Dissecting The Stuxnet Malware: An Introduction To Forensic Analysis On Windows Machines

Jared M. Smith
Twitter: @jaredthecoder
Web: jaredthecoder.com

Codestock 2017

About me

- Security Researcher and Project Lead at Oak Ridge National Laboratory
- Graduate Research Assistant (PhD Student) at UT
- Founder of HackUTK and VolHacks
- Avid hiker and very reluctant backpacker

OAK RIDGE National Laboratory

University of Tennessee VOLSEC — COMPUTER SECURITY LAB —

Security incidents are inevitable...

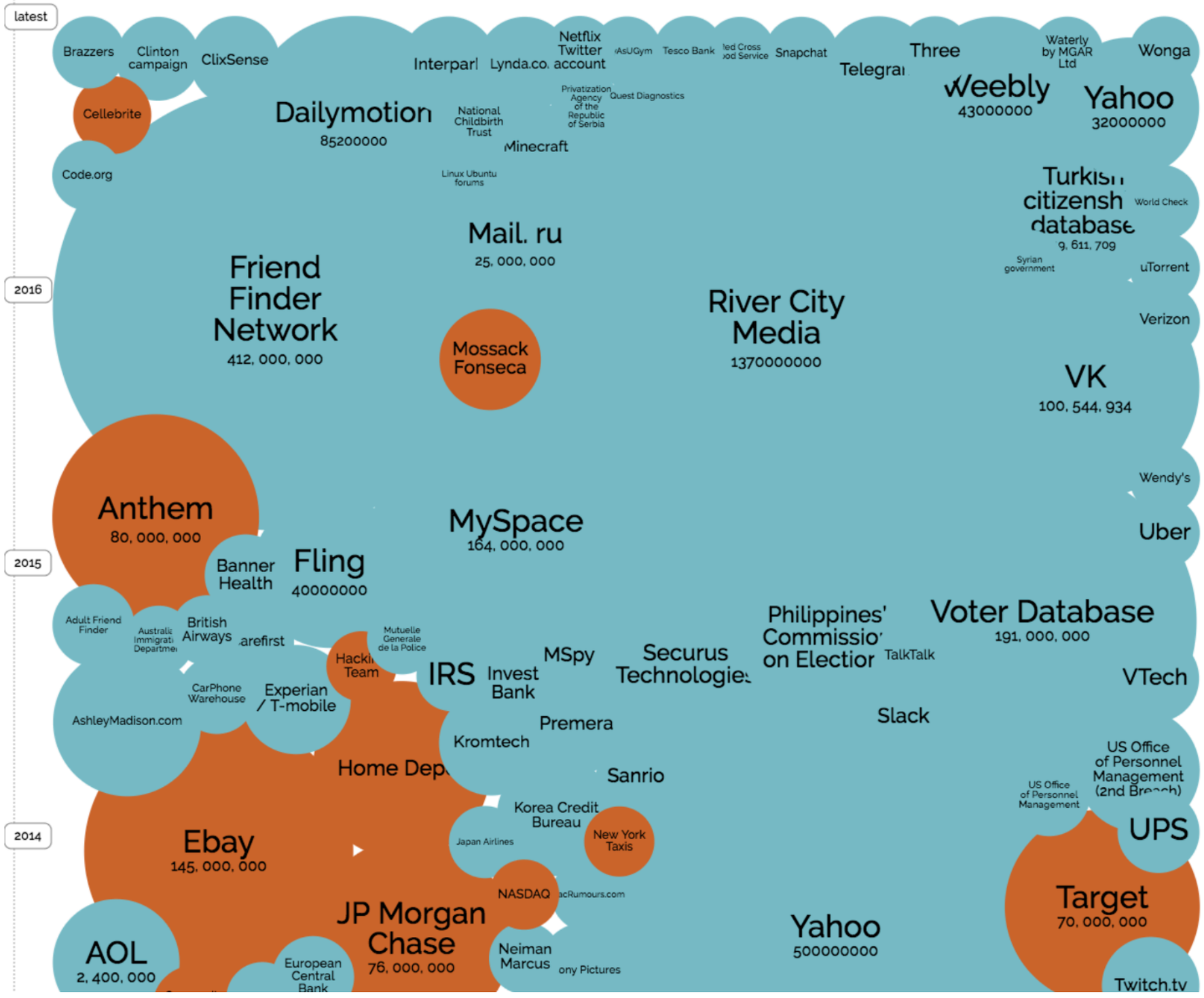
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 25th Apr 2017)

interesting story

YEAR | *BUBBLE COLOUR* YEAR | METHOD OF LEAK | *BUBBLE SIZE* NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



@jaredthecoder | Codestock 2017

When they do happen,
they cost both
reputation *and* money....

