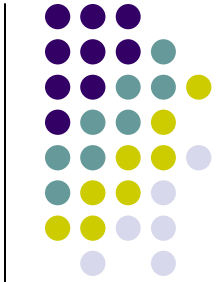
Extrusion Detection with Aanval and Bleeding Edge Threats

Russ McRee

holisticinfosec.org

BLEEDING EDGE THREATS

Introduction

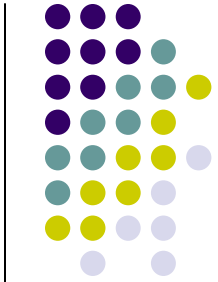


- The threats are real
- Malware (e.g. viruses, worms, trojans, bots, rootkits) are becoming more sophisticated
- Security breaches and attacks are becoming more publicized
- People are becoming more concerned with their online privacy…
- However, people *still* lack awareness re: basic computer security issues
    - Credit to Ming Chow for his presentation “What Is Outstanding In Your Security and Compliance Practice?”, Tufts University

Threat Matrix

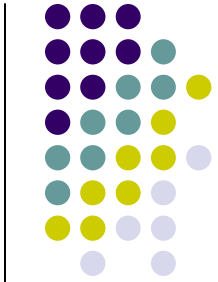
Internal Threats	External Threats
• Disgruntled employees • Disgruntled consultants • User misuse / theft of data and resources • Malware (viruses, worms, trojans, rootkits) • Software bugs and flaws	• Theft of hardware / disks / tapes • Theft of personnel desktops • Theft of personnel laptops • Computer vendor / developer failure (e.g. bankruptcy) • Random hackers / crackers • Terrorism

Security Issues Facing Us All



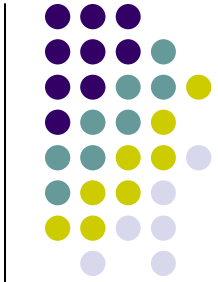
- Enormous disconnect between IT and general users
- Lack of awareness re: computer security fundamentals (poor practices)
- Social engineering
- Insider threat
- Lack of low-tech and low-cost planning
- Lack of testing environments to understand threats and potential security breaches
- ***Security is most often a reactive process***
- ***Can it not be proactive?***

Summary of Concerns



- Data security
- Privacy
- More sophisticated malware
- Peer-to-Peer (P2P) networks and torrents
- IM
- Compliance and auditing

Malware sophistication



Evolution of blended threats

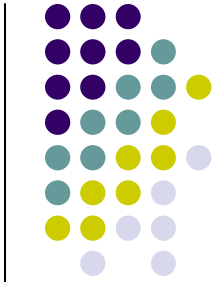
- According to Jim Murphy, in Feb. 2006 issue of IT Defense:

  In corporate environments, blended threats result in productivity loss, higher bandwidth utilization, and costly cleanup. Companies also face legal liability if inappropriate or illegal content is accessed or stored by employees. Successful blended attacks often enable criminals to steal or corrupt valuable data and engage in extortion, potentially damaging a company's brand and credibility, and making regulatory compliance (e.g., with the Sarbanes-Oxley act or HIPAA) difficult, if not impossible.

Why So Many Data Privacy Problems Recently?

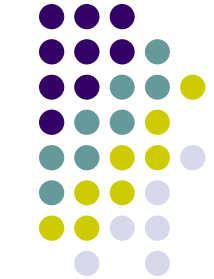
- Heavy usage of and dependency on Social Security Numbers and credit card numbers
- Poor web security
- Insider threats
- Social engineering (scam artists, phishing)
- Pharming
- Third-part businesses
  - In recent arrest of bot herder, evidence trail included PayPal payments from “pay per install” adware companies

Common Compliance and Legal Frameworks



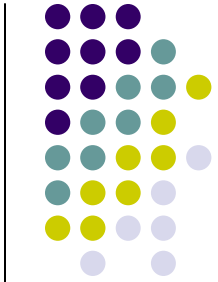
- Health Insurance Portability and Accountability Act (HIPPA)
- Gramm-Leach-Bliley Act (GLBA)
- Computer Fraud and Abuse Act (CFAA)
- Sarbanes-Oxley Act
- USA PATRIOT Act
- Visa USA Cardholder Information Security Program (CISP) / MasterCard Site Data Protection Program / Payment Card Industry (PCI) Data Security Standard
- SB6043 (WA) & SB1386 (CA)

Significance of the Compliance Frameworks



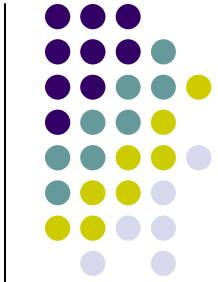
- *HIPAA* - Safeguarding of electronic protected health information
- *GLBA* - Protects privacy of consumer information in the financial sector
- *Sarbanes-Oxley Act* - Executives need to report quickly and accurately

Impact of Breaches



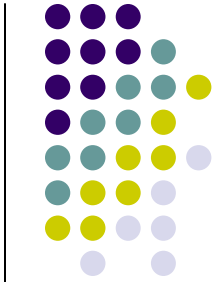
- Heavy network consumption
- Direct impact on leadership
- Legal consequences
- Bad press
- Loss of competitive edge
- Long road to recovery

The questions to ask…



- Ask yourself, and management (revisit the questions):
  - What are your security goals?
  - What are you really protecting?
  - What are your priorities, especially in a product (e.g. interface, administration, prevention)?

Opportunities:



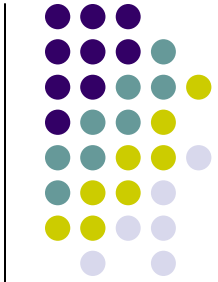
- Security related situational awareness
- Profiling users and traffic
- Linking relationships (correlation)
- Network traffic classification
- Intrusion detection/prevention
- Detecting abnormalities

Aanval & Bleeding-Edge Threats

- “Aanval is an advanced data management, correlation and analysis console designed specifically for Snort…a web-based solution…to give users comprehensive management and correlation.”
- Bleeding-Edge Snort - “The Aggregation Point for Snort Signatures and Related Security Research”

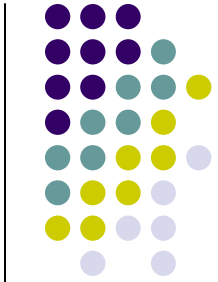
BLEEDING EDGE THREATS

We won't cover…



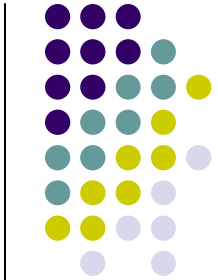
- System installation
- Snort installation, but…
  - Be sure to install with ./configure --with-mysql for version 2.4 or ./configure --with-mysql --enable-dynamicplugin for version 2.6
  - If you're new to Snort, utilize Patrick Harper's install doc at http://internetsecurityguru.com/.
- Aanval installation or its Syslog capability
  - Extremely straightforward and well documented at: http://www.aanval.com/downloads/aanval_installation_v1.pdf

We will cover…

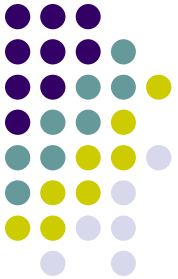


- Bleeding Edge Threat rules
  - Basic Snort rules
  - Specific Bleeding Edge Threat rules as they pertain to spyware, malware, IM, and content monitoring
- Aanval use
  - The Go! Search tool and search syntax
  - Searches relevant to our cause: identify OUTBOUND risks, in whatever form they may come

Similar platforms



- OSSIM
  - Open Source Security Information Manager
  - Trying to be all things to all people, still maturing, a bit convoluted
- Sguil
  - Very promising, but difficult to install
  - Also still maturing, but under constant development
- ACID/BASE
  - Ye olde standard-bearer
  - Work well, but limited in functionality, aesthetics, and reporting



- Bleeding Edge Threats is a Free Zone for Snort signature development, and a number of other related security projects. Bleeding Edge Threats brings together the most experienced, and the least experienced security professionals.

- There was no real way to make sure you had the latest signatures, or contribute effectively a tweak to improve a signature. Bleeding Edge Threats was founded by Matt Jonkman and James Ashton to fill that need.

