Advanced Topics in Malware Analysis

Dynamic Malware Analysis Tools and Techniques

Brendan Saltaformaggio, PhD

Assistant Professor

School of Electrical and Computer Engineering

Automated Malware Analysis Framework

Georgia Tech

1

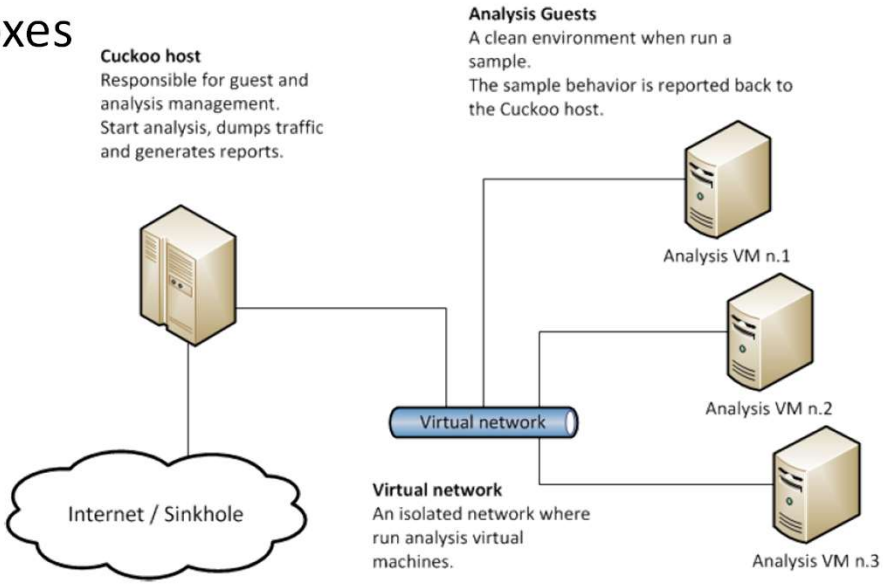
Learning Objectives

- Use **debuggers** to analyze malware executable at runtime
- Monitor and modify an **executable**
- Discuss real world **examples** to detect malware
- Utilize **virtual machines** for dynamic malware analysis

