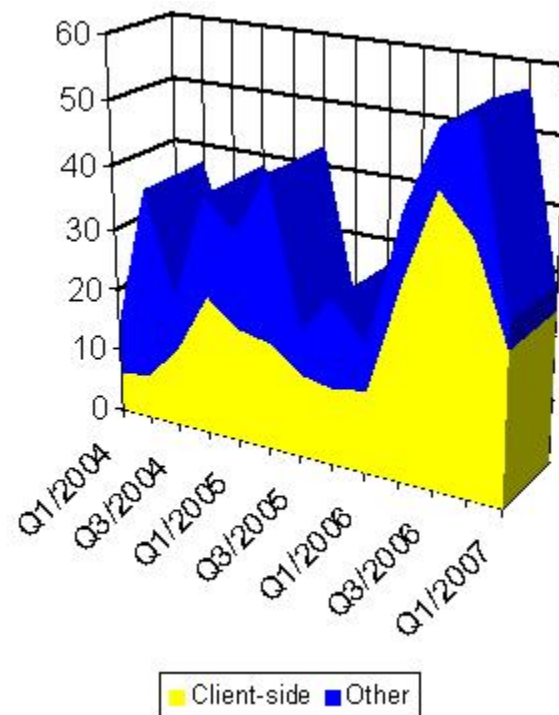






Vulnerability Landscape

- In 2006 the patches for client-side vulnerabilities overcame other categories in Microsoft software.
- In 2010, Symantec's *Global Internet Security Threat Report* indicated that over 93% vulnerabilities exploited worldwide are now client-side



Source: <http://www.symantec.com>



Protecting the Client

- Client-side attacks have special properties compared to traditional server-side attacks
 - ▶ Extremely complex structures for document formats
 - ▶ Embedding of interpreters and scripting languages
 - ▶ Embedding of arbitrary formats within other container formats
 - ▶ Obfuscation techniques
 - ▶ Multiple delivery channels for the same vulnerability



Network Intrusion Prevention Systems

- Intrusion prevention platforms are evaluated by market analysis firms according to two criteria
 - ▶ Throughput
 - ▶ Coverage
- A key term in modern IPS is deep packet inspection but implementation is practically limited by the main two evaluation criteria
- A supplemental system is required to defend against client side attacks



Razorback Framework

- Razorback is a distributed data collection and analysis framework
- Modular architecture allows for collection and analysis modules to be distributed over a network in arbitrary configurations
 - ▶ Retrieval of data over the wire or from server software after delivery
 - ▶ Analysis of complex file formats distributed over a server farm

