

COLLECT ALL

THE THING^S

from other computers!

Directed by **GREG CASTLE**
Blackhat 2014

COLLECT ALL

THE THING^S

from other computers!

Directed by **GREG CASTLE**
Blackhat 2014

COLLECT ALL

THE THING^S

from other computers!

Directed by **GREG CASTLE**
Blackhat 2014

COLLECT ALL

THE THING^S

from other computers!

Directed by **GREG CASTLE**
Blackhat 2014

COLLECT ALL

THE THING^S

from other computers!

Directed by **GREG CASTLE**
Blackhat 2014

Who am I

GRR Developer, Google IR team

OS X Security

Former lives: pentesting, IR, security audits etc.

Live forensics

GET /beacon HTTP/1.1

Host: evil.com

from Joe's machine



Joe 



GET /beacon HTTP/1.1

Host: evil.com

Joe is on vacation with 3G internet



**New malware report
BEAR EAGLE SHARK
LASER is out: check all
the things**



New malware report BEAR EAGLE SHARK LASER is out: check all the things

50+ IOCs for Win/Mac and “all the things” is
the machines of a highly mobile global
organisation with 50k+ employees

GRR: GRR Rapid Response



Open source live forensics
Scalable



Raw memory, raw disk
Stable, low-impact client
2-party authorization workflow
Hunting, binary collection
much more....





GET /beacon HTTP/1.1
Host: evil.com

Joe is on vacation with 3G internet

**SANS: “a combination of
description, location, and
interpretation”**

I prefer

“that stuff I want”

Chrom(e)ium), Firefox, IE, Safari: 3 OSes

%%users.localappdata%%\Google\Chrome\User Data*Archived History
%%users.localappdata%%\Google\Chrome\User Data*History
%%users.localappdata%%\Chromium\User Data*Archived History
%%users.localappdata%%\Chromium\User Data*History
%%users.homedir%%\Library\Application Support\Google\Chrome*/Archived History
%%users.homedir%%\Library\Application Support\Google\Chrome*/History
%%users.homedir%%\Library\Application Support\Chromium*/Archived History
%%users.homedir%%\Library\Application Support\Chromium*/History
%%users.homedir%%\config\google-chrome*/Archived History
%%users.homedir%%\config\google-chrome*/History
%%users.homedir%%\config\chromium*/Archived History
%%users.homedir%%\config\chromium*/History
%%users.localappdata%%\Mozilla\Firefox\Profiles*\places.sqlite
%%users.appdata%%\Mozilla\Firefox\Profiles*\places.sqlite
%%users.homedir%%\Library\Application Support\Firefox\Profiles*\places.sqlite
%%users.homedir%%\mozilla/firefox*/places.sqlite

%%users.localappdata%%\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
%%users.localappdata%%\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat
%%users.localappdata%%\Microsoft\Microsoft\Windows\History\History.IE5\index.dat
%%users.localappdata%%\Microsoft\Microsoft\Windows\History\Low\History.IE5\index.dat
%%users.localappdata%%\Microsoft\Microsoft\Windows\History\History.IE5*\index.dat
%%users.localappdata%%\Microsoft\Microsoft\Windows\History\Low\History.IE5*\index.dat
%%users.localappdata%%\Microsoft\Feeds Cache\index.dat
%%users.appdata%%\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat
%%users.localappdata%%\Microsoft\Windows\WebCache\WebCacheV*.dat
%%users.localappdata%%\Apple Computer\Safari\History.plist
%%users.appdata%%\Roaming\Apple Computer\Safari\History.plist
%%users.homedir%%\Library\Safari\History.plist

add in browser cache locations = 67 paths

%%users.localappdata%%\Google\Chrome\User Data*Application Cache\Cache\
%%users.localappdata%%\Google\Chrome\User Data*Cache\
%%users.localappdata%%\Google\Chrome\User Data*Media Cache\
%%users.localappdata%%\Google\Chrome\User Data*GPUCache\
%%users.localappdata%%\Chromium\User Data*Application Cache\Cache\
%%users.localappdata%%\Chromium\User Data*Cache\
%%users.localappdata%%\Chromium\User Data*Media Cache\
%%users.localappdata%%\Chromium\User Data*GPUCache\
%%users.homedir%%/Caches/Google/Chrome/*Cache/
%%users.homedir%%/Library/Caches/Google/Chrome/*Cache/
%%users.homedir%%/Library/Caches/Google/Chrome/*Media Cache/
%%users.homedir%%/Library/Application Support/Google/Chrome/*Application Cache/Cache/
%%users.homedir%%/Library/Application Support/Google/Chrome/*GPUCache/
%%users.homedir%%/Library/Caches/Google/Chrome/PnaclTranslationCache/
%%users.homedir%%/Caches/Chromium/*Cache/
%%users.homedir%%/Library/Caches/Chromium/*Cache/
%%users.homedir%%/Library/Caches/Chromium/*Media Cache/
%%users.homedir%%/Library/Application Support/Chromium/*Application Cache/Cache/
%%users.homedir%%/Library/Application Support/Chromium/*GPUCache/
%%users.homedir%%/Library/Caches/Chromium/PnaclTranslationCache/

