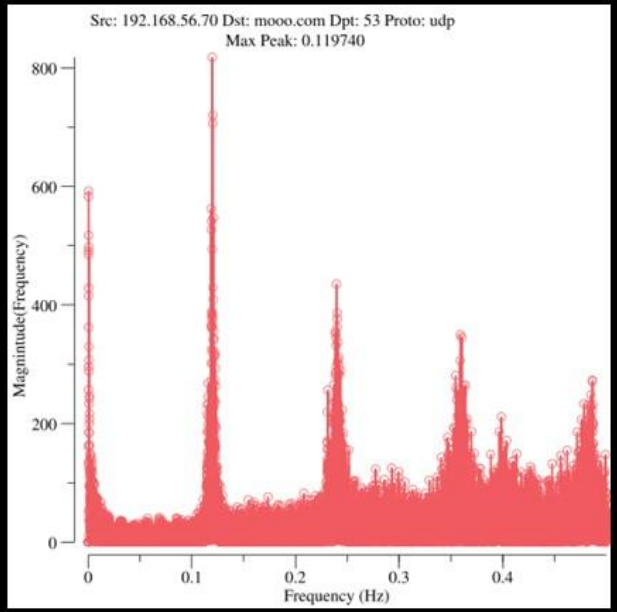


Sep 16	15:00:01	CIzovx3XUqblvJz0y	192.168.56.72	50681	24.111.1.136	443	TLSv12
Sep 16	15:00:11	Ctsujd46BF6s3XW3W5	192.168.56.72	50685	24.111.1.136	443	TLSv12
Sep 16	15:00:21	CPHVOY1y8u3lBQ2QMh	192.168.56.72	50686	24.111.1.136	443	TLSv12
Sep 16	15:00:31	C3HSk52hxonXEZeH6i	192.168.56.72	50689	24.111.1.136	443	TLSv12
Sep 16	15:00:41	ClnvN7x0crD7ZxTee	192.168.56.72	50692	24.111.1.136	443	TLSv12
Sep 16	15:00:51	Cn2NTz2J1EWkGrJE64	192.168.56.72	50694	24.111.1.136	443	TLSv12

BLACK HILLS
Information Security

DNS Beaconing

- DNSCat
  - C2 via DNS TXT records
  - One Second Interval




```
Sep 16 08:00:00 COAOKuU8Ju1Elrzvl      192.168.56.70   60515   8.8.8.8 53      udp     20211   1dab0117815db6915c.a.bovine1234.mooo.com
Sep 16 08:00:01 COAOKuU8Ju1Elrzvl      192.168.56.70   60515   8.8.8.8 53      udp     31978   77a30117815db6915c.a.bovine1234.mooo.com
Sep 16 08:00:02 COAOKuU8Ju1Elrzvl      192.168.56.70   60515   8.8.8.8 53      udp     18725   10420117815db6915c.a.bovine1234.mooo.com
Sep 16 08:00:03 COAOKuU8Ju1Elrzvl      192.168.56.70   60515   8.8.8.8 53      udp     17594   706b0117815db6915c.a.bovine1234.mooo.com
Sep 16 08:00:04 COAOKuU8Ju1Elrzvl      192.168.56.70   60515   8.8.8.8 53      udp     21778   69980117815db6915c.a.bovine1234.mooo.com
Sep 16 08:00:06 COAOKuU8Ju1Elrzvl      192.168.56.70   60515   8.8.8.8 53      udp     21411   06160117815db6915c.a.bovine1234.mooo.com
Sep 16 08:00:07 COAOKuU8Ju1Elrzvl      192.168.56.70   60515   8.8.8.8 53      udp     5239    585e0117815db6915c.a.bovine1234.mooo.com
```

BLACK HILLS
Information Security

Conclusions
John Strand

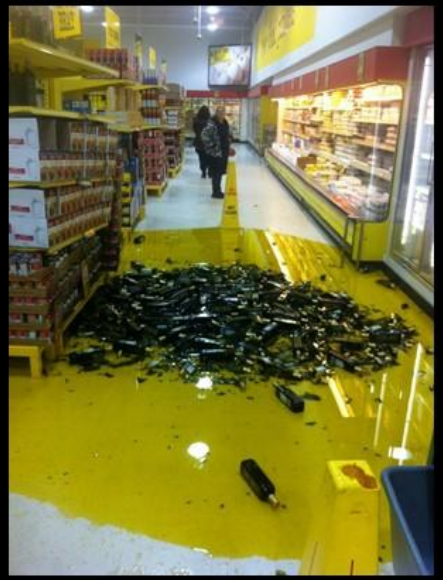
What did you think security was going to be?

YOU HAVE BEEN HACKED !

Security Weekly

BLACK HILLS Information Security

What did you get?



Cleanup… Aisle 3

Come and Play

- RITA Download
  - https://github.com/blackhillsinfosec/rita.git
- You will need…
  - A Debian Based Distrobution
  - ELK Stack
  - SciPy Libraries
  - Flask
- I will be releasing videos next week on the framework
  - Because that and PowerPoint is what I do…
- This is an invitation
  - Something sucks? Make a recommendation
  - This is the beginning of a framework
  - dev-hunt@blackhillsinfosec.com
- We have a great group working on this