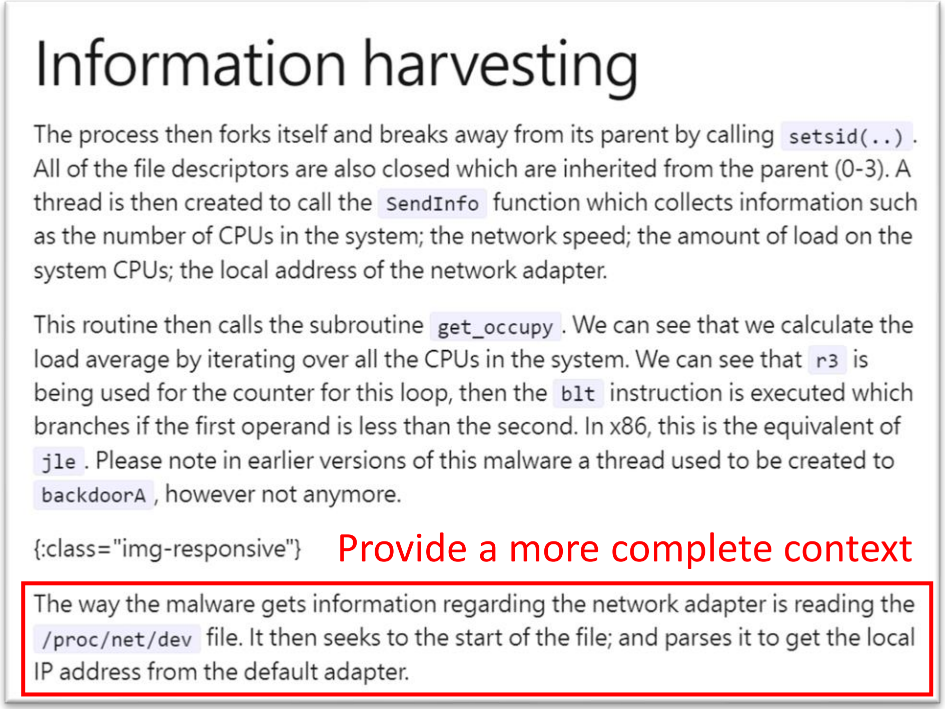
Analysis Report



Information harvesting

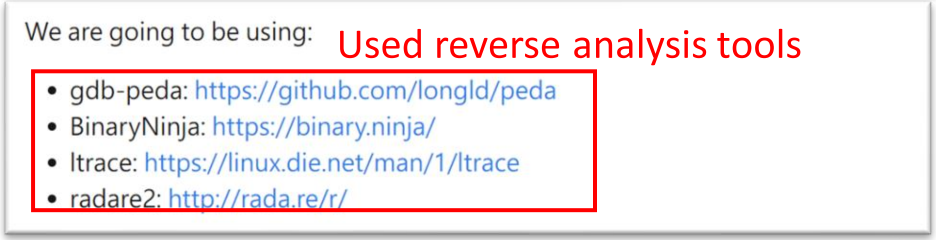
The process then forks itself and breaks away from its parent by calling `setsid(..)`. All of the file descriptors are also closed which are inherited from the parent (0-3). A thread is then created to call the `SendInfo` function which collects information such as the number of CPUs in the system; the network speed; the amount of load on the system CPUs; the local address of the network adapter.

This routine then calls the subroutine `get_occupy`. We can see that we calculate the load average by iterating over all the CPUs in the system. We can see that `r3` is being used for the counter for this loop, then the `blt` instruction is executed which branches if the first operand is less than the second. In x86, this is the equivalent of `jle`. Please note in earlier versions of this malware a thread used to be created to `backdoorA`, however not anymore.

{:class="img-responsive"}

Provide a more complete context

The way the malware gets information regarding the network adapter is reading the `/proc/net/dev` file. It then seeks to the start of the file; and parses it to get the local IP address from the default adapter.

