How misdirection can be used to steal information without being detected

Deceptive Hacking

Bruce “Grymoire” Barnett
Magician & Computer Scientist
Magicians and hackers have a lot in common

- They like to wear black
- They like to “shock” people
- They have Secret Knowledge
SECRET KNOWLEDGE = Profit
Magicians’ Arsenal

• Actions
• Props
• People
• Basic Psychology
  – Misdirection
• Advanced Psychological Techniques
• Example of the Magician-Hacker
ACTIONS
Feint

- Pretend to do something, but in reality nothing happens (the hand is empty)
- “A False Show”

Hack: Purposeful delay, “Checking your computer for viruses”
Bluff

• “Feint” but calling attention to the action
• Pretending, when nothing really has happened or will happen.

Hack: “We have detected a virus on your computer”
Phish, Used in Social Engineering
Sleight

- ..is a Secret Action, combined with technique
- Sleights are less valuable if they are well known
- Sleights may require years of practice
- Sleights can be worth money
- Sleights are sold with an underground economy
- The best sleights look natural

Hack: Exploit, Buffer Overflow, 0Day. Etc.
Temps or Timing

- Timing is used to improve deception
- Or make people forget

Hack: Planning ahead, low frequency port scan
Gimmick

- A secret device
- Performs some useful function which is unexpected because it is secret

Hack: Rootkit
Gaff

- A visible device with a secret function

Hack: Easter Egg, backdoor, hidden function
Fake (Feke)

- A simulation or emulation of a real device

Hack: Trojan Horse, Man-in-the-middle
Secret Accomplice, Stooge, Shill, Trusted Insider

- Someone who knowingly helps the attacker
- The victim does not know the insider is an enemy
- The more trusted, the less they are suspected
- “The Enemy of my Enemy” ploy

Hack: Insider Threat, “Friend Request” from stranger
Unwitting accomplice

• Someone who **unknowingly** helps
  – “Please forward this to everyone you know”
  – “I’m trying to help one of your colleagues who’s visiting us today…”

Hack: Social Engineering
The Patsy, or “Fall Guy”

- Innocent
- But takes the blame
BASIC PSYCHOLOGY
Naturalness – first principle of magic

• Often takes years to perfect some sleights
• Failure to deceive occurs if unnatural
  – i.e. Email from your “friend”
    • The more natural it is, the greater probability of it succeeding
• The Nemesis of the magician is the video recording
  – Forensics

Hack: Everywhere
And when naturalness isn’t possible

• Minimize the unnaturalness as much as possible
  – E.g. Reduce the number of log entries, alerts
  – Make log entries look more natural
    • “AAAAAAAAAAAAAAAAAAAAA” => “ProjectDirectory”
    • English Shellcode

• Hide what you can’t eliminate
  – E.g. Oracle.com vs Orade.com vs. 0racle.com

Hack: replicate legitimate e-mail, similar domain names
And when you can’t, make the unnatural natural

- Contrived Justification
  - Create a reason for the unnatural action
  - Social Engineering

- Repetition
  - Making the unnatural natural
  - Make a script kiddy attack have the same log pattern as your attack

Hack: Social engineering, port scans with secret attack
Misdirection

• A way to control attention so they don’t see anything unnatural
Focus their attention away from the unnatural

- Stimulate Interest
  - Attract attention
  - Appeal to their interests

- Distract attention from the unnatural part
  - “OMG! Check out what she is doing in this picture!”

Hack: Spam, thumbnails w/fleshtones
Directed Misdirection

• Can be caused by an action, or be distracting by its very nature.
• Can cause suspicion
• Attracts interest because of the topic
  – Lady Gaga!/Beyonce!
  – Justin Bieber!
  – Free iPad!
• or uniqueness of the event
  – Setting off a fire alarm
  – Manipulating the HVAC
  – Another attack
Discovered Misdirection

• Done ahead of time
• Undetermined when it happens. However, when discovered, it commands attention.
• If you can control the timing.....

Hack: Discovering a server is infected with a virus
Constrained Misdirection

- Hacker controls the “view” of the victim
- Getting the victim to remotely access the system that is secretly under control

Hack: Virtual Machine, Man-in-the-middle
Encourage false conclusion

• Develop a false premise
  – Provide evidence that the false premise is correct

• Create a false alarm
  – Purposely create a condition that “raised an alarm” and then proves it was wrong. Repeat
  – Causes alarms to be distrusted

• Repetition can be used to encourage a false conclusion
  – A Feint can mask a Sleight.

