

GRR: FIND ALL THE BADNESS!

COLLECT ALL

**THE
THINGS**

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



```
>>>
 35563 1286 STATUS
20fx89c 20fx89c REPORT
mov CONFRO
idlepro IDLEPRO

SARE: 4567 3816
3816 S
CH57 7P57
CEPORS R606

STATUS
REPORT
CONFRO
IDLEPRO

Mt IDEEIDb
QUE
```

```
>>>
Security Xv7
-OVERRIDE 35563
-DUMPSEG 1286
REPORT 11100110x01
CONFRO 11100011100
IDLEPRO 0000010x011

SARE: 4567 3816
3816 S
CH57 7P57
CEPORS R606

STATUS
REPORT
CONFRO
IDLEPRO

Mt IDEEIDb
QUE
```

```
>>>
Security Xv7
-OVERRIDE 35563
-DUMPSEG 1286
REPORT 11100110x01
CONFRO 11100011100
IDLEPRO 0000010x011

SARE: 4567 3816
3816 S
CH57 7P57
CEPORS R606

STATUS
REPORT
CONFRO
IDLEPRO

Mt IDEEIDb
QUE
```

```
>>>
Security Xv7
-OVERRIDE 35563
-DUMPSEG 1286
REPORT 11100110x01
CONFRO 11100011100
IDLEPRO 0000010x011

SARE: 4567 3816
3816 S
CH57 7P57
CEPORS R606

STATUS
REPORT
CONFRO
IDLEPRO

Mt IDEEIDb
QUE
```

```
>>>
Security Xv7
-OVERRIDE 35563
-DUMPSEG 1286
REPORT 11100110x01
CONFRO 11100011100
IDLEPRO 0000010x011

SARE: 4567 3816
3816 S
CH57 7P57
CEPORS R606

STATUS
REPORT
CONFRO
IDLEPRO

Mt IDEEIDb
QUE
```

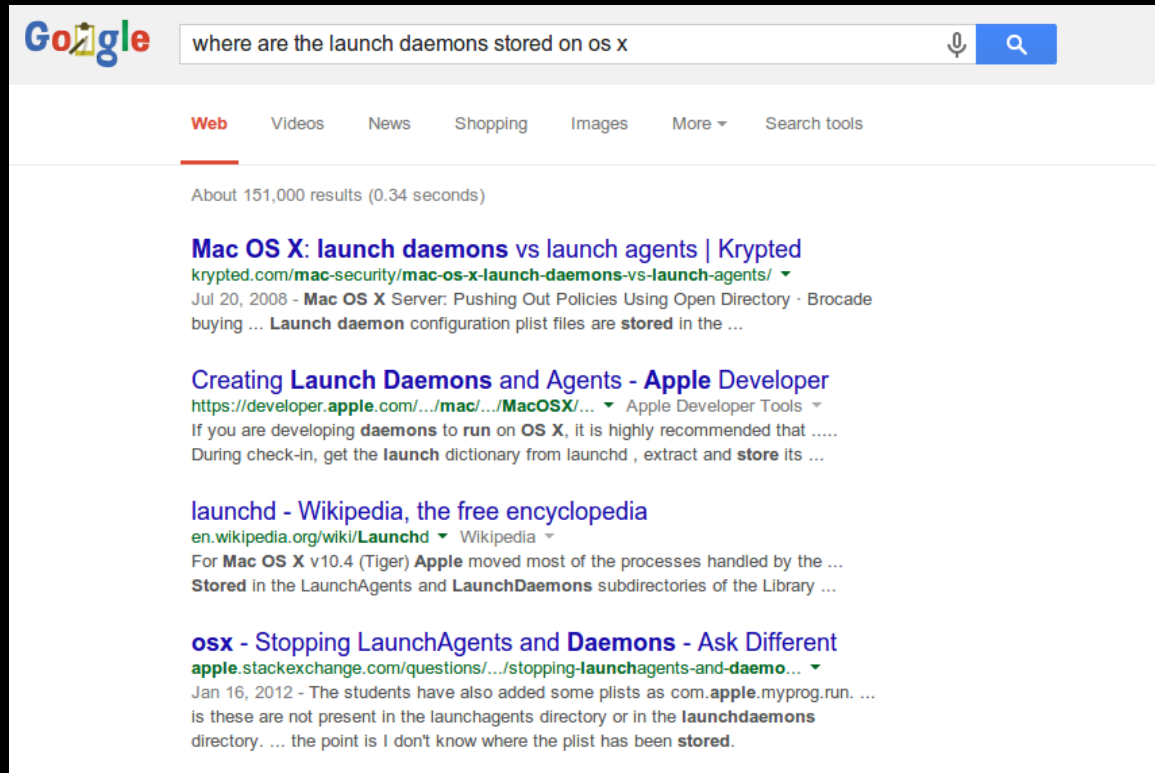
```
>>>
Security Xv7
-OVERRIDE 35563
-DUMPSEG 1286
REPORT 11100110x01
CONFRO 11100011100
IDLEPRO 0000010x011

SARE: 4567 3816
3816 S
CH57 7P57
CEPORS R606

STATUS
REPORT
CONFRO
IDLEPRO

Mt IDEEIDb
QUE
```


What actually happens



The image shows a screenshot of a Google search page. The search bar contains the text "where are the launch daemons stored on os x". Below the search bar, there are navigation links for "Web", "Videos", "News", "Shopping", "Images", "More", and "Search tools". The search results are displayed below, showing about 151,000 results in 0.34 seconds. The first result is titled "Mac OS X: launch daemons vs launch agents | Krypted" and is from the website "krypted.com". The second result is titled "Creating Launch Daemons and Agents - Apple Developer" and is from "https://developer.apple.com/.../mac/.../MacOSX/...". The third result is titled "launchd - Wikipedia, the free encyclopedia" and is from "en.wikipedia.org/wiki/Launchd". The fourth result is titled "osx - Stopping LaunchAgents and Daemons - Ask Different" and is from "apple.stackexchange.com/questions/.../stopping-launchagents-and-daemo...".

