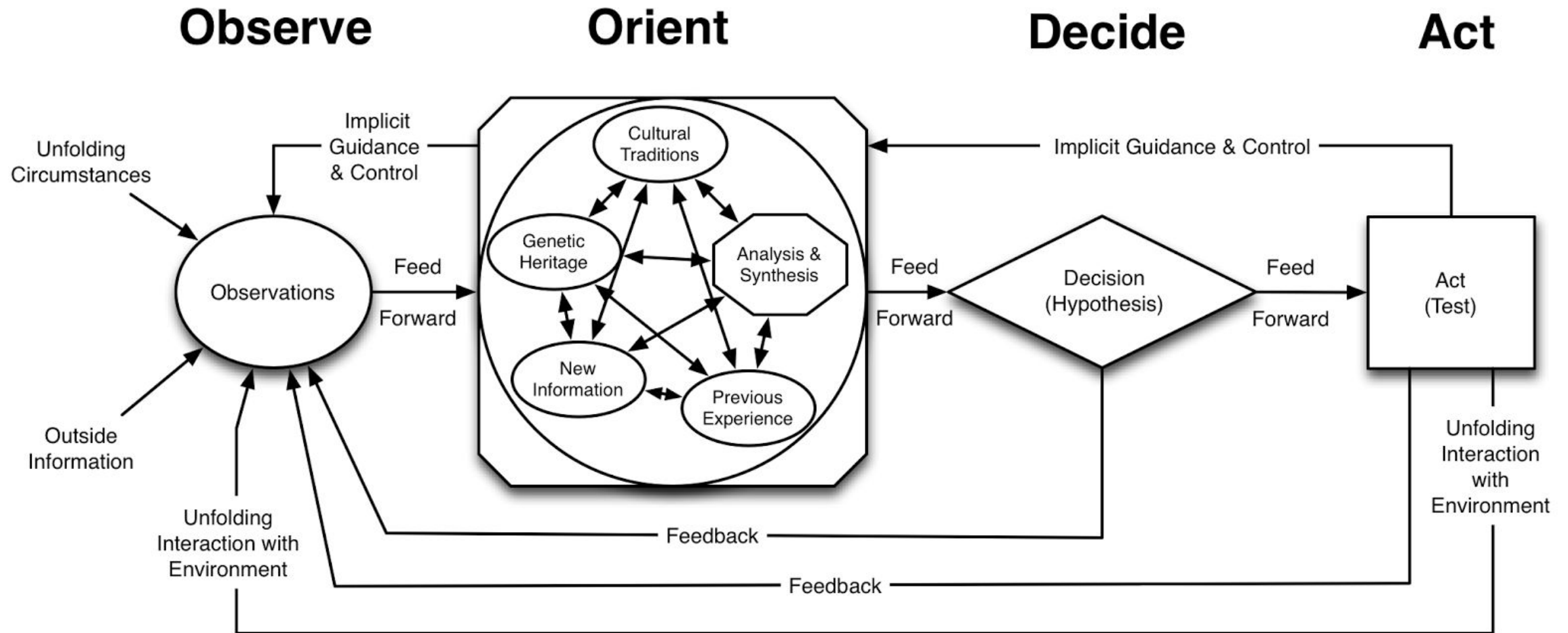


# How to Cover C&C in the MITRE ATT&CK Matrix

John Strand

# The OODA Loop



## Problems with IDS: What Exactly is Going on Here?

- We fell into a bad habit with IDS
  - Standard signature detection
  - Worked great for years!
  - Now, not so much
- Attackers are using encryption and obfuscation
- TLS 1.3 is also not going to help the process of inspection
- IDS/IPS still has value, it just does not do the level of detection that it once did



Bad Habit

## Endpoint Protection Review: A Change in the Landscape

- “Passive” detection is quickly a thing of the past
- Let's take the Endpoint
  - Signature -> Heuristic
  - AI Algorithms
  - Need for a story, not a signature
- In many ways IDS/NDR did not keep up
- This created blind spots
- IDS is rarely (if ever) a concern for more advanced attackers