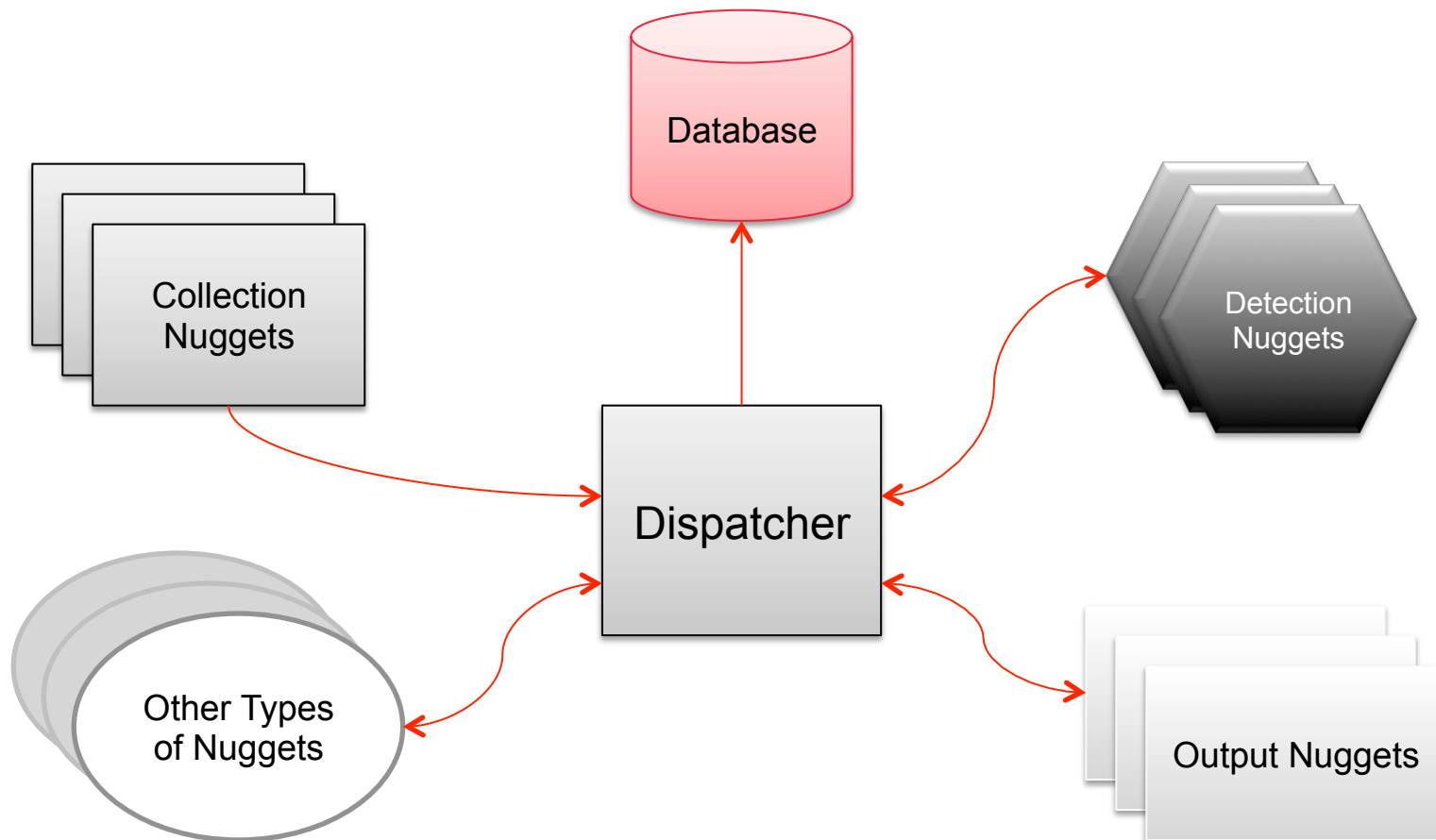


Razorback Framework

- A collection of elements working together
- Each element performs a discrete task
- Elements are tied together via the Dispatcher
- Nugget types:
 - Data Collection
 - Data Detection/Analysis
 - Output
 - Intelligence
 - Correlation
 - Defense Update
 - Workstation



Razorback Framework Architecture





Database

- Configuration information
- Event information
- Contextual information
- Metadata
- Provides a wealth of information for correlating events and activities