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

I reply to this topic

ldrock

Novemian Posted 24 June 2009 - 01:08
where does Internet Explorer 8 stores browsing history?

member

Joined: 23 February 06

Ad Bot (disabled when logged in)

Regular to remove me

Group: Treasury
Regrator: It's Free!

OS X Lion Artifacts v1.0

File Edit View Insert Format Data Tools Help View Only

OS X Lion Artifacts By: Saeed Chahang

File Name	Path	Description
1. Last Modified: 12/16/2011 - added some links to link4me	last	last
2. User Directories	Users	Users
3. Desktop Directories	Desktops	Desktops
4. Music Directories	Music	Music
5. Downloads Directories	Downloads	Downloads
6. Library Directories	Library	Library
7. Movies Directories	Movies	Movies
8. Pictures Directories	Pictures	Pictures
9. Public Directories	Public	Public
10. Sites Directories	Sites	Sites
11. Applications	Applications	Applications
12. Applications	Applications	Applications
13. Safari	Safari	Safari
14. Safari Bookmarks	Bookmarks.plist	Bookmarks
15. Safari Downloads	Downloads.plist	Downloads
16. Safari Extended Datastores	ExtendedDatastores.plist	ExtendedDatastores
17. Safari Extensions	Extensions.plist	Extensions
18. Safari History	History.plist	History
19. Safari History Index	HistoryIndex.plist	HistoryIndex
20. Safari Local Storage	LocalStorage.plist	LocalStorage
21. Safari Local Storage Database	LocalStorageDatabase.plist	LocalStorageDatabase
22. Safari Saved Desktop Pages	SavedDesktopPages.plist	SavedDesktopPages
23. Safari Webpage Icons Database	WebpageIconsDatabase.plist	WebpageIconsDatabase
24. Safari Webpage Database	WebpageDatabase.plist	WebpageDatabase
25. Safari Webpage Database Database	WebpageDatabaseDatabase.plist	WebpageDatabaseDatabase
26. Safari Cache Database	CacheDatabase.plist	CacheDatabase
27. Safari Cache	Cache	Cache
28. Safari Extended Cache	ExtendedCache.plist	ExtendedCache
29. Safari Webpage Preview	WebpagePreview.plist	WebpagePreview
30. Safari Preferences	Preferences.plist	Preferences
31. Safari Recent Applications State Directory	RecentApplicationsStateDirectory.plist	RecentApplicationsStateDirectory
32. Safari Bookmarks Cache	BookmarksCache.plist	BookmarksCache
33. Safari History Cache	HistoryCache.plist	HistoryCache
34. Mail	Mail	Mail
35. Mail Cache	Cache	Cache
36. Mail Extended Datastores	ExtendedDatastores	ExtendedDatastores
37. Mail Mailbox	Mailbox	Mailbox
38. Mail Mailbox Extended Datastores	MailboxExtendedDatastores	MailboxExtendedDatastores
39. Mail Mailbox Index	MailboxIndex	MailboxIndex
40. Mail Mailbox Preferences	MailboxPreferences	MailboxPreferences
41. Mail Mailbox State Directory	MailboxStateDirectory	MailboxStateDirectory
42. Mail Message	Message	Message
43. Mail Message Extended Datastores	MessageExtendedDatastores	MessageExtendedDatastores
44. Mail Message Index	MessageIndex	MessageIndex
45. Mail Message Preferences	MessagePreferences	MessagePreferences
46. Mail Message State Directory	MessageStateDirectory	MessageStateDirectory
47. Mail Message Summary	MessageSummary	MessageSummary
48. Mail Message Summary Extended Datastores	MessageSummaryExtendedDatastores	MessageSummaryExtendedDatastores
49. Mail Message Summary Index	MessageSummaryIndex	MessageSummaryIndex
50. Mail Message Summary Preferences	MessageSummaryPreferences	MessageSummaryPreferences
51. Mail Message Summary State Directory	MessageSummaryStateDirectory	MessageSummaryStateDirectory
52. Mail Message Summary Summary	MessageSummarySummary	MessageSummarySummary
53. Mail Message Summary Summary Extended Datastores	MessageSummarySummaryExtendedDatastores	MessageSummarySummaryExtendedDatastores
54. Mail Message Summary Summary Index	MessageSummarySummaryIndex	MessageSummarySummaryIndex
55. Mail Message Summary Summary Preferences	MessageSummarySummaryPreferences	MessageSummarySummaryPreferences
56. Mail Message Summary Summary State Directory	MessageSummarySummaryStateDirectory	MessageSummarySummaryStateDirectory
57. Mail Message Summary Summary Summary	MessageSummarySummarySummary	MessageSummarySummarySummary
58. Mail Message Summary Summary Summary Extended Datastores	MessageSummarySummarySummaryExtendedDatastores	MessageSummarySummarySummaryExtendedDatastores
59. Mail Message Summary Summary Summary Index	MessageSummarySummarySummaryIndex	MessageSummarySummarySummaryIndex
60. Mail Message Summary Summary Summary Preferences	MessageSummarySummarySummaryPreferences	MessageSummarySummarySummaryPreferences
61. Mail Message Summary Summary Summary State Directory	MessageSummarySummarySummaryStateDirectory	MessageSummarySummarySummaryStateDirectory
62. Mail Message Summary Summary Summary Summary	MessageSummarySummarySummarySummary	MessageSummarySummarySummarySummary
63. Mail Message Summary Summary Summary Summary Extended Datastores	MessageSummarySummarySummarySummaryExtendedDatastores	MessageSummarySummarySummarySummaryExtendedDatastores
64. Mail Message Summary Summary Summary Summary Index	MessageSummarySummarySummarySummaryIndex	MessageSummarySummarySummarySummaryIndex
65. Mail Message Summary Summary Summary Summary Preferences	MessageSummarySummarySummarySummaryPreferences	MessageSummarySummarySummarySummaryPreferences
66. Mail Message Summary Summary Summary Summary State Directory	MessageSummarySummarySummarySummaryStateDirectory	MessageSummarySummarySummarySummaryStateDirectory
67. Mail Message Summary Summary Summary Summary Summary	MessageSummarySummarySummarySummarySummary	MessageSummarySummarySummarySummarySummary
68. Mail Message Summary Summary Summary Summary Summary Extended Datastores	MessageSummarySummarySummarySummarySummaryExtendedDatastores	MessageSummarySummarySummarySummarySummaryExtendedDatastores
69. Mail Message Summary Summary Summary Summary Summary Index	MessageSummarySummarySummarySummarySummaryIndex	MessageSummarySummarySummarySummarySummaryIndex
70. Mail Message Summary Summary Summary Summary Summary Preferences	MessageSummarySummarySummarySummarySummaryPreferences	MessageSummarySummarySummarySummarySummaryPreferences
71. Mail Message Summary Summary Summary Summary Summary State Directory	MessageSummarySummarySummarySummarySummaryStateDirectory	MessageSummarySummarySummarySummarySummaryStateDirectory