# How to Handle MITRE Command and Control and Exfiltration

- Very few companies have the ability to test their ability to detect network level C2
- Heck, very few companies are doing adversarial simulation
- Another chat about the need to be testing your company's detective capabilities
- MITRE has two columns dedicated to network extrusion detection
  - Command and Control
  - Exfiltration

Command and Control	Exfiltration
16 techniques	9 techniques
Application Layer Protocol (4)	Automated Exfiltration (1)
Communication Through Removable Media	Data Transfer Size Limits
Data Encoding (2)	Exfiltration Over Alternative Protocol (3)
Data Obfuscation (3)	Exfiltration Over C2 Channel
Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)
Encrypted Channel (2)	Exfiltration Over Physical Medium (1)
Fallback Channels	Exfiltration Over Web Service (2)
Ingress Tool Transfer	Scheduled Transfer
Multi-Stage Channels	Transfer Data to Cloud Account
Non-Application Layer Protocol	
Non-Standard Port	
Protocol Tunneling	
Proxy (4)	
Remote Access Software	
Traffic Signaling (1)	
Web Service (3)	



# MITRE Shield

The Shield matrix consists of the following core components:

- Tactics, denoting what the defender is trying to accomplish (the columns).
- Techniques, describing how the defense achieves the tactic(s) (the individual cells).

Channel	Collect	Contain	Detect	Disrupt	Facilitate	Legitimize	Test
Admin Access	API Monitoring	Admin Access	API Monitoring	Admin Access	Admin Access	Application Diversity	Admin Access
API Monitoring	Application Diversity	Baseline	Application Diversity	Application Diversity	Application Diversity	Burn-In	API Monitoring
Application Diversity	Backup and Recovery	Decoy Account	Behavioral Analytics	Backup and Recovery	Behavioral Analytics	Decoy Account	Application Diversity
Decoy Account	Decoy Account	Decoy Network	Decoy Account	Baseline	Burn-In	Decoy Content	Backup and Recovery
Decoy Content	Decoy Content	Detonate Malware	Decoy Content	Behavioral Analytics	Decoy Account	Decoy Credentials	Decoy Account
Decoy Credentials	Decoy Credentials	Hardware Manipulation	Decoy Credentials	Decoy Content	Decoy Content	Decoy Diversity	Decoy Content
Decoy Network	Decoy Network	Isolation	Decoy Network	Decoy Credentials	Decoy Credentials	Decoy Network	Decoy Credentials
Decoy Persona	Decoy System	Migrate Attack Vector	Decoy System	Decoy Network	Decoy Diversity	Decoy Persona	Decoy Diversity
Decoy Process	Detonate Malware	Network Manipulation	Email Manipulation	Email Manipulation	Decoy Persona	Decoy Process	Decoy Network
Decoy System	Email Manipulation	Security Controls	Hunting	Hardware Manipulation	Decoy System	Decoy System	Decoy Persona
Detonate Malware	Network Diversity	Software Manipulation	Isolation	Isolation	Network Diversity	Network Diversity	Decoy System
Migrate Attack Vector	Network Monitoring		Network Manipulation	Network Manipulation	Network Manipulation	Pocket Litter	Detonate Malware
Network Diversity	PCAP Collection		Network Monitoring	Security Controls	Peripheral Management		Migrate Attack Vector
Network Manipulation	Peripheral Management		PCAP Collection	Standard Operating Procedure	Pocket Litter		Network Diversity
Peripheral Management	Protocol Decoder		Pocket Litter	User Training	Security Controls		Network Manipulation

# MITRE Shield: Behavioral Analytics

## Behavioral Analytics

Deploy tools that detect unusual system or user behavior.

