Arthur Liou
CS373

Week 3 Writeup

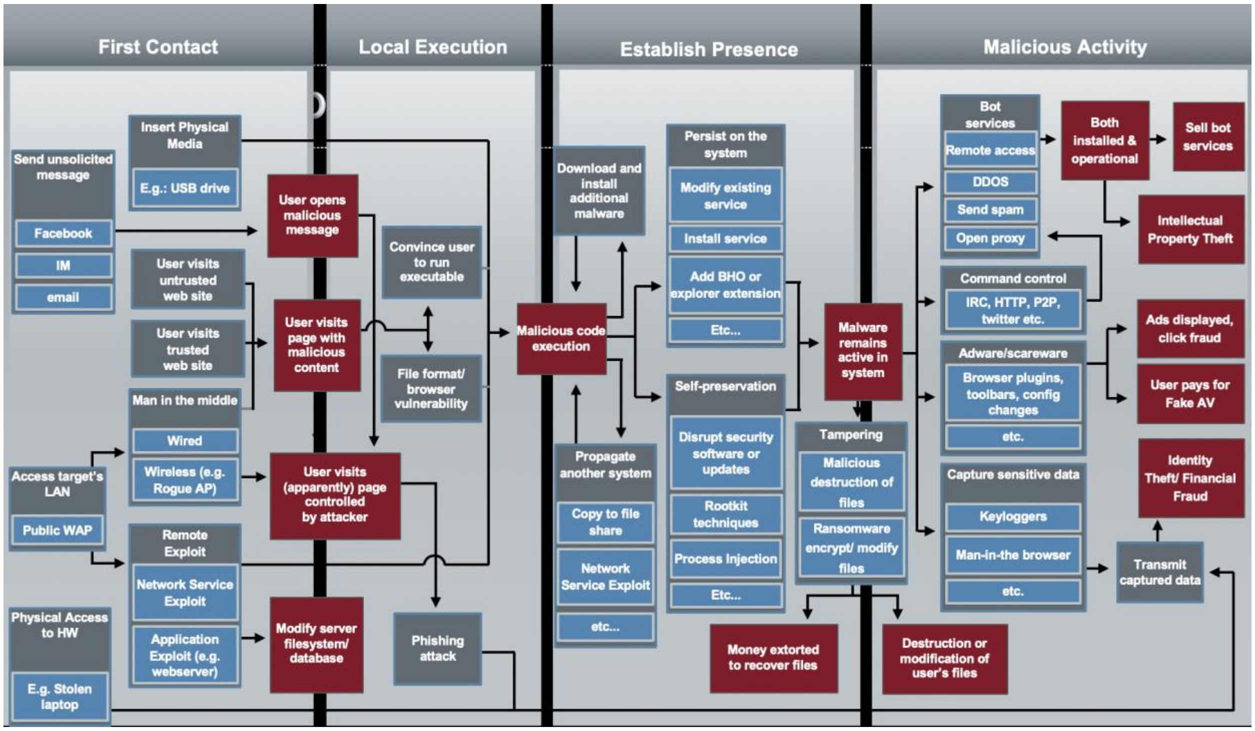
Prompt: Submitting a write-up of your thoughts, impressions, and any conclusions based on the material from the week. Each week will have its own assignment in the grades page.

For this week's writeup, I'm reflecting on the lectures content that we had over the two lessons (and multiple videos per lesson). This week, we went over Malware Defense and went through the YARA and Cuckoo labs. We also reviewed an attach graph in the first lesson that illustrate the typical breakdown of the procedural steps malware takes when it attacks. I found the idea of these steps to be straightforward and it made sense / nothing really surprised me. While informative, the YARA Lab pales in comparison to the Cuckoo lab, due to the process of automation and scale, which was covered in the beginning part of the second lesson. I also found the visuals of the procedures very useful, and I added those in my notes below.

Lecture Notes

Malware Defenses Lesson 1

- Goal this week: Gain an understanding and experience in the role of a malware researcher, primarily from Windows host-based protection.
- This is an attack graph that represents the vast majority of malware attacks on a user/system. We're going to break down the sections such that by the end of the class, you'll have a good mid-to-high level of understanding.
  - Execute code on the system
  - Blend in or Hide
  - Persist
  - Harvest information
  - Phone home