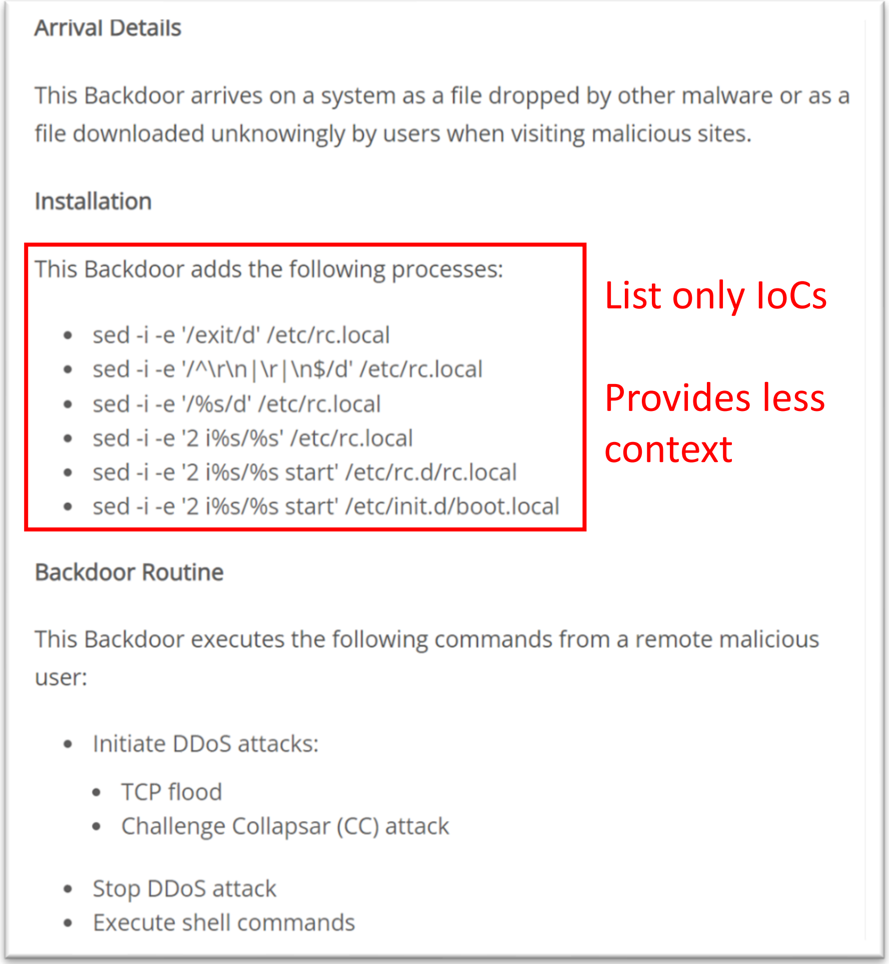


We are going to be using:

Used reverse analysis tools

- gdb-peda: https://github.com/longld/peda
- BinaryNinja: https://binary.ninja/
- ltrace: https://linux.die.net/man/1/ltrace
- radare2: http://rada.re/r/

Technical Report



Arrival Details

This Backdoor arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

Installation

This Backdoor adds the following processes:

- sed -i -e '/exit/d' /etc/rc.local
- sed -i -e '/^\r\n|\r|\n$/d' /etc/rc.local
- sed -i -e '/%s/d' /etc/rc.local
- sed -i -e '2 i%s/%s' /etc/rc.local
- sed -i -e '2 i%s/%s start' /etc/rc.d/rc.local
- sed -i -e '2 i%s/%s start' /etc/init.d/boot.local

List only IoCs

Provides less context

Backdoor Routine

This Backdoor executes the following commands from a remote malicious user:

- Initiate DDoS attacks:
  - TCP flood
  - Challenge Collapsar (CC) attack
- Stop DDoS attack
- Execute shell commands