Monthly Research

A survey of Environment-Sensitive Malware

F F R I , Inc
http://www.ffri.jp

Ver 2.00.01

Background

- A damage is increasing by MITB (Man-in-the-Browser) malware such as “Citadel”
  - The Citadel targets money of online banking users
- Citadel-like malware restricts malicious behavior except infected host to evade dynamic analysis[1]
- We explain execution environment detection techniques and its countermeasures

Why malware switched behavior?

- Malware builders are sold on the Internet
  - Its make easier to build MITB malware(e.g., SpyEye)

- “Malware operator” is not the same person with “Malware builder developer”

- Malware builder developers are afraid that security vendor’s rounds up the malware manufactured by their builder
  - Developer does not want:
    - To clearly indicate malware behavior using automated dynamic analysis
    - To create effective signature for detecting malware that generated by their builder

Environment-sensitive malware

- These malware detect the execution environment and do not engage in malicious behavior when the current host differs from the infected host
  - To avoid behavior based malware detection[2]

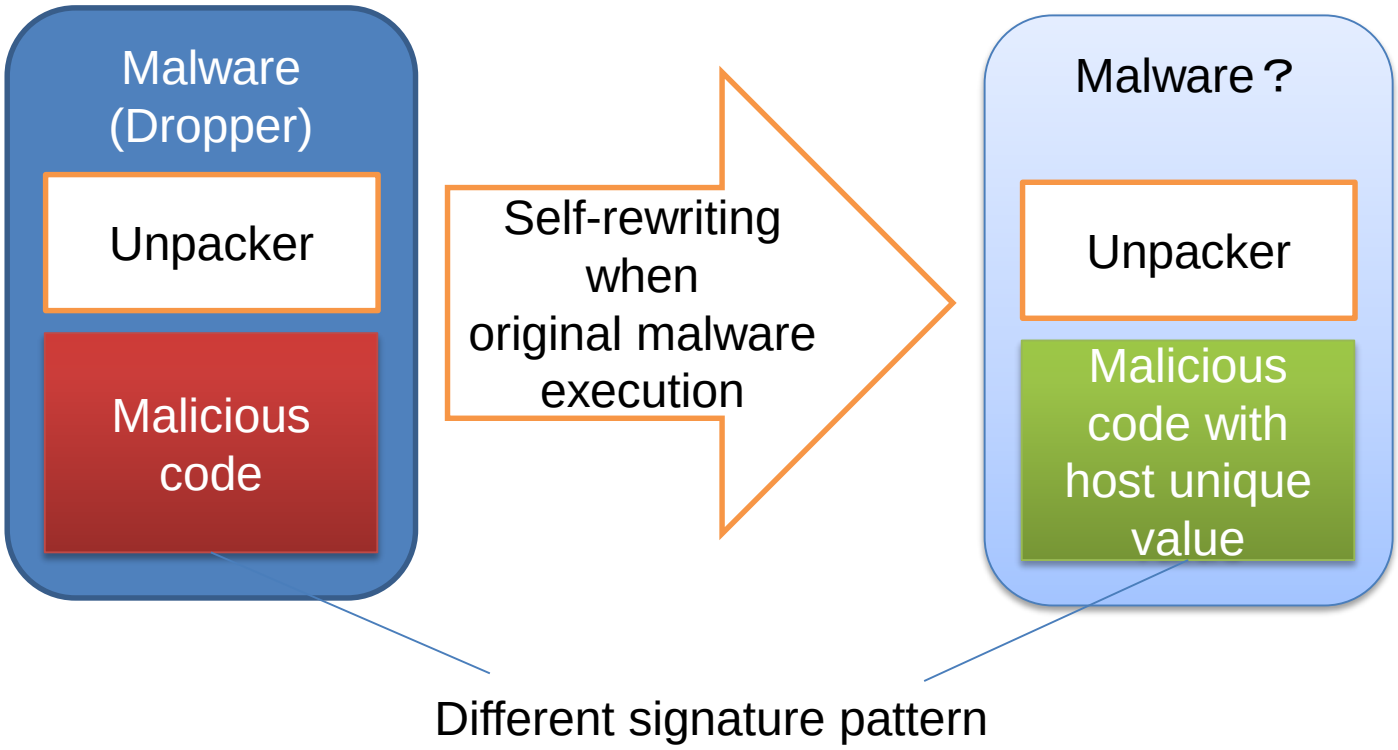
Execution environment detection techniques

- Host fingerprinting
  - Identifying the host using host unique value
  - Detecting infected host or not

- Virtual Machine Environment(VME) Detection
  - Detecting host's execution environment which running on virtual machines