%%users.homedir%%/.cache/google-chrome/*Cache/
%%users.homedir%%/.cache/google-chrome/*Media Cache/
%%users.homedir%%/.cache/google-chrome/PnaclTranslationCache/
%%users.homedir%%/.config/google-chrome/*Application Cache/
%%users.homedir%%/.config/google-chrome/*Cache/
%%users.homedir%%/.config/google-chrome/*Media Cache/
%%users.homedir%%/.config/google-chrome/*GPUCache/
%%users.homedir%%/.cache/chromium/*Cache/
%%users.homedir%%/.cache/chromium/*Media Cache/
%%users.homedir%%/.cache/chromium/PnaclTranslationCache/
%%users.homedir%%/.config/chromium/*Application Cache/
%%users.homedir%%/.config/chromium/*Cache/
%%users.homedir%%/.config/chromium/*Media Cache/
%%users.homedir%%/.config/chromium/*GPUCache/
%%users.localappdata%%\Microsoft\Windows\Temporary Internet Files\Content.IE5*
%%users.localappdata%%\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5*
%%users.localappdata%%\Apple Computer\Safari\cache.db
%%users.homedir%%/Library/Caches/com.apple.Safari/cache.db

What we think we do



What actually happens

The screenshot shows a Google search interface. The search bar contains the text "where are the launch daemons stored on os x". Below the search bar, there are tabs for "Web", "Videos", "News", "Shopping", "Images", "More", and "Search tools". The "Web" tab is selected. The search results show "About 151,000 results (0.34 seconds)". The first result is titled "Mac OS X: launch daemons vs launch agents | Krypted" with a green link to krypted.com/mac-security/mac-os-x-launch-daemons-vs-launch-agents/. The snippet mentions "Jul 20, 2008 - Mac OS X Server: Pushing Out Policies Using Open Directory · Brocade buying ... Launch daemon configuration plist files are stored in the ...". The second result is titled "Creating Launch Daemons and Agents - Apple Developer" with a green link to <https://developer.apple.com/.../mac/.../MacOSX/...>. The snippet says "If you are developing daemons to run on OS X, it is highly recommended that ... During check-in, get the launch dictionary from launchd, extract and store its ...". The third result is titled "launchd - Wikipedia, the free encyclopedia" with a green link to en.wikipedia.org/wiki/Launchd. The snippet states "For Mac OS X v10.4 (Tiger) Apple moved most of the processes handled by the ... Stored in the LaunchAgents and LaunchDaemons subdirectories of the Library ...". The fourth result is titled "osx - Stopping LaunchAgents and Daemons - Ask Different" with a green link to apple.stackexchange.com/questions/.../stopping-launchagents-and-daemo.... The snippet mentions "Jan 16, 2012 - The students have also added some plists as com.apple.myprog.run. ... is these are not present in the launchagents directory or in the launchdaemons directory. ... the point is I don't know where the plist has been stored."

Google

where are the launch daemons stored on os x

Web Videos News Shopping Images More Search tools

About 151,000 results (0.34 seconds)

Mac OS X: launch daemons vs launch agents | Krypted
krypted.com/mac-security/mac-os-x-launch-daemons-vs-launch-agents/
Jul 20, 2008 - **Mac OS X** Server: Pushing Out Policies Using Open Directory · Brocade buying ... **Launch daemon** configuration plist files are **stored** in the ...

Creating Launch Daemons and Agents - Apple Developer
<https://developer.apple.com/.../mac/.../MacOSX/...> Apple Developer Tools
If you are developing **daemons** to **run** on **OS X**, it is highly recommended that During check-in, get the **launch** dictionary from launchd, extract and **store** its ...

launchd - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Launchd Wikipedia
For **Mac OS X** v10.4 (Tiger) **Apple** moved most of the processes handled by the ... **Stored** in the LaunchAgents and **LaunchDaemons** subdirectories of the Library ...

osx - Stopping LaunchAgents and Daemons - Ask Different
apple.stackexchange.com/questions/.../stopping-launchagents-and-daemo...
Jan 16, 2012 - The students have also added some plists as com.apple.myprog.run. ... is these are not present in the launchagents directory or in the **launchdaemons** directory. ... the point is I don't know where the plist has been **stored**.

Not (easily) machine readable

[1 reply](#) to this topic

tlrook

Newest first

Posted 24 June 2009 - 01:08

where dose Internet Explorer 8 stores browsing history?

 member

★★★★★ verified
joined 23 February 08

Ad Bot (disabled when logged in)



Register to remove this

★★★★★★

Group: Treasury

Register: It's Free!