First Contact
Local Execution
Establish Presence
Malicious Activity
Send unsolicited message
Facebook
IM
email
Insert Physical Media
E.g.: USB drive
User visits untrusted web site
User visits trusted web site
Man in the middle
Wired
Wireless (e.g. Rogue AP)
Access target's LAN
Public WAP
Remote Exploit
Network Service Exploit
Application Exploit (e.g. webserver)
Physical Access to HW
E.g. Stolen laptop
User opens malicious message
User visits page with malicious content
User visits (apparently) page controlled by attacker
Modify server filesystem/ database
Convince user to run executable
File format/ browser vulnerability
Phishing attack
Malicious code execution
Download and install additional malware
Propagate another system
Copy to file share
Network Service Exploit
etc...
Persist on the system
Modify existing service
Install service
Add BHO or explorer extension
Etc...
Self-preservation
Disrupt security software or updates
Rootkit techniques
Process Injection
Etc...
Tampering
Malicious destruction of files
Ransomware encrypt/ modify files
Malware remains active in system
Money extorted to recover files
Destruction or modification of user's files
Bot services
Remote access
DDOS
Send spam
Open proxy
Command control
IRC, HTTP, P2P, twitter etc.
Adware/scareware
Browser plugins, toolbars, config changes
etc.
Capture sensitive data
Keyloggers
Man-in-the browser
etc.
Both installed & operational
Sell bot services
Intellectual Property Theft
Ads displayed, click fraud
User pays for Fake AV
Identity Theft/ Financial Fraud
Transmit captured data

- Add some channels here: email, IM, compromised sites & servers, malvertising, physical access (USB), etc
    - Social engineering: Social networks, IM, Email,
    - Exploitation: Watering hole attacks, malvertising, physical access
    - Combination: Poisoned search results,
    - Physical access:
    - Social engineering: Users knowingly run executable (copy cat apps)
    - Exploitation: Browser-based exploit kits (script, pdf, java)
    - Abusing features: USB Autorun, physical access,
- Establish presence Slide – Persist – System Startup, Windows Startup, Application Startup, Other such as scheduled tasks.
- Proxy Auto Config - http://securelist.com/blog/virus-watch/29680/benign-feature-malicious-use/
- Run Keys - https://www.virusbtn.com/virusbulletin/archive/2014/03/vb201403-Simbot#id3507994
- Local Execution – Harvest information – enumerate (pw, docs, emails, processes)
- Hook (browser, keylog, screenscrap), Parse (pw, CC), Logs, Phone home, web, email
- First Contact
    - Spam: Anti-spam
    - Network: Firewall, Network IPS
    - Web: IP, Domain, & URL reputation
    - Physical access: Disk encryption
- Local Execution
    - Spam: Client-side content filtering
    - Network: Network IPS

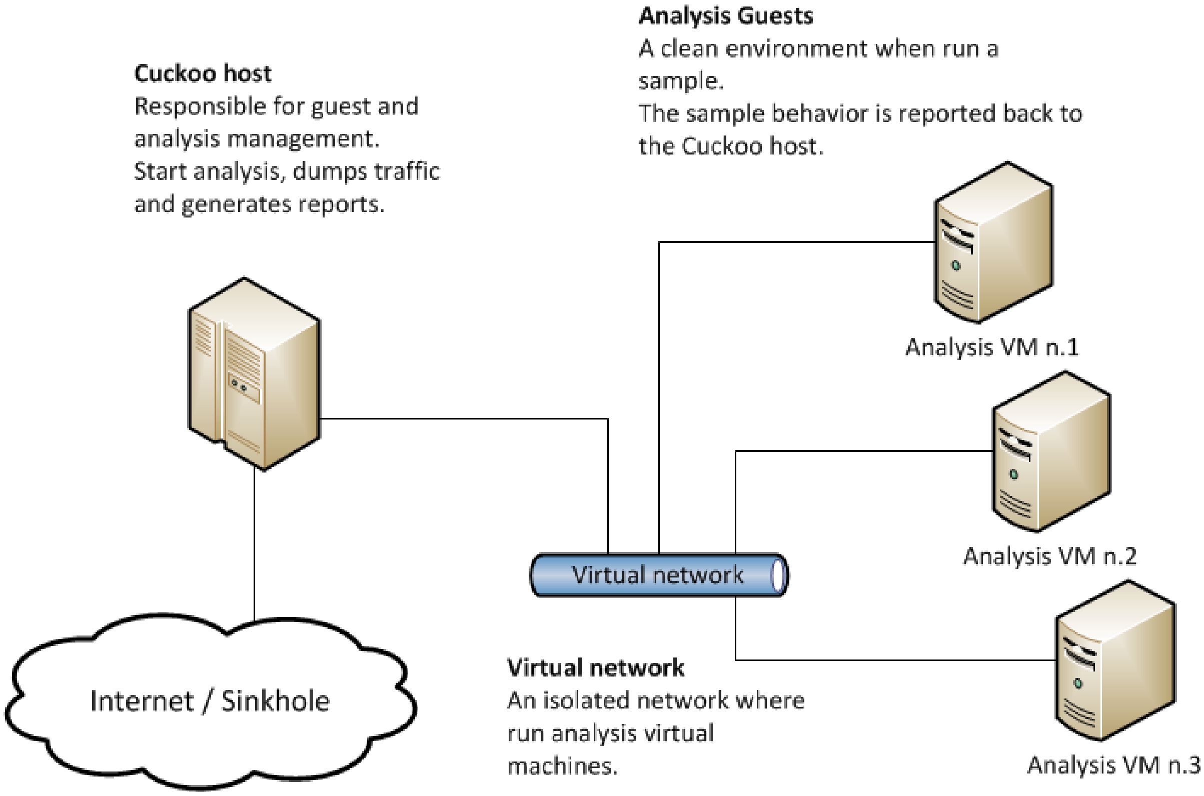
  - Web: Content filtering/scanning
  - Host: Host IPS, Anti-virus, Whitelisting
- <u>Establish Presence</u>
  - Host: Anti-virus, Whitelisting, HIPS
  - Network: Firewall, Network IPS
  - Web: IP, Domain, & URL reputation
- <u>Malicious Activity</u>
  - Host: Anti-virus
  - Network: NIPS, Firewall
  - Web: IP, Domain, URL rep & content filtering
  - Data Loss Prevention
- Malware Def – Popular Tech – Network Firewall, Network Intrusion Prevention, Message Reputation, Network Reputation, Web Reputation, Host Firewall, Host IPS, Access Control, Anti-malware
- Content Engines interpret Content Rules, that define what is good or bad
- EndPoint Dependencies – Management Server, Point Product, Scanner Core, Engine, Content
- Anti-malware features: Traditional File Scanning (OAS, ODS), Registry & Cookies, Cloud scanning, Memory Scanning, Scripts, Heuristics, Decomposition, Configuration: Exclusions, Sensitivity, Reporting, etc
- YARA - The pattern matching Swiss knife for malware researchers
  - String expression, byte patterns,
- LAB / Code.google YARA Broswer - Using Yara to Author Static File Signatures
- Find commonalities, discuss what's strong and what's weak
- Maybe have a group of samples that require a memory dump to find the commonalities
- Sample Group 1: Straight-forward executable
- Syto has a mix of packed and not packed samples
- rule Generated_Rules
- {
- meta:
- author="Generated by Yara-Editor"
- comment="Yara Editor"
-
- strings:
- $str40="Jenna Jam"
- $str27="AikaQ"
- condition:
- all of them
- }
- Find commonalities, discuss what's strong and what's weak
- Maybe have a group of samples that require a memory dump to find the commonalities
- Sample Group 2: Obfuscated executables
- CVE-2008-2551

