Detecting Host-Based Code Injection Attacks

Thomas Barabosch

SPRING 2014, Bochum

Fraunhofer FKIE

Malware…

Source: http://www.digitaltrends.com/wp-content/uploads/2012/12/Who-can-fight-Android-malware.jpg

HOST-BASED CODE INJECTION ATTACKS

Code Injection Attacks

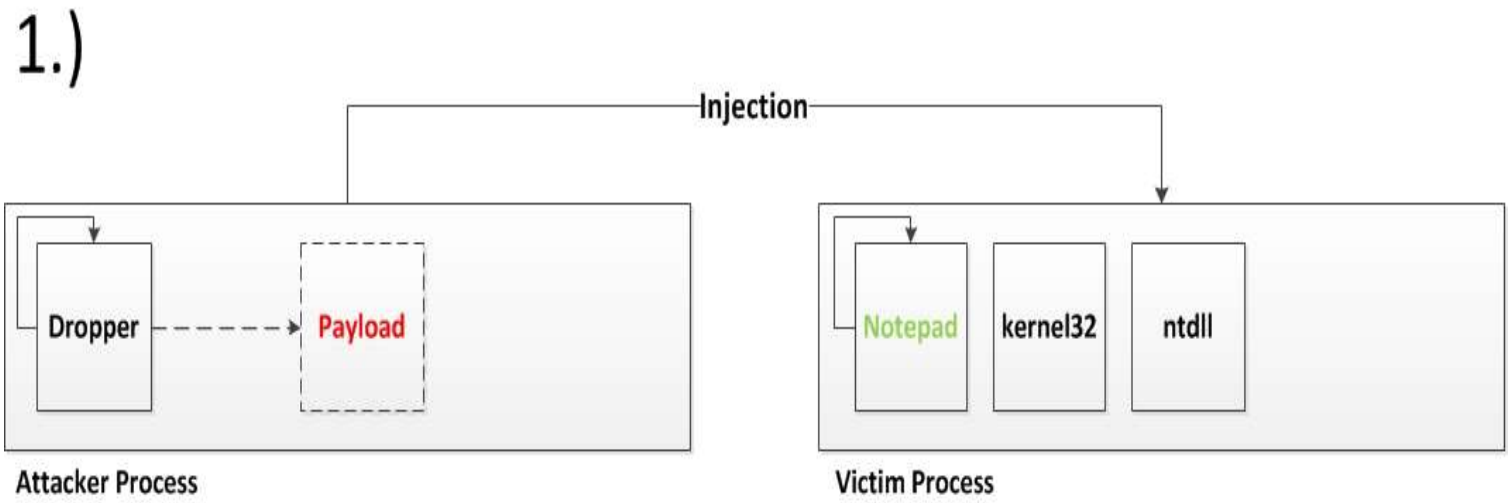
Let E be an entity controlled by an attacker.
Let P be a process targeted by the attacker.
An active attack on P by E, that aims at executing a payload defined by E within the context of P is called code injection attack.

- Remote
- Host-Based

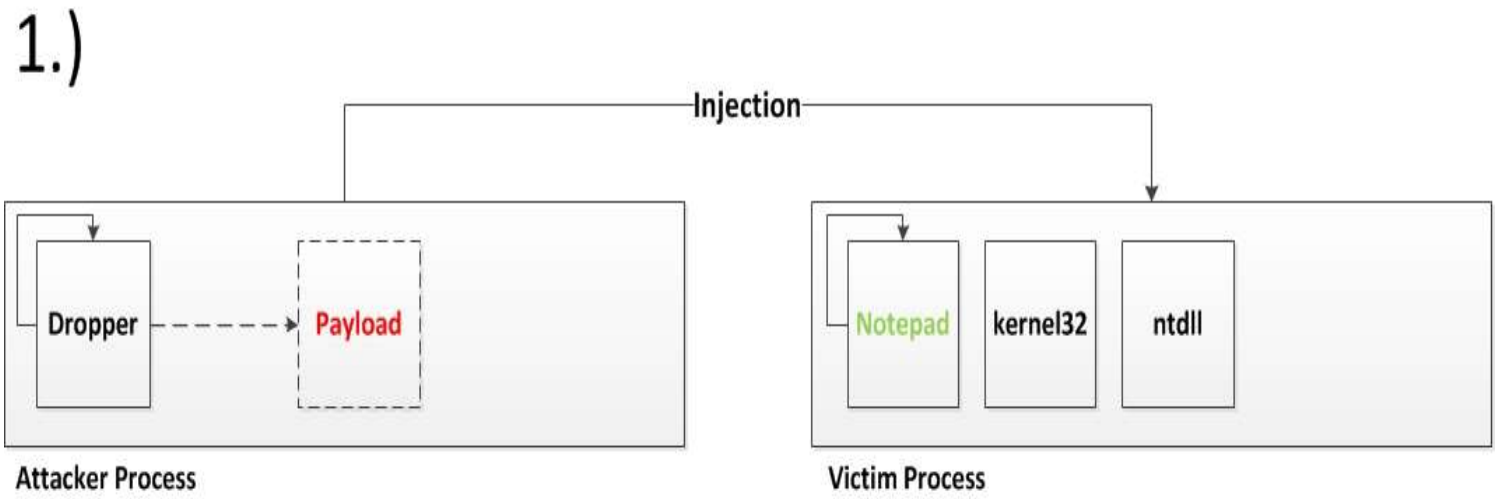
Host-Based Code Injection Attacks (HBCIAs)