5 Unsung Tools of DevOps

Download Now



Yusuf M.



★★★★★ 20K

Tech Issues Solved: 1
Joined: 25-May-04
Location: Toronto, ON
OS: Windows 8.1 Pro
Phone: Nexus 5
(CyanoGenMod 11 M7)

Posted 24 June 2009 - 01:43

The browsing history itself is stored in Internet Explorer

Windows Vista:

Quote

`C:\Users\%username%\AppData\Local\Microsoft\Windows\Temp`

Windows XP:

Quote

`C:\Documents and Settings\%username%\Local Settings\Temp`

Computer Hope
Free computer help and information

Help Tips Dictionary

AdSense Dr
Migrate to 4th
Generation Xel
vPro Processors

LEARN MORE

You are here: [Help](#) > [Microsoft Windows](#) > [Registry](#)

How do I open and edit the Windows Registry

- ⚠ **Caution:** Before editing or changing anything in the Microsoft Windows Registry, we recommended that you [backup the Registry](#). We also highly recommend new to the registry become familiar with all the [Windows Registry basics](#).

To open the Windows Registry follow the steps below.

1. Click **Start**.
2. In the Start Menu either in the **Run Box** or **Search box** type **regedit** Enter.
3. If prompted by **User Account Control**, click **Yes** to open the Registry Editor.
4. Once opened successfully you should be in the **Windows Registry Editor**.

Tip: If you have restricted access to the Windows computer you're logged into you may not be able to access the Windows Registry.

ForensicArtifacts.com ARTIFACTS SUBMIT ABOUT
...the definitive database

Artifacts

[illegible]

Windows Prefetch File Format

A Windows Prefetch file consists of one file header and multiple file sections with different content. Not all content has an obvious forensic value

As far as have been possible to ascertain, there is no public description of the format. The description below has been synthesised from examination of multiple prefetch files

- Contents** [\[hide\]](#)
- 1 Characteristics
- 2 File header
 - 2.1 Format version
 - 2.2 File information
 - 2.2.1 File information - version 17
 - 2.2.2 File information - version 23
 - 2.2.3 File information - version 26
- 3 Section A - Metrics array
- 4 Section B - Trace chains array
- 5 Section C - Filename strings
- 6 Section D - Volumes information (block)
 - 6.1 Volume information
 - 6.1.1 Volume information - version 1
 - 6.1.2 Volume information - version 2
 - 6.1.3 Volume information - version 3
 - 6.2 Sub section E - NTFS file reference
 - 6.3 Sub section F - Directory strings
- 7 See Also
- 8 External Links

Characteristics

Integers	stored in little-endian
----------	-------------------------

Strings	Stored as UTF-16 little-endian without a byte-order-mark (BOM)
---------	---

Strings	Stored as UTF-16 in the database without
Timestamps	Stored as Windows FILETIME in UTC

File header

The file header is 84 bytes of size and consists of

Problems:
brain storage capacity,
format

a centralized, free, community sourced,
knowledge base of forensic artifacts that the
world can use both as an information source
and within other tools

**Didn't we build this
already?**



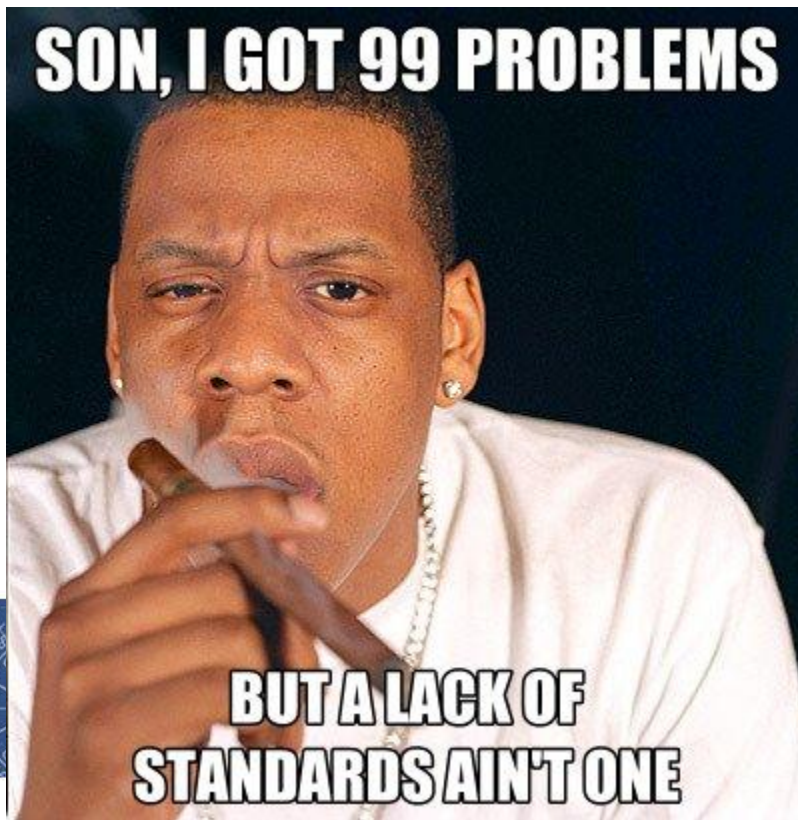
Veris

OpenIOC

An Open Framework for Sharing Threat Intelligence
Sophisticated Threats Require Sophisticated Indicators