72. Mail Message Summary Summary Summary Summary Summary Summary	MessageSummarySummarySummarySummarySummarySummary	MessageSummarySummarySummarySummarySummarySummary
73. Mail Message Summary Summary Summary Summary Summary Summary Extended Datastores	MessageSummarySummarySummarySummarySummarySummaryExtendedDatastores	MessageSummarySummarySummarySummarySummarySummaryExtendedDatastores
74. Mail Message Summary Summary Summary Summary Summary Summary Index	MessageSummarySummarySummarySummarySummarySummaryIndex	MessageSummarySummarySummarySummarySummarySummaryIndex
75. Mail Message Summary Summary Summary Summary Summary Summary Preferences	MessageSummarySummarySummarySummarySummarySummaryPreferences	MessageSummarySummarySummarySummarySummarySummaryPreferences
76. Mail Message Summary Summary Summary Summary Summary Summary State Directory	MessageSummarySummarySummarySummarySummarySummaryStateDirectory	MessageSummarySummarySummarySummarySummarySummaryStateDirectory
77. Mail Message Summary Summary Summary Summary Summary Summary Summary	MessageSummarySummarySummarySummarySummarySummarySummary	MessageSummarySummarySummarySummarySummarySummarySummary
78. Mail Message Summary Summary Summary Summary Summary Summary Summary Extended Datastores	MessageSummarySummarySummarySummarySummarySummarySummaryExtendedDatastores	MessageSummarySummarySummarySummarySummarySummarySummaryExtendedDatastores
79. Mail Message Summary Summary Summary Summary Summary Summary Summary Index	MessageSummarySummarySummarySummarySummarySummarySummaryIndex	MessageSummarySummarySummarySummarySummarySummarySummaryIndex
80. Mail Message Summary Summary Summary Summary Summary Summary Summary Preferences	MessageSummarySummarySummarySummarySummarySummarySummaryPreferences	MessageSummarySummarySummarySummarySummarySummarySummaryPreferences
81. Mail Message Summary Summary Summary Summary Summary Summary Summary State Directory	MessageSummarySummarySummarySummarySummarySummarySummaryStateDirectory	MessageSummarySummarySummarySummarySummarySummarySummaryStateDirectory
82. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary	MessageSummarySummarySummarySummarySummarySummarySummarySummary	MessageSummarySummarySummarySummarySummarySummarySummarySummary
83. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Extended Datastores	MessageSummarySummarySummarySummarySummarySummarySummarySummaryExtendedDatastores	MessageSummarySummarySummarySummarySummarySummarySummarySummaryExtendedDatastores
84. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Index	MessageSummarySummarySummarySummarySummarySummarySummarySummaryIndex	MessageSummarySummarySummarySummarySummarySummarySummarySummaryIndex
85. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Preferences	MessageSummarySummarySummarySummarySummarySummarySummarySummaryPreferences	MessageSummarySummarySummarySummarySummarySummarySummarySummaryPreferences
86. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary State Directory	MessageSummarySummarySummarySummarySummarySummarySummarySummaryStateDirectory	MessageSummarySummarySummarySummarySummarySummarySummarySummaryStateDirectory
87. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummary	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummary
88. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Extended Datastores	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummaryExtendedDatastores	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummaryExtendedDatastores
89. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Index	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummaryIndex	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummaryIndex
90. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Preferences	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummaryPreferences	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummaryPreferences
91. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary State Directory	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummaryStateDirectory	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummaryStateDirectory
92. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Summary	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummary	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummary
93. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Summary Extended Datastores	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryExtendedDatastores	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryExtendedDatastores
94. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Summary Index	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryIndex	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryIndex
95. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Summary Preferences	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryPreferences	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryPreferences
96. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Summary State Directory	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryStateDirectory	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryStateDirectory
97. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Summary Summary	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummarySummary	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummarySummary
98. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Summary Extended Datastores	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryExtendedDatastores	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryExtendedDatastores
99. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Summary Index	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryIndex	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryIndex
100. Mail Message Summary Summary Summary Summary Summary Summary Summary Summary Summary Summary Preferences	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryPreferences	MessageSummarySummarySummarySummarySummarySummarySummarySummarySummarySummarySummaryPreferences