Instrument a system to collect detailed information about process execution and user activity, develop a sense of normal or expected behaviors, and alert on abnormal or unexpected activity. This can be accomplished either onboard the target system or by shipping data to a centralized analysis and alerting system.

DUC0166	A defender could monitor for anomalous behavior from client applications, such as atypical module loads, file reads/writes, or network connections.
---------	---

DUC0212	A defender can detect the use of non-standard protocols. By implementing behavior analytics specific to a rise in protocol traffic to a system or set of systems, one might be able to detect malicious communications from an adversary.
---------	---

DUC0213	A defender can detect the use of external web services for communication relay. By implementing behavior analytics anomalies in what domains a system is communicating with, how frequently, and at what times, a defender can potentially identify malicious traffic.
---------	--

# MITRE Shield: PCAP Collection

## PCAP Collection

Collect full network traffic for future research and analysis.

PCAP Collection allows a defenders to use the data to examine an adversary's network traffic more closely, including studying if it is encoded and/or encrypted. PCAP can be run through tools to replay the traffic to get a real-time view of what happened over the wire. These tools can also parse the traffic and send results to a SIEM for monitoring and alerting.

DOS0116	There is an opportunity to detect adversary activity that uses obfuscated communication.
DOS0170	There is an opportunity to collect network data and analyze the adversary activity it contains.



# A Wider View...

## Opportunities

ID	Description
DOS0116	There is an opportunity to detect adversary activity that uses obfuscated communication.
DOS0170	There is an opportunity to collect network data and analyze the adversary activity it contains.

## Use Cases

ID	Description
DUC0116	A defender can capture network traffic for a compromised system and look for abnormal network traffic that may signal data obfuscation.
DUC0170	Collecting full packet capture of all network traffic allows you to review what happened over the connection and identify command and control traffic and/or exfiltration activity.

## Procedures

ID	Description
DPR0049	Collect PCAP on a decoy network to improve visibility into an adversary's network activity.

## ATT&CK® Techniques

ID 	Name	ATT&CK Tactics
T1001	Data Obfuscation	Command and Control
T1020	Automated Exfiltration	Exfiltration

# MITRE Shield: Network Monitoring

## Network Monitoring

Monitor network traffic in order to detect adversary activity.

Network monitoring involves capturing network activity data, including capturing of server, firewall, and other relevant logs. A defender can then review them or send them to a centralized collection location for further analysis.

### Opportunities

ID	Description
DOS0198	There is an opportunity to monitor network traffic for different protocols, anomalous traffic patterns, transfer of data, etc. to determine the presence of an adversary.

### Use Cases

ID	Description
DUC0089	A defender can monitor network traffic for anomalies associated with known MiTM behavior.
DUC0159	A defender can monitor for systems establishing connections using encapsulated protocols not commonly used together such as RDP tunneled over TCP.
DUC0198	The defender can implement network monitoring for and alert on anomalous traffic patterns, large or unexpected data transfers, and other activity that may reveal the presence of an adversary.

### Procedures

ID	Description
DPR0047	Capture network logs for internet-facing devices and send those logs to a central collection location.
DPR0048	Capture all network device (router, switches, proxy, etc.) logs on a decoy network and send those logs to a central collection location.

# Why is this Necessary?

byt3bl33d3r Update README.md 39b266c on Nov 16, 2018 29 commits

data	Re-added the lockscreen and screenshot commands.	6 years ago
.gitignore	added .gitignore	6 years ago
LICENSE	added a license	5 years ago
README.md	Update README.md	2 years ago
gcat.py	Added some crazy 1337 ascii art	5 years ago
implant.py	Added some crazy 1337 ascii art	5 years ago

README.md

## Gcat

A stealthy Python based backdoor that uses Gmail as a command and control server

This project was inspired by the original [PoC code](#) from Benjamin Donnelly

## This is PoC code...

... that was released for organizations to test their defenses against these type of attacks. In order to detect them see projects like [RITA](#).