Security Content Automation Protocol

SCAP



IDMEF



IOC vs artifact

IOC: If filename "temp.exe" contains string "evil" or is signed by "stolen cert" -> **you're owned**

Artifact: security event log is at

C:\Windows\System32\winevt\Logs\Security.evtx

As seen in the wild

HardDrive\Documents and Settings\USERNAME\Local Settings\Application Data\Google\Chrome\User Data\Default\History

HKU\S-1-5-21-xxxxxxxx-xxxxxxxx-xxxxxxxx-
xxxx\Software\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\InstallLocation

/Users/<user>/Library/Mail Downloads/

/home/user/.local/share/Trash/

What do I do with these?

HardDrive\Documents and Settings\USERNAME\Local
Settings\Application Data\Google\Chrome\User Data\Default\History

HKU\S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
xxxx\Software\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\InstallLoc
ation

/Users/<user>/Library/Mail Downloads/

/home/user/.local/share/Trash/

Common language for interpolation

%%users.localappdata%% \Google\Chrome\User Data*\History

HKEY_USERS**%%users.sid%%**
\Software\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\InstallLocation

%%users.homedir%% /Library/Mail Downloads/

%%users.homedir%% /.local/share/Trash/

Artifact

name: ApplicationEventLog

doc: Windows Application Event log.

collectors:

- **collector_type:** FILE

args: {**path_list:** ['%%environ_systemroot%%\System32\winevt\Logs\AppEvent.evt']}

conditions: [os_major_version >= 6]

labels: [Logs]

supported_os: [Windows]

urls: ['http://www.forensicswiki.org/wiki/Windows_Event_Log_(EVT)']

Artifact repository: get it here

~130 artifacts, 30 parsers:

<https://code.google.com/p/grr/source/browse/#git%2Fartifacts>

Review, bug reports, patches etc. very welcome

Collection/Definition Demo

Challenges

Testing

Populating the knowledge base

Dependency Logic

**New malware report
BEAR EAGLE SHARK
LASER is out: check all
the things**



What we have to work with



C:\Windows\System32\zuur9x.dll

C:\Windows\System32\winimlog.dll

C:\Windows\System32\abdfdc32.dll

....

d4e088ba921c0420428b1f73d5caad23

415710a29ffb55e53044fc1914509872

....

HKLM\Software\Classes\CLSID\{EFFAABBE-0718-4453-9993-
0AFE88D6F0C}\InprocServer32

What to collect?

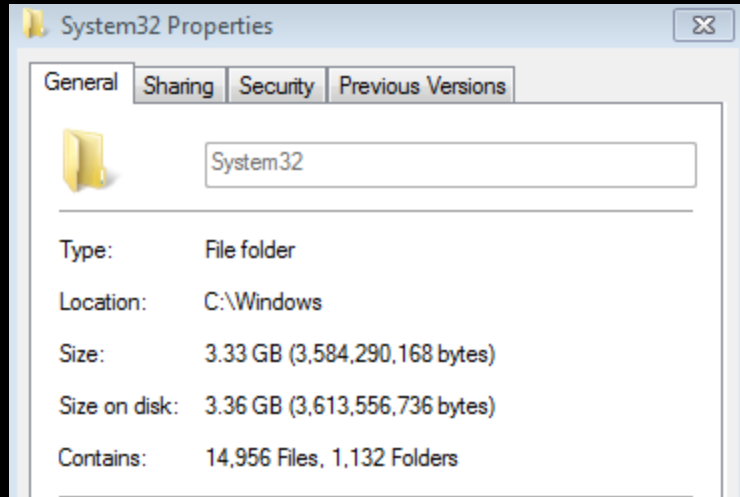
Why not all system32 executables?

