These views are mine alone and don’t reflect those of my employer
You are compromised

- Player (1) Insert coin -
Why?
login: root
Password: **********

Welcome back, root.

root@localhost:~# _
Welcome back, root.
Assume compromise.
3 PILLARS OF INCIDENT RESPONSE
FLEET MANAGEMENT.
DATA COLLECTION.
DETECTION AND RESPONSE.
FLEET MANAGEMENT.
DATA COLLECTION.
DETECTION AND RESPONSE.
DETECTION AND RESPONSE.
DETECTION AND RESPONSE.
DETECTION AND RESPONSE.

P: We're not great at sharing information.
L: github.com/kbandla/APTnotes
Hall of shame of intel sharing.

[on a 3-page threat intel document]

“Here’s a list of domains related to malware X to review your network logs for. Typically, they’re used for phishing or C&C.”

[proceeds with a list of domains]

- Hello? C2 traffic and phishing are two very different things.
Hall of shame of intel sharing.

[... on a sample’s C2 callback format ...]

GET /{ID1}/{ID2} HTTP/1.0
User-Agent: {IE6_UA}HOST: {C2_HOSTNAME}:{PORT}”

- Oooooh, shiny! Signature!
- Wait, is it a typo?
Hall of shame of intel sharing.

Same report, later on, in a packet capture of the sample:

POST /{ID1} HTTP/1.0
User-Agent: {IE6_UA}
HOST: {IP}:{PORT}
Pragma: no-cache

- Probably a typo... what about that Pragma? Signature or typo?

ALT+F4... == (╯°□°)╯︵┻━┻
Hall of shame of intel sharing.

[... talking about a phishing e-mail ...]

“The hash of the message is ________________”
DETECTION AND RESPONSE.

P: Our methods are weak against determined actors.
DETECTION AND RESPONSE.
C:\> md5sum a.exe
10e4a1d2132cccb5c6759f038cdb6f3c9  a.exe

[append data to a.exe]
C:\> md5sum a.exe
17e6317e1a13844078943ba876a31e70  a.exe
C:\> a.exe

[still runs fine : (]
DETECTION AND RESPONSE.
DETECTION AND RESPONSE.
DETECTION AND RESPONSE.
DETECTION AND RESPONSE.
DETECTION AND RESPONSE.
DETECTION AND RESPONSE.
Hire the best. Reward them. Keep them fresh.
Know the limits of your approach. Up your game.
Train. Train. Train.
Become a hunter.
PS: YOU MIGHT WANT TO CHECK OUT
GRR: SCALABLE REMOTE FORENSICS

- Enables quick, scalable remote forensics.
- Agent-based. Cross platform (Win, OS X, Linux).
  - OS or RAW (TSK) access to the filesystem.
- Most of the logic is server-side.
- Captures state. Stores history.
- Enables hunting on the fleet for host artifacts.
  - Apply flows on all or a portion of your fleet.
- Built for analysts.
GRR // LINK GALORE

github.com/google/grr

Presentations
Yahoo! on GRR Hunting - youtu.be/4qCvx3SnAm4
GRR + Plaso + Timesketch - goo.gl/EHjTTa
Greg Castle on Artifacts and Hunting - goo.gl/hVsNrf
PLASO & TIMESKETCH

- Plaso is the next generation log2timeline
  - Python-based. Bye, Perl!
  - Efficient container format.
  - Powerful new capabilities: Hashing, VSS, BDE, etc.

- Timesketch: collaborative timeline analysis
  - Experimental. Horizontal view across the fleet.
  - Tagging and saving of views.

github.com/log2timeline/plaso & www.timesketch.org
VOLATILITY: MEMORY FORENSICS

- The original. Tried and tested.
- De facto standard.
- Bleeding-edge
  - Has most of the state of the art in memory analysis
- Large community.
  - Plenty of external contributions and documentation.

www.volatilityfoundation.org
Robust acquisition and analysis
- All platforms
- Auto-detection, heap, pagefile, virtualization support...

**Reporting**: Web UI, JSON.

Simplicity, accuracy, reusable.

**GRR+Rekall**:
- Scalable, remote, live memory forensics \m/
[NEW!] OSQUERY

- "Easily ask questions about your Linux and OSX infrastructure."
- SQL-like interface against endpoints.
- Processes, firewall rules, packages, etc.

```sql
osquery> SELECT uid, name FROM listening_ports l, processes p WHERE l.pid=p.pid;
```

osquery.io
[NEWish!] **SYSMON**

- Designed by the Sysinternals team
  - Mark Russinovich and Thomas Garnier. Enough said.
- One of the most comprehensive background monitoring solutions for Windows.
  - Process and network monitoring.
  - Hashes of process image files.
- **FREE!**
[NEW!] **STENOGRAPHER**

- Open-source full-packet-capture solution.
- “Writes packets to disk, very quickly (~10Gbps on multi-core, multi-disk machines).”
- Designed for very light-weight querying of the data (<1%).
- Ideal for IR work.

[github.com/google/stenographer](https://github.com/google/stenographer)
Jordi Sanchez  ['ʒɔrði]
You may remember me from….
   “LNK Parsing: you’re doing it wrong”
Currently, Incident Response (+R&D)
   Rekall  - Linux support, Virtualization...
   GRR   - Rekall integration, plist.
Before: forensics & expert witness, pentester...

github.com/parkisan    @parkisan