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
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\Windows\History\History.IE5\index.dat
%users.localappdata%%\Microsoft\Windows\History\Low\History.IE5\index.dat
%users.localappdata%%\Microsoft\Windows\History\*\index.dat
%users.localappdata%%\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/Caches/Google/Chrome/*/GPUCache/*
- %%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.homedir%%/.cache/chromium/PnaclTranslationCache/*

- %%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

Google search results for "where are the launch daemons stored on os x"

1. 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...

2. Creating Launch Daemons and Agents - Apple Developer
   https://developer.apple.com/.../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...

3. launchd - Wikipedia, the free encyclopedia
   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...

4. osx - Stopping LaunchAgents and Daemons - Ask Different
   apple.stackexchange.com/questions/.../stopping-launchagents-and-daemo...
   Jan 16, 2012 - The students have also added some plist's 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
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?
SON, I GOT 99 PROBLEMS

BUT A LACK OF STANDARDS AIN'T ONE
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-xxxxxxxxx-xxxxxxxxx-xxxxxxxxx-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-xxxxxxxxx-xxxxxxxxxx-xxxxxxxxx-xxxx\Software\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\InstallLocation

/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/`
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]

text: Logs

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
...

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
Client limits for hunt testing
Output
Input
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

GRR

SnortWatcher

Collect "SnortHostContext" artifact from joe.myorg.com

Artifact Collector

Clients
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

Host context for alert 123 at 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%2Farifarts

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

Contact: grr-dev@googlegroups.com