Snort rules

- Snort, originally created by Martin Roesch, is powerfully flexible in its ruleset. A visual representation of a Snort rule looks like this:

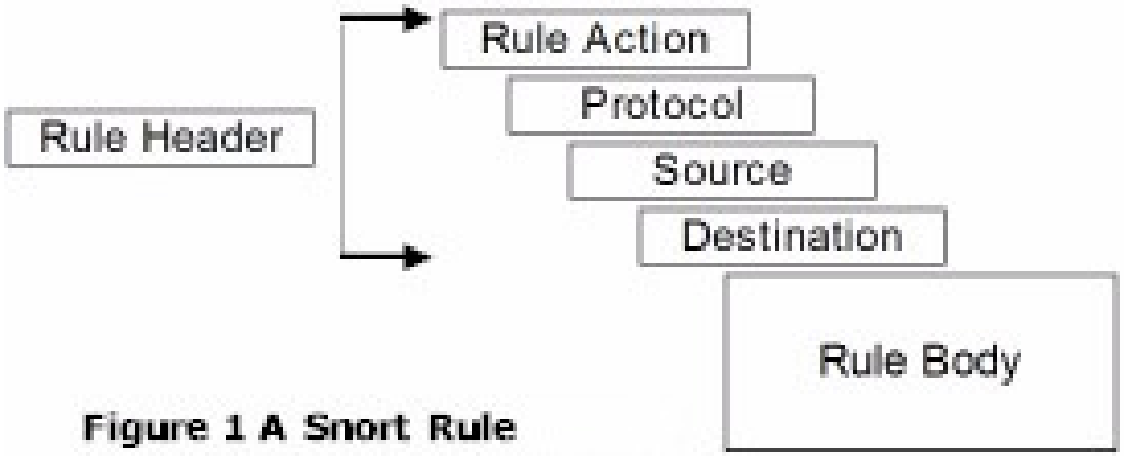
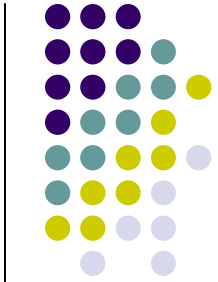


Figure 1 A Snort Rule

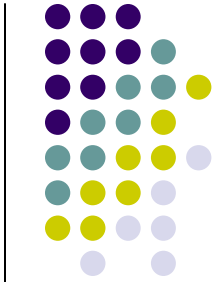
A basic rule



- With our visual reference in mind lets use a very simple rule, one that might be used to enforce a “no telnet” policy in your organization:

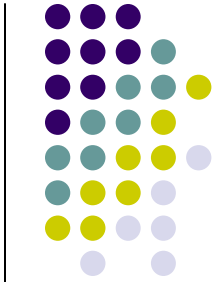
alert tcp any any <> any 23 (msg:"TELNET Viewable Session"; session:printable;)

A basic rule interpreted



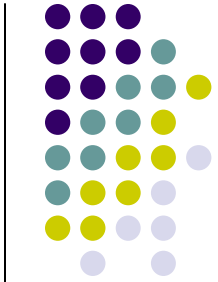
- *alert* indicates our rule action, in this case to alert as opposed to log or pass.
- *any any* represents our source address and port while <> denotes a bi-directional operator which tells Snort to review address/port pairs in both ingress and egress traffic.
- The second *any 23* pair corresponds to our destination address and port.
- Finally, in parentheses enclosing the rule body, we find the message (*msg*) returned to our console, namely *TELNET Viewable Session*. *session:printable* defines that we should be alerted with data that users can see or type.

More complex rules



- As we roll through a variety of Bleeding Edge Threat rules, we'll break them down specifically as to their rule details
- We'll visit spyware, IM, policy violations, and information leaking

Aanval features



- Aanval is an event management and analysis console designed specifically for Snort and Syslog data.
- Remote Sensor Management
  - Take control of sensors, signatures and data using Sensor Management Tools (SMT's).
- Full Text Event and Payload Searching
  - The only Snort console that allows users to perform full text searches of dynamic packet payload data.
- Artificial Intelligence
  - Aanval includes a custom AI engine which helps to automate many tasks within the Aanval Console such as auto-alerting, optimizing performance, limiting false positives and ensuring your console and sensors are always running.

Main Console Screen

- Provides a diverse data set in one simple view.
  - Attack and signature counts, hourly and daily statistics, and charts & graphs.
- Each block is customizable, colors are configurable and each user can select the type and time period of data to be displayed.

Main Console Screen

Series 2 > Aanval Console™

Live Monitor | Features | Console | Logout

Search > Go! Help

Aanval Home > Main Console | View Today's Events | View Yesterday's Events

Frequent Events > Aanval Console

Signature	Options	Events	% of 28833
COMMUNITY WEB-MISC mod_jrun overflow attempt	Report	6408	22.2%
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	Report	3824	13.2%
ICMP Destination Unreachable Port Unreachable	Report	3805	13.1%
NPI - High Ports Password	Report	2505	8.68%
COMMUNITY MISC BAD-SSL tcp detect	Report	2328	8.07%
(ftp_telnet) Telnet traffic encrypted	Report	2206	7.65%
SHELLCODE x86 NOOP	Report	1596	5.53%
ICMP PING *NIX	Report	983	3.40%
ICMP L3retriever Ping	Report	681	2.36%
(http_inspect) BARE BYTE UNICODE ENCODING	Report	635	2.20%
INFO web bug 1x1 gif attempt	Report	540	1.87%
NETBIOS SMB IPC$ unicode share access	Report	536	1.85%
(portscan) Open Port	Report	302	1.04%
NETBIOS SMB-DS IPC$ unicode share access	Report	248	0.86%
NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt	Report	244	0.84%
NPI - High Ports Date of Birth	Report	169	0.58%
WEB-CGI album.pl access	Report	150	0.52%
WEB-MISC weblogic/tomcat .jsp view source attempt	Report	150	0.52%
WEB-IIS %2E-asp access	Report	134	0.46%
(http_inspect) OVERSIZE REQUEST-URI DIRECTORY	Report	104	0.36%
WEB-IIS view source via translate header	Report	96	0.33%
ATTACK-RESPONSES 403 Forbidden	Report	81	0.28%
BLEEDING-EDGE Hotmail Inbox Access	Report	71	0.24%
WEB-CGI calendar access	Report	62	0.21%
MULTIMEDIA Windows Media download	Report	56	0.19%
BLEEDING-EDGE WEB-MISC cross site scripting attempt to execute Javascript code	Report	53	0.18%
WEB-MISC Chunked-Encoding transfer attempt	Report	47	0.16%
DNS SPOOF query response with TTL of 1 min. and no authority	Report	43	0.14%
WEB-MISC cd..	Report	42	0.14%
ICMP PING NMAP	Report	42	0.14%
(http_inspect) OVERSIZE CHUNK ENCODING	Report	42	0.14%

More - Less | Stats Display Toggle | Time Toggle | Page Display

Hourly Statistics > Aanval Console

Total Events		Unique Source		Unique Destination	
4 PM	4.05%	4 PM	7.56%	4 PM	7.36%
3 PM	10.5%	3 PM	10.7%	3 PM	12.7%
2 PM	8.39%	2 PM	9.51%	2 PM	9.00%
1 PM	9.12%	1 PM	10.0%	1 PM	9.72%
12 PM	8.89%	12 PM	11.7%	12 PM	11.3%
11 AM	7.81%	11 AM	8.95%	11 AM	9.43%
10 AM	19.7%	10 AM	12.7%	10 AM	12.1%
9 AM	7.90%	9 AM	11.2%	9 AM	8.95%
8 AM	7.06%	8 AM	8.13%	8 AM	8.32%
7 AM	4.32%	7 AM	4.06%	7 AM	4.95%
6 AM	3.02%	6 AM	2.52%	6 AM	2.21%
5 AM	2.54%	5 AM	0.97%	5 AM	1.34%
4 AM	2.46%	4 AM	0.89%	4 AM	1.25%
3 AM	2.56%	3 AM	0.81%	3 AM	1.20%