`%%environ_systemroot%%\System32\**{exe,dll}`

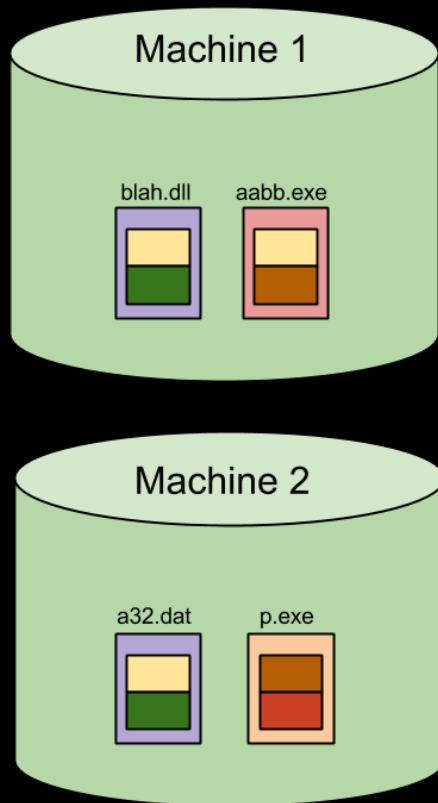
Pros/cons

- + leak less intelligence
- + collect currently unknown malware
- lots of files

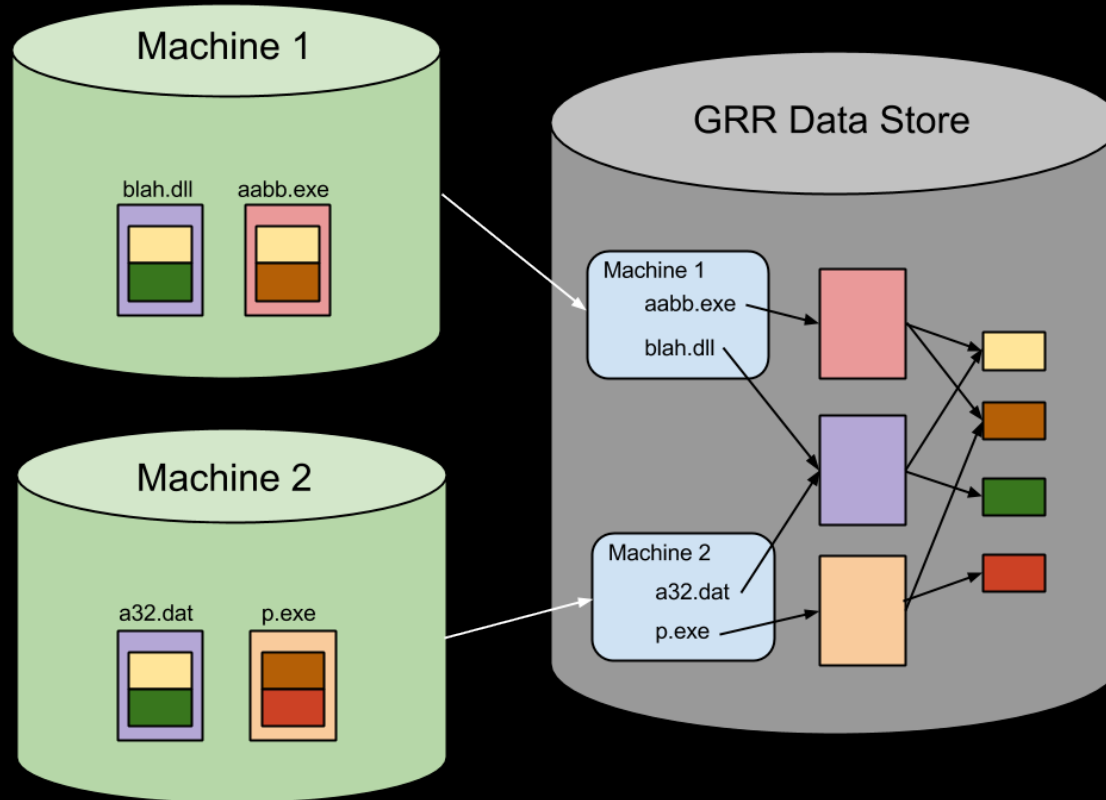
Is that really practical?



File-level and block-level de-dup



File-level and block-level de-dup



Client limits for hunt testing

New Hunt - What to run?

