

# Deceptive Defense

## Beyond Honey pots



# Who am I?

- SecOps Architect
  - Security architecture
  - Security operations
  - Threat and vuln mgmt
  - SIRT lead
- PADI Divemaster
- Aspiring longboarder



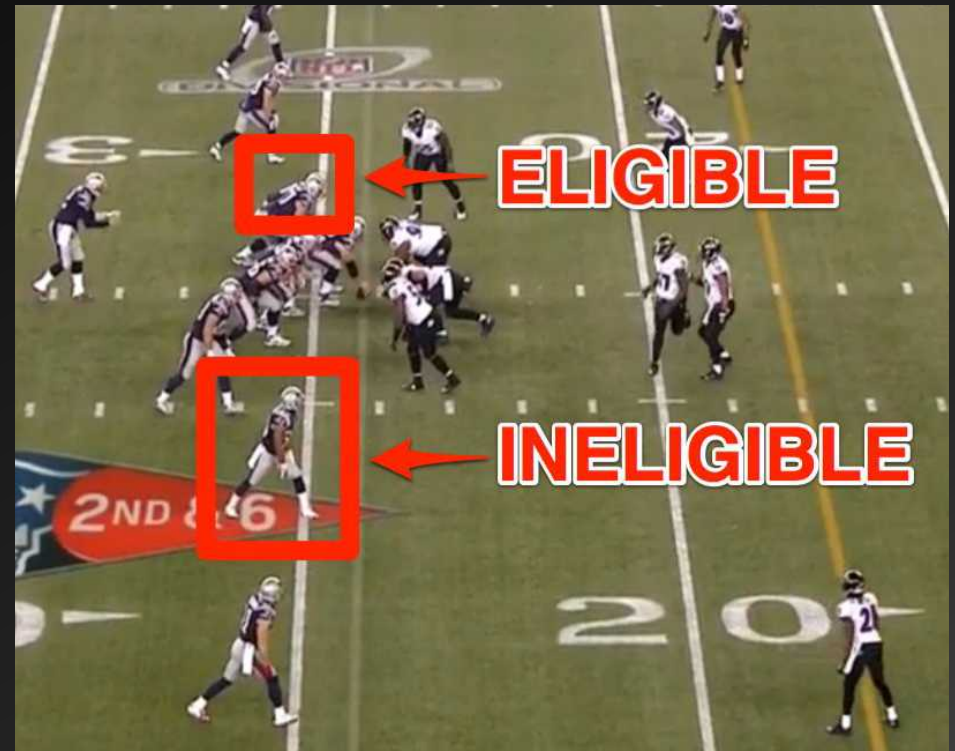
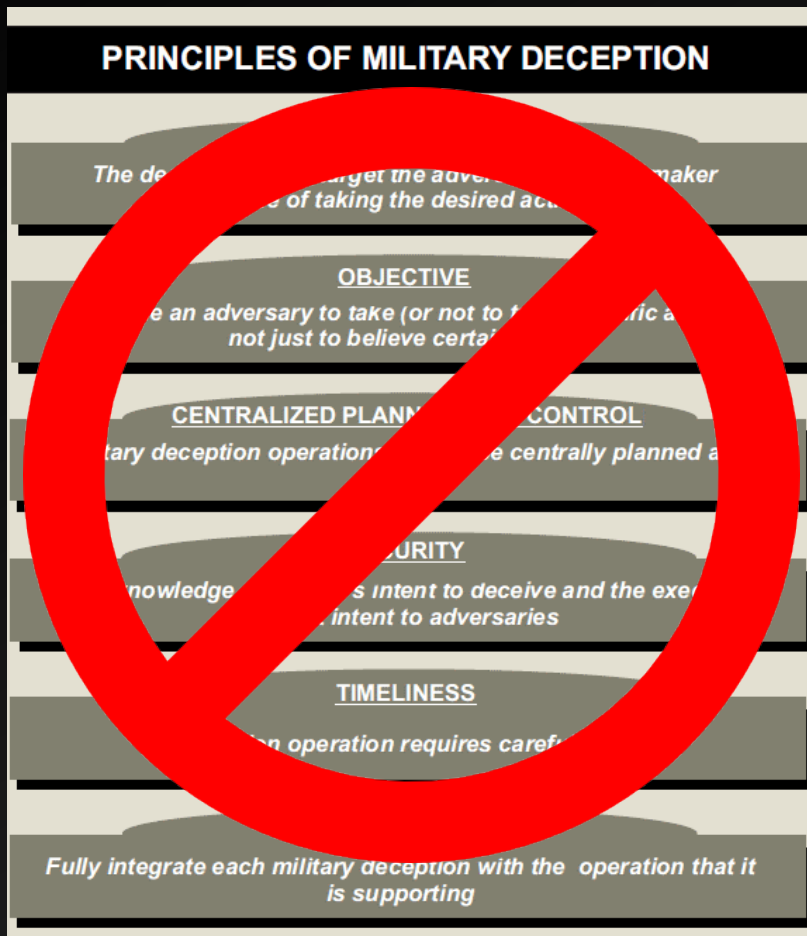


Deception is **all around** us.