Frequent Events | Change

Hourly Statistics | Change

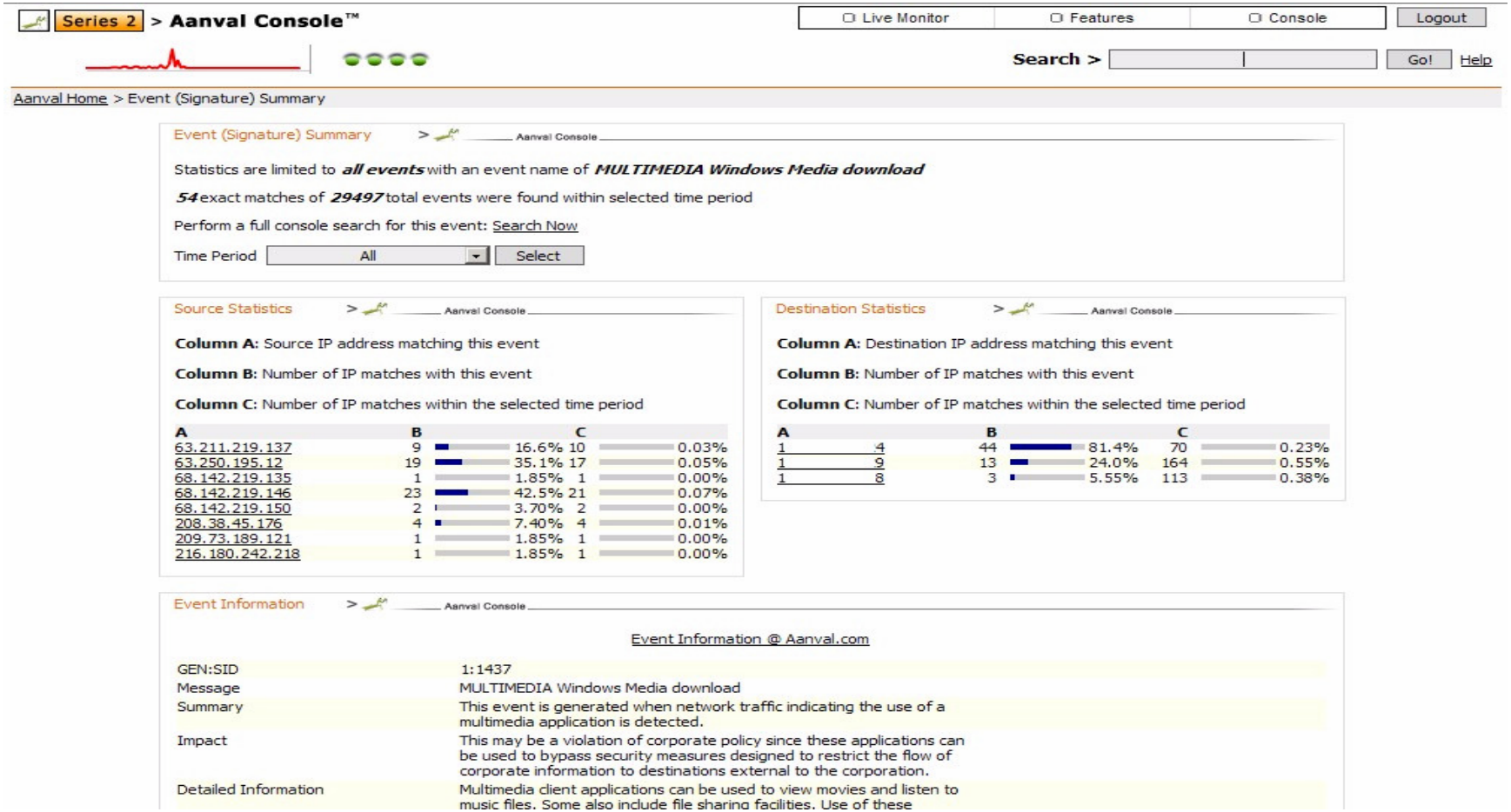
Frequent Offenders > Aanval Console

Selected Graph Display > Aanval Console

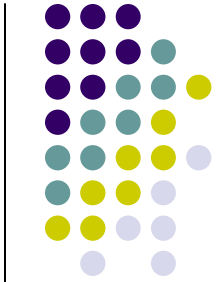
Event (Signature) Summary

- Clicking a signature name within the Aanval Console brings users to the Event (Signature) Summary screen which provides detailed source and destination details over a selective time period.
- In addition, this screen also provides the latest available signature information to help determine if this signature type is of any concern.

Event (Signature) Summary

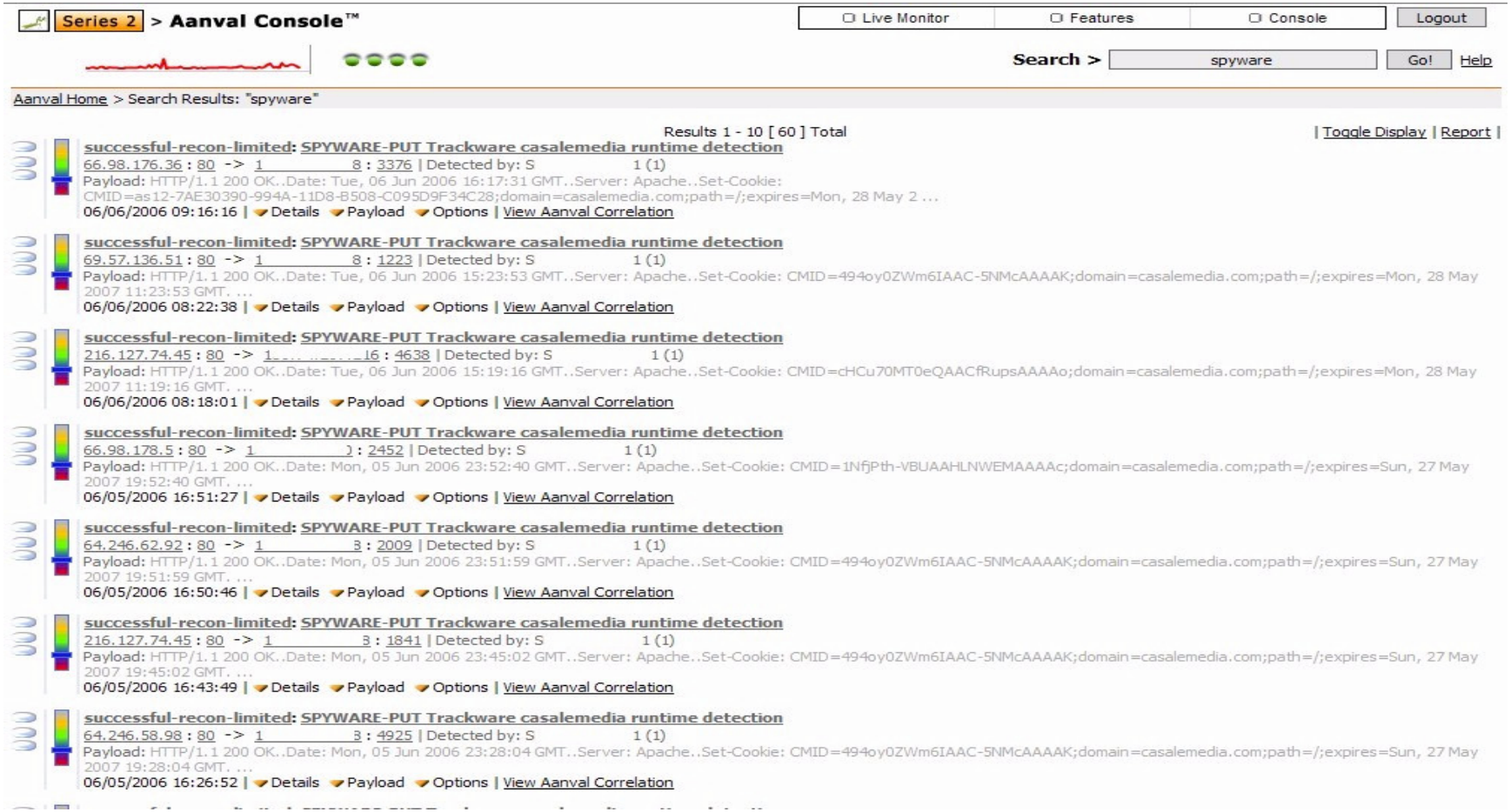


Aanval Search Display

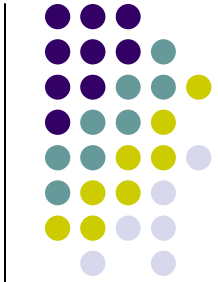


- Aanval is a search engine for your network data as captured by Snort rules.
- Quickly view source, destination, signature details and a payload summary right from one screen.