Georgia Tech

2

Sandboxes



Source: http://www.cuckoosandbox.org/

Georgia Tech

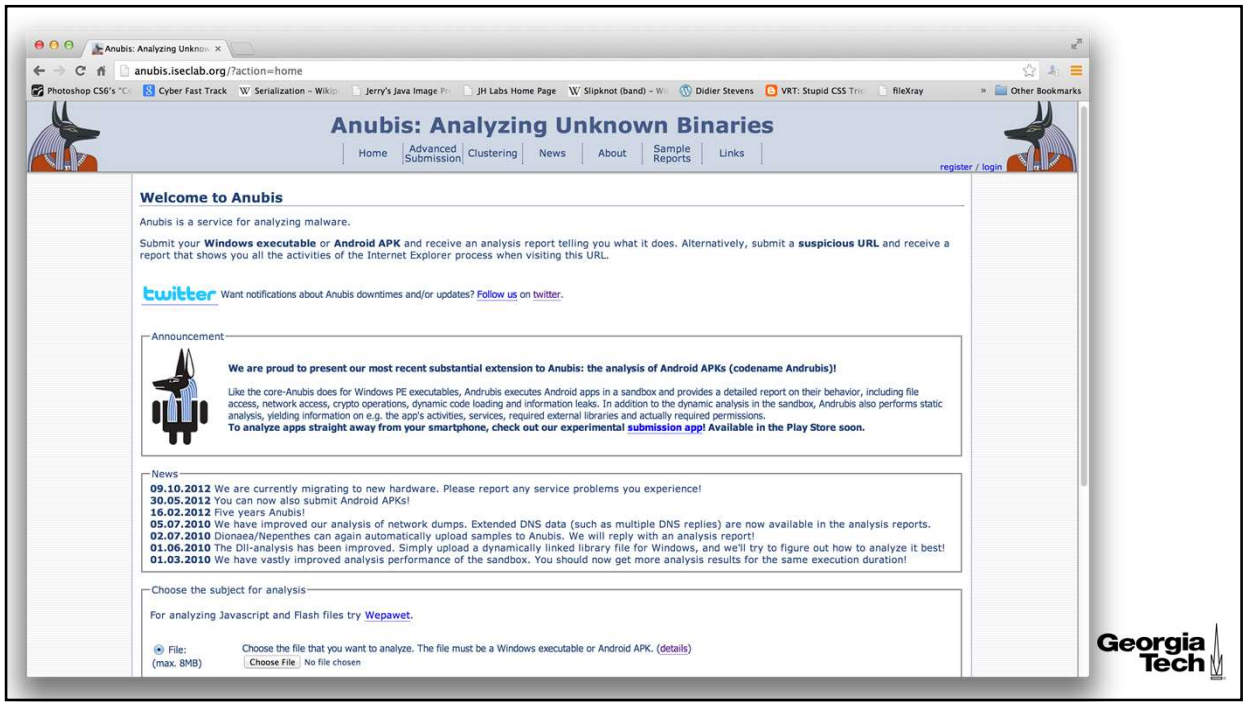
3

Automated Malware Analysis Frameworks

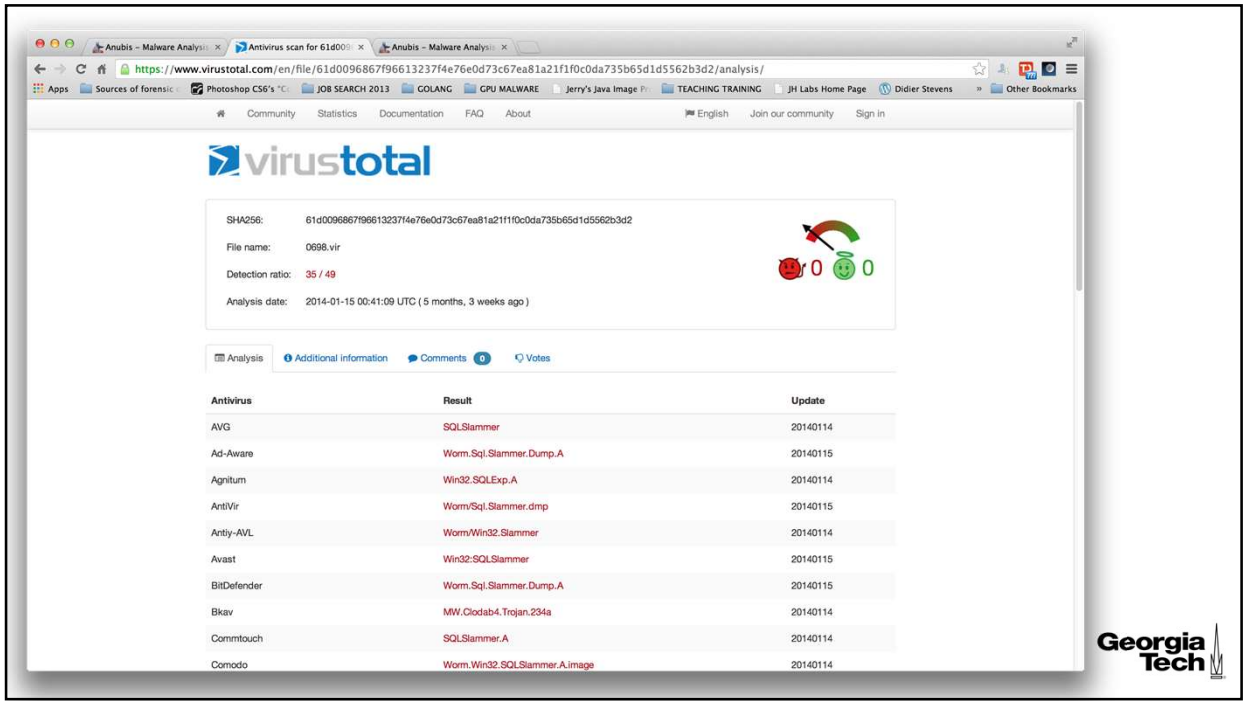
- Not as “deep” as reverse engineering, but can provide much quicker answers!
  - **Anubis (Rest In Peace)**
    - http://anubis.iseclab.org/
    - Analyzes malware and generates PDF reports
    - Now Lastline Inc.
  - **Cuckoo**
    - https://cuckoosandbox.org/
    - Analyzes malware
    - Performs advanced memory analysis
  - **Joe Sandbox Document Analyzer**
    - http://www.document-analyzer.net/
    - PDF, RTF and Microsoft Office files
  - **Malwr**
    - www.malwr.com
    - Executables
  - Visual Threat
    - http://www.visualthreat.com/
    - Android applications
  - **XecScan**
    - http://scan.xecure-lab.com/
    - PDF and Office files
  - Many More …