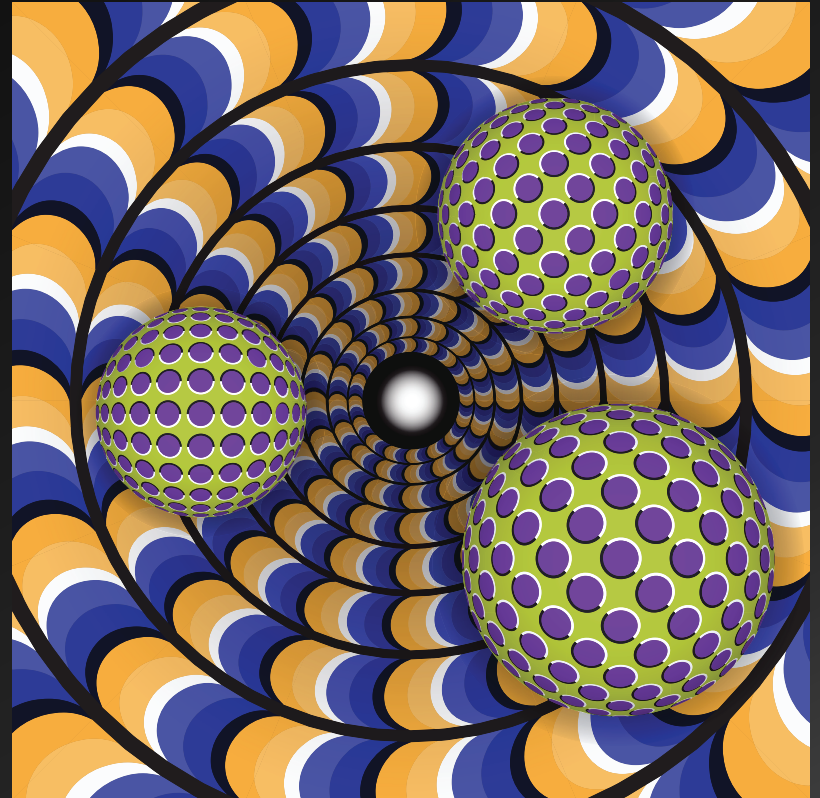
# Masters of Deception





# To deceive, or not...

- Align to security objectives
- Planning and preparation
- Execution of plan
- Monitoring
- Morality / ethics



# Types of Deception

Concealment	Hiding your forces from the enemy
Camouflage	Hiding your troops and movements from the enemy by artificial means
Disinformation / Lies	False and planted information
Displays	Techniques to make the enemy see what isn't there
Ruses	Tricks, such as displays that use enemy equipment and <b>procedures</b>
Demonstrations / Feints	Making a move with your forces that implies imminent action, but is not followed through—feints result in actual attacks
Insights	Deceive the opponent by outthinking him or her



# Types of Deception

## Concealment

# Concealment



"Sideline Hangout"



# Concealment

## Access Gateway

- Access sensitive applications or data through VPN or other gateway.

## Confidentiality

- Carefully manage access to sensitive information.

## Misleading Files

- Hide sensitive information inside innocuous looking files.

## Passwords

- Conceal information behind authentication.

## Low Building Profile

- House critical systems (DR, backups) inside inconspicuous buildings.