How do I open and edit the Windows Registry

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

Caution: Before editing or changing anything in the Microsoft Windows registry, we highly recommend that you backup the Registry. We also highly recommend that you 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 enter in the Run Box or Search box type **regedit** Editor.

3. If prompted by User Account Control, click **Yes** to open the Registry.

4. Once opened successfully you should be in the Windows Registry Editor Window, similar to the screenshot given below.

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

Artifacts

Search on site

28 ActionVoiP – Windows client

Posted by admin | Tags: windows, VoIP

Author Name

Mohammed Faiz Quadri

Artifact or Program Version

Not specified (36 older versions)

voip client for Windows.

to make VoIP calls from a PC or a Smart phone. It is used by thousands of free/cheap phones calls. It is not mandatory for a user to provide their identity g call. The user ID shown on the receiving phone is usually an "Unknown"

kor\voip\ActionVoiP\Accounts\Password <<<<

kor\voip\ActionVoiP\Accounts\UserName <<<<<<

Recent Submissions

- ActionVoiP - Windows client
- Windows Essentials 2012
- Skype shared and the "Classified" feature
- TeamViewer 8
- AnCrypt Artifacts
- Bluetooth Personal Area Network (PAN) Service Artifacts (Bluetooth Wireless)
- Bluetooth Connected Device Artifacts (Bluetooth Wireless)
- Forensic Artifacts Profile

Tags

- Apple application artifacts
- Bluetooth Bluetooth browsing history
- cloud cloud forensics
- Quantumcast
- scan scan Firefox
- Google Chrome Browser scan

Page Discussion

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 [show]

- 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 20
- 3 Section A - Metrics array
- 4 Section B - Trace chains array
- 5 Section C - Filename string
- 6 Section D - Volumes information (back)
 - 6.1 Volume information
 - 6.1.1 Volume information - version 17
 - 6.1.2 Volume information - version 20
 - 6.2 Sub section E - NTFS file references
 - 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 or without a byte-order-mark (BOM).
- 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



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-0718-4453-9993-0AFE888D6F0C}\InprocServer32

What to collect?

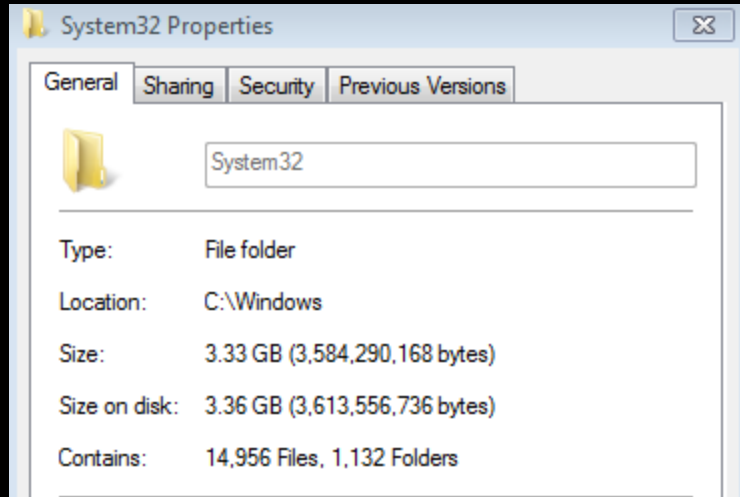
Why not all system32 executables?

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

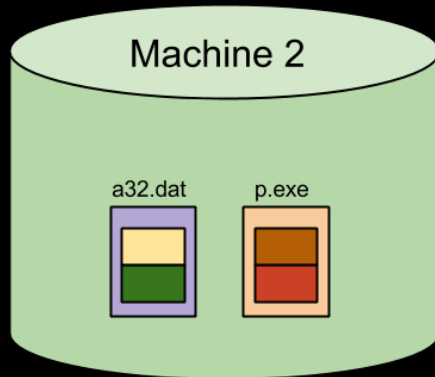
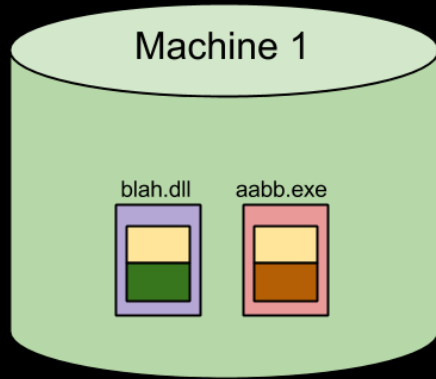
Pros/cons