Georgia Tech

4

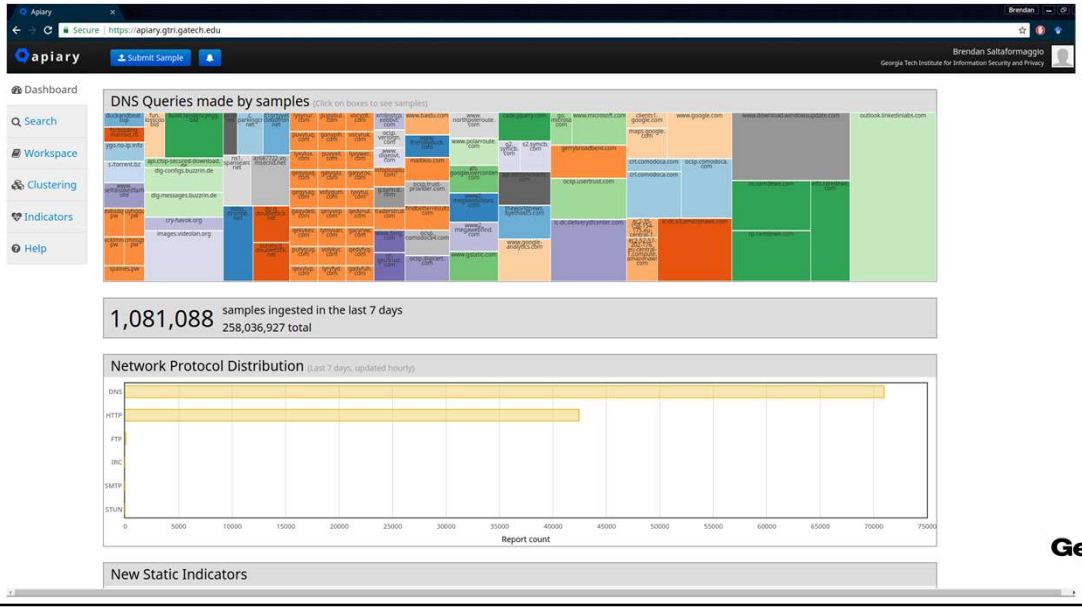

Anubis: Analyzing Unknown Binaries
anubis.iseclab.org/?action=home
Home
Advanced Submission
Clustering
News
About
Sample Reports
Links
register / login
Welcome to Anubis
Anubis is a service for analyzing malware.
Submit your Windows executable or Android APK and receive an analysis report telling you what it does. Alternatively, submit a suspicious URL and receive a report that shows you all the activities of the Internet Explorer process when visiting this URL.
twitter Want notifications about Anubis downtimes and/or updates? Follow us on twitter.
Announcement
We are proud to present our most recent substantial extension to Anubis: the analysis of Android APKs (codename Andrubis)!
Like the core-Anubis does for Windows PE executables, Andrubis executes Android apps in a sandbox and provides a detailed report on their behavior, including file access, network access, crypto operations, dynamic code loading and information leaks. In addition to the dynamic analysis in the sandbox, Andrubis also performs static analysis, yielding information on e.g. the app's activities, services, required external libraries and actually required permissions.
To analyze apps straight away from your smartphone, check out our experimental submission app! Available in the Play Store soon.
News
09.10.2012 We are currently migrating to new hardware. Please report any service problems you experience!
30.05.2012 You can now also submit Android APKs!
16.02.2012 Five years Anubis!
05.07.2010 We have improved our analysis of network dumps. Extended DNS data (such as multiple DNS replies) are now available in the analysis reports.
02.07.2010 Dionaea/Nepenthes can again automatically upload samples to Anubis. We will reply with an analysis report!
01.06.2010 The Dll-analysis has been improved. Simply upload a dynamically linked library file for Windows, and we'll try to figure out how to analyze it best!
01.03.2010 We have vastly improved analysis performance of the sandbox. You should now get more analysis results for the same execution duration!
Choose the subject for analysis
For analyzing Javascript and Flash files try Wepawet.
File: (max. 8MB)
Choose the file that you want to analyze. The file must be a Windows executable or Android APK. (details)
Choose File
No file chosen

5


https://www.virustotal.com/en/file/61d0096867f96613237f4e76e0d73c67ea81a21f1f0c0da735b65d1d5562b3d2/analysis/
Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign in
virustotal
SHA256: 61d0096867f96613237f4e76e0d73c67ea81a21f1f0c0da735b65d1d5562b3d2
File name: 0698.vir
Detection ratio: 35 / 49
Analysis date: 2014-01-15 00:41:09 UTC (5 months, 3 weeks ago)
0 0
Analysis
Additional information
Comments 0
Votes
Antivirus
Result
Update
AVG
SQLSlammer
20140114
Ad-Aware
Worm.Sql.Slammer.Dump.A
20140115
Agnitum
Win32.SQLExp.A
20140114
AntiVir
Worm/Sql.Slammer.dmp
20140115
Antiy-AVL
Worm/Win32.Slammer
20140114
Avast
Win32:SQLSlammer
20140115
BitDefender
Worm.Sql.Slammer.Dump.A
20140115
Bkav
MW.Clodab4.Trojan.234a
20140114
Commtouch
SQLSlammer.A
20140114
Comodo
Worm.Win32.SQLSlammer.A.image
20140114

6

Hometown Hero – APIARY (Run by GTRI)