For a more up to date and maintained version of this project see [GDog](#)

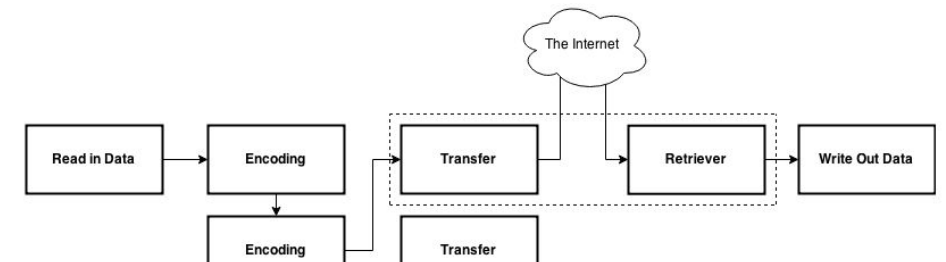
DakotaNelson update requirements.txt 155b117 on Mar 7, 2018 193 commits

sneakers	some small bugfixes and improvements	3 years ago
.gitignore	merge davinerd/library-refactor into dakotanelson/library-refactor	5 years ago
.travis.yml	trying again	3 years ago
LICENSE	Initial commit	6 years ago
README.md	google spreadsheet module works!	3 years ago
client.py	add a little demo client and server	3 years ago
diagram.png	renamed diagram	5 years ago
requirements.txt	update requirements.txt	3 years ago
screep	whoops	3 years ago
secrets.tar.enc	attempt at adding encrypted config files for use with Travis	3 years ago
server.py	add a little demo client and server	3 years ago

README.md

## sneaky-creeper

Using social media as a tool for data exfiltration.



# Malware PCAP Samples



**Malware of the Day – APT1 Virtually There**

🕒 October 22, 2020



**Malware of the Day – Backoff**

🕒 October 1, 2020



**Malware of the Day – Asprox**

🕒 September 10, 2020



**Malware of the Day – Comfoo**

🕒 September 2, 2020



**Malware of the Day – Saefko**

🕒 August 26, 2020



**Malware of the Day – Magnitude**

🕒 August 5, 2020



# Malware PCAP Samples

## Malware of the Day: BACKOFF

### Lab Setup

**Malware:** Backoff

**AKA:** Backoff POS Malware

**Traffic Type:** Crimeware

**Connection Type:** Reverse HTTP

**C2 Platform:** Cobalt Strike

**Origin of Sample:** <https://github.com/rsmudge/Malleable-C2-Profiles/blob/master/crimeware/backoff.profile>

**Host Payload Delivery Method:** Powershell one-liner

**Target Host/Victim:** 192.168.99.55 – Windows 10 x64

**C2 Server:** 157.245.128.27

**Beacon Timing:** 30s

**Jitter:** 10%



# Malware PCAP Samples

```
./rita show-beacons beakerdemo-2020-08-25 -H | less -S
```

SCORE	SOURCE IP	DESTINATION IP	CONNECTIONS	AVG BYTES	INTVL RANGE	SIZE RANGE	TOP INTVL	TOP SIZE
0.951	192.168.99.55	157.245.128.27	9993	911	30	1629	28	671
0.893	192.168.99.54	159.65.220.246	10239	1061	30	898	26	738
0.892	192.168.99.52	68.183.138.51	10131	1044	30	1474	29	743
0.835	192.168.99.11	52.6.160.3	126	152	1	0	2048	76
0.835	192.168.99.52	52.179.224.121	153	391	61	1	1680	181
0.833	192.168.99.53	104.71.255.238	36	5415	61143	92	1800	505
0.833	192.168.99.52	104.71.255.238	33	5405	59402	40	1800	505
0.833	192.168.99.53	104.86.8.104	21	5424	35942	40	1800	505
0.833	192.168.99.52	23.210.141.30	54	5401	16219	40	1800	505
0.833	192.168.99.55	23.210.141.30	42	5411	20154	40	1800	505
0.833	192.168.99.53	23.210.141.30	36	5408	1803	40	1800	505
0.828	192.168.99.51	23.210.141.30	39	5408	1802	40	1800	505
0.827	192.168.99.51	23.37.83.178	24	5433	50091	52	1799	505
0.826	192.168.99.53	13.107.42.23	39	7445	5418	186	7200	1191
0.826	192.168.99.54	13.107.42.23	39	7442	3754	186	7201	1191
0.826	192.168.99.55	13.107.42.23	39	7442	3786	186	7200	1191
0.822	192.168.99.51	104.248.234.238	54036	234772	16	4680	5	2062