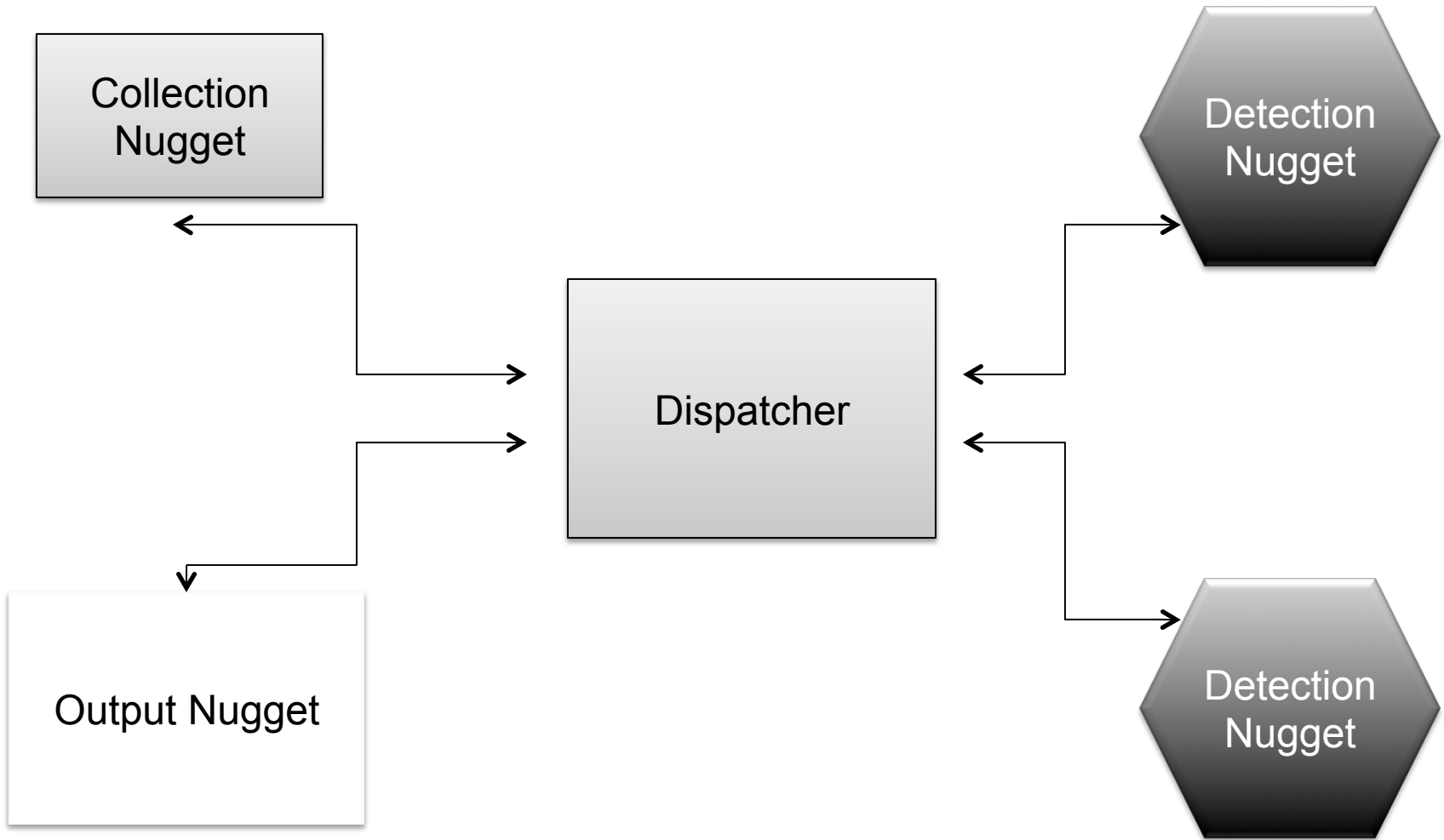
Nuggets

- Dispatcher Registration
 - ▶ Types of data handled
 - ▶ Types of output generated

- UUIDs
 - ▶ Identifier of nuggets
 - ▶ Type of nugget
 - ▶ Types of data handled and/or provided
 - ▶ Allows for easy addition and removal of elements



Nugget Registration





Collection Nugget

- Capture data
 - ▶ From the network
 - ▶ From a network device directly
 - ▶ From log files
- Contact dispatcher for handling
 - ▶ Has this data been evaluated before?
 - ▶ Send the data to the Dispatcher



Collection Nuggets

- Snort-as-a-Collector (SaaC)
 - ▶ SMTP mail stream capture
 - ▶ Web capture
 - ▶ DNS capture

- Custom post-mortem debugger
 - ▶ Traps applications as they crash
 - ▶ Sends the file that triggered the crash to Dispatcher
 - ▶ Sends the metadata of the crash to the Dispatcher