Aanval Search Display

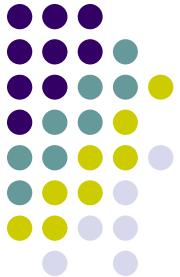


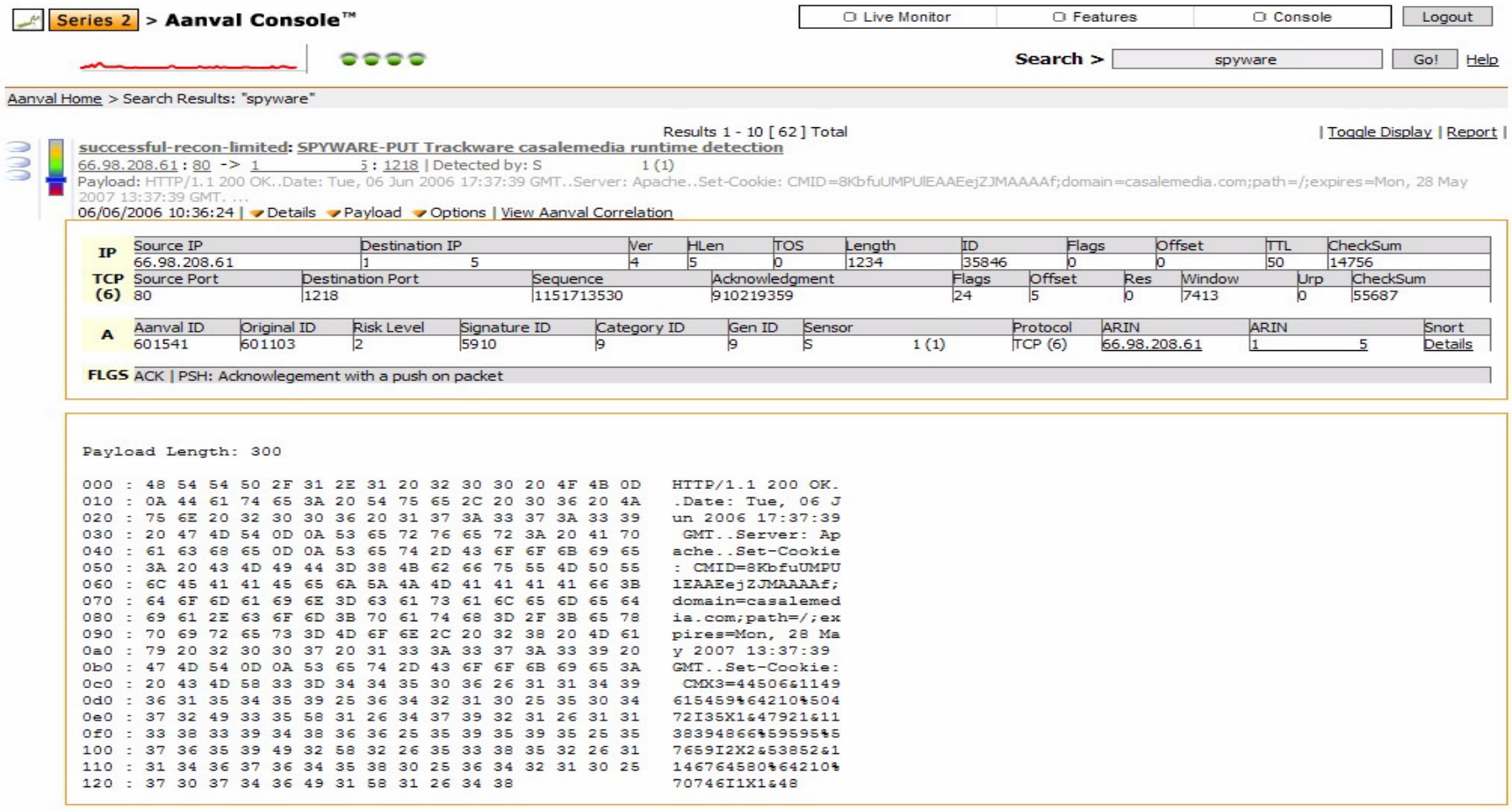
Enhanced Search Display



- Compare events side by side, view full packet payloads and perform quick actions such as delete, ignore and more.
- The details drop down, provides every detail of every packet including TTL, Window Lengths, Checksums and more.

Enhanced Search Display





Specific queries: Go! Search

- Every view in Aanval includes the Go! Box
  - Syntax can be found in Help, but it's as simple as keyword searches
  - Examples include *report:spyware, report:chat* or *report:p2p* or more simply, just *spyware* for an event view
  - Deeper queries are as easy as *report:spyware sip:192.168.123.4*
    - This search looks for spyware specific to source IP 192.168.123.4

Specific queries: spyware

Series 2 > Aanval Console™

Live Monitor | Features | Console | Logout

Search > report:spyware Go! Help

Aanval Home > Reports > Reports Results: "spyware" @ 06/06/2006 13:43:16

Confidentiality Statement > Aanval Console

This document contains sensitive and / or confidential information, do not distribute, email, fax or transfer via any electronic mechanism without proper authorization. Information contained within this document should be handled with appropriate caution. While reasonable attempts have been made to confirm the accuracy of the data contained herein, Remote Assessment assumes no liability for the completeness, use of, or conclusions drawn from such data.

Report Statistics > Aanval Console

Total System Results	53342	100%
Total Results	64	0.11%

Event Details > Aanval Console

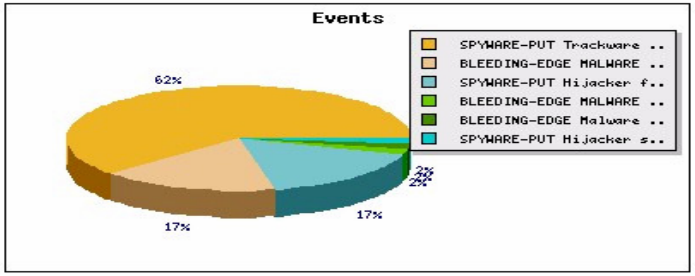
Unique Events		6
SPYWARE-PUT Trackware casalemedia runtime detection (ID: 5910)	37	57.8%
BLEEDING-EDGE MALWARE Fun Web Products Spyware User Agent (1) (ID: 2001855)	10	15.6%
SPYWARE-PUT Hijacker funbuddyicons runtime detection - funwebproducts user-agent string (ID: 5856)	10	15.6%
BLEEDING-EDGE MALWARE Possible Spyware -- Wise User Agent (ID: 2002167)	1	1.56%
BLEEDING-EDGE Malware Fun Web Products Cursorchooser Spyware (ID: 2002306)	1	1.56%
SPYWARE-PUT Hijacker smart shopper runtime detection - track/upgrade/report activities (ID: 6197)	1	1.56%

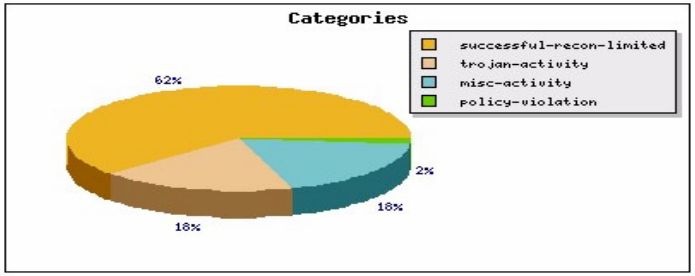
Category Details > Aanval Console

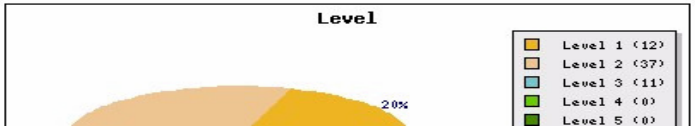
Unique Categories		4
successful-recon-limited (ID: 9)	37	57.8%
trojan-activity (ID: 2)	11	17.1%
misc-activity (ID: 4)	11	17.1%
policy-violation (ID: 5)	1	1.56%

Source Details > Aanval Console

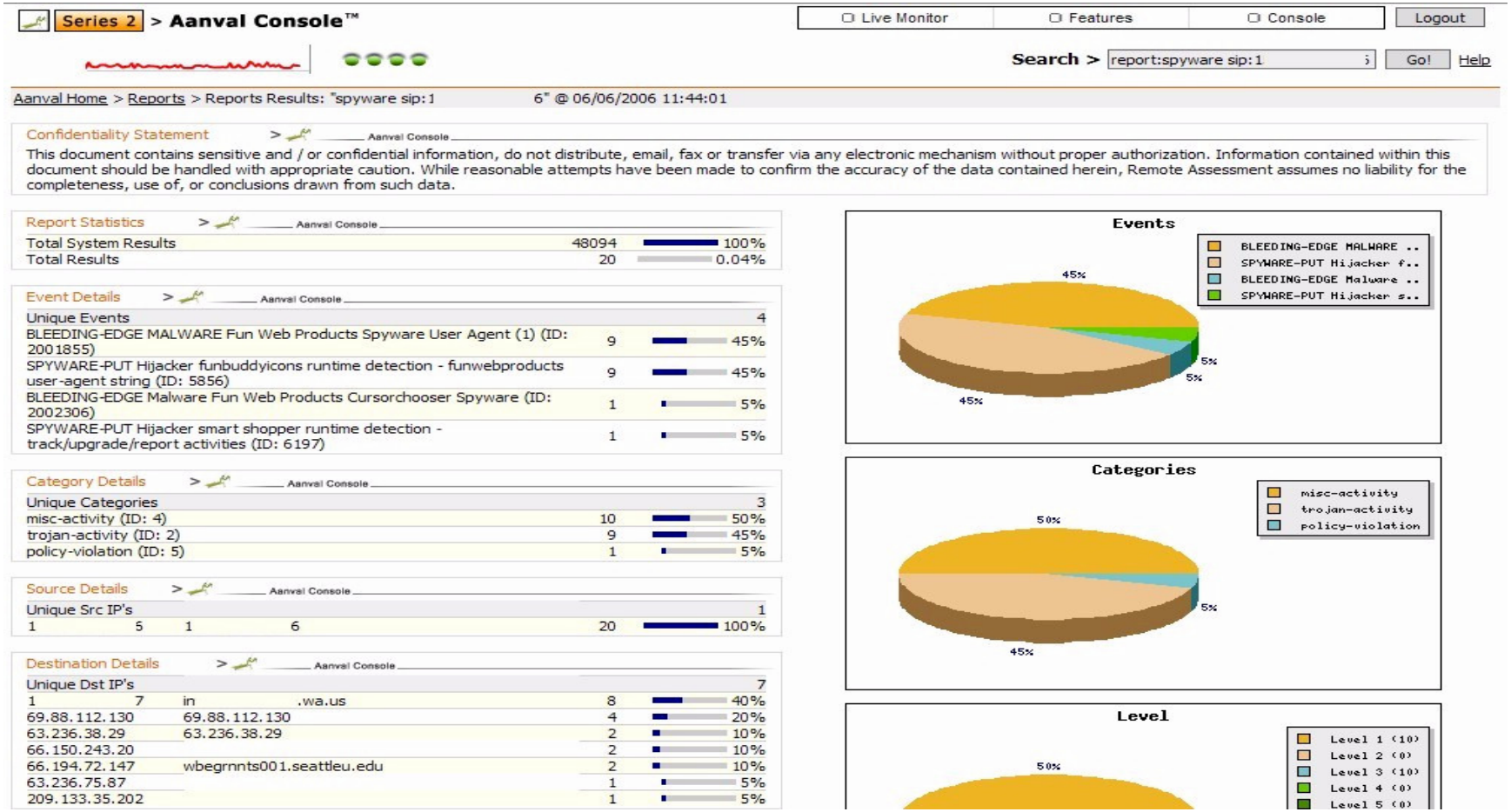
Unique Src IP's			26
1 6	1 6	20	31.2%
64.246.58.98	a062.casalemedia.com	4	6.25%
216.127.74.45	a120.casalemedia.com	3	4.68%
64.246.62.92	a066.casalemedia.com	3	4.68%
1	1	2	3.12%
207.44.242.8	a073.casalemedia.com	2	3.12%
66.98.130.81	a053.casalemedia.com	2	3.12%
66.98.132.8	a067.casalemedia.com	2	3.12%