# Types of Deception

**Camouflage**

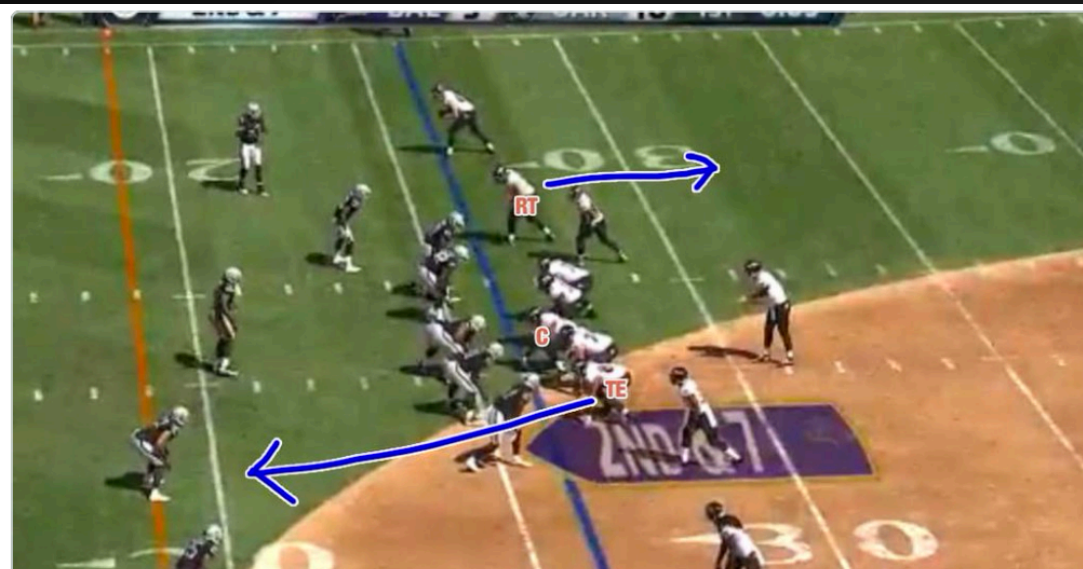


# Camouflage



"Deploring "unsportsmanlike tendencies" as represented by the use of **camouflage** in designing uniforms, the committee adopted a resolution which "deprecates the use of head protectors, jerseys, or attachments which are so similar in color that they give the wearers an unfair advantage"

# Camouflage



**Greg**  
@patsfb

 [Follow](#)

Umm... look what those a-hole Ravens did yesterday after petitioning to outlaw this

5:20 PM - 21 Sep 2015



# Camouflage

## Relocate Resources

- Change resource IP addresses. Modify service ports.

## Noise Manipulation

- Noise injection—electrical, sonic, other to reduce emanations; Noise reduction—eliminate C2 for speech input devices.

## DNS

- DNS Sinkholes for C2 and undesired application access.. AWS: Route 53 failover. Short TTLs. Custom domain names.

## Service Banners

- Yup—"security through obscurity" = deception.

## Cloaking Assets


- Cloak valuable targets so they look uninteresting.

# Types of Deception

**Disinformation / Lies**

# Disinformation / Lies

[NEWS](#) [ABOUT US](#) [MY CITY PAPER](#) [PROMOTIONS](#) [PUZZLES](#) [ADVERTISE](#) [DEALS](#) [ARCHIVES](#)



**CityProperties**  
**Open House**  
**Directory**

## True lies: In world of NFL injury reports, nothing is as it seems


Monday, July 16, 2012 at 1:57pm

By [David Bocclair](#)

Here's the simple truth about injuries in the National Football League: It's a lie.

All of it. Everything — from comments by coaches and players to the injury report issued by the league office each week during the regular season, to the way teams use the information in their preparation — is riddled with half-truths and falsehoods.

A lot of times the deception includes some nugget of fact. Others are well-crafted deceptions intended to send a completely false message. Sometimes the lie is the result of circumstances that change over the course of several days.





# Disinformation / Lies

## Fictitious Users

- Create users and online personas for defense and attack detection.

## Fictitious Files

- Files that appear sensitive and authentic e.g. Finance, Legal.

## Perception Management

- Appear to have better, or in some cases, worse security than actual.

## Unhelpful Error Messages

- Failed logins. Access to forbidden (403)? Return 404 instead.

## Time Manipulation

- Network and application throttling.

# Types of Deception

## Displays

# Displays



# Displays

## Ransomware Tripwires

- Seed file servers with huge, useless files at top of file system (alphabetically)—monitor and respond.

## DTK TCP/365

- Announce the use of defensive deception practices.

## Internal Darknet

- There's nothing to see here, really. If here, we're watching you.

## Cameras


- Some, blatantly visible. Others, not so much.




## Fictitious Employee Portals

- "Hey, Mr. Threat Actor, try those credentials here!".