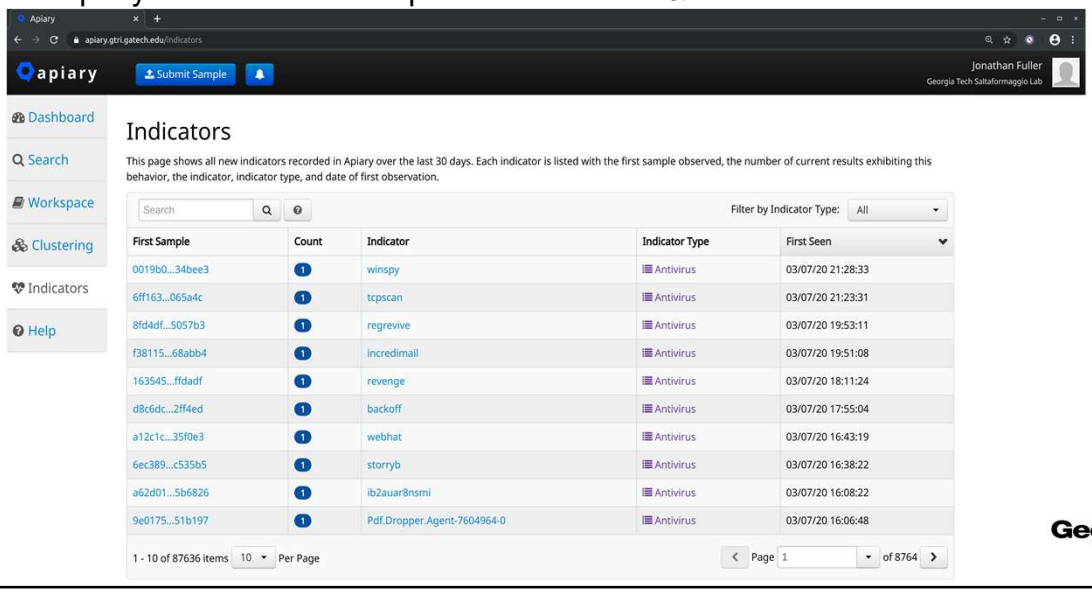


Georgia Tech

7

Indicators

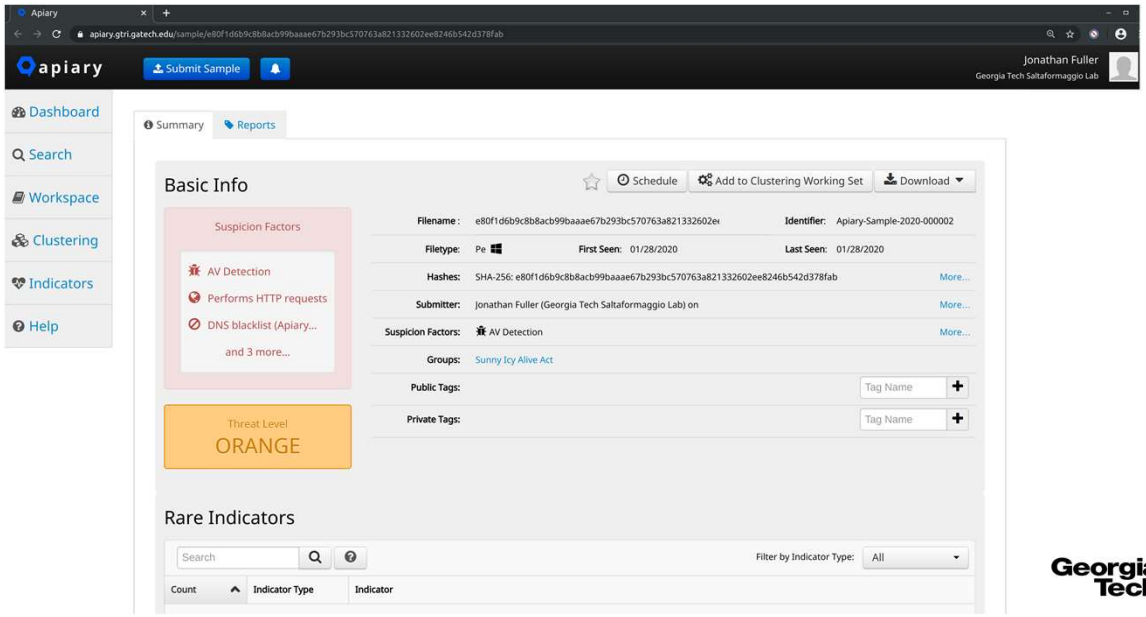
- Apiary runs malware samples in a sandbox & collects “indicators”



Georgia Tech

8

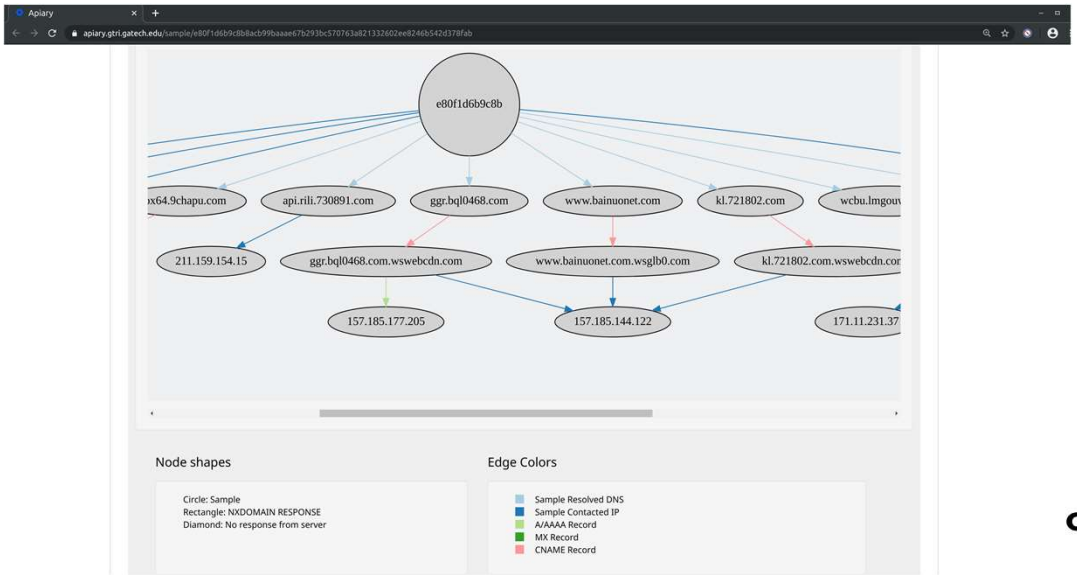
Basic Sample Report



9

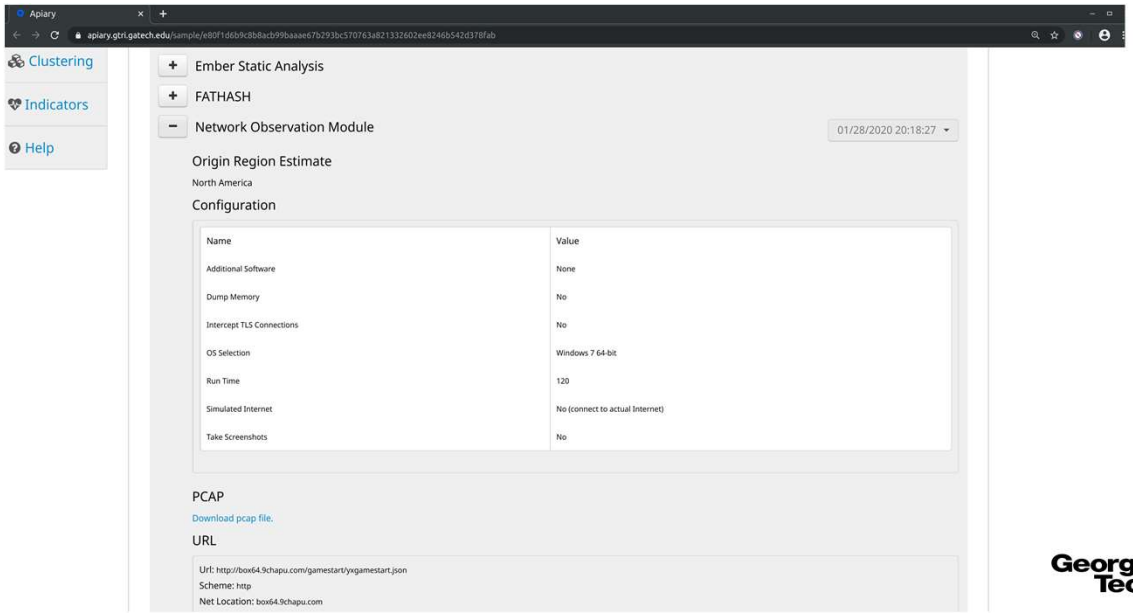
DNS → IP Resolutions!