$4 million

Average cost of a data breach in 2016 from 350 companies studied by IBM and the Ponemon Institute

$236 million

Cost of Target's data breach recovery efforts after losing over 100 million customer records

$62 million

Cost of Home Depot's data breach recovery efforts after losing over 65 million customer payment records

Once you discover you've been compromised, you need to know how to prevent it next time.

You also have to deliver this information clearly to your managers and executives...

NOPE. I'M OUT.

What's the good news?

You discovered this **before it was openly leaked**, you notified **all affected parties**, and you **locked down your systems** from further attacks.

Thanks to effective incident response.

This could have been much, much worse, though.


LiveSlides web content
To view
Download the add-in.
liveslides.com/download
Start the presentation.

Forensic Analysis

Types of Forensic Analysis

- Crime investigation
- Victim identification
- Forensic Anthropology
- Computer Forensics
  - Network Analysis
  - User Behavioral Analysis
  - Memory Forensics

Memory Forensics

@jaredthecoder | Codestock 2017

What is Memory Forensics?

The art of examining a host's memory (RAM) for anomalous data, often revealing indicators of compromise.

What are the Goals?

- Find artifacts of a compromise
  - What was affected
  - When was it affected
  - How was it affected
    - What subsystems were affected
    - What external systems were affected
- Find why the attack was done
- Find out what to improve to not let it happen again

Why not X instead?

- Capturing system logs and parsing out relevant info can miss key insights
- Endpoint security agents typically don't capture all system state and can also be resource-intensive
- Manual inspection by actual humans is often needed for complex incidents
- AI doesn't solve everything

State of the Art Tools (and free!)

- Autopsy and Sleuth Kit: https://www.sleuthkit.org/autopsy/
- Rekall: http://www.rekall-forensic.com
- GRR: https://github.com/google/grr
- Volatility: http://www.volatilityfoundation.org

Volatility

@jaredthecoder | Codestock 2017

Volatility

"Volatile memory extraction utility framework"

Dig Into the Heart of Your Machines

- Takes a memory (RAM) dump from every major modern OS as input
- Extracts system state
- Includes process info, registry info, DLLs, networking info, handles, logs, files, syscalls, process trees, open ttys, etc.

