Plausible Deniability Toolkit

Weasel & Simple Nomad
Nomad Mobile Research Centre

Introduction

- To provide resources and concepts that may be used to protect privacy by reducing the probability of incrimination as a result of computer misuse, be it criminal, civil or otherwise.

Clarifications

- What PDTK is
  - A new type of “toolkit” that provides its users with the knowledge and theory to reduce/remove incrimination risk?
- What PDTK is NOT
  - PDTK is not a suite of tools in the classic sense, rather it is a collection of theories and technologies to get its users on the path of deniability
- The PDTK is NOT Anti-forensics
  - However, there ARE (and always will be) some overlaps between the two
  - Some aspects of PDTK are anti-forensic, but for the most part anti-forensics is anti-alibi and may contradicts some of PDTK’s goals

Objectives

- Provide methods to the users to reduce the threat of incrimination
- Bring forward technologies for legitimate uses such as protecting activists and whistleblowers that have most likely been used in the underworld for years
- The PDTK will be focused on not providing a fingerprint to investigators. Those components that cannot be hidden will be “legitimized” by having multiple uses so that they do not point directly to the PDTK.

Strategies

- Data Generation
  - Generate “evidence” to provide alibi as well as give the appearance of compromise
    - Creating “deleted” files
    - Leaving compromise residue
    - Replicate data that cannot be removed/controlled across multiple systems
- Data Tampering
  - Alter data to be less “incriminating”
  - Alter data to be more “incriminating”
- Tool Injections
  - Sony Rootkit
  - Roll a sterile backdoor
- Anti-Forensics arcs and overlaps
- Automation/Scripting Tools

Tools

- Types of Tools
- New Uses for Old tools
- Legitimizing Tools

Types of Tools

- Forensics tools and books alone are bad
- As a security person…
  - Possessing dozens of security books and a few forensics books is normal
  - Having comprehensive security toolkits with forensics tools is normal, e.g. the BackTrack Linux security distro

New Uses for Old Tools

- Use tools that already exist on your system, and learn how they work (hex editors, dd, etc)
- Fsck checks for an inode's valid parent, so have two inodes point to each other, and store "data" there
  - A forensics exam that does a fsck of the drive looking for orphaned inodes will miss these two
  - It is possible to hide evidence of a rootkit here in case a forensics exam does uncover it

New Uses for Old Tools (cont.)

- Matt Conover's "Profiling Rootkits and Malware through Executive Objects"
  - Presented at InterZone West and RSA
- Discussed monitoring of system activity to detect the presence of rootkits on Windows systems
- The technique itself could be used to become a (currently) undetectable rootkit
- Do this now, hide it on your system
  - Maybe by the time a forensics examiner looks on your system, common tools will exist to "uncover" it

Legitimizing Tools

- If you have a forensics tool in your possession, you better have a damn good reason for having it there besides covering your ass

This is a picture of Bruce Potter's crotch taken during DefCon 13. Attend ShmooCon in March, www.shmoocon.org.

Distribution

Distribution

- www.nmrc.org/pub/pdtk
  - Tools, links, theories
  - Use privacy measures when visiting
    - i.e. Don't Google it
    - Onion Routing (Tor)
    - Public (unmonitored) terminals
    - Secure browsing measures
- Alternative/Diverse distribution methods needed

Caveats

Caveats

- Although the primary focus of the PDTK is to provide privacy measures for the oppressed, it does have the potential for misuse
- Presenting yourself as a dumbass is a bad idea when there is plenty of proof stating otherwise
- Don’t overestimate the capabilities of prying eyes and hide ‘evidence’ too well
- If you are already being investigated, it’s too late

Balancing Act

- If you are a Linux security expert, there should be nothing on your Linux box
  - The plausible deniability should exist on your Windows box, to which you are not an expert
- If you are trying to prove that you are innocent due to someone else hacking your box, the techniques used to hack your box should appear to be beyond your skillset
  - The 0day used to root your system by "that other guy" should not be in a dir on your system called cool_0day_nooneelsehas

Real World Examples

Real World Examples

- These are not real world examples of plausible deniability, but real world examples of forensics and their influence on investigations, indictments, and trials

Real World Example #1

- Child porn case, defendant determined to go to trial as he swears innocence
- Defense expert witness finds a remote-access trojan on the Windows system
- Defense asks Prosecution for details on this file including a binary copy etc
- Prosecution drops the case shortly after, having figured out where the Defense was going

Real World Example #1 Learning Points

- Defendant was not a computer security expert
  - If you attend DefCon, this defense won't work
- Prosecution only goes to trial if it thinks it will win
- Prosecution Forensics Examiner missed the RAT
  - They are overworked, underpaid, with huge backlogs of cases awaiting attention

Real World Example #2

- Another child porn case. Defendant claims innocence. Accused of trading child porn via IRC.
- Defendant claims seeing “black screens with text” at random intervals
- Defendant was determined to be savvy enough to understand that his system was backdoored/trojaned
- The hacker defense did not stick and defendant was found guilty