# Ransomware? Pfft, bring it!

 draggeta / **kick-user**




 Watch **3**  Star **2**  Fork **3**

[Code](#) [Issues 1](#) [Pull requests 0](#) [Wiki](#) [Pulse](#) [Graphs](#)

Branch: **master** **kick-user / Kick-User.ps1** [Find file](#) [Copy path](#)

 draggeta SMB cmdlet ef231ce on Aug 20, 2015

1 contributor

128 lines (97 sloc) 6.17 KB [Raw](#) [Blame](#) [History](#)   

```
1 <#
2 .SYNOPSIS
3     Activates when an audited file gets edited and disables the user's account and computer
4 .DESCRIPTION
5     The Kick-User.ps1 script gets activated by a file audit event. This means that you need to attach a task to the specific events you want.
6     If the hashes don't match, the user will be extracted from the logs and the computername from the active sessions. Lastly, the user account is disabled.
7
8     Due to the way the workstation is detected, you need to run this script on the server you are auditing. If you want to forward the event to a log, use the net session command.
9
10    Regarding the script:
11    - ReplacementStrings are the values you can pull from the Event Viewer. 1 is the username, 6 is the folder.
12    - InstanceID's 4659 is delete, ID 4663 is modify. Change these to suit your environment if needed.
13    - The DNS and SMB cmdlets work only on Windows Server 2012/Windows 8 and newer. If this script is run on an older OS, use the net session command.
```

# Types of Deception

**Ruses**

# Ruses



Ruses



honeypot

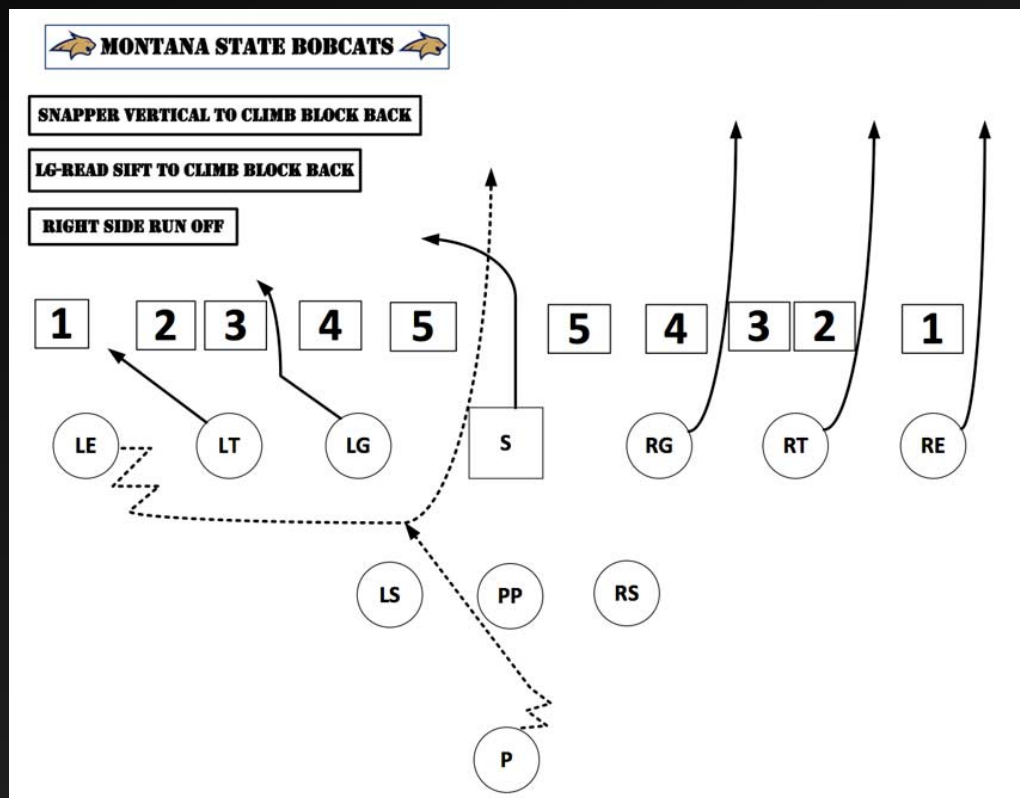
the delicious griefer treat



# Types of Deception

**Demonstrations / Feints**

# Demonstrations / Feints



# Demonstrations / Feints

## **Prosecution**

- Massive, coordinated busts psychologically impair attacker ops.

## **Termination of Insiders**

- Property theft, intellectual property, customer data.

## ***Communicate***

- Pass communications letting the actor know you're on to them.