- What websites & command and control servers does the malware use?



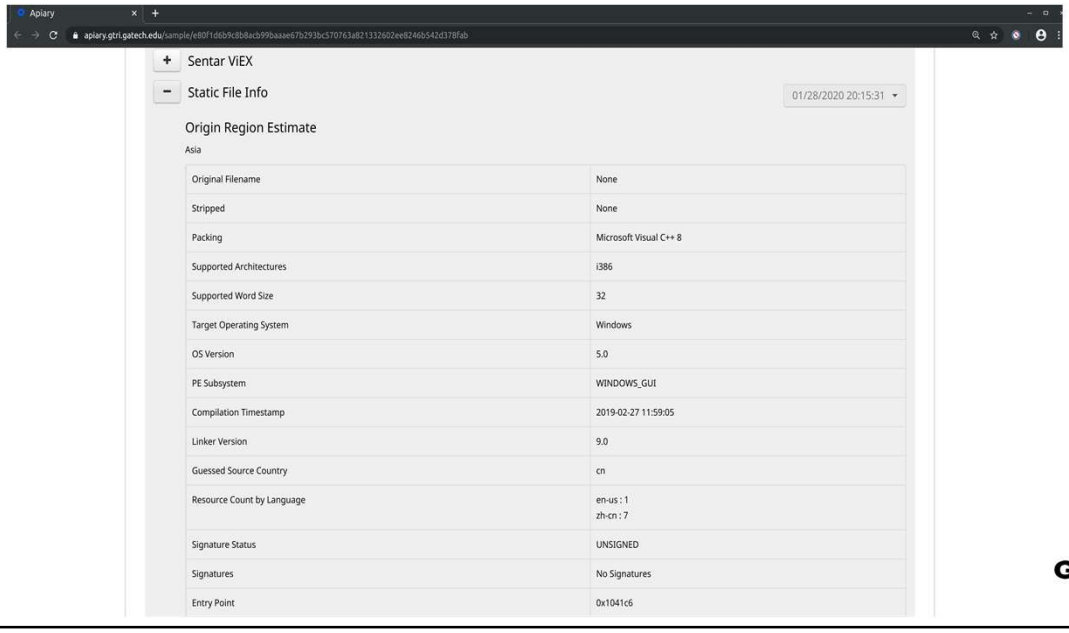
10

Network Observations – region/urls/pcap File



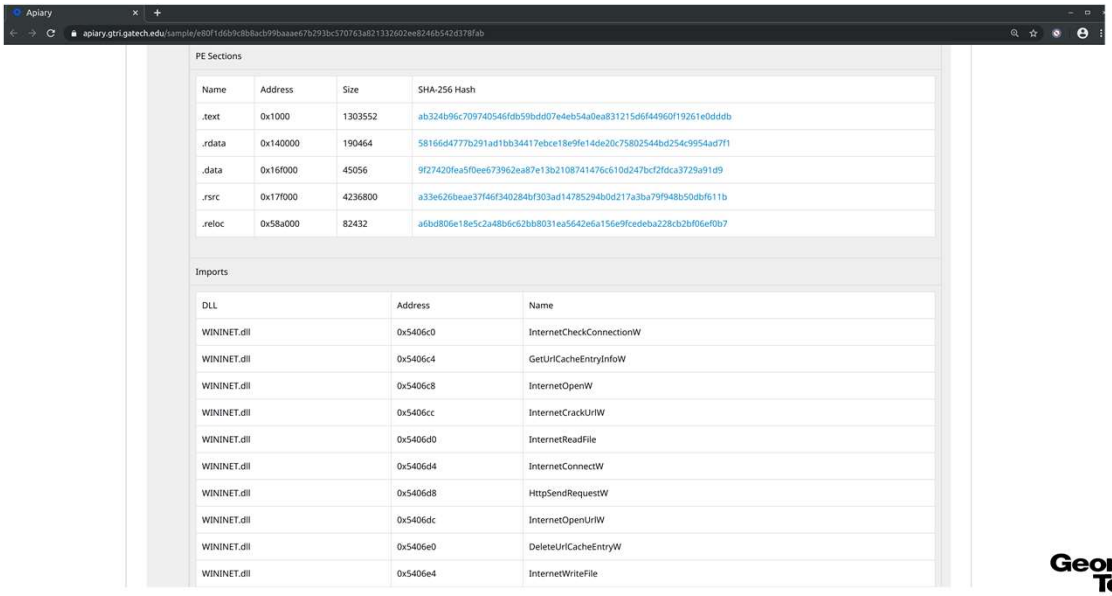
11

Static File Info



12

Executable File Sections & Imports



13

Advanced Topics in Malware Analysis

Dynamic Malware Analysis Tools and Techniques

Brendan Saltaformaggio, PhD

Assistant Professor

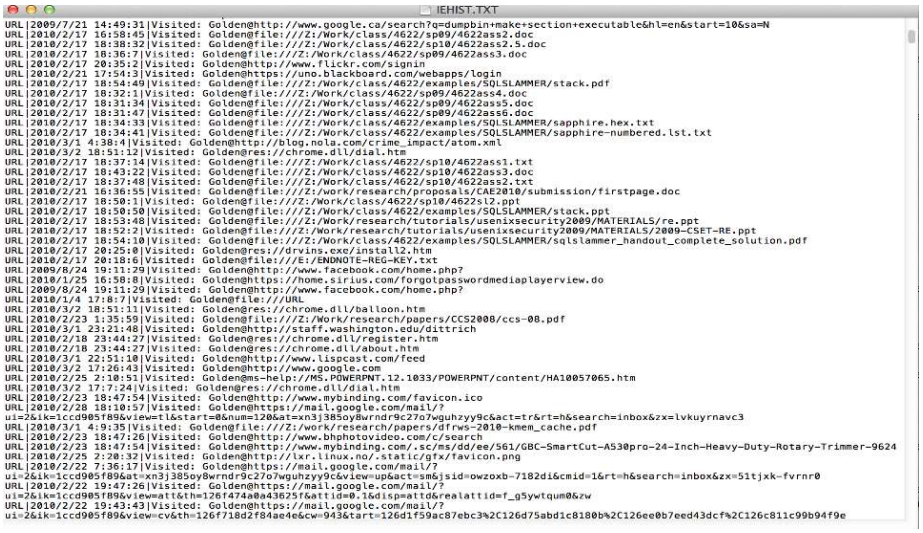
School of Electrical and Computer Engineering

Real World Malware Investigation: Employee “Misconduct”

14

Internet Browser Forensics Case

- The employee sued the company for wrongful termination!



Internet Browser Forensics Case

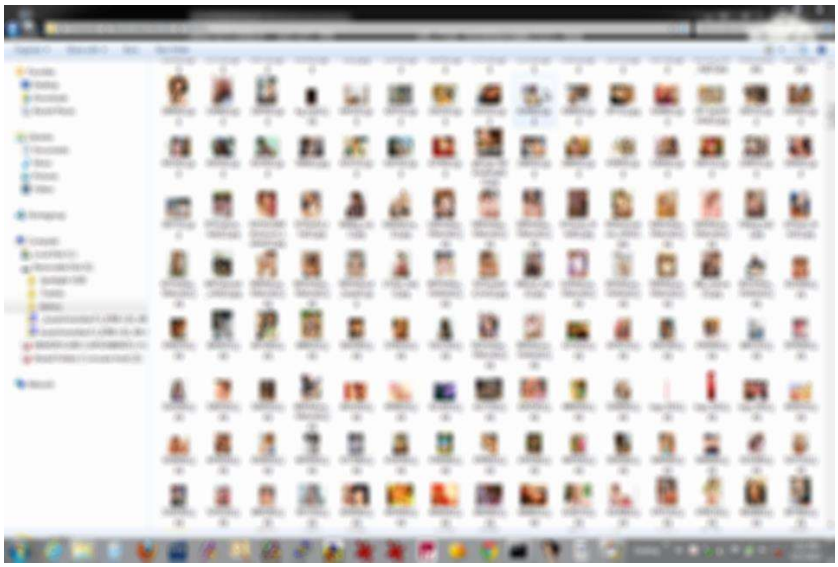
- The employee sued the company for wrongful termination!

!!

URL | Visited: Virginia:http://www.fullXXXmovies.net
URL | Visited:
Virginia@http://www.XXX.org/index.htm?Ha1phuCjWiVsEp01CdmC
URL | Visited: Virginia@http://www.mysweetXXX.com
URL | Visited: Virginia@http://www.XXX.org/index.htm

…
…
…
URL | Visited: Virginia@http://www.XXXswat.com