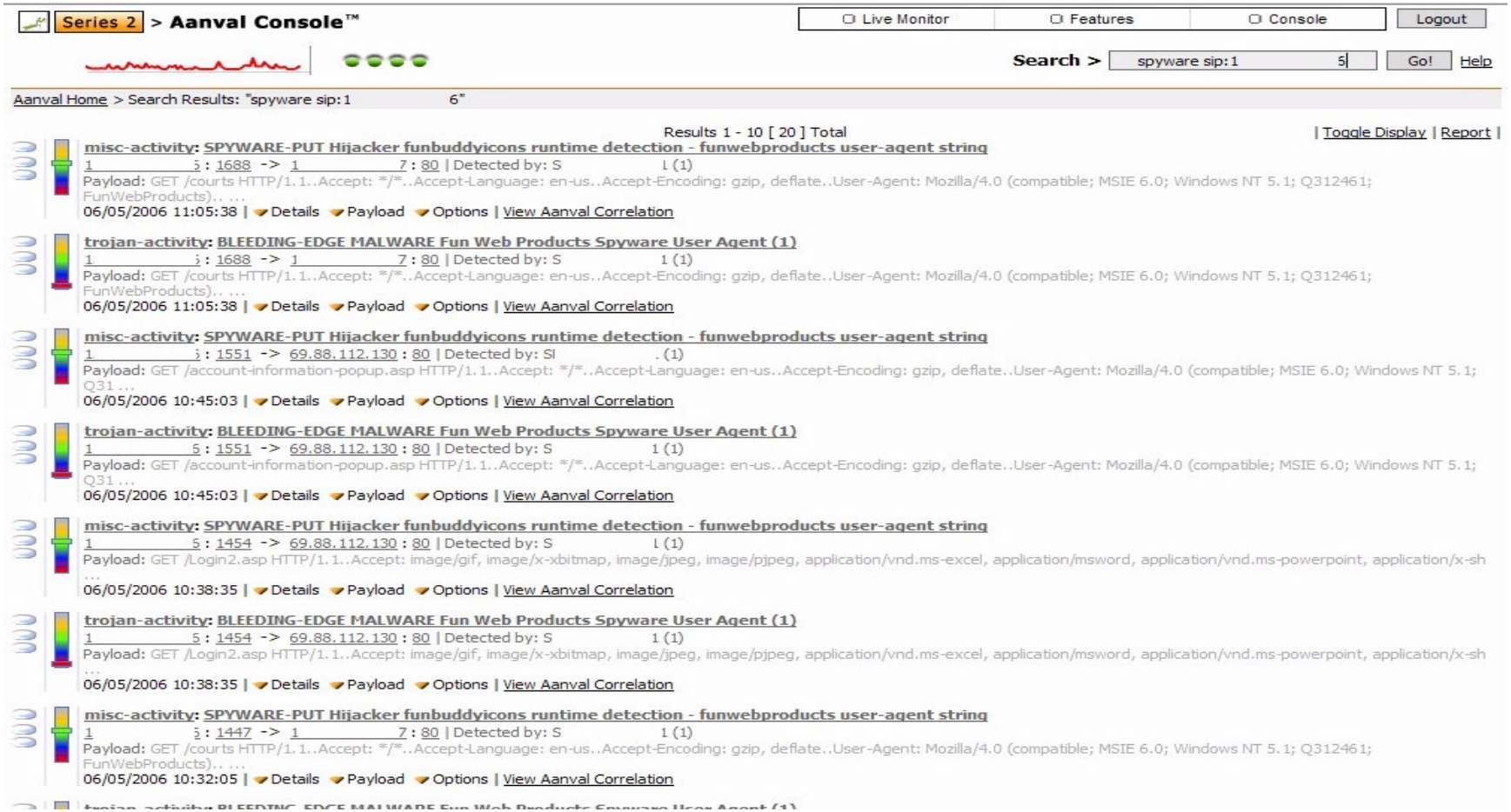




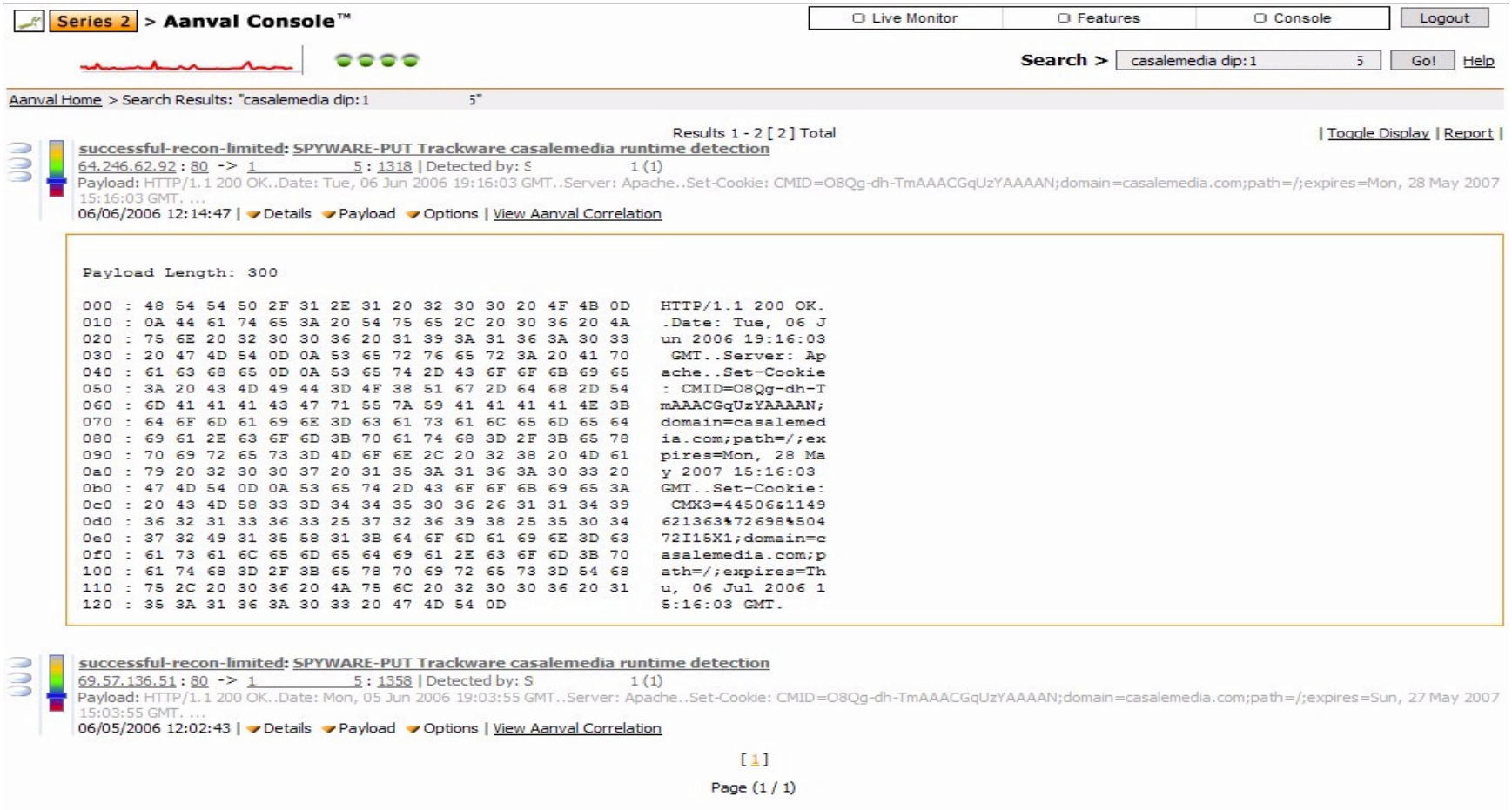
Spyware & SIP


Series 2 > Aanval Console™
Live Monitor
Features
Console
Logout
Search > report:spyware sip:1
Go!
Help
Aanval Home > Reports > Reports Results: "spyware sip:1 6" @ 06/06/2006 11:44:01
Confidentiality Statement
This document contains sensitive and / or confidential information, do not distribute, email, fax or transfer via any electronic mechanism without proper authorization. Information contained within this document should be handled with appropriate caution. While reasonable attempts have been made to confirm the accuracy of the data contained herein, Remote Assessment assumes no liability for the completeness, use of, or conclusions drawn from such data.
Report Statistics
Total System Results 48094 100%
Total Results 20 0.04%
Event Details
Unique Events 4
BLEEDING-EDGE MALWARE Fun Web Products Spyware User Agent (1) (ID: 2001855) 9 45%
SPYWARE-PUT Hijacker funbuddyicons runtime detection - funwebproducts user-agent string (ID: 5856) 9 45%
BLEEDING-EDGE Malware Fun Web Products Cursorchooser Spyware (ID: 2002306) 1 5%
SPYWARE-PUT Hijacker smart shopper runtime detection - track/upgrade/report activities (ID: 6197) 1 5%
