ShockWorm - A shellshock-based worm

Mathieu Valois - M1 Informatique

Université de Caen Basse-Normandie

April 22, 2015

What the hell are worms ?

What the hell are worms ?

- Self-replicating programs
- Different than viruses : worms don't use host programs, they stand alone
- Use security holes to move from machine to machine
- Can be peaceful or aggressive
- Travel incredibly faster than viruses because they don't need any user interaction

The point of my project

The point of my project

- The goal is to program a worm, possibly one that doesn't already exist, that can replicate over multiple machines
- I'm free to chose which security hole I would like it to exploit
- Then inject the worm in a secured bunch of connected computers that are vulnerable (some might not be) for testing

The vulnerability: ShellShock

The vulnerability: ShellShock

The shellshock is:

- A bash vulnerability
- Introduced in bash code in 1989 (according to the bash main developer, Brian Fox) and discovered in September 2014 (I'll let you guess how long it went undiscovered)
- Since bash is massively used on all UNIX systems, ShellShock was present on a lot of machines, from servers to embedded devices and even IP cameras

What can my worm do ?

What can my worm do ?

For now, ShellWorm is fitted with these abilities:

- Moving from an infected (or starting) machine to a new one that is vulnerable (infection)
- Can be started at boot without root permissions
- Can intercept users passwords by overriding the "sudo" command

What's next ?

What's next ?

- Persist on reboots with root access, to ensure not to be killed or to be able to hide, for example from scanning processes
- Spy on the system, to get users information and eventually send it to a remote server

Questions ?

Why did I chose this project ?

- I've read interesting books on the subject
- The moment ShellShock was discovered matched the moment where we had to chose a project
- No really other interesting E-Secure projects were announced