Hack: fabricated evidence, EICAR signature in real virus Stuxnet?
Use multiple methods

• Spectator thinks that because a method wasn’t used one time, concludes it wasn’t used ever.
• Allows multiple ways to accomplish the same thing if one method will be detected
• Purposely reveal method to encourage false conclusion

Hack: Multiple 0days in virus
The Switch

• Let them examine everything before and/or after

Hack: Switching malware in and out, self destruction
Fake Revelation

• Reveal an inferior method used by “others”
• An example will follow……
Conclusion

• By combining the toolkit and psychology of a magician
• With the skills of a hacker
• Creates a new style of hacking
• The goal: undetectable hacking
Now let’s create a scenario for the magician-hacker

- Company XYZ has valuable IP
- XYZ has excellent security
- Hacker is already inside
- If it is discovered that the IP is stolen, it is worth less $$
- Obvious exfiltration attempts would be detected

**WHAT WOULD THE MAGICIAN-HACKER DO?**
The Patsy

- Unlucky Lucy is administrator of the IP server
- Lucy is smart and alert!
- The magician-hacker has partial access to Lucy’s account and places some files in a directory she owns…….
- Which are propagated through the network
- He also creates some web\forum accounts using Lucy’s name, and posts outrageous comments
- There is also Innocent Ivy……..

Magic: Discovered Misdirection
More preparation from the Magician Hacker

- Places an archive of files on a public-facing server in an obscure but publicly accessible URL
- Causes the off-site backup to increase in size each day
- The file Lucy is sharing contains a 0day virus
- Next he generates a faked press release

Magic: Temps/Timing
“Company XYZ announces Adult Services”

Magic: Creating a False Conclusion
Then he makes a phone call to Innocent Ivy

- “I found some porn on your web server.”
- Ivy reports this to Chief.
- Magician-Hacker reveals details of “new exploit”

Magic: Bluff, Unwitting Accomplice, Creating a False Conclusion, Reveal an inferior method used by others
Meanwhile...

- CEO is told of “adult content” found on web site.
- Blogs are now commenting on it
- PR Nightmare begins.
- XYZ published Press Release in response
- CEO wants quick remedy. NOW!
- Virus signatures created by AV companies

**FIRST ROUND OF CHAOS**

Magic: Creating a False Alarm, Appeal to their interests
“Random” e-Mail to Ivy

• “One of your people, Lucy, was bragging about XYZ’s new adult services on a web forum.”
• Rough draft of the forged Press Releases, and jpegs, are also found in Lucy’s Directory
• Ivy reports to Chief, Lucy gets fired
• Virus signatures updated to include new attack

SECOND ROUND OF CHAOS

Magic: Bluff, Directed Misdirection
And then...

- Second bogus Press Release published
  - Announces “Public Key,” with URL, signed w/key
  - Reiterates that Company is going into “Adult Services”
  - Claims CEO has “Issues” with company’s new direction
  - Anti-virus finds hundreds of infected files

**THIRD ROUND OF CHAOS**

Magic: False Conclusion, misdirection
The plot thickens

• Infected machines start exporting random data to machines on the Internet
• Anti Virus software detected infected files in Innocent Ivy’s directory, but these are different
The Sucker Punch

- Source code of the virus is found in Ivy’s Directory
- Also — ”Adult” web pages are found
- Drafts of the second forged press release found
- Innocent Ivy fired

FIFTH ROUND OF CHAOS

Magic: Discovered Misdirection, Naturalness, Repetition
TO COMPLETE THE ILLUSION
The goal of the magician-hacker

- Steal the information from the database
- Don’t be detected while it happens
- Be as natural as possible
- Leave no evidence
What happened

1. A full backup of the server started
2. One small change DNS poisoning
3. When done, all traces of the modifications are removed

Magic: Sleight, Gaff, The Switch, Naturalness
Lessons

- Detecting the magician-hacker requires understanding new actions and motivations
- Unrelated events may not be unrelated
- The obvious answer may not be the right answer
- Increased forensics
- People, like computers, are assets too