Improving Scalable, Automated Baremetal Malware Analysis

Adam Allred

Paul Royal

Agenda

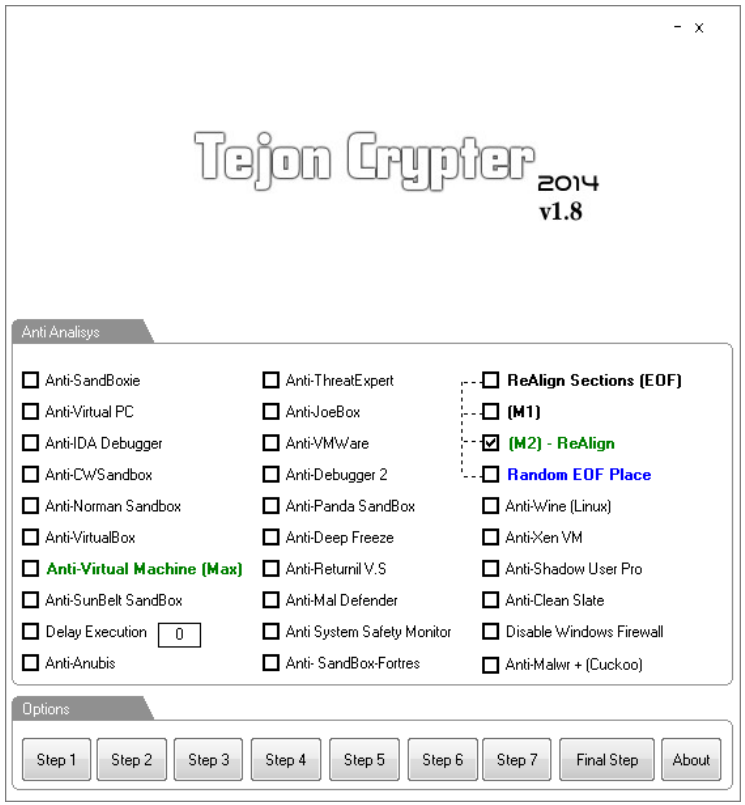
- Baremetal Malware Analysis
  - Motivation, Hardware, Technologies
- Improving Baremetal Malware Analysis
  - Reliability Testing
- Conclusion/Future Work

an introduction to

BAREMETAL MALWARE ANALYSIS

Malware Analysis Detection

- Analysis environment detection has become commoditized



Georgia Institute of Technology

Detection Cont'd

- In-Guest Tools
  - No higher privilege
  - Exception handling issues
- Emulation (QEMU)
  - No identical instruction execution semantics
- Hardware virtualization extensions
  - Non-privileged side effects

Detecting QEMU

- IRETD with 0x26 prefix

```
#include <stdlib.h>
#include <stdio.h>
#include <windows.h>

int seh_handler(struct
_EXCEPTION_RECORD
*exception_record,
            void *established_frame,
            struct _CONTEXT *context_record,
            void *dispatcher_context)
{
      printf("Malicious code here.\n");
      exit(0);
}
```

```
int main(int argc, char *argv[]) {

      unsigned int handler =
            (unsigned int) seh_handler;

      printf("Attempting QEMU detection.\n");

      __asm("movl %0, %%eax\n\t"
            "pushl %%eax\n\t"::
            "r" (handler): "%eax");

      __asm("pushl %fs:0\n\t"
            "movl %esp, %fs:0\n\t");

      __asm(".byte 0x26, 0xcf");

      __asm("movl %esp, %eax");
      __asm("movl %eax, %fs:0");
      __asm("addl $8, %esp");

      return EXIT_SUCCESS;
}
```

Why Transparency?

- Analysis environment detection commoditized
- Detection vulnerability trend does not suggest decrease over time
- Certain types of detection vulnerabilities automatically discoverable

Baremetal Challenges

- Conceptual
  - Physicalizing virtual machine
- Scalability
  - Cost of hardware
  - Efficiency of processing
- Automation
  - Managing system state
  - Ensuring longevity of hardware

Baremetal Cluster Hardware

- Baremetal Controller
  - Standard 1U Single Socket Server
- Baremetal Non-Virtual Machine (NVM)
  - Inexpensive Half-depth 1U Server
- Cluster Networking
  - Inexpensive Cisco switch
    - 24 10/100Mb ports, 2 1Gb ports

Initial Cluster Technologies

- Linux Device Mapper
  - Create Copy-on-Write block device
- ATA over Ethernet
  - Make CoW device available over network
- g Preboot eXecution Environment
  - Boot NVM into OS on network CoW device
- Intelligent Platform Management Interface
  - Manage NVM system state

NVMTrace

- Software controller for automated baremetal malware analysis
  - Executes each sample in its own sterile, isolated non-virtual machine
- Provides access to NVM disk contents and network traffic
  - Use with your favorite network traffic and disk forensic tools

GTISC NVMTrace Deployment

Georgia Institute of Technology

GTISC Deployment Cont’d

Georgia Institute of Technology

evaluation and enhancement of

BAREMETAL MALWARE ANALYSIS

NVMTrace Reliability Testing

- Anecdotal observation indicated potential issue in sample processing
- Subsequent investigation revealed occasional hang during Windows boot
- ATA over Ethernet suspected

ATA over Ethernet (AoE)

- Simple (12 page specification)
  - TFTP-like connection
- Unreliable
  - No packet retransmission, checksumming
- Network analysis confirmed AoE traffic ceases at hang
  - Packet loss or corruption impedes node execution

iSCSI

- Proposed as replacement for AoE
  - Provides reliable transport via TCP
- Candidate implementation must handle atypical use
  - Constant iSCSI LUN add/remove
- Evaluated several iSCSI implementation candidates that did *not* work
  - SCST, STGT, Open-iSCSI
- Eventually tried LIO, which did work

Results

- > 99% of samples in well-known malware set successfully processed using LIO
  - Verified via multiple rounds of testing
- Additional testing with separate, ~200,000 sample dataset
  - Represented 24 hours of real-world collection
  - Virtualization-based processing results used as reference
  - Results reaffirm > 99% success rate
- Subsequent stable production use for months

Conclusion

- Analysis environment detection commoditized, increasingly popular
  - Virtualization still a valuable analysis tool, but can be supplemented
- Advances in hardware make scalable baremetal malware analysis possible
- Baremetal analysis systems must be carefully engineered for reliability

Future Work

- Increase cluster density via Supermicro MicroClouds
  - Yields three-fold increase in processing density
- Real-time disk forensics
  - Examine controller-NVM iSCSI network traffic
  - Record disk-level events as they occur

Acknowledgements

- Artem Dinaburg
  - Environment detection
- Robert Edmonds
  - System architecture
- David Dagon
  - System concept

Questions?

NVMTrace Source Code,
Build Instructions
http://code.google.com/p/nvmtrace