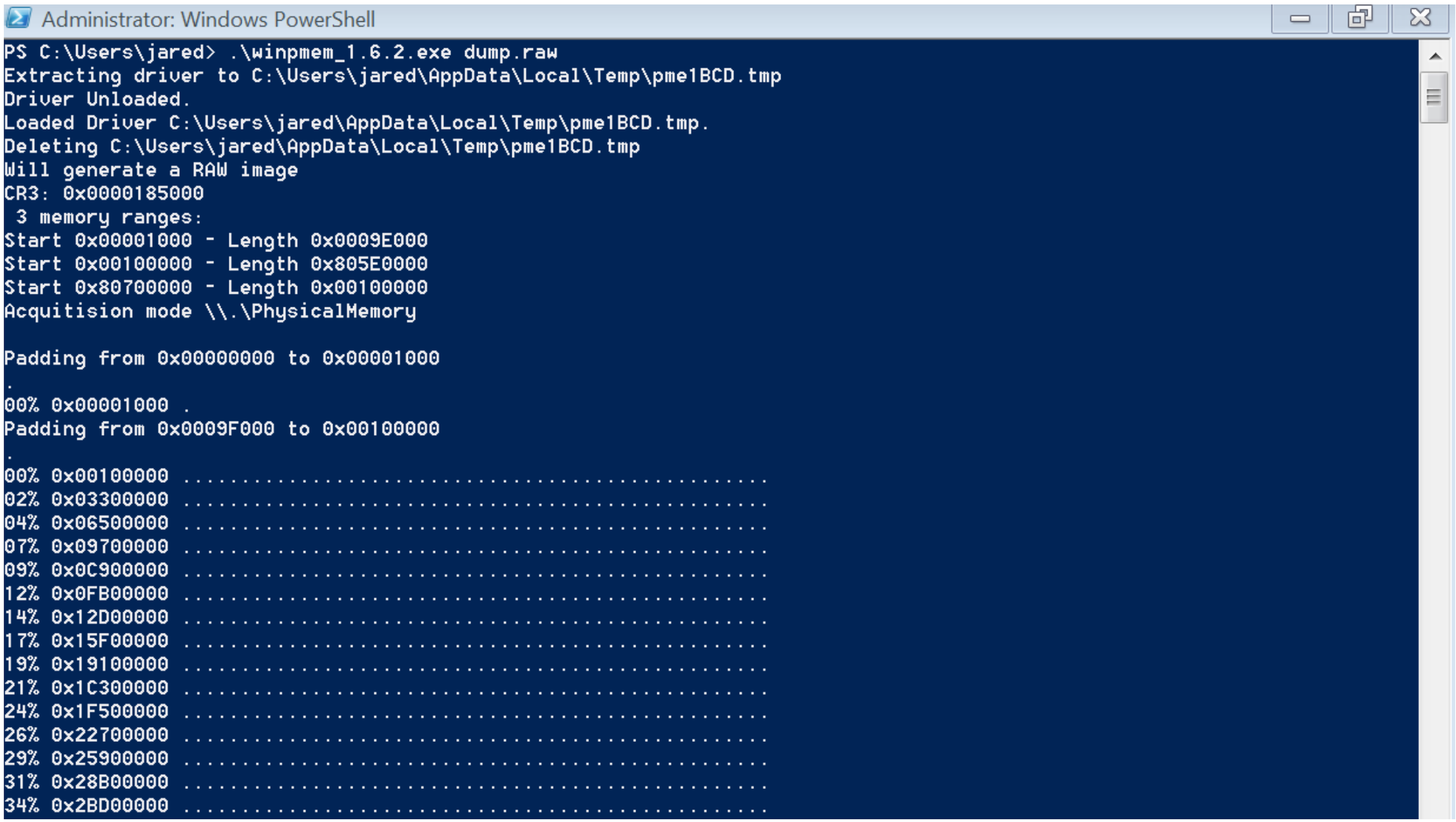
Architecture

- Written in Python, cross-platform (Windows, Mac, Linux)
- Analyze memory images from VM dumps, raw images, specific Virtual Machine providers, and more
- Represents memory images as layers of objects
  - Allows us to analyze VM images just like a regular host image
- Plugin-based architecture for core host analysis

Dependencies

- Python 2.7.x
- Imaging software
  - Pmem Acquisition Suite: **http://www.rekall-forensic.com/docs/Tools/index.html**
- Download: **http://www.volatilityfoundation.org/releases**
- Source Code: **https://github.com/volatilityfoundation/volatility**

Taking an Image



Stuxnet

What was Stuxnet?

- A highly advanced malicious computer worm that caused substantial damage to Iran's nuclear program by destroying nuclear centrifuges
- Targeted SCADA systems in general, but a few major targets with the follow characteristics:
  - Windows machines
  - Windows machines with Siemens control system software
  - Siemens PLC's

What was Stuxnet?

- Utilized 4 non-publicly known critical bugs (zero-days)
- One of the most advanced pieces of malware seen to date as of 2011
- Not domain-specific, could target power plants, factory lines, and other industrial processes

An Aside: Security Tip

Iranian President Mahmoud Ahmadinejad during a tour of centrifuges at Natanz in 2008.
Source: Wired

Security Tip: Don't post potentially sensitive pictures of your work or business online, or you could end up with a bad day down the road.

Analyzing the Aftermath of Stuxnet

@jaredthecoder | Codestock 2017

The Process

1. Get a pre-infected memory sample **(optional, but extremely helpful)**
2. Get a post-infected memory sample.
3. Make sure you have the Volatility binary.
4. Go into CSI Cyber Mode. (analyze the image)

Let’s do it!

Further Analysis of Stuxnet

- https://mnin.blogspot.com/2011/06/examining-stuxnets-footprint-in-memory.htmlm (where much of this analysis came from)
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (Symantec's whitepaper on Stuxnet)
- https://blogs.technet.microsoft.com/markrussinovich/2011/03/26/analyzing-a-stuxnet-infection-with-the-sysinternals-tools-part-1/ (and part 2 and 3)
- https://www.youtube.com/watch?v=zBjmm48zwQU (A talk from one of the people who did a very in-depth analysis of Stuxnet)

What Did We Learn?

Conclusions

- Security incidents can destroy or severely hurt your organization
- Logging, dashboards, and alerts don't always indicate compromises
- You can dive deeper into system state and find artifacts of compromises with tools like Volatility

Thanks!

Jared M. Smith

jaredthecoder.com

jaredthecoder

jaredthecoder

jaredthecoder

jared@jaredthecoder.com