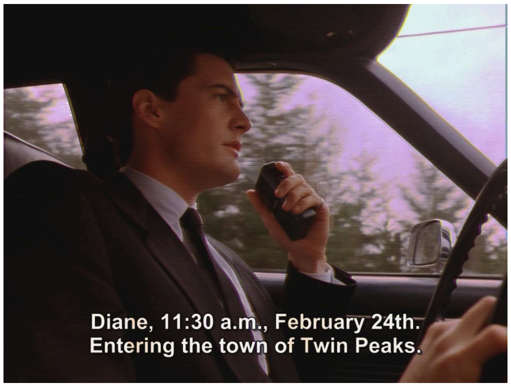
Federal Bureau of Intelligence
Division of Cybercrime Investigations

INTERIM BRIEFING: LAURA PALMER (WEEK 4)


Diane, 11:30 a.m., February 24th.
Entering the town of Twin Peaks.

Below is a briefing document compiled by Special Agent Cooper, in an effort to assist with the mission directives of Phase 1 of the Laura Palmer case. This report contains helpful information regarding the hotel's network, potential remediation steps, and possible indicators of compromise.

Use this document as a reference to guide your ongoing investigation and remediation efforts.

NOTES ON OBJECTIVE ONE

Regarding Objective 1 (*Regaining Control*), Agent Cooper mentions the following:

- Nmap: You know, this is — excuse my language — a damn fine network analysis tool.
    - Running `nmap <machine_IP>` is all well and good, but rumor has it that `nmap -A -Pn <machine_IP>` will get you even more sweet details. Run `man nmap` if you're curious as to what the `-A` means.
    - Windows machines… they can be a little tricky. Since they don't respond to network "pings" by default, nmap will think they're offline even if they're really online. That's why we add the -Pn option — don't trust anything just because the terminal program said it!
        - Again, run `man nmap` to see the manual, and scroll down to see the different flags ("-Pn", "-A", etc.)

- The FTP client on Linux is not the most user friendly program ever… even the `help` command doesn't really help you much at all!
    - Probably best to look up an online guide on how to use it or something…

- The Bureau is telling us that Laura liked to keep password lists. A great tool on Linux that I've used to run through and try a bunch of passwords at once is Hydra… Gotta hope it supports the service that you're using it against!

WARNING: This document contains TOP SECRET, SENSITIVE information pertaining to an ongoing federal investigation. Distribution or disclosure is strictly limited to authorized personnel. Any unauthorized sharing or use of this information will result in immediate disciplinary and legal action.

NOTES ON OBJECTIVE TWO

Regarding Objective 2 (*Access Remediation*), Agent Cooper mentions the following:

- If there's one thing I know about Linux, it's that the settings and configurations for services are almost always stored in the `/etc/` directory. A beautiful thing to behold.
    - By now, you've probably had better luck than me with that Ubuntu machine. Whatever you used to get access to sensitive information, there's got to be a way to disable it. Of this I am sure!
    - Hmm. If it's a Linux machine, maybe you would want to use some sort of command to prevent easy modification in the future… perhaps a command that changes… the attributes?

- Did you gain access to the Windows machine yet? I saw you were able to get the list of potential passwords for it. Here's the thing about that pesky operating system: Sometimes, the local Administrator account won't have a lockout policy enabled.
    - Isn't that simply insane? Special Agent Cole says that we gotta prevent any further compromise of the network, so something tells me we should find a way to prevent The Black Lodge from attempting infinite password guesses with no repercussions.

NOTES ON OBJECTIVE THREE

Regarding Objective 3 (*Eradicating Compromise*), Agent Cooper mentions the following:

- This is where it all comes together. It's time to put your pre-investigation training (*hint: Lab 1 and 2*) to use and find these system compromises, my friend.
    - Analyzing your system processes before your network activity is like looking for a black cat in a coal cellar. Let the suspect network activity guide you to the suspect system processes, when possible!

- Do you remember that lecture at The Bureau from last Monday? This is just a hunch, but I think some of the tools they mentioned might help us get rid of the malware once and for all.
    - Remember: Just because you found the malware file doesn't mean you have the full story. How was that malware executed? Was it automated or did it involve manual interaction from the victim user? This is vital information needed for our report.

  - The Sysinternals Suite is a must-have for Windows - I feel naked without it. Try taking a look at tools included such as Autoruns and Process Explorer**.** WinPEAS may also be of use
  - I wish we had Sysinternals for Linux… At least LinPEAS should help you out a bit. Check for any potential persistence mechanisms that The Black Lodge may have set up.
    - Note that LinPEAS is a command-line tool. Scroll down on the Github link to find out how to use it