Things Were *REALLY* Not Looking Good!



Georgia Tech

17

So. Much. Web Activity…

- Internet Explorer browser cache loaded with thousands of “NSFW” images
- Appears that the user spent their entire day doing nothing but downloading porn
- Images are located in precisely the right places to indicate web browsing activity
- Times that images are downloaded correspond to times the user was “working” at the computer

- The employee keeps saying…
- The user didn’t actually download any of the images
- They weren’t even using IE when the images were downloaded

Georgia Tech

18

Heard It All Before: Trojan Defense

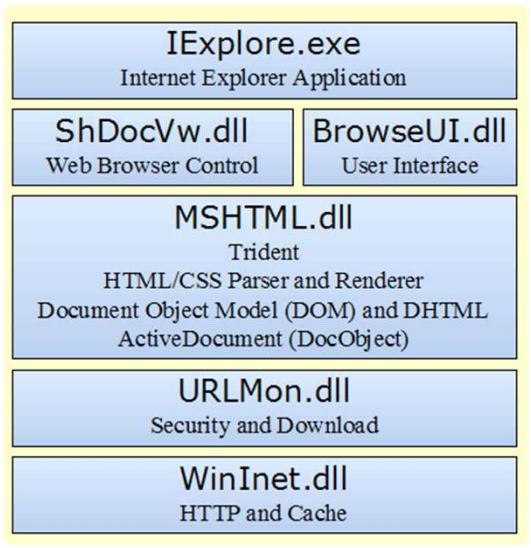
- Of course Trojan defense is popular in, e.g., child porn cases
- "I didn't download that stuff—a virus must have done it"
- Generally, not taken very seriously by button-pushing cyber investigators
- Run antivirus, find nothing, assume user was lying
- Unsophisticated investigators can't really do much more, anyway
- Except…

Georgia Tech

19

IE Architecture

Actually hooked into the Web Browser Control DLL for IE!