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

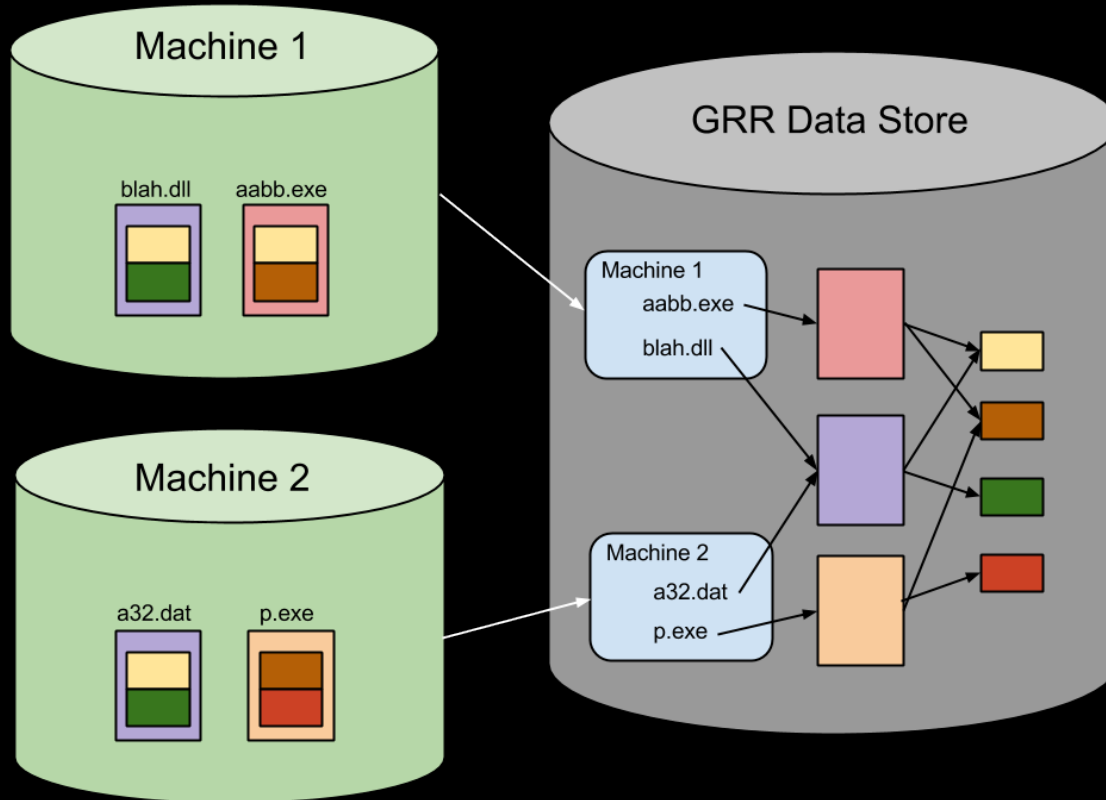
Is that really practical?



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

Administrative
Browser
Collectors
Filesystem
 File Finder
 GetMBR
 ListVolumeShadowCop
Memory
Misc
Network
Processes
Registry
Timeline