- Widely used by current malware
- Several benefits
  - Interception of critical information
  - Avoidance of detection
  - Privilege escalation
  - Manipulation of security products

Concurrent Execution



Process Hollowing

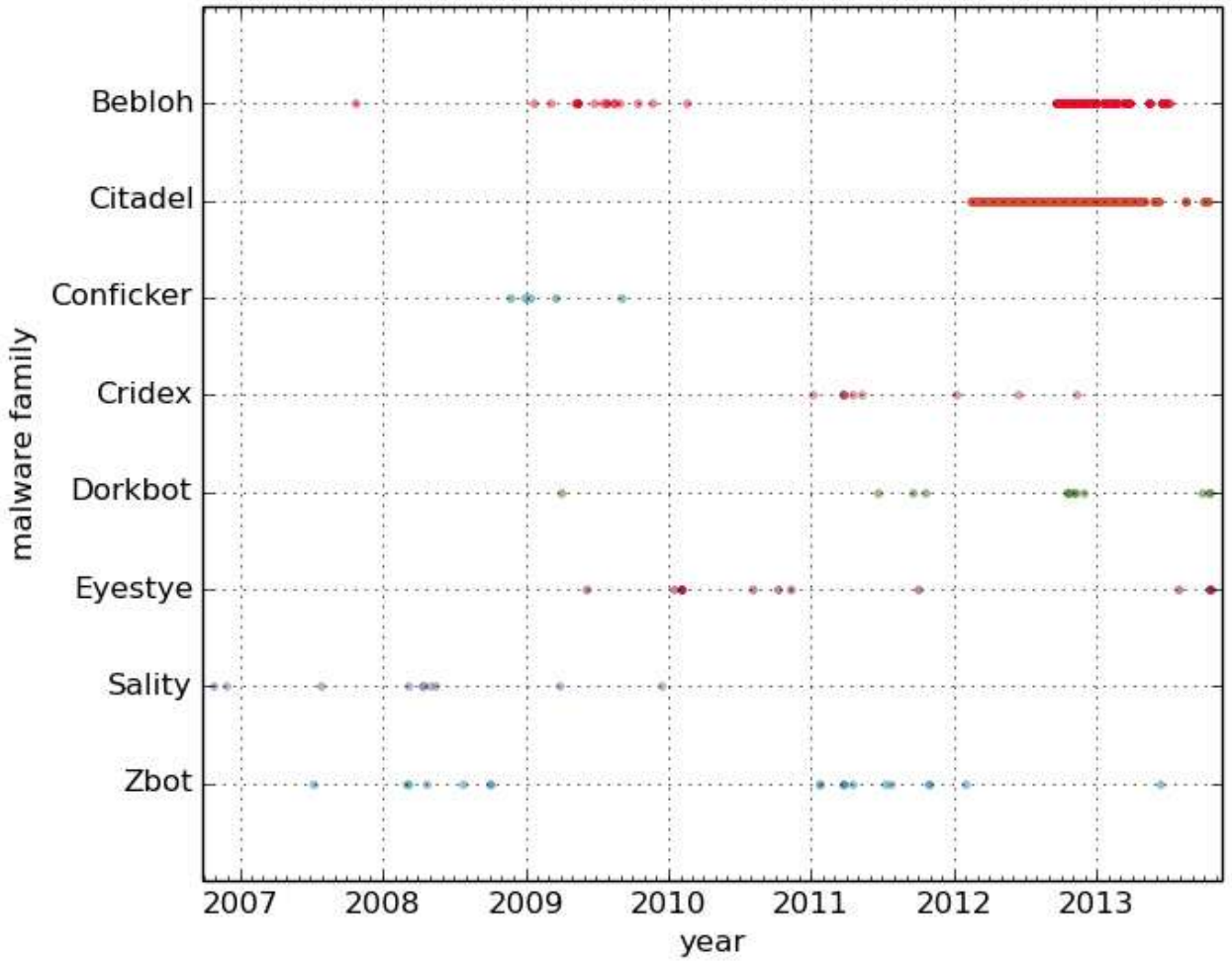


HBCIA is a malware family feature

The HBCIA is an inherent malware family feature, i.e. a malware author does neither remove this feature nor does he change the underlying injection method over time.