Detection Nugget

- Handles incoming data from Collection Nuggets
- Splits incoming data into logical sub-blocks
 - Requests additional processing of sub-blocks
- Provides alerting feedback to the Dispatcher



Detection Nuggets

- Zynamics PDF Dissector
 - ▶ Deobfuscation and normalization of objects
 - ▶ Target known JavaScript attacks
- JavaScript Analyzer (w/ Zynamics)
 - ▶ Search for shellcode in unescaped blocks
 - ▶ Look for heap spray
 - ▶ Look for obvious obfuscation possibilities



Detection Nuggets

- Shellcode Analyzer (w/ libemu)
 - ▶ Detection and execution of shellcode
 - ▶ Look for code blocks that unwrap shellcode
 - ▶ Win32 api hooking
 - Determine the function call
 - Capture the arguments
 - ▶ Provide alerts that include shellcode action

libemu.carnivore.it



Detection Nuggets

- Office Cat Nugget
 - ▶ Full Office file parsing
 - ▶ Vuln-centric detection against known threats
- SWF Nugget
 - ▶ Decompresses and analyzes flash
 - ▶ Detects known flash threats



Detection Nuggets

- ClamAV Nugget
 - ▶ Analyze any format
 - ▶ Signature- and pattern-based detection
 - ▶ Updatable signature DB
 - ▶ Can further serve as a collector
 - ▶ Can issue defense updates



Output Nugget

- Receives alert notification from Dispatcher
- If alert is of a handled type, additional information is requested:
 - ▶ Short Data
 - ▶ Long Data
 - ▶ Complete Data Block
 - ▶ Normalized Data Block
- Sends output data to relevant system



Output Nuggets

- Deep Alerting System
 - ▶ Provide full logging output of all alerts
 - ▶ Write out each component block
 - ▶ Include normalized view of documents as well
- Maltego Interface
 - ▶ Provide data transformations targeting the Razorback database

www.paterva.com



Analysis Nuggets

- Intelligence Nugget
 - ▶ Generate metadata for correlation
- Correlation Nugget
 - ▶ Compare results of various intelligence nuggets



Defense Update Nugget

- Receives update instructions from dispatcher
- Performs dynamic updates of network device(s)
- Update multiple devices
- Update multiple devices of different types!
- Notifies dispatcher of defense update actions