Category Details
Unique Categories 3
misc-activity (ID: 4) 10 50%
trojan-activity (ID: 2) 9 45%
policy-violation (ID: 5) 1 5%
Source Details
Unique Src IP's 1
1 5 1 6 20 100%
Destination Details
Unique Dst IP's 7
1 7 in .wa.us 8 40%
69.88.112.130 69.88.112.130 4 20%
63.236.38.29 63.236.38.29 2 10%
66.150.243.20 2 10%
66.194.72.147 wbegrnnts001.seattleu.edu 2 10%
63.236.75.87 1 5%
209.133.35.202 1 5%
Events
BLEEDING-EDGE MALWARE ..
SPYWARE-PUT Hijacker f..
BLEEDING-EDGE Malware ..
SPYWARE-PUT Hijacker s..
45%
45%
5%
5%
Categories
misc-activity
trojan-activity
policy-violation
50%
45%
5%
Level
Level 1 (10)
Level 2 (0)
Level 3 (10)
Level 4 (0)
Level 5 (0)
50%

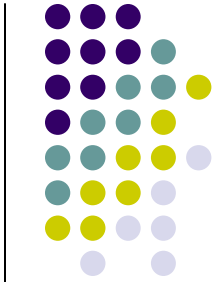
Event View - Spyware & SIP



Spyware & DIP - payload



The rule that catches it…

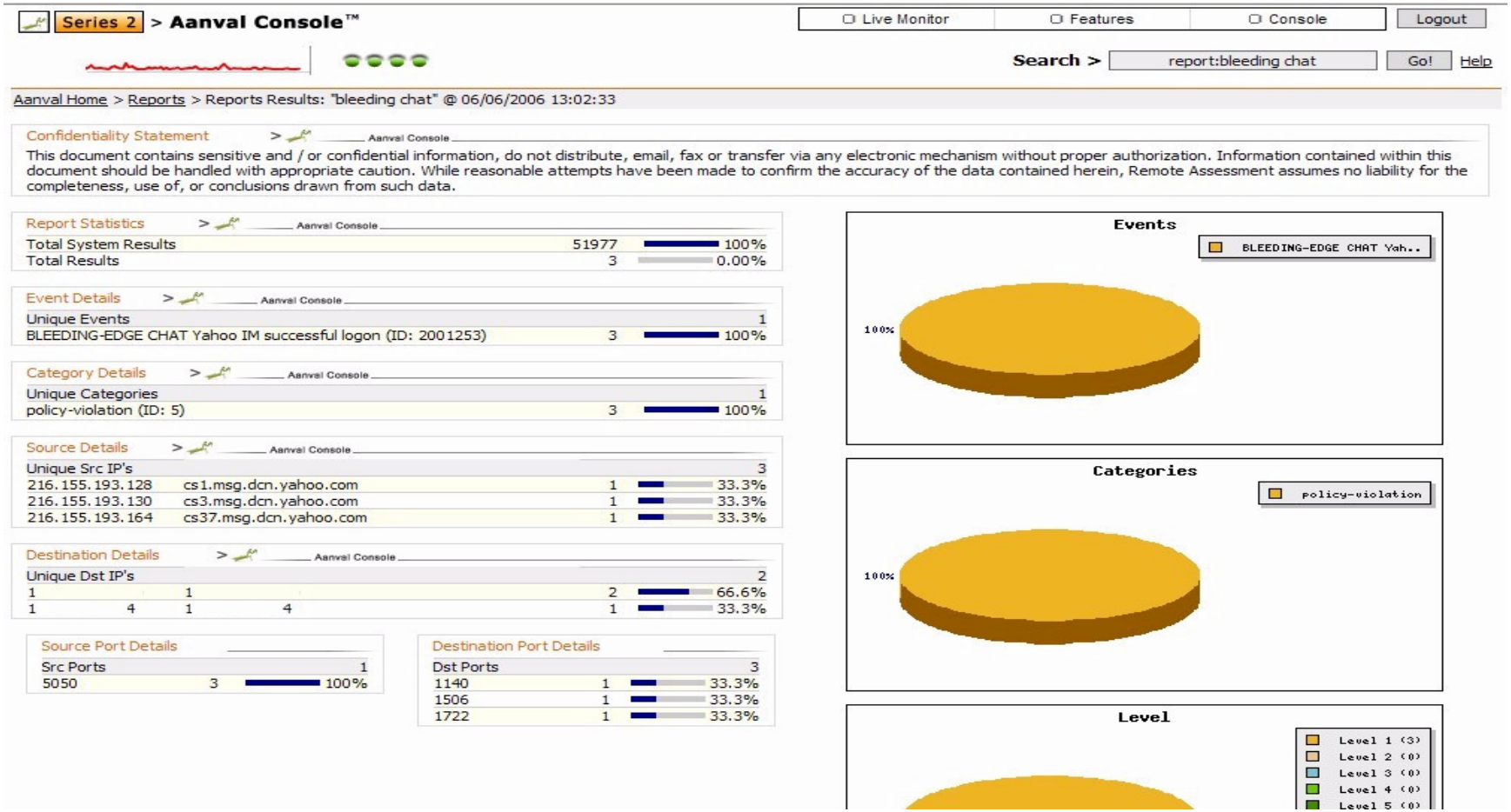


- alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "BLEEDING-EDGE MALWARE 180solutions Spyware (tracked event reported)"; flow: to_server,established; uricontent:"/TrackedEvent.aspx?"; nocase; uricontent:"eid="; nocase; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; classtype: trojan-activity; sid: 2001397; rev:6;)