Georgia Tech

20

More on Sample

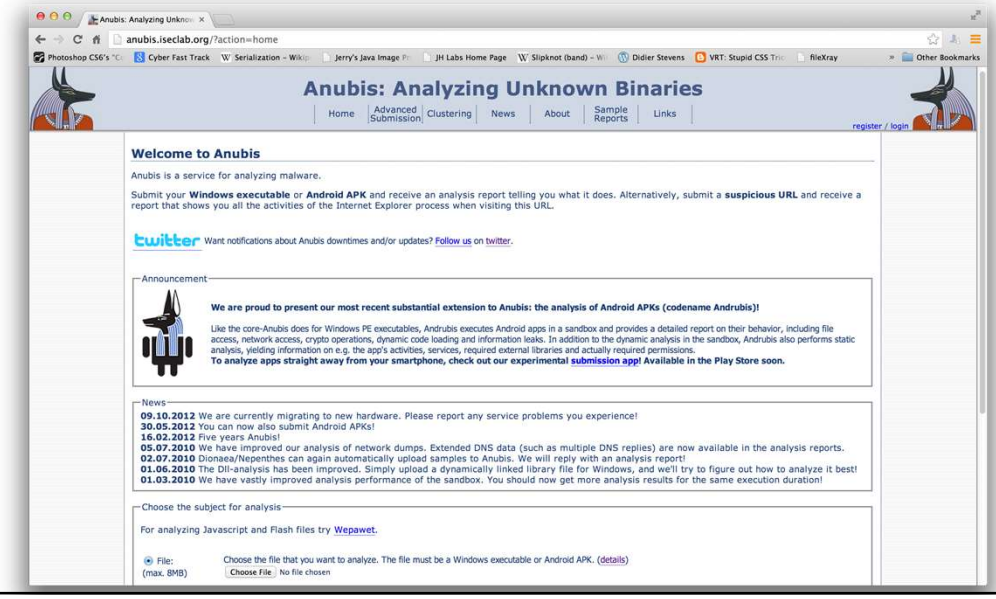
- Appears to be inhibited by process monitors, such as procmon
- Nightmare (ish) to analyze
- Packed with Asprotect (can deal)
- Written in Borland Delphi
  - Can I retire yet?
- Unpacking to date yields to static analysis in IDA
- Dumped binary too broken for DeDe, et al Delphi decompilers… <<BOOM>>

- Anubis Sandbox to the rescue --- Ran the sample, produced logs and a nice report! ☺

Georgia Tech

21

Anubis (RIP) Got The Employee Rehired!



Georgia Tech

22

Advanced Topics in Malware Analysis

Dynamic Malware Analysis Tools and Techniques

Brendan Saltaformaggio, PhD

Assistant Professor

School of Electrical and Computer Engineering

Anti-VM Techniques

Georgia Tech

23

Anti-VM

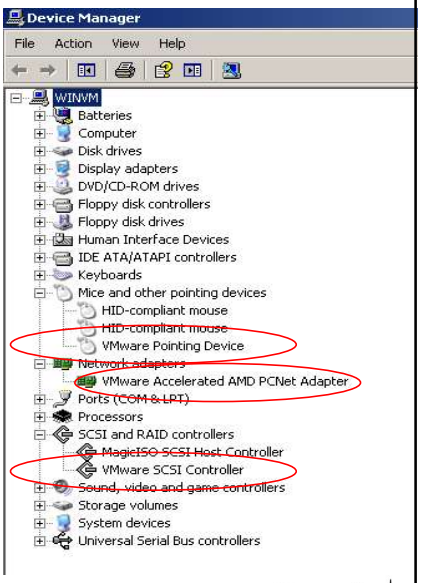
- The Achilles heel of sandboxes!
- Modern malware sometimes contain measures to detect that they are running in a virtual machine, such as VMWare Workstation or Fusion
- Malware may refuse to run or alter behavior if a VM is detected
- Most legitimate applications don't do this, but some, including testing software, may
- The reasons we use VMs for malware analysis are obvious—and we would like to continue using them!

Georgia Tech

24

Anti-VM: Detect VMWare Devices

- VMs provide virtual (i.e. fake) hardware devices
- An easy way to detect that you are in a virtual machine is to detect if your hardware is made by VMWare (or others)!
- VMWare installs network, audio, display drivers
- Network device has MAC address range assigned to VMWare
- Other devices also have unique names and characteristics that are detectable as VMWare-installed



25

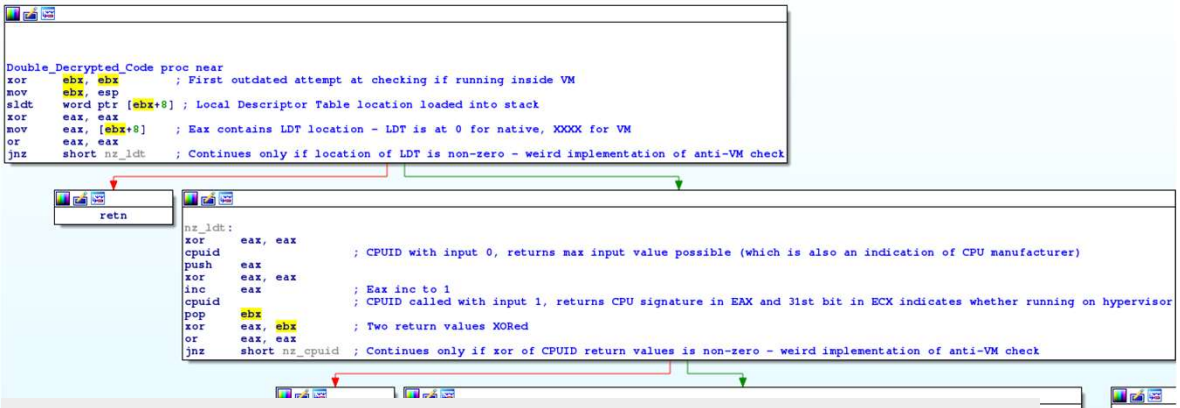
Anti-VM: Detect Artifacts

- All VMs do this, but we will use VMWare as an example
- VMWare places entries in the Windows registry
- Particularly true if VMWare Tools are installed
  - VMWare Tools provides enhanced capabilities such as shared folders, etc.
  - But requires software installed in the guest to do that!
- Malware can scan the system's memory to reveal matches on "vmware"
  - Many will exist!
- The IDT is in a different place in VMWare Guest than on bare hardware
- Many many more…