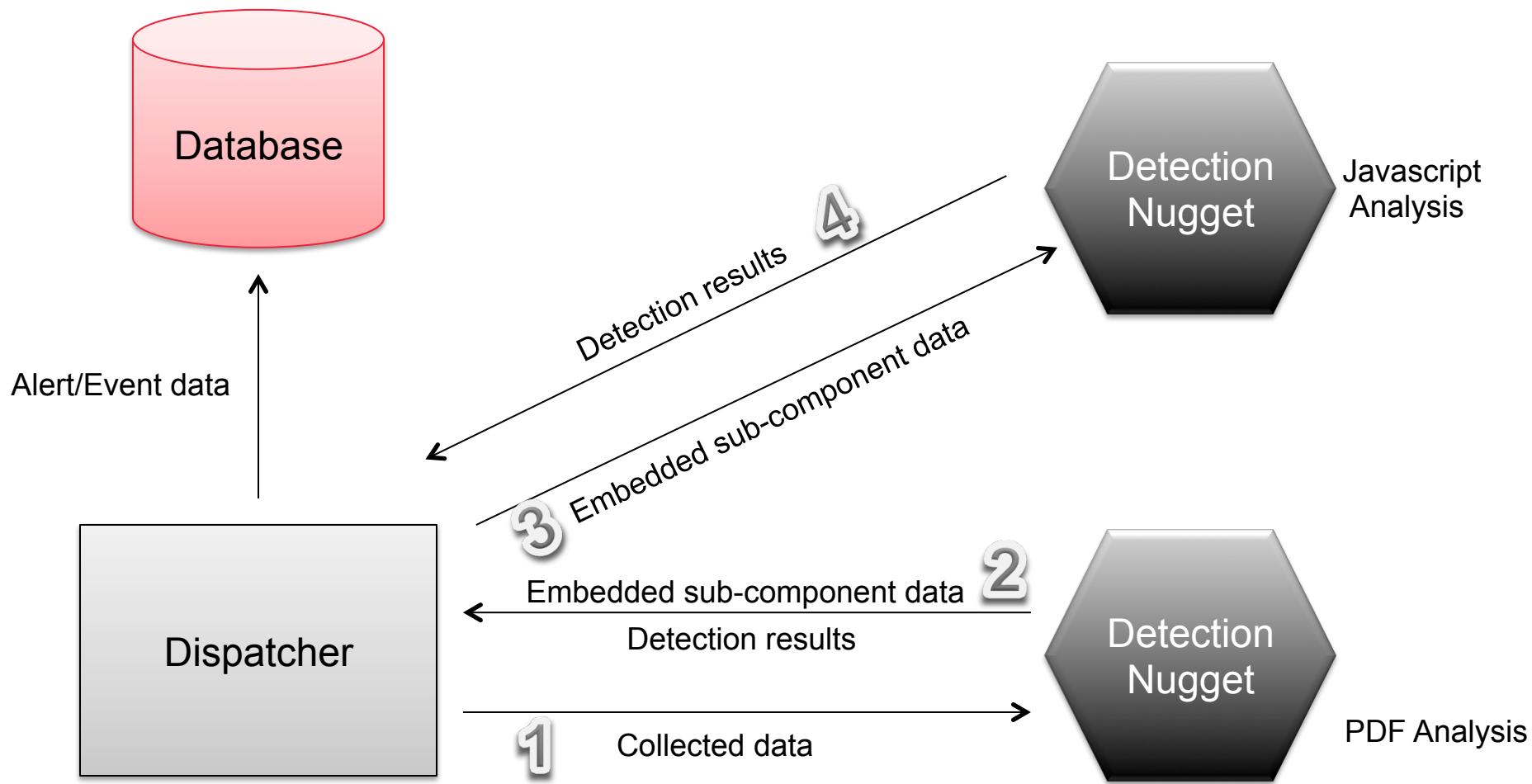


Workstation Nugget

- Authenticates on a per-analyst basis
- Provides analyst with ability to:
 - ▶ Manage nugget components
 - ▶ Manage alerts and events
 - Consolidate events
 - Add custom notes
 - Set review flags
 - Delete events
 - ▶ Review system logs



Dispatcher Operation





DEMO



System Status

Name	Status
MySQL	✘
memcached	✘
ActiveMQ	✘
Razorback Dispatcher	✔
Razorback masterNugget (restart)	✔

Nugget Status

Nugget	Status
Archive Inflate Sample	✔
ClamAV Sample	✔
SWF Scanner Sample	✔
OfficeCat Sample	✔
Sample PDF Dissector nugget	✔
Yara Sample	✔
Master Nugget Sample	✔
File Inject Sample	✘

Routing Table

Data type	App type
ANY_DATA	YARA
ANY_DATA	CLAMAV
PDF_FILE	PDF_DISSECTOR
OLE_FILE	OFFICECAT
FLASH_FILE	FLASH_INSPECTOR
BZ2_FILE	ARCHIVE_INFLATE
GZIP_FILE	ARCHIVE_INFLATE
COMPRESSION_FILE	ARCHIVE_INFLATE
LZMA_FILE	ARCHIVE_INFLATE
XZ_FILE	ARCHIVE_INFLATE
AR_FILE	ARCHIVE_INFLATE
TAR_FILE	ARCHIVE_INFLATE
ZIP_FILE	ARCHIVE_INFLATE
CPIO_FILE	ARCHIVE_INFLATE
ISO9660_FILE	ARCHIVE_INFLATE