Paths +
X c:\windows\system32\notepad.*

Pathtype OS (default) ▾

Conditions +

Action
Action Download ▾
Advanced >

Notify at Completion

Advanced >

Hunt Parameters ⓘ

Description

Client Limit

Expiry Time

Client rate

Advanced >

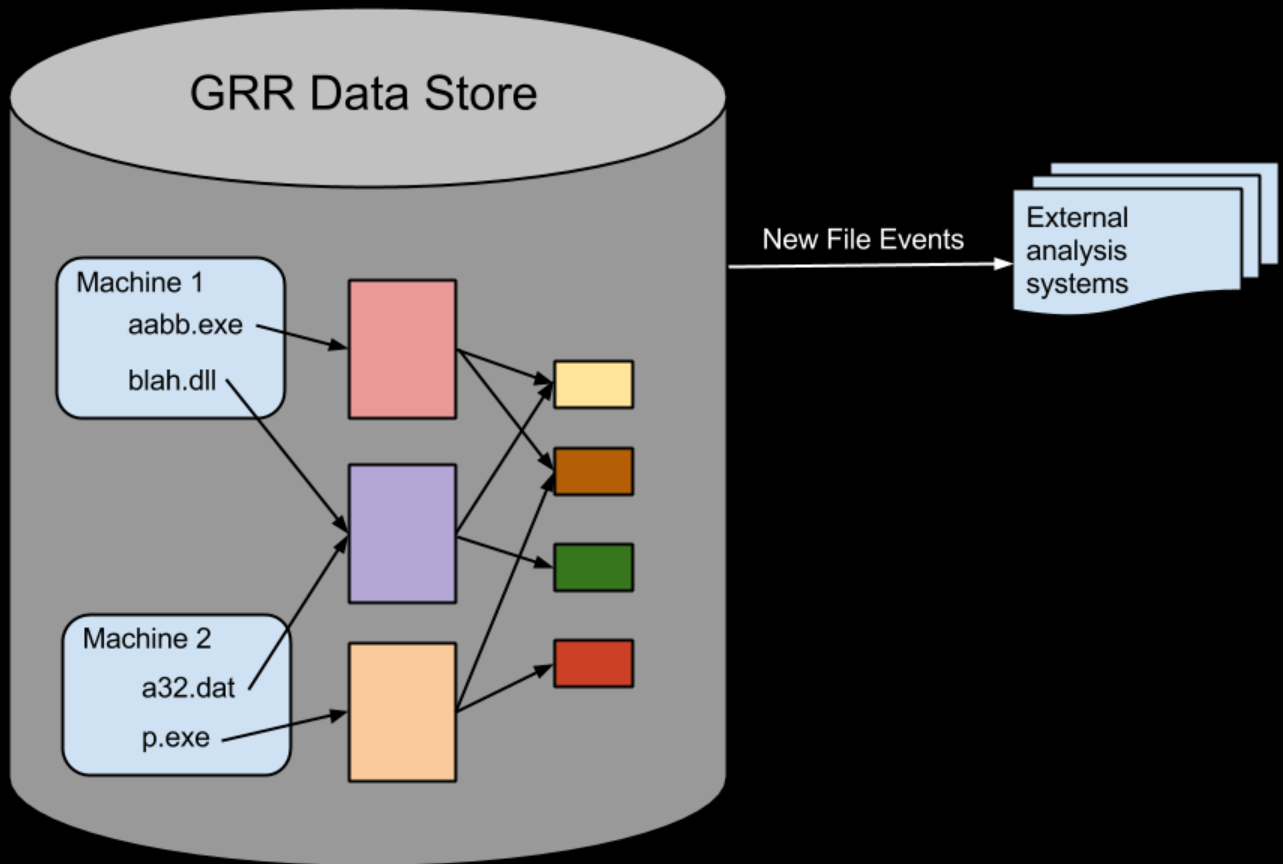