# Malware PCAP Samples

The image shows a Wireshark packet capture of a TLS handshake. The filter bar at the top is set to `tls.handshake.type == 11`. The packet list shows several TLSv1.2 records, with packet 507 (Handshake Protocol: Certificate) highlighted. The packet details pane shows the structure of the TLSv1.2 Record Layer: Handshake Protocol: Certificate. The raw data pane shows the hex and ASCII representation of the certificate, with the domain `www.virtuallythere.com` visible in the ASCII column.

apt|virtuallythere\_1hr.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

`tls.handshake.type == 11`

No.	Time	Source	Destination	Protocol	Length	Info
25	4.124688	13.107.21.200	192.168.99.55	TLSv1.2	94	Server Hello, Certificate, Certificate Status, Serv
94	7.615433	204.79.197.222	192.168.99.55	TLSv1.2	418	Server Hello, Certificate, Certificate Status, Serv
135	9.791369	13.107.42.254	192.168.99.55	TLSv1.2	514	Server Hello, Certificate, Certificate Status, Serv
179	9.972439	204.79.197.254	192.168.99.55	TLSv1.2	418	Server Hello, Certificate, Certificate Status, Serv
213	10.136381	72.21.81.200	192.168.99.55	TLSv1.2	1514	Certificate [TCP segment of a reassembled PDU]
507	19.726291	157.245.128.27	192.168.99.55	TLSv1.2	1303	Certificate, Server Key Exchange, Server Hello Done
908	246.020627	104.122.146.167	192.168.99.55	TLSv1.2	1230	Certificate [TCP segment of a reassembled PDU]

> Frame 507: 1303 bytes on wire (10424 bits), 1303 bytes captured (10424 bits)

> Ethernet II, Src: Routerbo\_d3:cc:33 (c4:ad:34:d3:cc:33), Dst: PcsCompu\_98:67:01 (08:00:27:98:67:01)

> Internet Protocol Version 4, Src: 157.245.128.27, Dst: 192.168.99.55

> Transmission Control Protocol, Src Port: 443, Dst Port: 49709, Seq: 91, Ack: 153, Len: 1249

▼ Transport Layer Security

> TLSv1.2 Record Layer: Handshake Protocol: Certificate

> TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange

> TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done

0000 08 00 27 98 67 01 c4 ad 34 d3 cc 33 08 00 45 20 ...g...4...3...E

0010 05 09 ba ea 40 00 28 06 50 f4 9d f5 80 1b c0 a8 ....@.(.P.....

0020 63 37 01 bb c2 2d c4 1e db b9 da c6 30 fa 50 18 c7.....0.P.

0030 01 f5 85 cb 00 00 16 03 03 03 81 0b 00 03 7d 00 .....}.

0040 03 7a 00 03 77 30 82 03 73 30 82 02 5b a0 03 02 .z..w0..s0..[...

0050 01 02 02 04 5b c2 eb ec 30 0d 06 09 2a 86 48 86 ....[...0...\*.H.

0060 f7 0d 01 01 0b 05 00 30 6a 31 0b 30 09 06 03 55 .....0 j1.0...U

0070 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 ....US1..0...U...

