

# Emotional Simian V 2.1

## Overview

EDG Project Lead: XXXXX Y

IOC/EDG/AE/OSB

Classified By: 2400845  
Derived From: CIA NSCG MET S-06  
Reason: 1.4(c)  
Declassify On: 25X1, 20621023

# Agenda

---

## Subject

- Requirements
- Concept of Operations
- Capabilities and Limitations

## Briefer

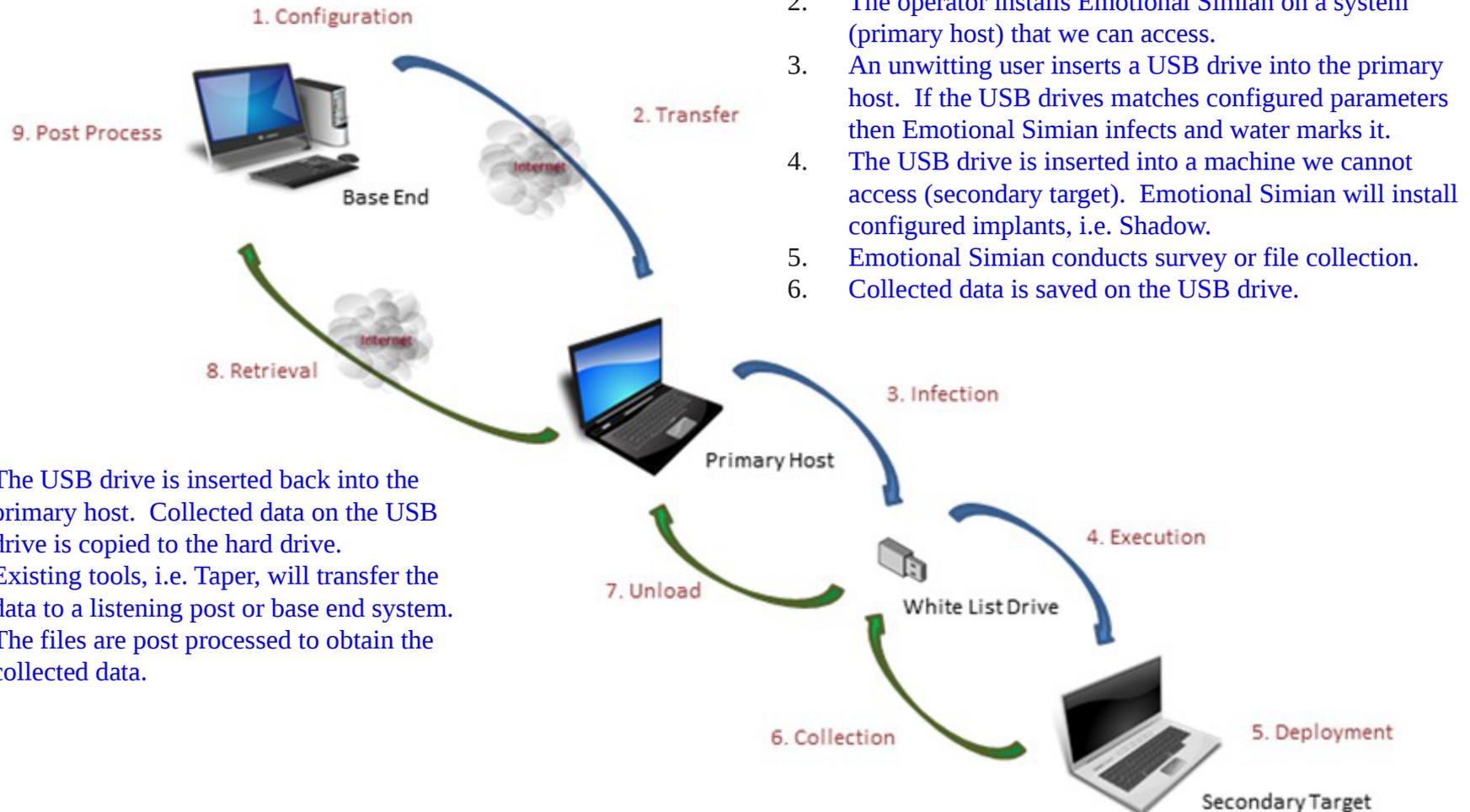
➤ XXXXX Y

# Requirements

---

- Requirements
- EmotionalSimian provides access to downstream machines that would otherwise be inaccessible. Communications between the machine to which we have access and downstream machines use USB thumbdrives inserted by unwitting users. Whitelisted thumbdrives are infected upon being inserted into a machine running EmotionalSimian. Infected thumbdrives use an exploit to initiate execution which will then deploy a configurable payload(s) and optionally conduct a system survey and/or collect files on a configurable maximum number of downstream machines.

# Concept of Operations



- The USB drive is inserted back into the primary host. Collected data on the USB drive is copied to the hard drive.
- Existing tools, i.e. Taper, will transfer the data to a listening post or base end system.
- The files are post processed to obtain the collected data.

# Capabilities and Limitations

---

- Emotional Simian can:
  - Configure and execute a system survey.
  - Load up to three payloads on the thumb drive.
  - Collect a directory listing.
  - Collect files from the target computer via a list of specific file extensions configured by the user.
  - Delete a configure list of files.
  - Configure Dll payload to run once per machine.
  - Load previous configuration files.