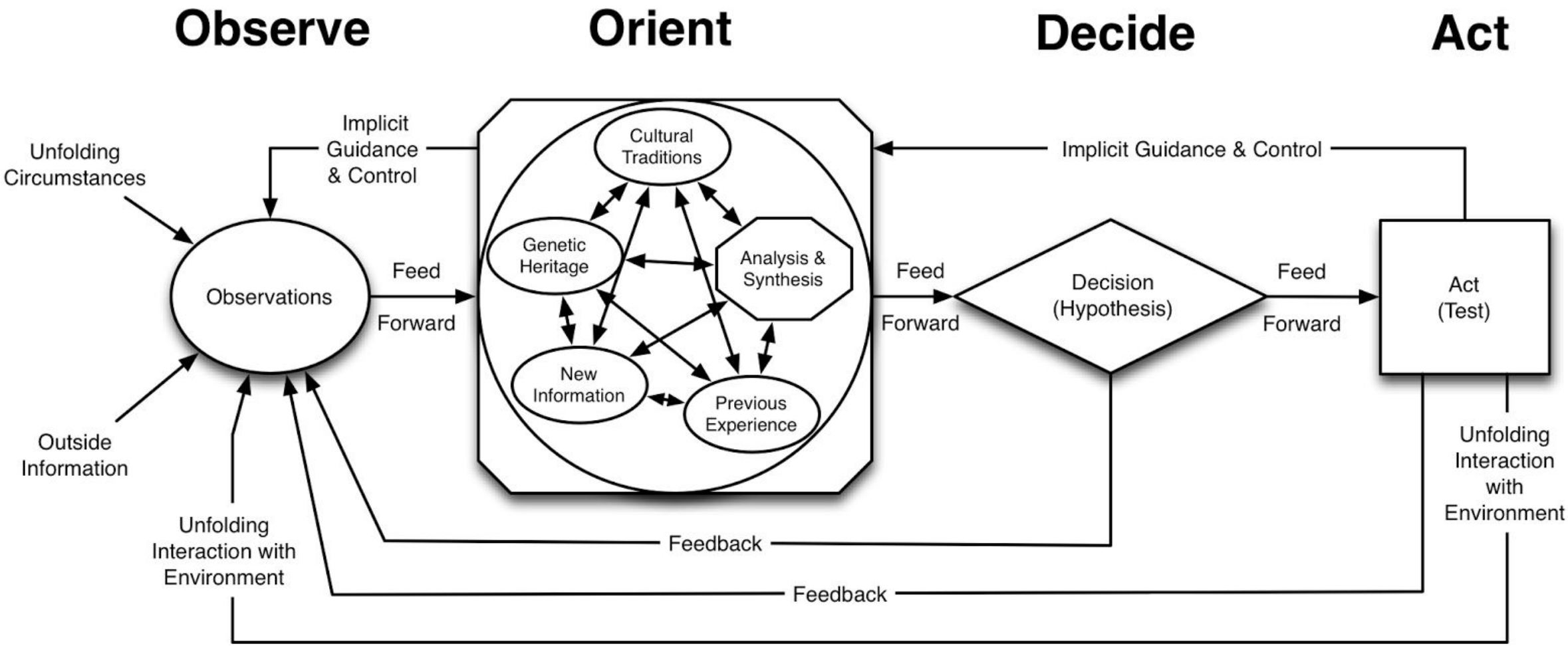
How to Cover C&C in the MITRE ATT&CK Matrix

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

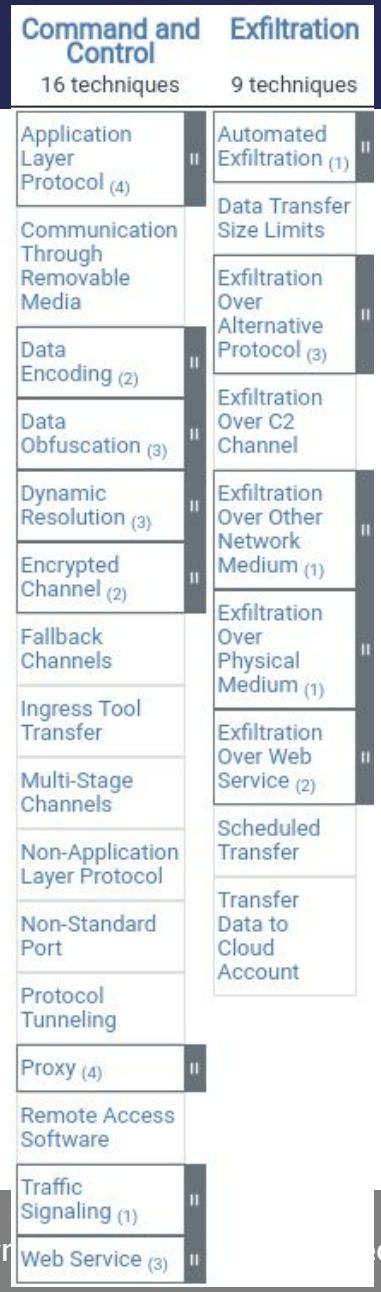
Bad Habit

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



MITRE Shield

MITRE | Shield

Matrix Tactics Techniques ATT&CK® Mapping Resources Blog Search Search

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

1

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 orginazations 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