Host Fingerprinting

- Embedding infected host's unique value into execution binary



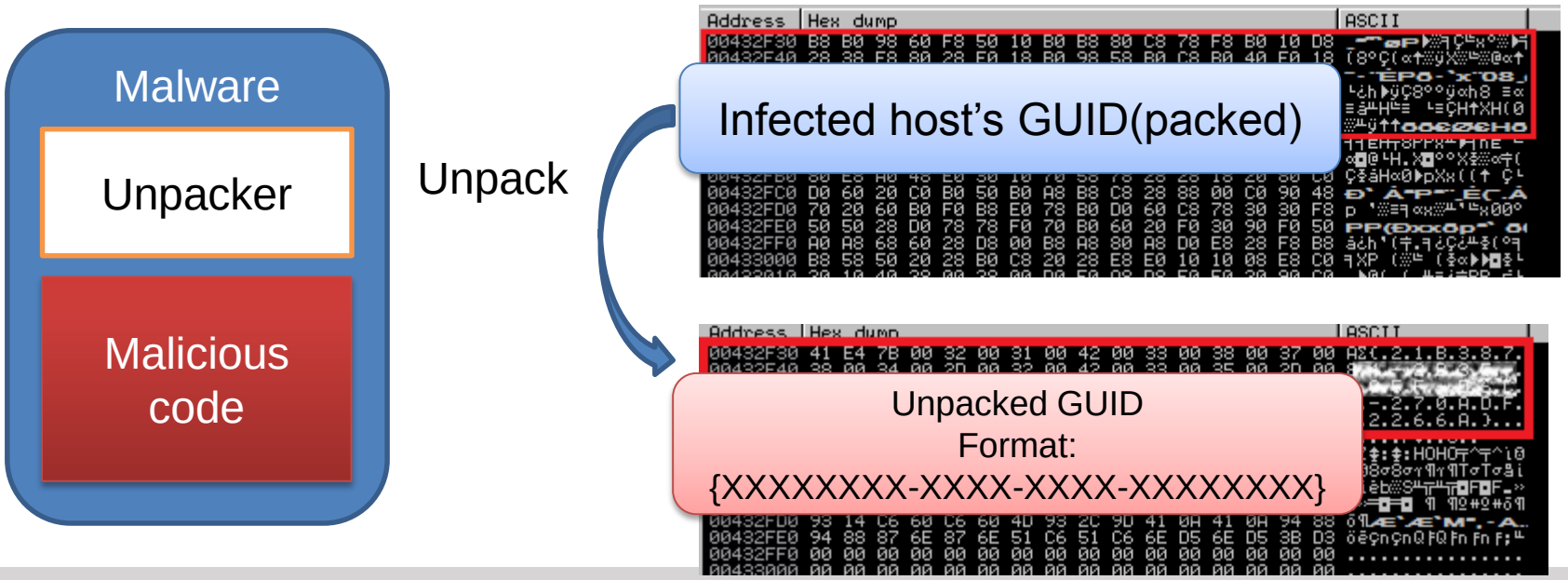
Examples of Host Unique Value

Category	Environment Unique Values
Hardware	***GUID(Disk)**, MAC address(NIC), etc.
System	OS Product ID, Computer(NetBIOS) Name, Registry entry, etc.
Application	***Execution path**, Username, etc.
Network	IP address(external check)

*Discovered in Citadel malware

In the real malware

- The Citadel malware (captured at 2013 later)
  - Getting GUID on system drive using the GetVolumeInformationA()
  - Comparing running host's GUID value and embedded infected host's value
  - Process executes malicious code if GUID values are consistent



Behavior of host unique value inconsistency

- For example:
  - Process termination
  - Running fake(or harmless) code

*We forecast that developers may implement advanced packing algorithm with host unique value in the future

Anti host fingerprinting

- Adding some rules of heuristic detection engine
  - Some APIs calling potential of host fingerprinting execution such as the GetVolumeInformation(), GeVolumeNameByHandle() , GetAdaptersAddresses()

- Full environment emulation
  - Camouflaging the infected host's unique value
    - Overriding API return value using system call proxy
    - In device emulation

- Symbolic execution[3]
  - Predicate transformation semantics
  - Generating comprehensive test/trace automatically

VME(Virtual Machine Environment) Detection

- 2% of observed malware over the world since 2013 have implemented VME detection logic[5]

- Approaches of VME detection[4][5][6]
  - Using virtual device feature bugs
  - Using VME specific resources
  - Using virtualized graphical environment features
  - Measuring timing and overheads

- Anti VME detection
  - Looking at p.10
    - Similar anti-host fingerprinting

Conclusions

- An environment-sensitive malware are in the wild
- Host fingerprinting is a type of execution environment detection that complicates automated malware analysis on sandbox and signature matching
- VME(Virtual Machine Environment) detection is yet another sandbox evasion technique
- These techniques are enough to complicate automated malware analysis and malware signature matching
- We must polish up robust automated malware analysis method against malware mass-production

References

- [1]: Analyzing Environment-Aware Malware, Lastline, 2014.05.25(viewed) http://labs.lastline.com/analyzing-environment-aware-malware-a-look-at-zeus-trojan-variant-called-citadel-evading-traditional-sandboxes

- [2]: Martina Lindorfer, Clemens Kolbitsch, and Paolo Milani Comparetti. 2011. Detecting environment-sensitive malware. In *Proceedings of the 14th international conference on Recent Advances in Intrusion Detection* (RAID'11). Springer-Verlag, Berlin, Heidelberg, 338-357. http://dx.doi.org/10.1007/978-3-642-23644-0_18

- [3]: Andreas Moser, Christopher Kruegel, and Engin Kirda. 2007. Exploring Multiple Execution Paths for Malware Analysis. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy* (SP '07). IEEE Computer Society, Washington, DC, USA, 231-245. http://dx.doi.org/10.1109/SP.2007.17

- [4] slabbed-or-not/github , 2014.05.25(viewed) https://github.com/kaniini/slabbed-or-not

- [5]: Aurélien Wailly. Malware vs Virtualization The endless cat and mouse play, 2014.05.25(viewed) http://aurelien.wail.ly/publications/hip-2013-slides.html

- [6]: Kang Li, Xiaoning Li. Comprehensive Virtual Appliance Detection. Black Hat Asia 1014. http://www.blackhat.com/docs/asia-14/materials/Li/Asia-14-Li-Comprehensive-Virtual-Appliance-Detection.pdf

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research