Routing Statistics

Routing Table



Nugget Status

Nugget	Status
Archive Inflate Sample	✓
ClamAV Sample	✓
SWF Scanner Sample	✓
OfficeCat Sample	✓
Sample PDF Dissector nugget	✓
Yara Sample	✓
Master Nugget Sample	✓
File Inject Sample	✗



Routing Table

Data type	App type
ANY_DATA	YARA
ANY_DATA	CLAMAV
PDF_FILE	PDF_DISSECTOR
OLE_FILE	OFFICECAT
FLASH_FILE	FLASH_INSPECTOR
BZ2_FILE	ARCHIVE_INFLATE
GZIP_FILE	ARCHIVE_INFLATE
COMPRESSION_FILE	ARCHIVE_INFLATE
LZMA_FILE	ARCHIVE_INFLATE
XZ_FILE	ARCHIVE_INFLATE
AR_FILE	ARCHIVE_INFLATE
TAR_FILE	ARCHIVE_INFLATE
ZIP_FILE	ARCHIVE_INFLATE
CPIO_FILE	ARCHIVE_INFLATE
ISO9660_FILE	ARCHIVE_INFLATE

Objects

- [gzip] 42a1e05-40288
- [pe] 19b0dd9-80946

19b0dd94019a2ca4a978b61b8dfb7548fe0063394c932f06b73b0784a97e409f

Size: 80946 Status: Bad
Data Type: PE Executable Sub Blocks: 0
Sourcefire Flags: 0x00000002 Enterprise Flags: 0x00000000
[Download](#) [Delete](#)

Alerts

Priority	Inspector	Message	Metadata
1	ClamAV Scanner	ClamAV Found: Trojan.Agent-145905	1
X			
Name	Metadata		
Name of detected malware	ClamAV:Trojan.Agent-145905		
1	Yara Integrated Detection Nugget	Yara signature detected: Armadillo	0

Events

Created	Nugget	Metadata
08/31/2011 14:45:59	Archive Inflate Sample	1

Known Filenames

Name	Metadata
File Name	data

Malware Names

Name	Metadata
Name of detected malware	ClamAV:Trojan.Agent-145905

Detection Engines

App type	Nugget name	Status
Yara Integrated Detection Nugget	Yara Sample	Done





e51ba80f267e8fc9bb634ce1561c022e0c9efaa42d3cf3515d6fa1bad18df754

Size: 92

Data Type: Adobe Flash

Sourcefire Flags: 0x00000002

[Download](#)

Status: Bad

Sub Blocks: 0

Enterprise Flags: 0x00000000

[Delete](#)

Alerts

Priority	Inspector	Message	Metadata
1	Flash Inspector	Macromedia Flash ActionDefineFunction Memory Access Vulnerability	2

Name	Metadata
CVE	CVE-2005-2628
Bugtraq ID	BID-15334

Events

Created	Nugget	Metadata
09/01/2011 15:54:53	File Inject Sample	1

Known Filenames

Name	Metadata
File Name	/tmp/CVE-2005-2628.swf

Detection Engines

App type	Nugget name	Status
Yara Integrated Detection Nugget	Yara Sample	Done
ClamAV Scanner	ClamAV Sample	Done
Flash Inspector	SWF Scanner Sample	Done



Contact

- Richard Johnson
 - ▶ rjohnson@sourcefire.com
 - ▶ [@richinseattle](#)
 - ▶ <http://rjohnson.uninformed.org>
- Sourcefire VRT
 - ▶ labs.snort.org
 - ▶ vrt-sourcefire.blogspot.com
 - ▶ [@VRT_Sourcefire](#)

Razorback Team:

Alex Kambis
Alex Kirk
Alain Zidouemba
Christopher McBee
Kevin Miklavcic
Lurene Grenier
Matt Olney
Matt Watchinski
Nigel Houghton
Patrick Mullen
Ryan Pentney
Sojeong Hong