Defending Critical Assets with Deception

Contact Us:
https://www.illusivenetworks.com/contact
sales@illusivenetworks.com
Who am I

- A Sr. Solutions Architect for Illusive Networks based
- Has over 22 years in the IT Industry
- With over 17 years of cybersecurity experience with leading companies like CloudPassage, RSA Security, SilverTail Systems, HP ArcSight and Crossbeam Systems.
- Has developed and employed effective security strategies across several verticals including financial, healthcare, telecom, retail, industrial, as well as federal, state, and local government.
- Chad is a proud husband and father to a 7 year old son a 5 year old daughter and a dog named Harper (don’t ask where the name came from)
“All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.”

— Sun Tzu, The Art of War
The Challenge

Current environment

- A **Breach Will Occur** - Assumed
- Advanced Attacks are Top of Mind
- Most of the security spend is on prevention
- Attackers still make their way through all defenses

Challenges

- Security has become a big data problem
- Budgets are tightening and resources are limited and talent is hard to find.
- Actionable alerts are scarce - **Alert Fatigue**
- Executive Management now have to answer to the Board
206 median number of days to detection

69% of organizations learned of the breach from an outside entity such as law enforcement

85% of budgets on Prevention technologies and...

15% only on Detect & Respond
Only Need to be Right Once  Enough to Get it Wrong Once
Getting Easier  Can’t Keep Pace
Almost No Cost  Cost of Defense is Skyrocketing
Dynamic  Predictable & Static
No Rules  Highly Regulated
THE ASYMMETRIC ARENA

99/100 = **LOSE** the battle
Organizations need to secure 360 degrees of their network to protect their business

1/100 = **WIN** the battle
Attackers only need a single attack path to successfully infiltrate the network
Department of Homeland Security issued a formal report titled IR-ALERT-H-16-056-01. In the DHS report, three Ukrainian distribution companies experienced a coordinated cyber-attack that were executed within 30 minutes of each other. These attacks were directed primarily at the regional distribute level impacting over 225,000 customers.

The motive and sophistication of the attacker was consistent with a highly organized and well-resourced adversary.

The attacker varied tactics and techniques to “Match” the defenses and environment of the impacted target.

• **Access** - Spear phishing to bypass automated controls or static policy and engage a “person”.
• **Recon/Exfiltrate** - State sponsored modified variant of Black Energy Malware used for subversion of system resources, data collection and exfiltration and network monitoring.
• **Navigate** - Leveraged stolen credentials from business networks to access VPN to Industrial Control System network (ICS).
• **Disrupt** - Used modified killdisk freeware to erase master boot records and to delete logs. Scheduled service outages in UPS System. Denied telephone service by attacking the call center.
Phishing continues to be the #1 way an attacker enters an environment
Phishing is Deception

Phishing works off the same principles as social engineering. It removes static logic and pre-defined policy to engage the human and trigger a favorable emotional response.

**What is Phishing:** Impersonation in an effort to fool **people** to respond to a call to action. Example: Click link, provide personal information, request access, provide credentials.

**Phishing Types:**
- Deceptive Phishing: Impersonates a business
- Spear Phishing: Highly personalized with a specific target
- Whaling: Specifically targets CEO or high level employee
- Pharming: DNS Cache poisoning to redirect victim to a “Deceptive” website
It's all about the PEOPLE behind the attack
FLIP THE ASYMMETRY
THINK LIKE AN ATTACKER
Just a matter of perspective
The keys are under the welcome matt
People and the Process

• Originally developed for fighter pilots by military strategist of the US Air Force Colonel John Boyd
• A set of interacting loops that are kept in continuous operation during an engagement
• Favors agility over raw power when dealing with human opponents in any endeavor
• Works both ways!

With current security models, how do we impact this process?

The OODA Loop
- Observe
- Orient
- Decide
- Act
People and the Process

- Observe Deceptions
- Automatic Forensic Response
- Decide Incorrectly
- Disorient Attacker

What if we create a different reality for the attacker?

What if we disorient the attacker?

What if we increase the probability that the attacker makes the wrong decision?

What if we Act by automatically deploying forensics at the point where the decision was made?
To be successful the Attacker has to move

After the attacker has entered the environment he must answer 3 questions for himself

- What is available around me
- How can I get there
- Now that I am here
Deception techniques as a defensive strategy enables:

- Create an environment where detection is nearly unavoidable
- Reduce False positives
- Actionable alerts enable automation.