Real World Example #2 Learning Points

- Don’t claim stupidity beyond believability
- The hacker defense rarely works and is heavily frowned upon by the judicial system
  - Hacker defense is often trumped by proven capability

Real World Example #3

- State Senator under investigation for fraud, etc in Pennsylvania
- Two system admins in Senator's office, under orders, start deleting every email related to the investigation
- The system admins are indicted because they (obviously) did not get all the email deleted, including the email to each other talking about the cover-up

Real World Example #4

- US vs. Zezov
- Zezov accused of extortion of Michael Bloomberg (now NYC mayor)
- Found flaws in the financial software used by Bloomberg and propositioned to “fix for cash”
- All emails contact was From: Bloomberg To: Bloomberg
- Defense expert found signs of evidence tampering (specifically the most incriminating evidence)
- Defendant was still convicted on strength of other evidence

Real World Example #4 Learning Points

- Politics change all the rules
- Erratic behavior can be very damaging
- Appearance is everything
- Technical evidence is not always enough

Real World Example #3 Learning Points

- PGP Wipe leaves a fingerprint that forensic investigators used to determine exactly when PGP Wipe was being run, and the wiping started after the FBI investigation but before the confiscation
- Windows squirrels away copies of email all over the place
  - Exchange server, local folders, Trash folders, etc etc
- While they didn't get evidence on the Senator, they at least got the admins, and will probably try to throw the book at them


Another picture of Bruce Potter's crotch, taken yesterday at DefCon 14. Support Bruce's crotch and go to ShmooCon, www.shmoocon.org.

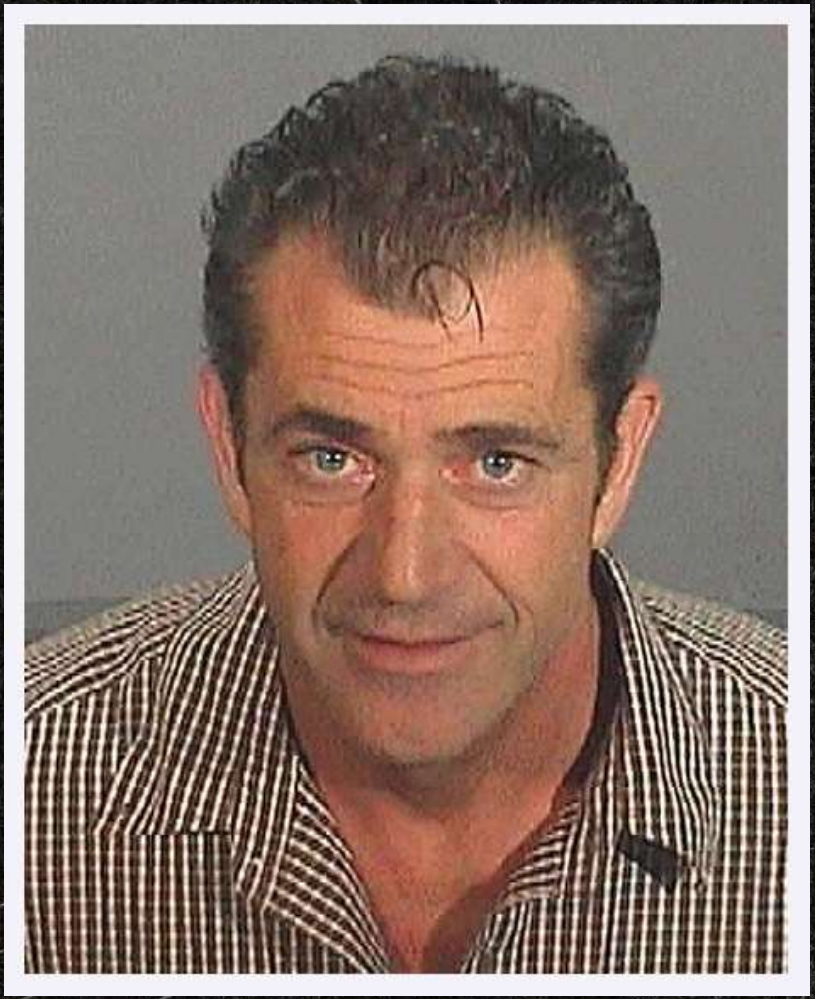
Conclusion

Conclusion

- If you control the bits and bytes on your computer, and know how forensics tools work, you can control the direction of a forensics investigation
- Forensics data could be direct or circumstantial evidence, but there will be other evidence as well
  - Data from the machine you popped or the IDS you triggered, affidavit from that guy you bragged to in IRC, etc
- Instead of trying to get out of it, embrace jury duty (learn the system and people)

Q&A

(No Jewish questions, please)



Links

- www.nmrc.org/pub/pdtk
  - Remember: Visit privately
- tor.eff.org
- www.usdoj.gov/usao/pae/News/Pr/2006/jun/luchkoeister_ind.pdf

- Send pictures of Bruce Potter's crotch to bruce_crotch@nmrc.org