Client limits for hunt testing

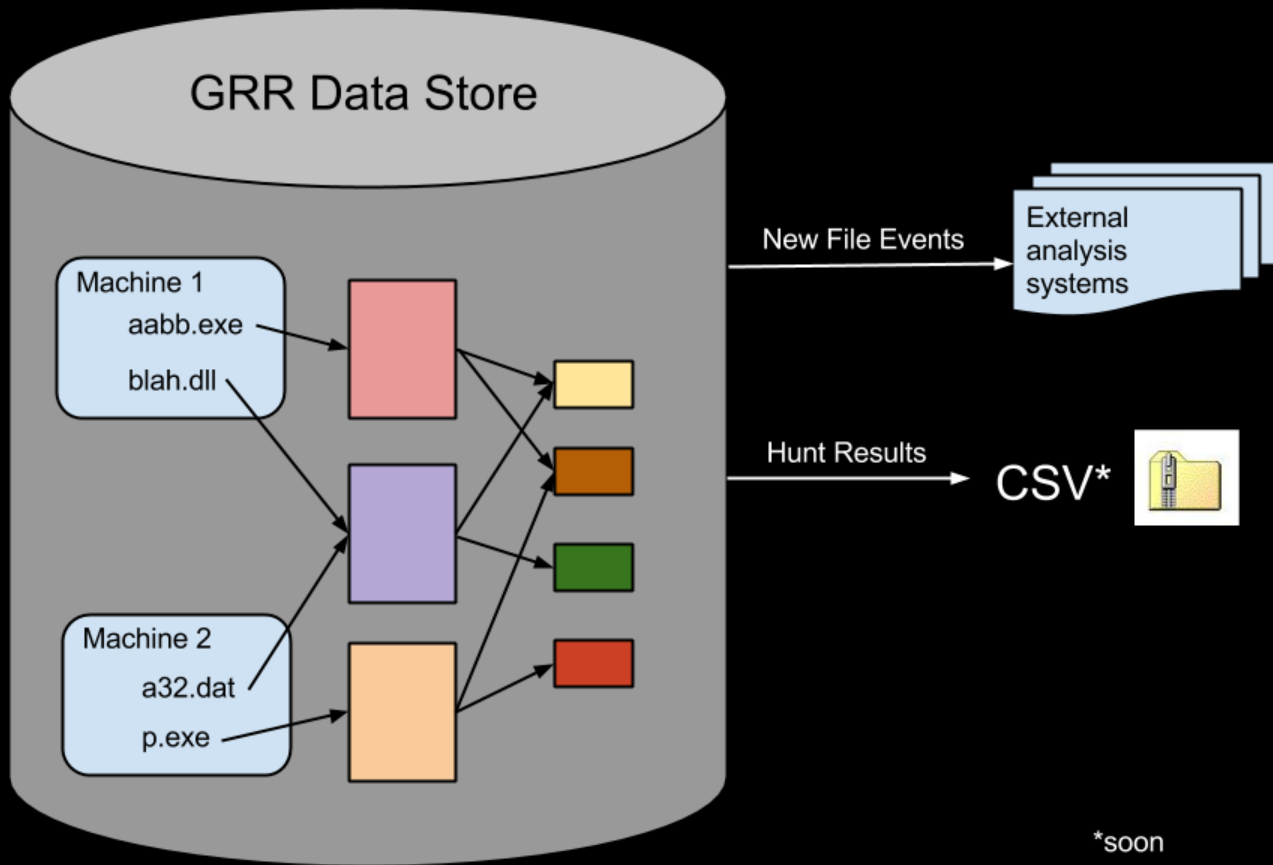
Hunt Parameters ⓘ

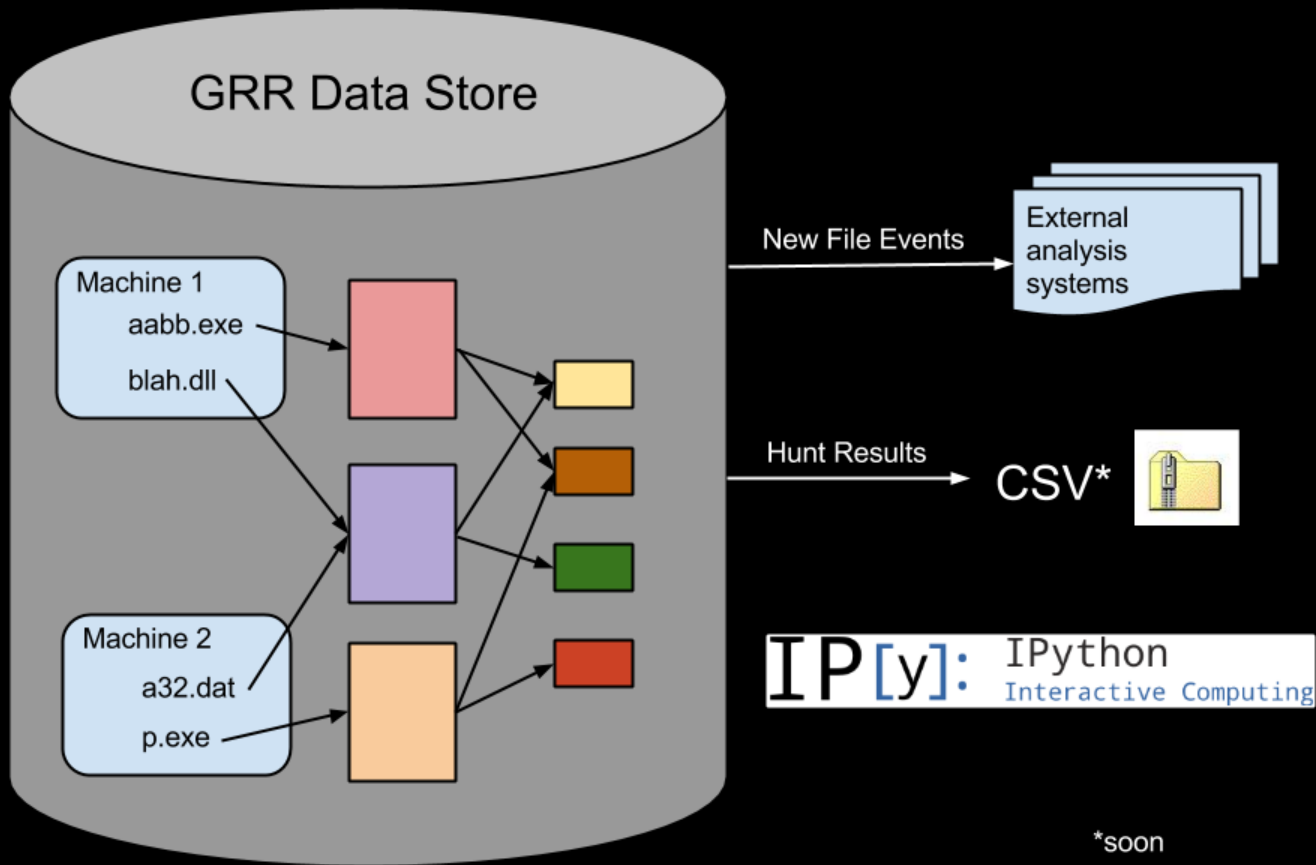
Description	<input type="text"/>
Client Limit	<input type="text" value="0"/>
Expiry Time	<input type="text" value="31d"/>
Client rate	<input type="text" value="20"/>