## **In Litigation We Trust**

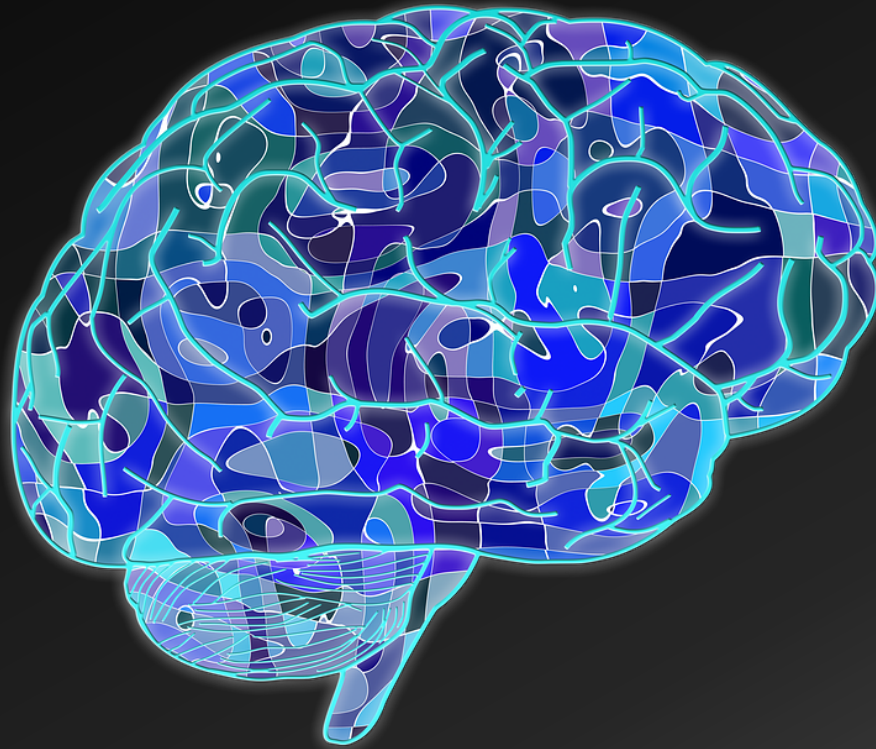
- Threat, and/or follow-through of litigation.

# Types of Deception

## Insights



# Insights



# Deception Intelligence



- Malware behaviors
- Threat actor TTP
- Defensive TTP
- Indicators
  - Domains, IP addr., files
- After-action report
  - Learn, refine, share



**Thanks for attending!**

**Joey Peloquin**

@jdpeloquin

# Sources

Deception in defense of computer systems from cyber-attack

<http://faculty.nps.edu/ncrowe/wardefdec.htm>

Neil C. Rowe

Two Taxonomies of Deception for Attacks on Information Systems

<http://www.au.af.mil/au/awc/awcgate/nps/mildec2.htm>

Neil C. Rowe

Hy S. Rothstein

Deception and Maneuver Warfare Utilizing Cloud Resources \*\*

[http://researchprofiles.herts.ac.uk/portal/en/publications/deception-and-maneuver-warfare-utilizing-cloud-resources\(3d5e0f30-0cbf-4984-9d35-8057a7707b3d\).html](http://researchprofiles.herts.ac.uk/portal/en/publications/deception-and-maneuver-warfare-utilizing-cloud-resources(3d5e0f30-0cbf-4984-9d35-8057a7707b3d).html)

Stilianos Vidalisa & Olga Angelopoulou

Active deception model for securing cloud infrastructure \*\*

<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?partnum=6849288&searchProductType=IEEE%20Conferences>

A. Brzeczko

Sch. of Electr. & Comput. Eng., Georgia Inst. of Technol., Atlanta, GA, USA

A. S. Uluagac ; R. Beyah ; J. Copeland

# Sources

Security Through Deception

Stilianos Vidalis, Zafar Kazmi

[https://www.researchgate.net/publication/220450031\\_Security\\_Through\\_Deception](https://www.researchgate.net/publication/220450031_Security_Through_Deception)

A note on the role of deception in information protection \*\*

<http://www.sciencedirect.com/science/article/pii/S0167404898800710>

Computers & Security, Volume 17, Issue 6, 1998, Pages 483-506

Fred Cohen

Victory and Deceit: Dirty Tricks at War (1995)

James F. Dunnigan

Albert A. Nofi

Victory and Deceit: Deception and Trickery at War (2001)

James F. Dunnigan

Albert A. Nofi

Deception and Trickery in Sport: The Patriots' "Formation-Gate" 2015

<http://law.scu.edu/sports-law/deception-and-trickery-in-sport-the-patriots-formation-gate-2015/>

Jack Bowen

Deception and Maneuver Warfare Utilizing Cloud Resources

Information Security Journal: A Global Perspective, 22:151–158, 2013

Stilianos Vidalis

Olga Angelopoulou