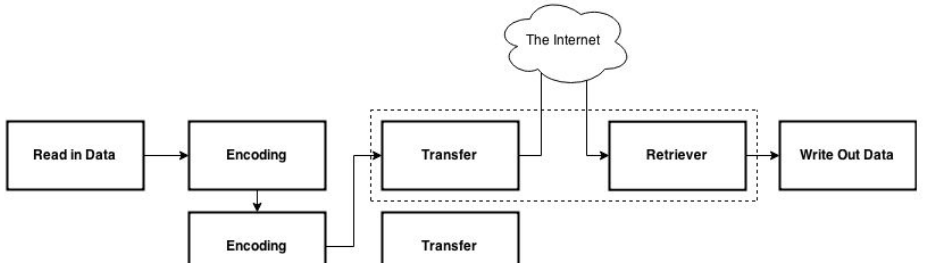
DakotaNelson update requirements.txt — 155b117 on Mar 7, 2018 — **193** commits

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

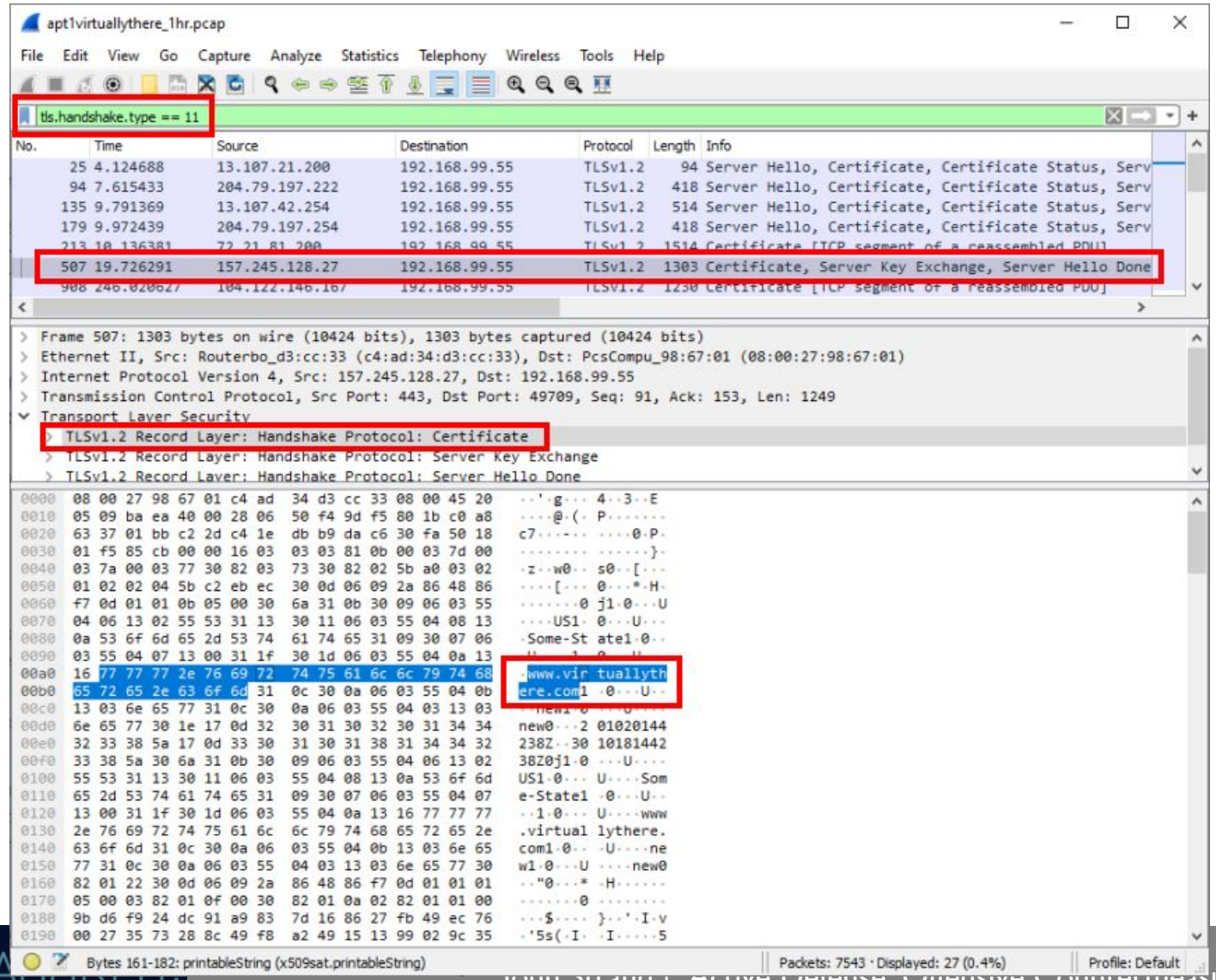
Jitter: 10%

Malware PCAP Samples

```
[redacted]$ ./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



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….