[Advanced](#) >

Output







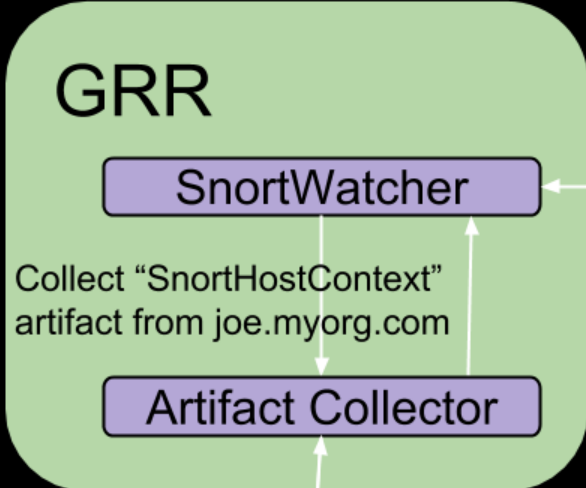
Input

GRR

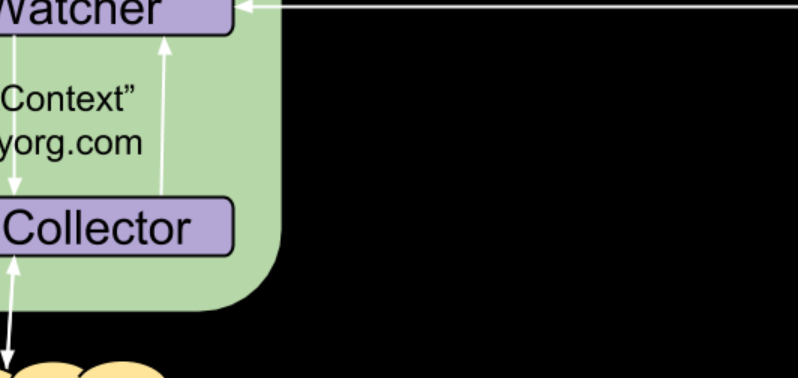
SnortWatcher

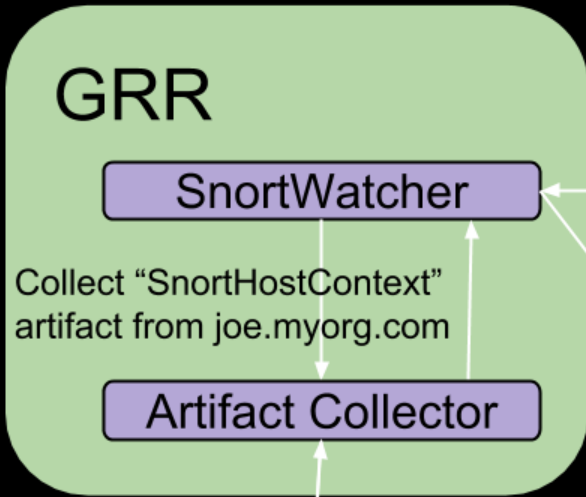
Evil! [Priority: 1] {TCP}
192.168.1.188:46496
-> X.X.X.X:80





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

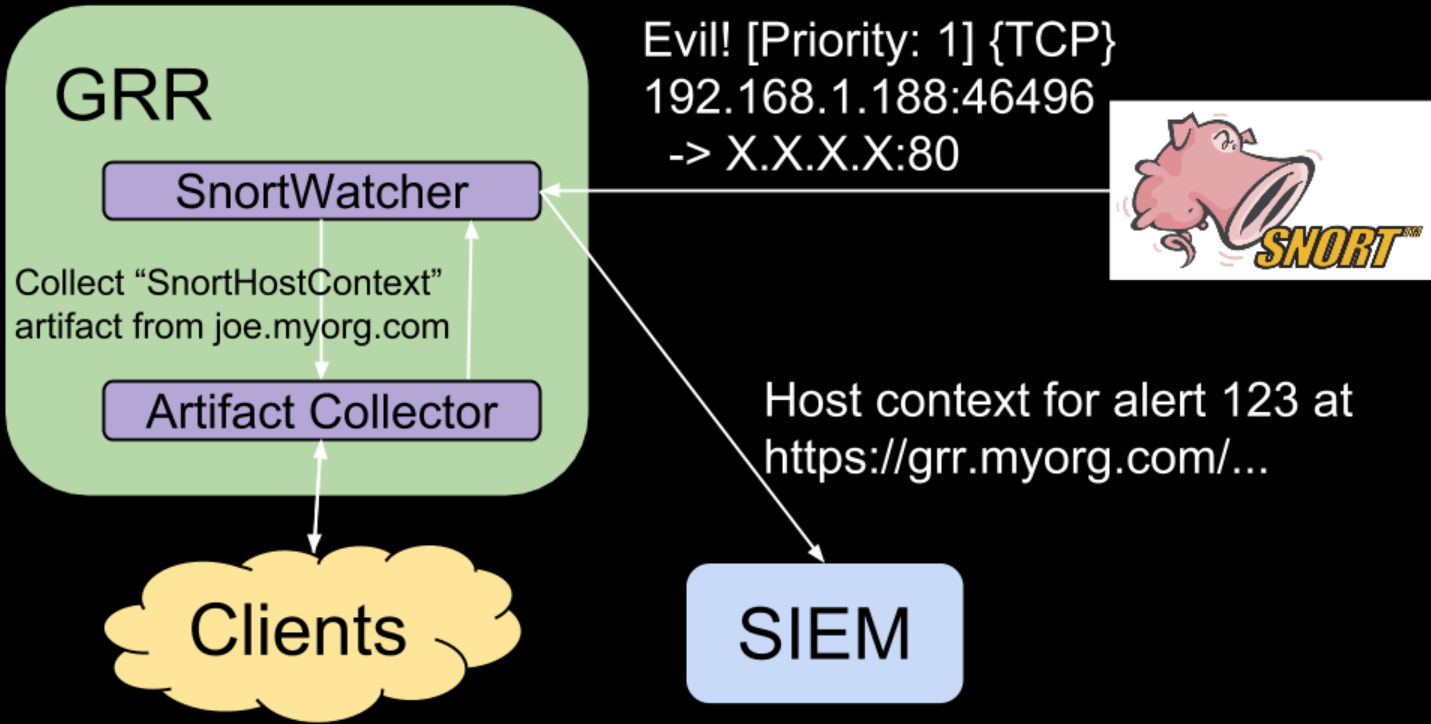




Evil! [Priority: 1] {TCP}
192.168.1.188:46496
-> X.X.X.X:80



Host context for alert 123 at
[https://grr.myorg.com/...](https://grr.myorg.com/)



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