Who Am I?

- Managing Consultant for the Trustwave SpiderLabs DFIR Team (Americas)
- Master’s degree in Information Security
- Author of “Unix and Linux Forensic Analysis” by Syngress
- Author of the award winning blog, “The Digital Standard”
- Chosen as a SANS “Thought Leader” in 2010
- Member of the USSS Electronic Crimes Task Force (Dallas, OKC, Miami)
- Former US Army Signal Corps Warrant Officer
SNIPER FORENSICS

http://dcdrawings.blogspot.com/
Twitter handle: @cpbeefcake
And here I sit at another airport, Dallas-Ft. Worth this time, writing another blog post. And yet again, I am reminded by an issue that continues to plague my forensic brethren. The heavy reliance on tools.

I am a member of several forensic/IR mailing lists, I read the blogsphere, and I try to keep up with many of you on twitter. In addition, I have a strong relationship and presence with many law enforcement agencies (local, state, federal and foreign) and the officers assigned to perform DF and IR. I intentionally don’t comment very much, mostly because I don’t think very many people would like my answers, but I help out when and where I can.

So to get right down to it, I still see a strong reliance on tools to solve cases for you. I have also seen a number of posts and tweets recently where investigators are trying to make certain tools do certain things they are either not well suited to do, or where a much better solution exists. To all this, I say, “stop”!

Stop stop stop stop it!

Relying on tools to solve your case for you is like relying on a pile of dirt to build your house.
Agenda

• Recap – What is Sniper Forensics?
• The Evolution of Sniper Forensics
• What are the benefits of using Sniper Forensics?
• Battlefield
• Gun Shy
• Lethal Forensication
• Conclusion
The Evolution of: Sniper Forensics

• “The process of taking a targeted, deliberate approach to forensic investigations.”
  – Create an investigation plan
  – Apply sound logic
    • Locard’s Exchange Principle
    • Occam’s Razor
    • The Alexiou Principle
  – Extract what needs to be extracted, nothing more
  – Allow the data to provide the answers
  – Report on what was done
  – Answer the questions
Sniper Forensics v2.0: Target Acquisition

• What do I snipe?
  • Registry Hives
    • SAM
    • Security
    • System
    • Software
    • NTUSER.DAT

• How do I actually DO that?
  • Manually via FTK using F-Response
  • Script it

• How do I interpret the data?
  • Infiltration
  • Aggregation
  • Exfiltration
Sniper Forensics v3.0: Hunt

- Identify Indicators of Compromise (IOC)
- 1000 yard stare
- In The Cross Hairs
- Lethal Forensication / Expert Eyes
- Endgame
Sniper Forensics v4.0: Reloaded

• Sniper Forensics has traditionally been used on single systems, or small business environments.
• On cases where you knew something was going on, and you likely had the right system(s).
• What happens when the environment is larger than just a few systems?
• What happens when you don’t exactly know what you’re looking for?
• Same weapon...different scope!
Battlefield
Current Operating Environment

“They’re P0wn1ng ery’body out here!”
Targets

• Data of value
  – Payment Card Data
  – Trade Secrets
  – Government Agencies
  – Emergency Response Data
  – Law Enforcement Agencies
  – Government Contractors

• Hacktivism / Occupy
  – They don’t like you
  – They don’t like what you stand for
Actors

- Foreign Governments
- Organized Crime Syndicates
- Terror Organizations
- Hacktivist Groups
- Individuals
Goals

• Monetization
  – Steal data of value
  – Monetize valuable data on the black market

• Havoc
  – Disrupt critical services
  – Destroy industry reputation

• Harm
  – Cause bodily harm or injury
  – Destroy physical property
Gun Shy
Perceived Complexity

• Often increased due to Analysis Paralysis
  – What do I do now?
  – There’s too much data!
  – Too many systems!

• This is often the step that crushes investigators.
  – Lack of an investigation plan
  – Erroneous steps are made
  – Real progress is hindered
Force Multiplier

“A capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment.”

http://www.thefreedictionary.com/force+multiplier
Force Multiplier #1 - Logic

• What were you brought in for?
  – What happened?
  – Who was involved and how?

• What intel was provided by the client?
  – Malware?
  – When did the activity take place?
  – What do they have that is worth taking (the bad guys are not there just for the heck of it)?
  – Which systems are known to be affected?
  – What is the significance of those systems?
Force Multiplier #2 – Alexiou Principle

• Apply the Alexiou Principle
  – What questions were you brought in to answer?
  – What data do you need to answer those questions?
  – How do you extract and analyze that data?
  – What does the data tell you?
Force Multiplier #3 - Wetware

• What is the attack (very simply, what’s going on)?
• Establish IOCs
• Expand the search to all potentially affected systems (go look for the IOCs)
• Use what the customer already has in place to aid your search
• Document the affected systems
Example Scenario
Example Scenario

- Company X has been hit by a Spear Phishing attack.
- During the attack, an undetermined number of employees clicked on a link provided in an email attachment.
- The client has secret formulas that if exposed to their competition, would adversely affect their business.
Intel

• You know that company X has secret formulas – *Something Worth Stealing*

• You know that a Spear Phishing Attack has been launched against company X. You have a copy of the email and the attachment – *Breach Triad*
  – You know how it got in, you can figure out what it did, and then you should know how it got data out.

• You know that at least one individual has clicked on the link.
Investigation Plan

• Analyze the email
  – Analyze the headers
  – Source?
  – Unique characteristics?

• Analyze the attachment
  – Embedded malware?
  – Functionality (Breach Triad)

• Generate Indicators of Compromise
Lethal Forensication
Lethal Forensication

• Analysis of the email should help you determine the intent of the attack
  – Where did it come from? (email headers)
  – Linguistic anomalies?
  – When was it sent?
  – How was it labeled?
  – Who was it sent to?
    • Where could the attackers have obtained that list?
    • What is unique about the targeted individuals?
  – What did it do?
Lethal Forensication

• Malware
  – How was it dropped
  – What type of data did it target
  – How did it aggregate that data
  – Where did it send the data
  – Does it propagate
    • If so, how
Lethal Forensication

• **Indicators of Compromise**
  – What are the characteristics of infection?
    • The more detailed this can be, the better! (and honestly, the smaller this can be, the better)
    • This is how you will know an infected system from a non-infected system
  – Propagation method
    • How does it move from one system to another
      – So you can contain it
      – So you can prevent re-infection
Lethal Forensication

• ICED – Four step incident response process
  – Identify
    • What is the threat
  – Contain
    • Using the IOCs, prevent further propagation
  – Eradicate
    • Remove the malware from the affected systems
  – Defend
    • Update, patch, train
Conclusion
Conclusion

• The Sniper Forensics methodology is no different in an Incident Response scenario within a larger infrastructure.
• The same principles apply
  – Occam
  – Locard
  – Alexiou
• Create an investigation plan
• Use intel provided by the client
Conclusion

- Establish IOCs
- Determine propagation method
- ICED
  - Identify
  - Contain
  - Eradicate
  - Defend
Conclusion

• Take good case notes
• Use the strengths of your teammates to tag team the investigation (High Powered Teaming)
  – May need expertise in:
    • Network forensics
    • Malware analysis
    • Single system forensics
      – Registry analysis
      – Timeline analysis
• Use the client’s utilities to your advantage
  – AV
  – IDS/IPS
Questions?

cepogue@trustwave.com
@cpbeefcake