FileFinder

Paths 

Pathtype OS (default) ▼

Conditions 

Action Download ▼

[Advanced](#) >

☒ Notify at Completion

[Advanced](#) >

Hunt Parameters 

Description

Client Limit

Expiry Time

Client rate

[Advanced](#) >

Client limits for hunt testing

Hunt Parameters

Description

Client Limit

0

Expiry Time

31d

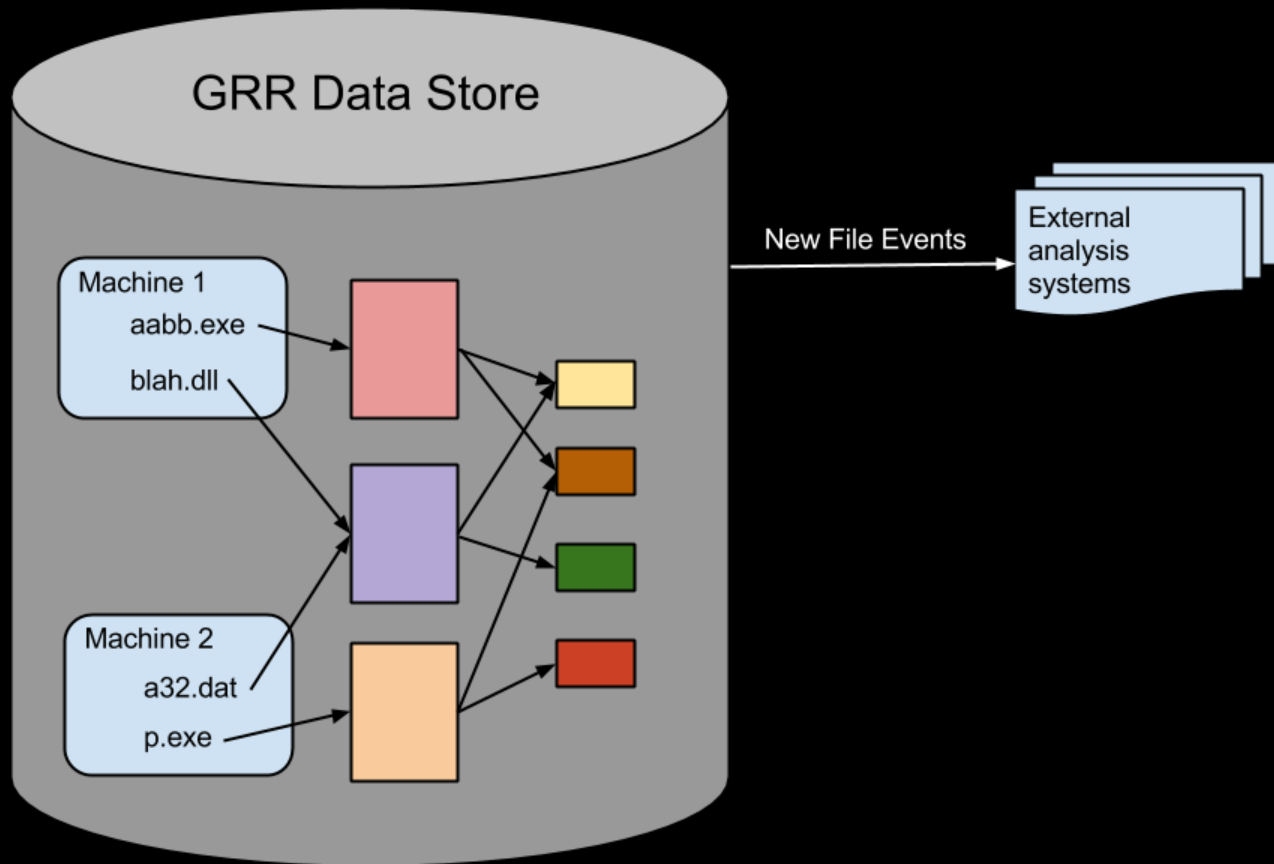
Client rate

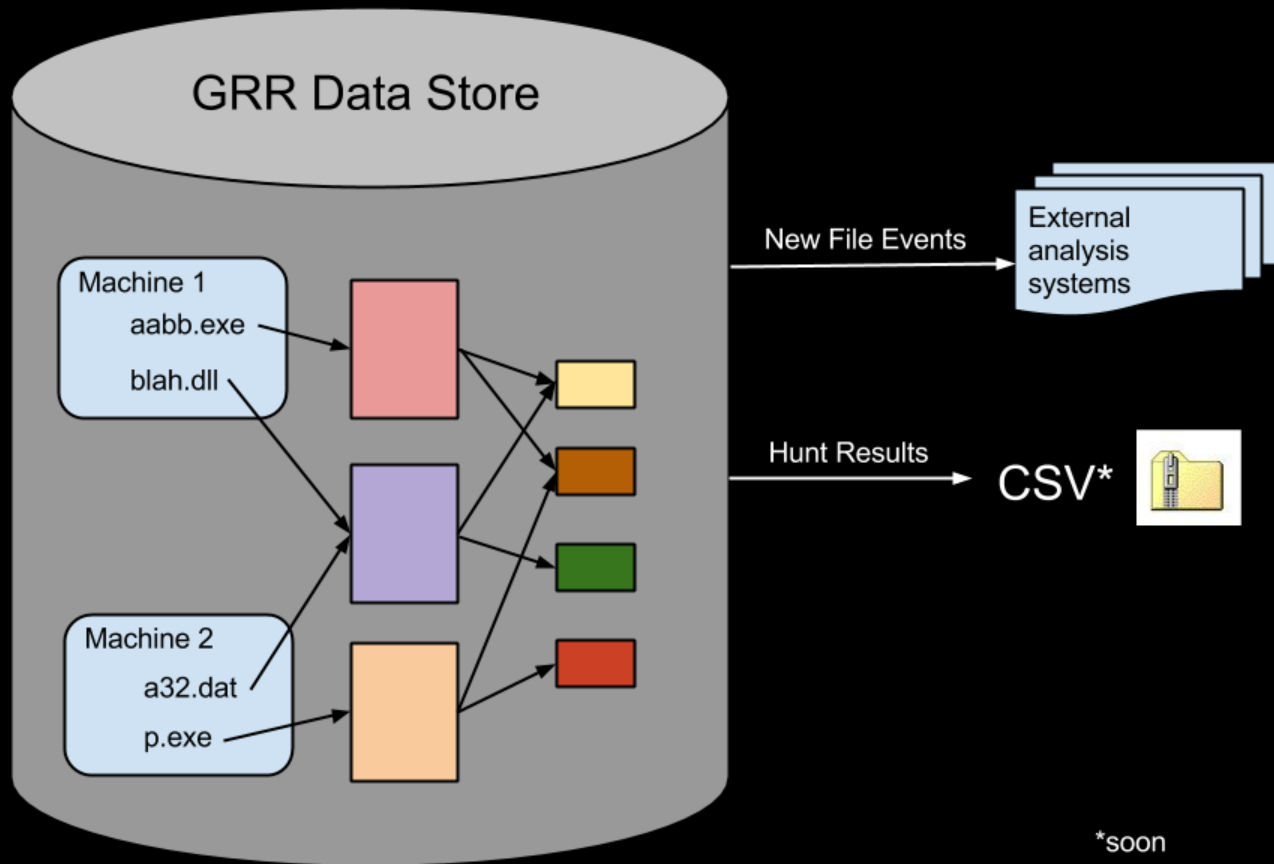