- rule Generated_Rules
- {
-    meta:
-       author="Generated by Yara-Editor"
-       comment="Yara Editor"
-
-    strings:
-       $str1="DownloaderActiveX"
-       $str2={63 31 62 37 65 35 33 32 [1-3] 33 65 63 62 [1-3] 34 65 39 65 [1-3] 62 62 33 61 [1-3] 32 39 35 31 66 66 65 36 37 63 36 31}
-    condition:
-       all of them
- }
- Find commonalities, discuss what's strong and what's weak
- Maybe have a group of samples that require a memory dump to find the commonalities
- Sample Group 3: Variants of encrypted scripts
-       Tuguu
- rule Generated_Rules
- {
-    meta:
-       author="Generated by Yara-Editor"
-       comment="Yara Editor"
-
-    strings:
-       $str1="existeClavePropiaAVG"
-       $str2={15 E4 96 38 3F 5A 03 96 A7 AD 86 D8 58 50 D5 BB}
-       $str3="TuguuAdw"
-    condition:
-       $str1 or $str2 or $str3
- }
- Does cb6f45f8f4d8d34f02dfb4a6b359db39807b68005e89d52f29a4991bead92ae5 belong?

Malware Defenses Lesson 2

- Over half-a-million new and unique malicious binaries discovered each day
- Deep analysis is not possible for the vast majority of threats, need automation.
- Advantages of anti-malware automation?
  - Scale
  - Consistency
  - Performance less of a concern (paranoid heuristics)
- Disadvantages?
  - Out of context

    - Prone to evasion
    - Potentially prone to probing and DoS attacks
- cuckoo automated analysis
    - Source: http://docs.cuckoosandbox.org/en/latest/introduction/what/
    - Cuckoo is an automated malware analysis system: a tool that allows you to understand what a given file does when executed inside an isolated environment.
    - Bypass sleep bombs by intelligently skipping sleeps
    - Emulate user interaction by moving mouse and pushing buttons
    - Randomizes the system clock with each run
    - Uses a randomly named cuckoomon.dll


Analysis Guests
A clean environment when run a sample.
The sample behavior is reported back to the Cuckoo host.
Cuckoo host
Responsible for guest and analysis management.
Start analysis, dumps traffic and generates reports.
Analysis VM n.1
Analysis VM n.2
Virtual network
Analysis VM n.3
Internet / Sinkhole
Virtual network
An isolated network where run analysis virtual machines.

- Cuckoo Design
- Source: http://docs.cuckoosandbox.org/en/latest/introduction/what/
- Cuckoo Replication in VM
- Malware Analysis aims to:
    - Discover if a threat is present
    - Isolate, Classify, and Remediate the malicious code
    - Defend against future attacks
    - Describe the attack
- Lab – Putting It All Together - altogether