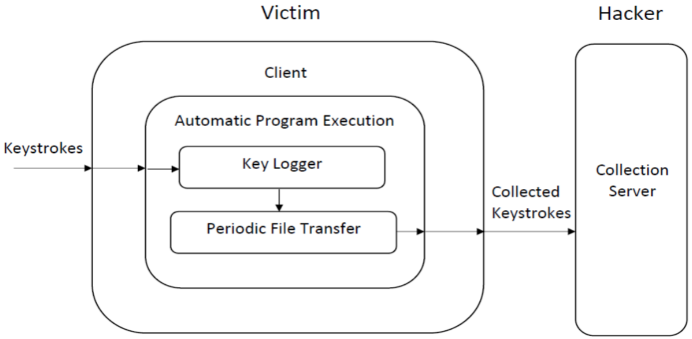
INL Cyber Security

Project

The growing frequency and severity of cyber attacks targeting all industries in the world has created a need for increased computer literacy among today's population. The goal of this software package is to train IT professionals and computer enthusiasts on a common cyber attack method. Particular skills users will learn include:

- Recognizing when a computer has been infected with malware
- Locating the malware on the hard drive
- Determining the function of the malware
- Identifying where the attack is coming from
- Identifying what information has been compromised

System



Methods

The software needed to be broken down into four main components:

- The permanence is being handled by the built-in cron system that runs scripts that ensure the malware is running and hasn't been deleted or moved. This was chosen due to the consistency and reliability.
- The victim and the hacker are connected over a TCP connection. This was chosen due to the ability to hide the output connection with the hacker's server with other output connections that would be normally made.
- The keylogging feature is reading in the keyboard buffer that is contained in the operating system.
- The Encryption is a mix of base64 and a custom XOR encryption. This was chosen due to the ability to encode and decode reliably.

Conclusion

The software that was developed taught us far more about the intricacies of the different aspects of cyber security then we could have learned anywhere else. This project allowed us to study and implement an attack that required us to thoroughly research the different aspects of a cyber attack that might be plausible in the real world. The value of this project came from the education and experience that we and others gain by interacting with and learning about this attack.

The software will be added to other attacks within a larger training that teaches people how to prevent and protect against a multitude of attacks.

College of Engineering
UtahStateUniversity

Levi Miller: levitmiller@gmail.com Robert van Oene: robert.van.oene@gmail.com

Thanks to the Idaho National Laboratory