CMSC 426
Principles of Computer Security

Introduction to Malware

Last Class We Covered

- Defenses against stack overflow attacks
  - ASLR
  - Stack canaries
  - Preventing stack execution

- Buffer overflow variations
  - return-to-libc
  - Return-oriented programming

Any Questions from Last Time?

Today's Topics

- Malware
- Threat actors
  - APT groups and others
- Attribution
- Threat actor examples

Why Hack Systems?

- Stack overflow attacks can let us gain control of a system (among other things), but what do you do with them?

- What is the end goal?
  - Notoriety
  - Money
  - LOTS of money
  - Political influence

Malware

- Short for “malicious software”
  - May attack applications, editors/compilers, or kernel level
  - Often delivered through compromised websites or spam emails

- May be silent, logging keystrokes (*e.g.*, passwords)
- May be annoying, constantly popping up advertisements
- May be disruptive, disallowing use of certain programs or parts of the system
- May be exploitative, using cycles or sending mass emails

Threat Actors

"Script Kiddies"

- Largely unskilled
  - Not necessarily young, despite the name
- Use scripts and code created by others

- Often vandalize websites or attack systems and networks
  - Sometimes assumed to not know/understand the consequences

- End goal is street cred, sense of superiority, petty crime

APT Groups

- Advanced
  - Use a wide variety of tactics (including custom malware) specifically chosen for the target
- Persistent
  - Attacks may happen over an extended period against a chosen target, maximizing the chance of success
- Threat
  - Focus on a specific target by experienced, well-funded attackers
  - Often actively involved, instead of simply using automated tools

More on APT Groups

- APT groups are often funded by a specific country
  - Countries do not normally admit to this
  - Makes more sense to keep details and information secret
    - “Effective” security through obscurity
    - (Really, just temporary)

- End goal varies based on the target
  - Information, influence, money, large amounts of personal data

Cybercriminals

- Higher skill level than script kiddies, less organized and well-funded than APT groups
  - Essentially anything that's not the other two
- May work alone or in groups
- End goal is generally money
  - Either directly (scams, hacking financial institutions) or indirectly (planting ransomware, selling access to created botnets)

Attempting Attribution

TTP (Tactics, Techniques, and Procedures)

- Analyzing the information on how attacks are managed and accomplished to try to identify the group(s) responsible

- Some examples of TTPs:
  - What were the tactics/techniques are used in the attack?
  - How was information gathered prior to attack being carried out?
  - How was the payload delivered?
  - What was the timeline for the attack?
  - What was the target's type?

IOC (Indicators of Compromise)

- Using evidence left behind to identify the group(s) responsible

- Examples:
  - Exact malware used by group (might have been seen before)
  - Infrastructure used for attack
    - IP addresses, domain names, etc.
  - URLs/domain names of botnet Command & Control servers
  - Metadata about the above

Difficulties of Attribution

- Even with this information, can be difficult to attribute attacks
  - Evidence is often ambiguous, or even contradictory
  - Who the target can also be a factor in attribution

- Possibility of false attribution can also be a problem
  - Some groups deliberately leave “fingerprints” after their attack
    - These fingerprints may be deliberate false flags
  - If incorrect, groups may offer evidence to the contrary
    - “Fake news”

Threat Actor Examples

APT 1 ("Comment Crew")

- Exposed in 2013 as being formed of a military group from China
  - People's Liberation Army Unit 61398
- Has stolen massive amounts of data from organizations
  - Hundreds of terabytes
  - Data includes blueprints, proprietary processes, and contact lists
  - Focus on English-speaking countries
- Maintain access to systems for nearly a year on average, continually revisiting and stealing additional data

Information taken from https://www.fireeye.com/current-threats/apt-groups.html

APT 28 ("Fancy Bear")

- Likely associated with the Russian government
  - US Special Counsel believes it is two GRU units
  - GRU is Russia's military intelligence agency

- Partially responsible for the DNC hack in early 2016
- Also attacked 2017 elections in France and Germany

- Main goal seems to be political influence

Information taken from https://www.fireeye.com/current-threats/apt-groups.html and https://en.wikipedia.org/wiki/Fancy_Bear

Daily Security Tidbit

- Yesterday, the creators of the Mirai botnet were sentenced to probation (instead of jail time)
  - Provided “extraordinary cooperation” with the government
- Mirai infects and takes over things like routers and DVRs
  - Then uses them in large-scale botnet attacks like DDoS
  - Creators rented out “slices” of the botnet to other cybercriminals
- Released the code in an attempt to obscure their authorship
  - Copied by others, and used to cause even more damage

Information taken from https://krebsonsecurity.com/2018/09/mirai-botnet-authors-avoid-jail-time/

Announcements

- Lab 1 and Paper 1 are out on Blackboard now
  - Both are due at midnight on Wednesday, September 26th
  - Paper must be completed in groups of 2 or 3 (no singles)

- Website is up-to-date on lectures and code
  - Still working on the schedule