- Dataset consists of eight malware families (32514 samples)
- Manual inspection of representatives in order to determine characteristic API call sequence
- Ran all samples in sandbox and checked for characteristic API call sequence

HBCIA is a malware family feature



Fraunhofer FKIE

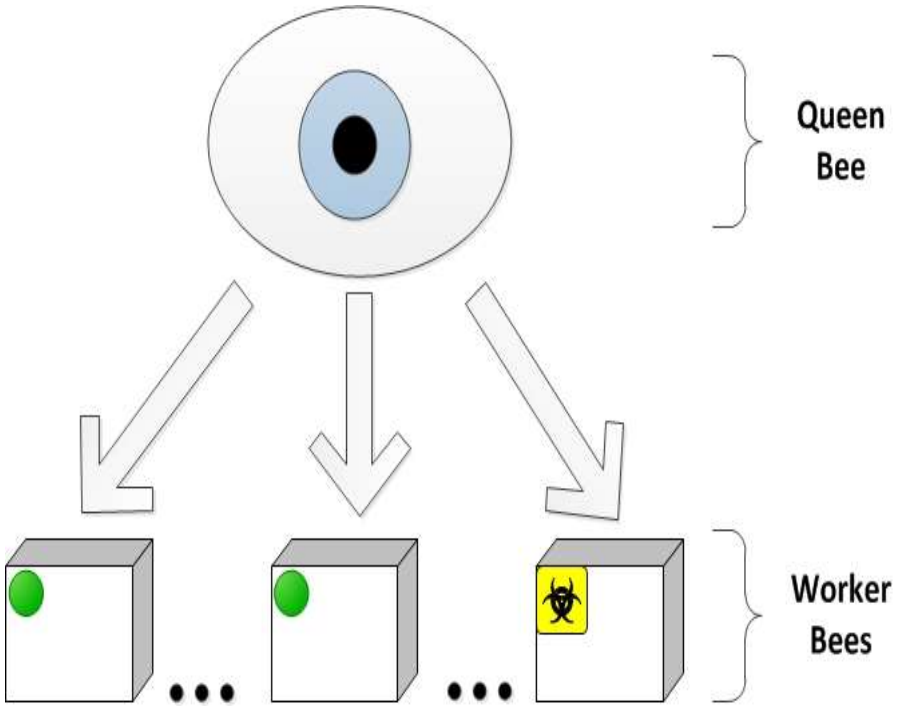
BEE MASTER

Bee Master

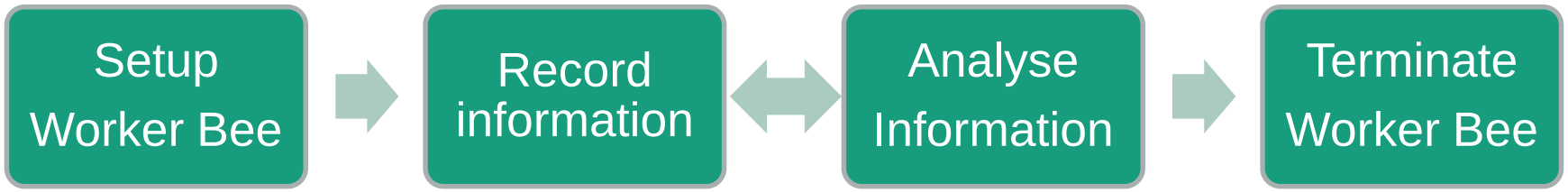
- Detection of ongoing HBCIAs
- Transfer of the honeypot paradigm to OS processes
- OS independent
  - Processes, Libraries, Threads
- Prototype implementation for Windows NT and Linux

Bee Master: Architecture

- Queen Bee
  - The system‘s brain
  - PoC implemented as user space process
- Worker Bees
  - The system‘s sensors
  - Passive behaviour
  - Behaviour a priori known
  - Configurable