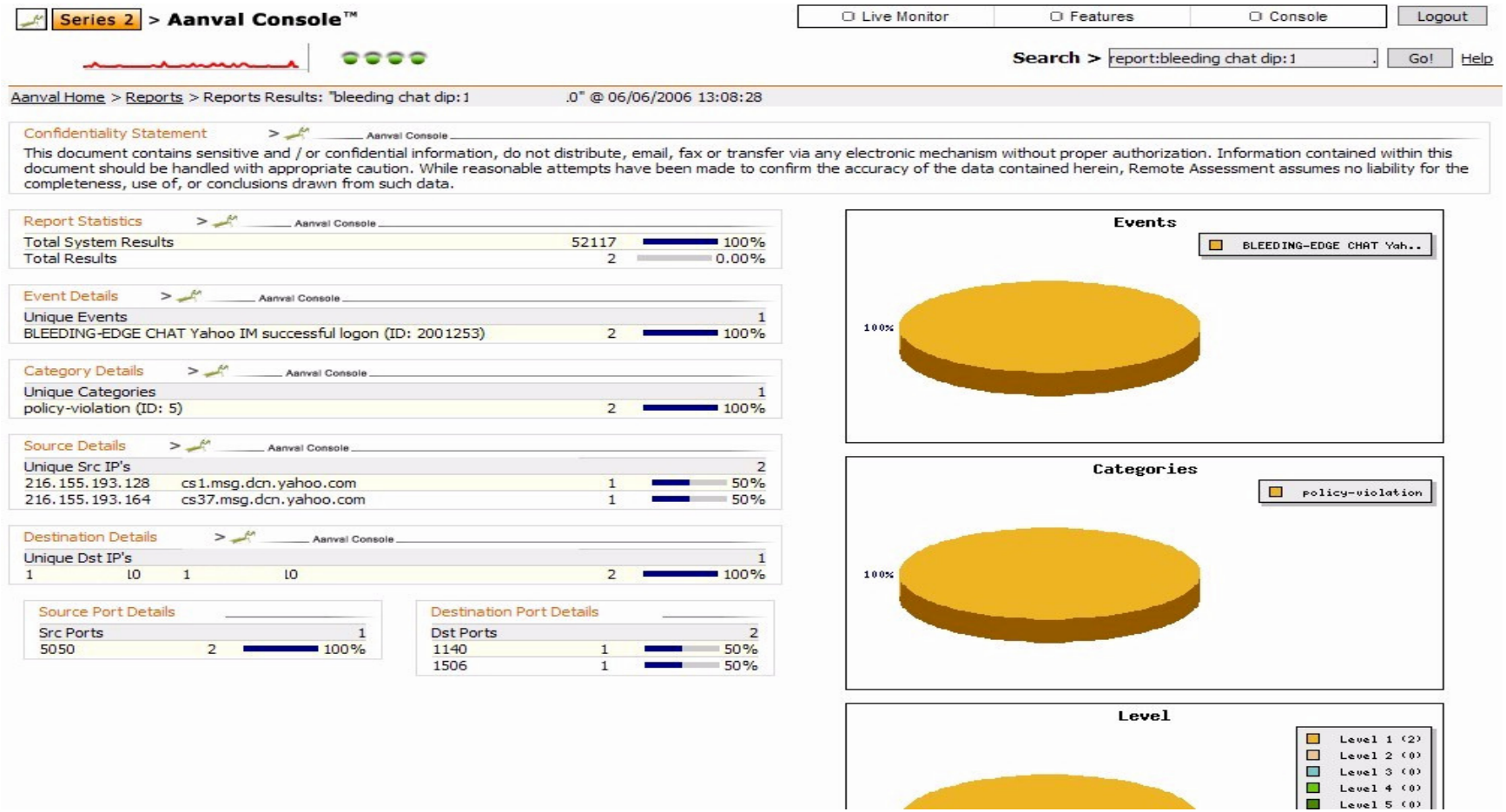
…is simple but effective

- Trolling for specific URI content to catch outbound calls to 180solutions
  - uricontent:"/TrackedEvent.aspx?"; nocase; uricontent:"eid="; nocase;

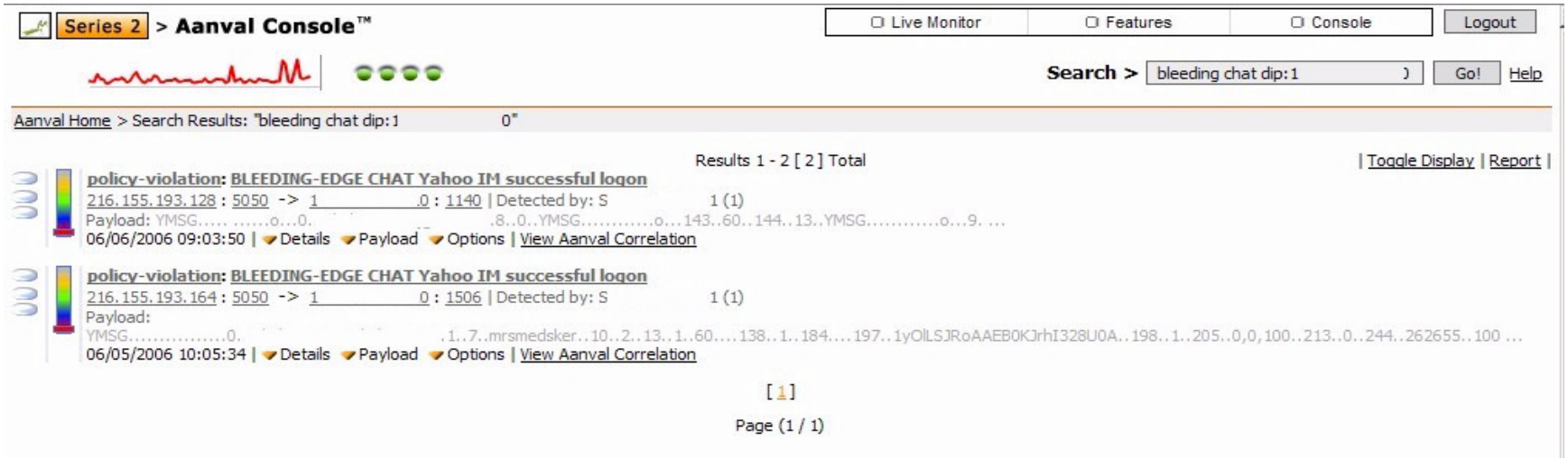
Specific queries: IM



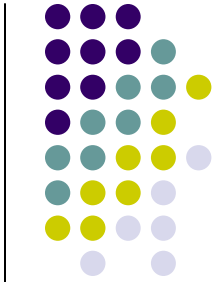
IM & DIP


Series 2 > Aanval Console™
Live Monitor
Features
Console
Logout
Search > report:bleeding chat dip:1
Go!
Help
Aanval Home > Reports > Reports Results: "bleeding chat dip:1 .0" @ 06/06/2006 13:08:28
Confidentiality Statement
Aanval Console
This document contains sensitive and / or confidential information, do not distribute, email, fax or transfer via any electronic mechanism without proper authorization. Information contained within this document should be handled with appropriate caution. While reasonable attempts have been made to confirm the accuracy of the data contained herein, Remote Assessment assumes no liability for the completeness, use of, or conclusions drawn from such data.
Report Statistics
Total System Results 52117 100%
Total Results 2 0.00%
Event Details
Unique Events 1
BLEEDING-EDGE CHAT Yahoo IM successful logon (ID: 2001253) 2 100%
Category Details
Unique Categories 1
policy-violation (ID: 5) 2 100%
Source Details
Unique Src IP's 2
216.155.193.128 cs1.msg.dcn.yahoo.com 1 50%
216.155.193.164 cs37.msg.dcn.yahoo.com 1 50%
Destination Details
Unique Dst IP's 1
1 l0 1 l0 2 100%
Source Port Details
Src Ports 1
5050 2 100%
Destination Port Details
Dst Ports 2
1140 1 50%
1506 1 50%
Events
BLEEDING-EDGE CHAT Yah..
100%
Categories
policy-violation
100%
Level
Level 1 (2)
Level 2 (0)
Level 3 (0)
Level 4 (0)
Level 5 (0)

Event View - IM & DIP

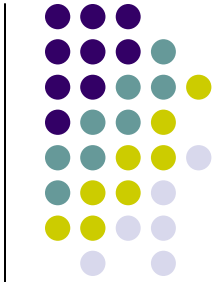


The rule that catches it…



- alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg: "BLEEDING-EDGE CHAT Yahoo IM successful logon"; flow: from_server,established; content:"YMSG"; nocase; depth: 4; content:"|00 01|"; offset: 10; depth: 2; classtype: policy-violation; sid: 2001253; rev:3;)