26

HARULF: Dual Anti-VM Checks

Value of the LDT Register is 0 for Windows. Here, it continues execution when non-zero (https://hunted.codes/writeups/challenges/practical-malware-analysis/practical-malware-analysis-lab-17-1/)



Only checks if return values of two CPUID calls XORed is non-zero. More advance checks like checking 31st bit of ecx when cpuid called with eax=1, is not performed. (https://en.wikipedia.org/wiki/CPUID#EAX.3D0:_Highest_Function_Parameter)

Georgia Tech

27

Red Pill … The Matrix?

- Detect you are in VM using (almost) one CPU Instruction

SIDT ADDR RET

```
int swallow_redpill () {
  unsigned char m[2+4], rpill[] = "\x0f\x01\x0d\x00\x00\x00\x00\xc3";
  *((unsigned*)&rpill[3]) = (unsigned)m;
  ((void(*)())&rpill)();
  return (m[5]>0xd0) ? 1 : 0; // 1 == VM
}
```

- SIDT instruction (0F010D [addr]) stores the IDT register (IDTR) value in the destination operand (memory location)
- Credit: Joanna Rutkowska, founder of Invisible Things Lab
- Read more:
  - **'Red Pill… Or How To Detect VMM Using (Almost) One CPU Instruction'**at http://www.securiteam.com/securityreviews/6Z00H20BQS.html

Georgia Tech

28

Anti-VM: Detect (More) Artifacts

- Similar to the Red Pill, GDT and LDT are also vulnerable
- Access locations of Global Descriptor Table and Local Descriptor Table with:
  - SGDT <addr>
  - SLDT <addr>
- ScoopyNG by Tobias Klein integrates a bunch of these types of tests with an additional one: host <-> guest communication channel detection
- Check out:
  - http://www.trapkit.de/tools/scoopyng/
  - https://community.rsa.com/community/products/netwitness/blog/2012/08/22/vm-detection-by-in-the-wild-malware
- Guest channel detection has become the most popular VM detection technique

Georgia Tech

29

Anti-VM: Detect Host <-> Guest Communication Channel

- **Step 1**: Try to communicate with the VMWare host

```
unsigned int a, b;
__try {
    __asm {
        …
        mov eax, 'VMXh'  // VMware magic value (0x564D5868)
        mov ecx, 0Ah     // special version cmd (0x0a)
        mov dx, 'VX'     // special VMware I/O port (0x5658)
        in eax, dx          // special I/O cmd
        mov a, ebx          // store data received
        mov b, ecx          // store data received
        …
    }
} __except (EXCEPTION_EXECUTE_HANDLER) {}
```

Georgia Tech

30

Anti-VM: Detect Host <-> Guest Communication Channel

- **Step 2**: Check if they answered

```
if (a == 'VMXh') {      // Did VMWare answer?
       printf ("Result  : VMware detected\nVersion : ");
       if (b == 1)
          printf ("Express\n\n");
       else if (b == 2)
          printf ("ESX\n\n");
       else if (b == 3)
          printf ("GSX\n\n");
       else if (b == 4)
          printf ("Workstation\n\n");
       else
          printf ("unknown version\n\n");
}
else
   printf ("Result  : Native OS\n\n");
```

Georgia Tech

31

Defeating Anti-VM Techniques

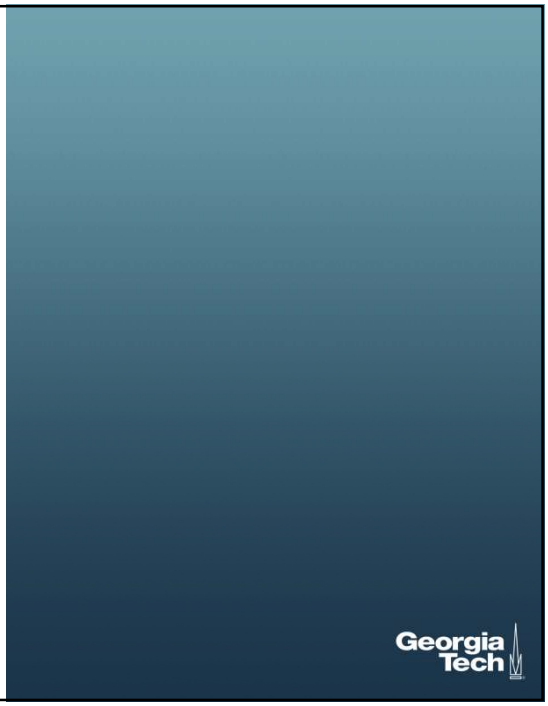
- For Anti-VM malware, there are some undocumented VMWare features that prevent **some** detection, not all!
- Unfortunate side-effect is that many VMWare features (including shared folders, clipboard stuff, etc.) are broken
- Recommended read:
  - Carpenter, M., Liston, T., & Skoudis, E. (2007). Hiding Virtualization from Attackers and Malware. *IEEE Security & Privacy Magazine*, *5*(3), 62–65. doi: 10.1109/msp.2007.63
- Some extreme attempts:
  - Patch VMWare binary to change magic number for communication
  - Write a custom virtual machine manager (if it gets popular, malware will detect it!)
  - VMMutate mentioned in the above paper seems to take a brute force approach, simply changing magic number values everywhere

Georgia Tech

32

Lesson Summary

- Utilize virtual machines for dynamic malware analysis
- Discuss real world examples to detect malware



33