Bee Master: Control flow



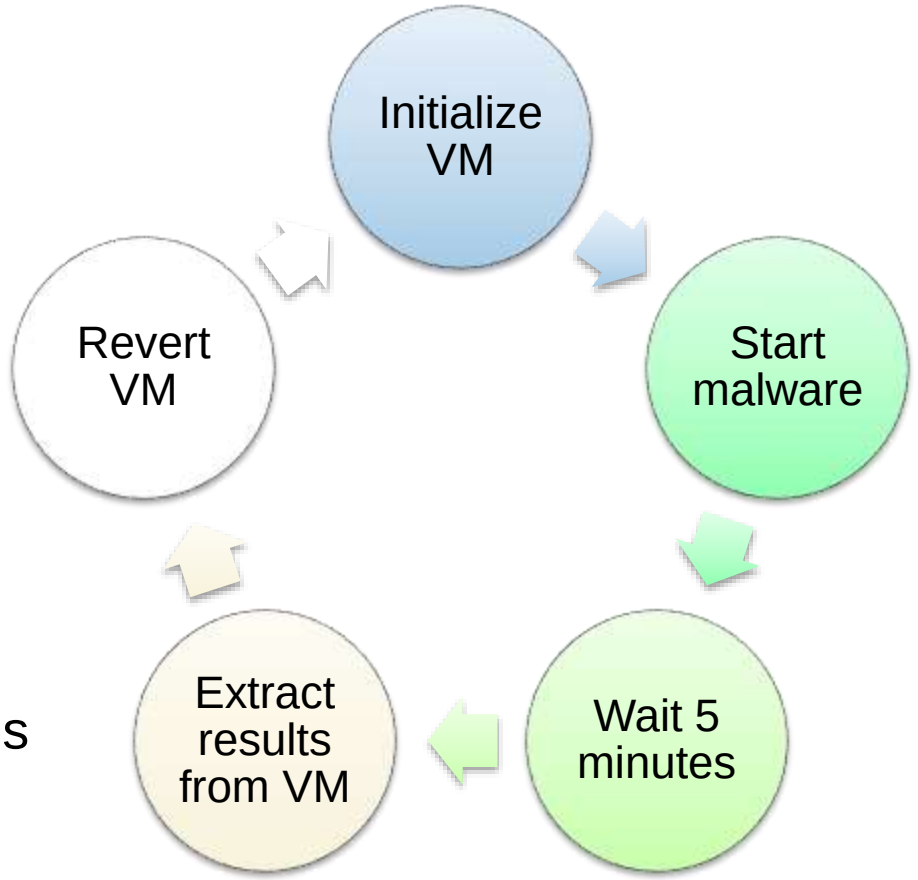
Bee Master: Limitations

- Missing attacks
- Detection of process hollowing

EVALUATION

Evaluation

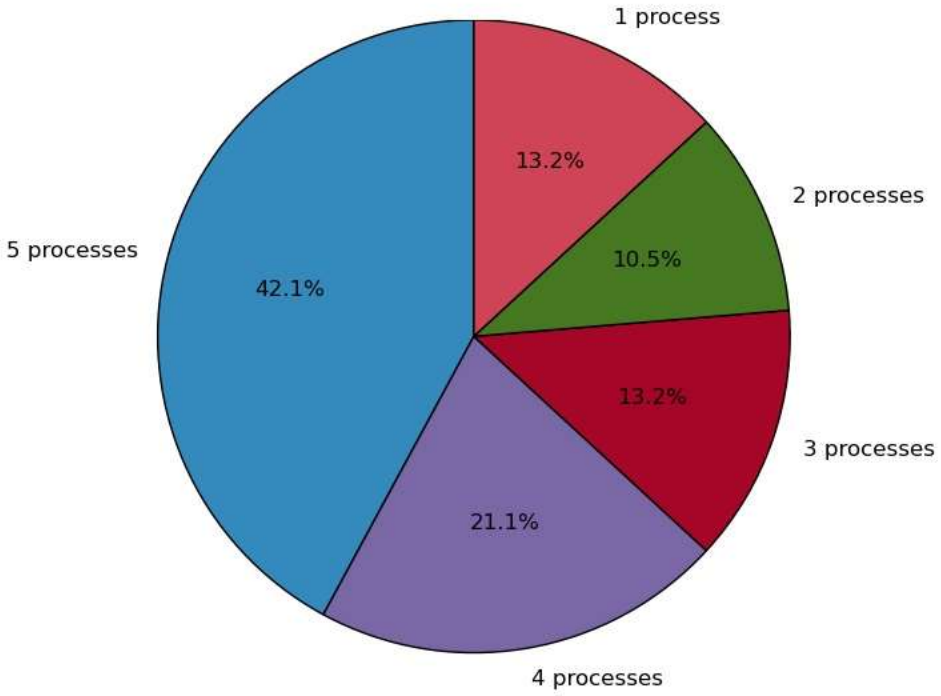
- Data set
  - 38 families (Windows)
  - One family (Linux)
  - 400 benign programs
- Configuration
  - Hardend VMs
    - Windows XP, 7, 8, Ubuntu 13.10
  - Queen Bee with five Worker Bees
    - Four frequently attacked processes
    - One random process