20

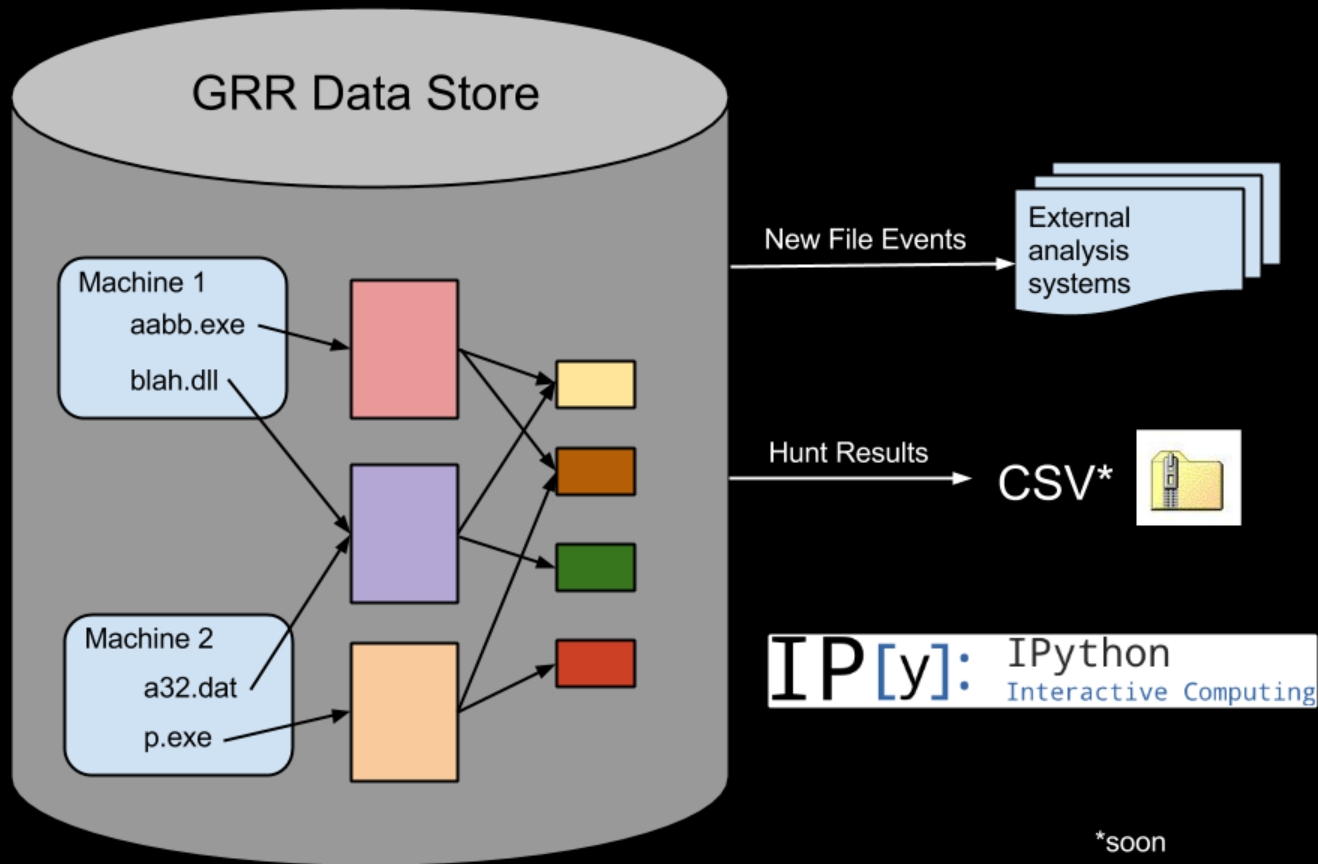
Advanced

>

Output







Input

GRR

SnortWatcher

Evil! [Priority: 1] {TCP}
192.168.1.188:46496
-> X.X.X.X:80



GRR

SnortWatcher

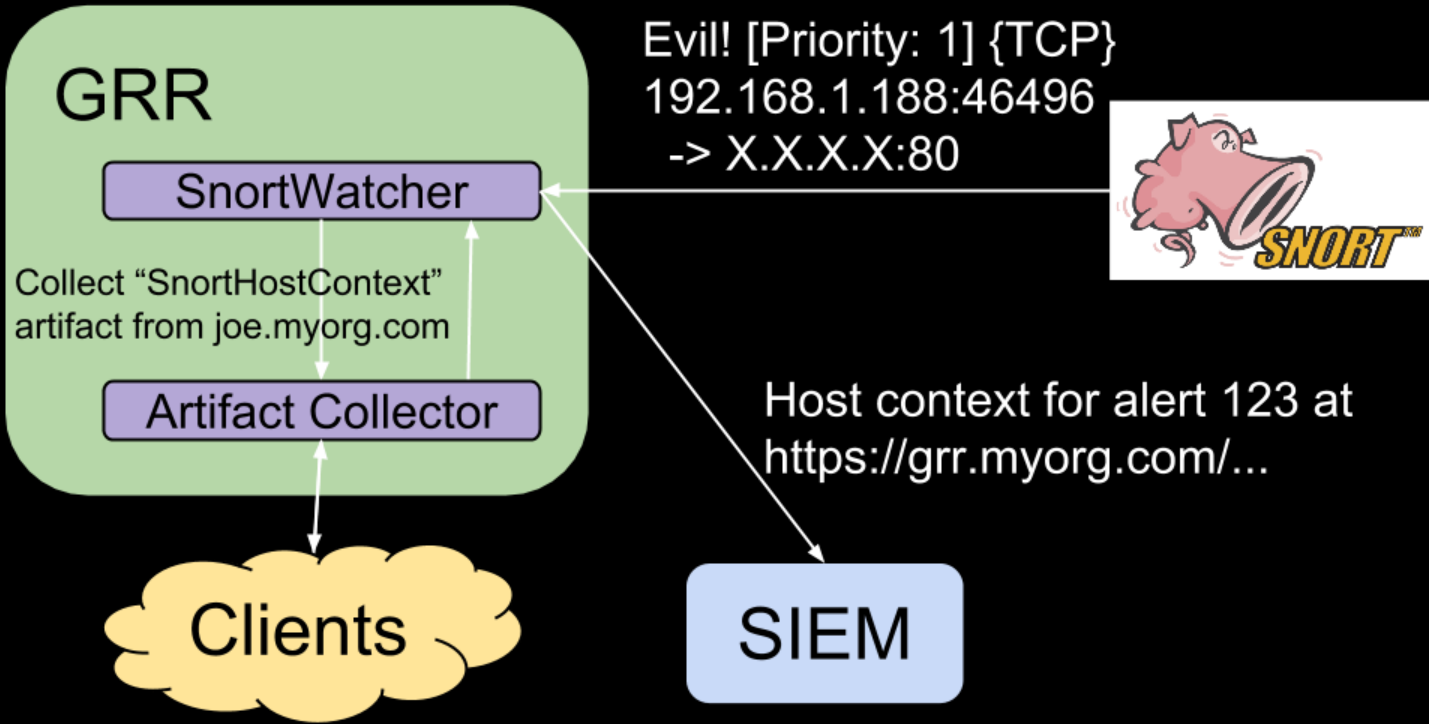
Collect "SnortHostContext"
artifact from joe.myorg.com

Artifact Collector

Clients

Evil! [Priority: 1] {TCP}
192.168.1.188:46496
-> X.X.X.X:80





What's coming for GRR

Artifacts: debug, own repo, UI, performance

Rekall and rekall-grr integration

Opensource datastore performance

Server/client load indicators

Hunting by labels

Links/Contacts

GRR: code.google.com/p/grr/ (artifacts whitepaper will be posted here)

Artifacts repository (for now): <https://code.google.com/p/grr/source/browse/#git%2Fartifacts>

Rekall Memory Forensics: <http://www.rekall-forensic.com/>

Contact: grr-dev@googlegroups.com