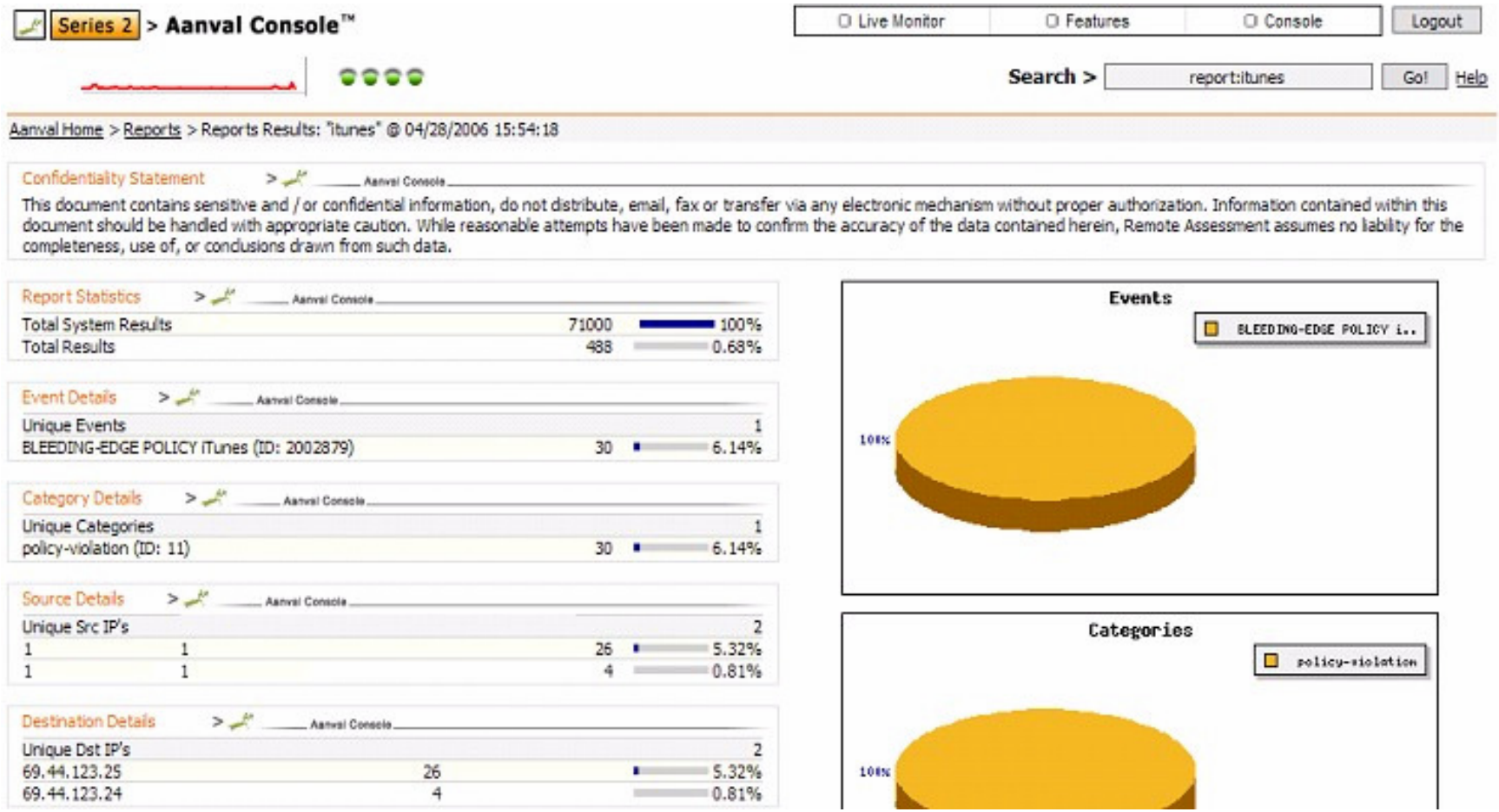
…is more complicated



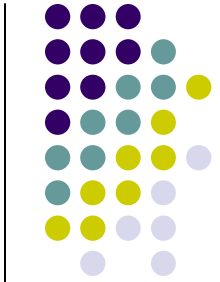
- content:"YMSG"; nocase; depth: 4; content:"|00 01|"; offset: 10; depth: 2;
  - *offset* is a content rule option modifier. In this case the offset is 10 bytes deep into the payload to avoid searching too early where relevant content may never be found.
  - *depth* is also a content rule option modifier. To quote Martin Roesch, “It is useful for limiting the pattern match function from performing inefficient searches once the possible search region for a given set of content has been exceeded.” So, *offset* protects the rule from firing too early, and *depth* too late. These are excellent efficiency options.
  - *content:"|00 01|";* allows the rule to capture specific bytecode good for describing complex binary data as hexadecimal numbers. *
  - This rule tightens the search to guarantee an accurate result when a user logs on to Yahoo Messenger.

* Writing Snort Rules, How To Write Snort Rules and keep your sanity, Martin Roesch, pg 7

Specific queries: Policy (iTunes)

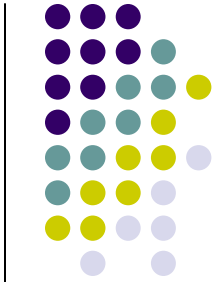


The rule that catches it…



- alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"BLEEDING-EDGE POLICY iTunes User Agent"; flow: established,to_server; content:"User-Agent\: "; nocase; pcre:"/User-Agent\:[^\n]+iTunes/i"; reference:url,hcsoftware.sourceforge.net/jason-rohrer/itms4all/; classtype:policy-violation; threshold: type limit, count 1, seconds 360, track by_src; sid:2002878; rev:2;)

…is straightforward

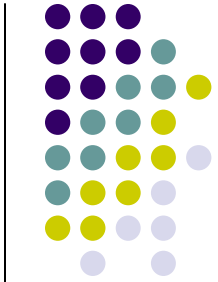


alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"BLEEDING-EDGE POLICY iTunes User Agent"; flow: established,to_server; content:"User-Agent\: "; nocase; pcre:"/User-Agent\:[^\n]+iTunes/i";

Looking for outbound traffic to iTunes over known http ports, using the User Agent IP addresses via http

- Also use pcre: Perl compatible regular expressions

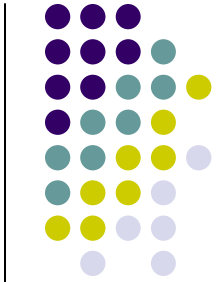
Catching leaking content



- NPI Snort Rules http://www.kgb.to/
  - Intended to detect sensitive information leaving your environment, including:

    US Government Data Classifications - Top Secret, NOFORN, COMINT, PROPIN, etc.
    HIPAA related - HCPCS, ICD-10, AMA CPT and other codes.
    GLBA related - Social Security and Credit Card numbers, etc.
    Other terms that indicate sensitive material - "password", "law enforcement sensitive", etc.

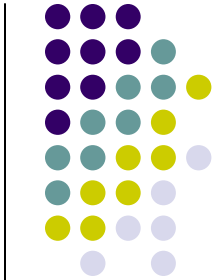
Catching leaking content



- Aanval search *report:ssn* would utilize the following NPI rules

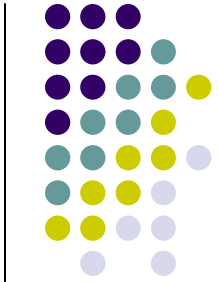
  - alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"NPI - SMTP SSN"; flow:to_server,established; pcre:"/(HELO|EHLO)\s.*\Ws(ocial\s)?s(ecurity\s)?(n(umber)?|#)\W.{0,20}[1-6][0-9]{2}[-]?[0-9]{2}[-]?[0-9]{4}\W.*\r\n\.\r\n/ism"; classtype:policy-violation;)
  - alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"NPI - HTTP SSN"; flow:to_server,established; pcre:"/\Ws(ocial\s)?s(ecurity\s)?(n(umber)?|#)\W.{0,20}[1-6][0-9]{2}[-]?[0-9]{2}[-]?[0-9]{4}\W/ism"; classtype:policy-violation;)
  - alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"NPI - High Ports SSN"; flow:to_server,established; pcre:"/\Ws(ocial\s)?s(ecurity\s)?(n(umber)?|#)\W.{0,20}[1-6][0-9]{2}[-]?[0-9]{2}[-]?[0-9]{4}/ism"; classtype:policy-violation;)

Conclusion



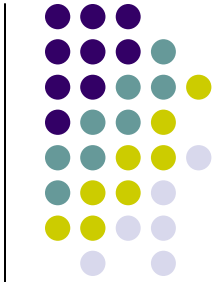
- Computer security and compliance is an endless task
- The first line of defense is to monitor your systems
- Being proactive in security and compliance is invaluable
- No matter what you do to improve security, it will not work if you're not informed
- Of all the opportunities to improve security and privacy in your infrastructure, monitoring outbound traffic will tell you the most about internal threats
- Aanval & Bleeding Edge Threats cost little or nothing, with an extraordinary return on investment

References:



- Ming Chow
  - Tufts University
  - *What Is Outstanding In Your Security and Compliance Practice?*
- Elizabeth Faultersack
  - Idaho National Engineering and Environmental Laboratory
  - *Understanding and Writing Snort Signatures*
- Martin Roesch
  - Sourcefire
  - *Writing Snort Rules, How To Write Snort Rules and keep your sanity*
- Jay Beale, *Snort Intrusion Detection*, Syngress
- Aanval Feature Summary, www.aanval.com, Remote Assessment

Snort Users Group



- Tuesday, October 17
  - South Seattle Community College
  - See James Affeld's excellent paper on writing Snort rules at holisticinfosec.org/howto.htm
  - Meeting details at snort.org

Questions?