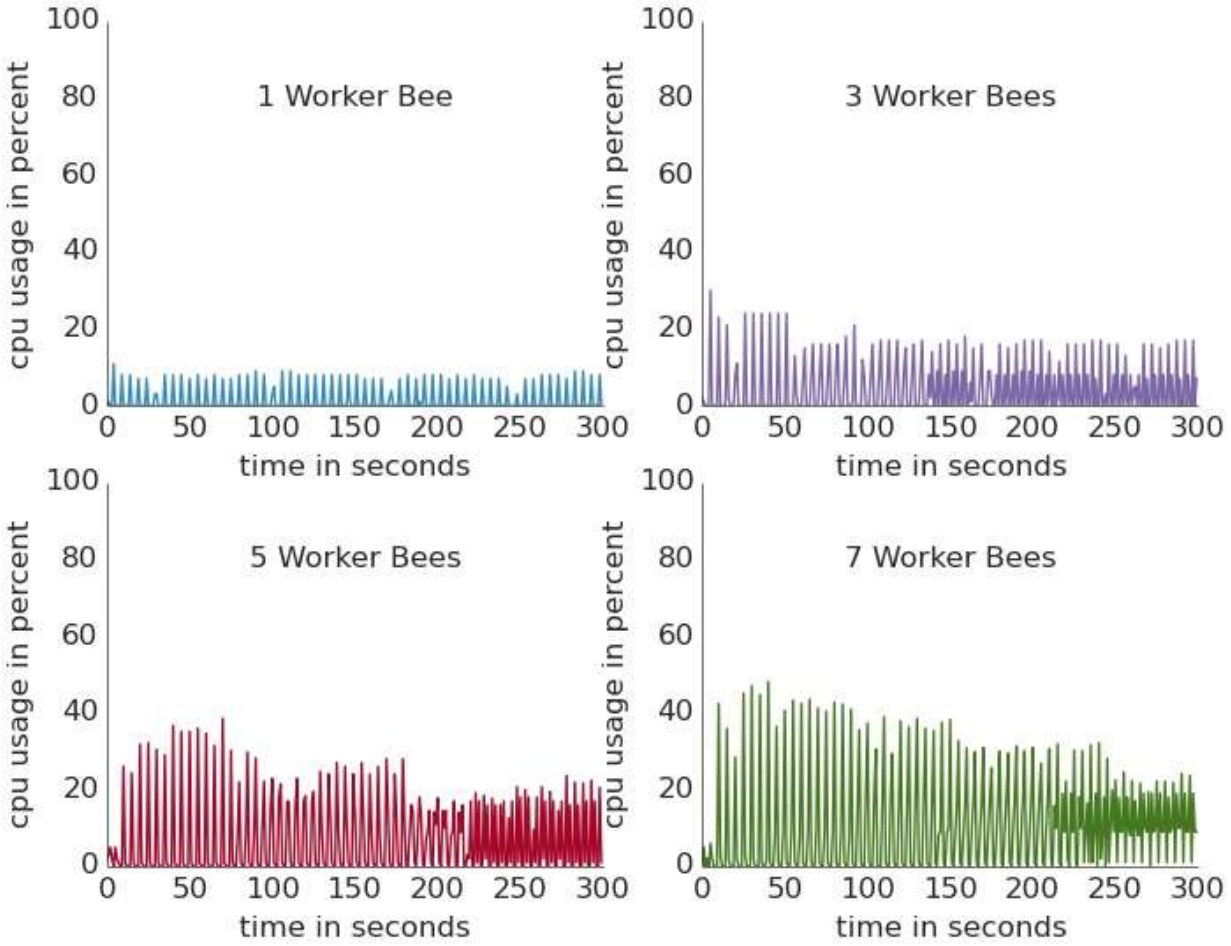
Fraunhofer FKIE

Results

- Detection of HBCIAs in all cases
- No false positives
- Many families have implemented a black listing
- Only two Worker Bees are needed for detecting all samples



Performance



Fraunhofer FKIE

CONCLUSION

Conclusion

- Host-Based Code Injection Attacks are a family feature
- Bee Master applies the honeypot paradigm to OS processes in order to detect ongoing HBCIAs
- Capable of detecting current malware operating system independently
- Malware is very prone to detection during HBCIAs