0080 0a 53 6f 6d 65 2d 53 74 61 74 65 31 09 30 07 06 .Some-St atel.0..

0090 03 55 04 07 13 00 31 1f 30 1d 06 03 55 04 0a 13 ..H...A...0...H.

00a0 16 77 77 77 7e 76 69 72 74 75 61 6c 6c 79 74 68 .www.vir tuallyth

00b0 65 72 65 2e 63 6f 6d 31 0c 30 0a 06 03 55 04 0b ere.com1..0...U...

00c0 13 03 6e 65 77 31 0c 30 0a 06 03 55 04 03 13 03 .new1..0...0...

00d0 6e 65 77 30 1e 17 0d 32 30 31 30 32 30 31 34 34 new0...2 01020144

00e0 32 33 38 5a 17 0d 33 30 31 30 31 38 31 34 34 32 238Z...30 10181442

00f0 33 38 5a 30 6a 31 0b 30 09 06 03 55 04 06 13 02 38Z0j1.0 ...U....

0100 55 53 31 13 30 11 06 03 55 04 08 13 0a 53 6f 6d US1.0...U....Som

0110 65 2d 53 74 61 74 65 31 09 30 07 06 03 55 04 07 e-Statel.0...U...

0120 13 00 31 1f 30 1d 06 03 55 04 0a 13 16 77 77 77 .1.0...U...www

0130 2e 76 69 72 74 75 61 6c 6c 79 74 68 65 72 65 2e .virtual lythere.

0140 63 6f 6d 31 0c 30 0a 06 03 55 04 0b 13 03 6e 65 com1.0...U...ne

0150 77 31 0c 30 0a 06 03 55 04 03 13 03 6e 65 77 30 w1.0...U...new0

0160 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 .."0...\*.H.....

0170 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 .....0 .....

0180 9b d6 f9 24 dc 91 a9 83 7d 16 86 27 fb 49 ec 76 ...\$.-----}.-'I.v

0190 00 27 35 73 28 8c 49 f8 a2 49 15 13 99 02 9c 35 .5s(-I- I.....5

Bytes 161-182: printableString (x509sat.printableString)

Packets: 7543 · Displayed: 27 (0.4%) Profile: Default

# Malware PCAP Samples

*Note: Only the 1hr PCAP has the initial SSL handshake and certificate.*

## **APT1 Virtually There 1 Hour Capture**

[apt1virtuallythere\\_1hr.pcap](#)

Size: 1.85 MB

MD5 Checksum: 32417bf3c7469c27359adf4dcb519627

## **APT1 Virtually There 24 Hour Capture**

[apt1virtuallythere\\_24hr.pcap](#)

Size: 108.96 MB

MD5 Checksum: 1e1824d26122159683d3d71d2a65ba6f

# MITRE and RITA

Insert RITA SCREENSHOT HERE



# MITRE and Passer



## Passer

### A Passive Sniffer and Inventory Tool

## What's on my network?

As a network security professional, one of my biggest frustrations has been knowing what's on my network. In addition to the normal laptops, desktops, and servers that should be there, people can add their own devices as soon as they have the wifi password or access to an ethernet port. I'd like to know what's connected – both approved and non-approved devices – so we can identify systems that may need to be patched, hardened, or removed.

Agent-based software can't completely perform this kind of inventory – we need to know what's there before we can install an agent, and may not have agents (or be able to install software at all) for many devices. The better approaches are active scans and passive detection.

Here's where Passer steps in – it can give you an inventory of what's on your network entirely passively. Let's first look at what kind of information it provides, then I'll show you how to get running with it in under a minute.



## Conclusions

- We fell into a rut with IDS
- There is still value for widespread malware
  - Less so for targeted attacks
- We need to start practicing
- We need different tools
- Those tools are available (for free!) right now
- And, they are easy to deploy
- We now have a call to action from MITRE
- Thanks!
- @strandjs



This is the end....